Le corps ordonné $\mathbb{R}$ posséde-t-il la propriété de la borne supérieure?

Alain Wazner,...

- Avez vous une inclination à penser qu'il y a moins de sons que d'instruments?
- Les éclairs peuvent être aveuglants mais je préfère qu'ils le ne soient pas.
- Vous croyez donc qu'ils ne le sont pas?

Prérequis

Dans tout le texte $(\mathbb{K}, +, \times, \leq)$ sera un corps totalement ordonné **non trivial** et possédant la propriété de la borne supérieure. On munira $(\mathbb{K}, +, \times, \leq)$ de la topologie séparée définie par la métrique (à valeur sur $\mathbb{K}$) $d(x, y) = |x - y| = x - y$ si $y \leq x$, $y - x$ sinon. Pour cette topologie les voisinages de $c \in \mathbb{K}$ sont les ensembles contenant les intervalles $I_{a,b} =]a, b[$ avec $]a, b[= \{x \in \mathbb{K}/a \leq x \leq b\} \backslash \{a, b\}$ avec $a \neq b$ et $c \in I_{a,b}$. Pour cette topologie :

- **$\mathbb{K}$ est complet.**
- **Toute fonction continue de $\mathbb{K}$ vers $\mathbb{K}$ vérifie le théorème des valeurs intermédiaires.**
- **$\mathbb{K}$ est archimédien.**

Preuve : consulter les classiques.

Les sous-groupes de $\mathbb{K}$

Tout $a \in \mathbb{K} \backslash \{0\}$ est d'ordre 0 (Soit $< a >$ est isomorphe à $\mathbb{Z}$ et $\mathbb{K}$ n'est pas fini) : Comme a et $-a$ sont deux éléments non-nuls de signes opposés et $< a >=< -a >$, on peut supposer $a > 0$. Soit $n \in \mathbb{N}$ alors $n.a = \underbrace{a + \cdots + a}_{n} > 0$ et en particulier $n.a \neq 0$: a est d'ordre 0.
On pose alors $\mathbb{Z}_{\mathbb{K}} \overset{déf}{=} < 1 >$, c'est un groupe isomorphe à $\mathbb{Z}$, le plus petit sous-corps de $\mathbb{K}$ contenant

$\mathbb{Z}_{\mathbb{K}}$ **est**

$$\mathbb{Q}_{\mathbb{K}} = \left\{ \left(\underbrace{1 + \cdots + 1}_{q} \right)^{-1} \left(\underbrace{\pm 1 \pm \cdots \pm 1}_{p} \right) / (p, q) \in \mathbb{N} \right\}$$

il est isomorphe à $\mathbb{Q}$.
$\mathbb{Q}_{\mathbb{K}}$ **est le corps premier de $\mathbb{K}$ qui a alors une structure de $\mathbb{Q}_{\mathbb{K}}$-algèbre.**
On peut de plus déduire de la propriété de la borne supérieure la classification suivante : tout sous-groupe additif de $\mathbb{K}$ est:

- **Soit** $a\mathbb{Z} =< a >$ **avec** $a \in \mathbb{K}$
- **Soit dense dans** $\mathbb{K}$

Consulter les classiques («sous-groupes additifs») pour une preuve.

Sur la topologie des sous-groupes de $\mathbb{K}$

$\mathbb{K}$ étant muni d'une topologie **qui le rend complet** c'est alors un espace vectoriel de dimension 1 et nous pouvons être tentés d'utiliser des théorèmes d'analyse propres aux espaces vectoriels complets comme **le théorème de Baire**. **Nous n'en utiliserons qu'une version restreinte** s'appliquant à un nombre fini d'ouverts et **fondée par le lemme des deux ouverts** dont l'énoncé suit :
Si $\mathcal{O}_1$ et $\mathcal{O}_2$ sont deux ouverts denses de $\mathbb{K}$ alors $\mathcal{O}_1 \cap \mathcal{O}_2$ est un ouvert dense de $\mathbb{K}$.

Preuve : Soit I un intervalle ouvert de $\mathbb{K}$ alors, comme $\mathcal{O}_1$ est un ouvert dense de $\mathbb{K}$, l'ouvert $I \cap \mathcal{O}_1$ contient un intervalle $I \cap \mathcal{O}_1 \supset I_1$; mais $\mathcal{O}_2$ est un ouvert dense de $\mathbb{K}$ et par le même raisonnement l'ouvert $I_1 \cap \mathcal{O}_2$ contient un intervalle $I_1 \cap \mathcal{O}_2 \supset I_2$. Tout intervalle I contient un intervalle I_2 inclus dans $\mathcal{O}_1 \cap \mathcal{O}_2$ qui est un ouvert dense de $\mathbb{K}$.

Nous pouvons en déduire que
Tout sous-groupe propre de $\mathbb{K}$ n'est pas ouvert : Si G est un sous-groupe propre de $\mathbb{K}$ qui est un $a\mathbb{Z}$ alors il n'est pas ouvert. Si G est dense dans $\mathbb{K}$ alors supposons le ouvert : en se donnant un élément x de $\mathbb{K}$, son translaté $x+G$ est encore un ouvert dense dans $\mathbb{K}$ et en se donnant un autre élément y de $\mathbb{K}$: l'intersection $(y+G)\cap(x+G)$ est un ouvert dense de $\mathbb{K}$ par le lemme des deux ouverts. En particulier cette intersection n'est pas vide. Ceci prouve que le groupe quotient $\mathbb{K}/G$ ne contient qu'un élément qui ne peut-être que son neutre et donc que $G = \mathbb{K}$ n'est pas un sous-groupe propre de $\mathbb{K}$ (en effet les éléments de $\mathbb{K}/G$ sont les classes $x+G$ qui forment une partition de $\mathbb{K}$).

Quelques éléments de théorie des groupes

Un théorème de structure de la théorie des groupes

Soit G un groupe, H et N deux sous-groupes dont H est un groupe normal, écrire que $G/H \simeq N$ c'est écrire qu'il existe un morphisme de groupe Ψ, tel que $Ker(\Psi) = H$ et $N = Im(\Psi)$, nous cherchons ici à comparer G et H et le principal résultat sera que ces deux groupes sont en «somme directe non-commutative» ou que $H = Ker(\Psi) \subset Im(\Psi) = N$: ce qui définit une **orientation**.
lemme 2 : Soit G un groupe et H, N deux sous-groupes **distingués** de G, alors

$$(N \simeq G/H) \;\Rightarrow\; (H \subset N) \vee (N \cap H = \{e\})$$

Preuve : Puisque G/H est isomorphe à N, il existe un morphisme $\Psi : G \to N$ de noyau H, le dit premier théorème d'isomorphisme de la théorie des groupes conclut à l'existence d'un isomorphisme $\overline{\Psi} : \begin{cases} G/H & \to \quad N \\ gH & \mapsto \quad \overline{\Psi}\,(gH) \end{cases}$ avec $\overline{\Psi}\,(gH) \overset{déf}{=} \Psi(g)$.
Si F est un sous-groupe distingué de G alors on a bien défini une action de groupe de G sur G/F par $h.gF \overset{déf}{=} hgF$ $(\forall h, g \in G)$ puisque si e est le neutre de G alors

$$e.gF = egF = gF$$
$$k.h.gF = k.hgF = khgF = (kh).gF$$

$\forall s \in G$, $\omega(sF)$ **l'orbite de** sF **est** G/F : Puisque $\omega(sF) = \{g.sF/g \in G\} = \{gsF/g \in G\}$ soit $\{g'F/g' \in G\} = G/F$ (où on a posé $g' = gs$).
G_{sF} **le fixateur de** sF **est** F **:**
G_{sF} est l'ensemble $\{g \in G/g.sF = sF\}$, lequel est $\{g \in G/gsF = sF\}$. Si $gsF = sF$ alors

$gse = gs \in gsF = sF$ donc $\exists f \in F$, $gs = sf$ et $g = sfs^{-1} \in F$ puisque F est un sous-groupe distingué de G.
Réciproquement si $g \in F$ alors

$$g.sF = gsF = gFs = Fs = sF$$

puisque F est un sous-groupe distingué de G et $gF = F$, $\forall g \in F$.
La bijection $\left\{ \begin{array}{lll} G/G_{sF} & \rightarrow & \omega(sF) \\ gG_{sF} & \mapsto & g.sF \end{array} \right.$ est le morphisme identique de G/F.

N et H étant des sous-groupes normaux de G : en faisant agir G à gauche sur G/N et G/H comme précédemment on a $\forall s \in G$, $G_{sN} = N$ et $G_{sH} = H$, $\omega(sH) = G/H$ et $\omega(sN) = sN$, les identiques sur G/H et G/N sont les bijections $\left\{ \begin{array}{lll} G/G_{sH} & \rightarrow & \omega(sH) \\ gG_{sH} & \mapsto & g.sH \end{array} \right.$ et $\left\{ \begin{array}{lll} G/G_{sN} & \rightarrow & \omega(sN) \\ gG_{sN} & \mapsto & g.sN \end{array} \right.$

On définit une deuxième action de G sur G/H en posant

$$(\forall g, s \in G) \; g.sH = \Psi(g)\overline{\Psi}^{-1} \circ \Psi(s) \; (= \Psi(g)sH)$$

puisque si e est le neutre de G alors $e.sH = \overline{\Psi}^{-1} \circ \Psi(s) = sH$ et puisque $(\forall u, t, s \in G)$

$$\begin{array}{rcl} u.(t.sH) & = & u.\left(\Psi(t)\overline{\Psi}^{-1} \circ \Psi(s)\right) = u.\left(\Psi(t)sH\right) \\ & = & \Psi(u)\Psi \circ \overline{\Psi}^{-1}\left(\Psi(t)sH\right) \\ & = & \Psi(u)\Psi(t)\left(\Psi \circ \overline{\Psi}^{-1}(sH)\right) \\ & = & \Psi(ut)\left(\Psi \circ \overline{\Psi}^{-1}(sH)\right) = (ut).sH \end{array}$$

$\forall s \in G$, $\omega(sH)$ **l'orbite de sH est sNH** car $\omega(sH) = \{\Psi(g)sH/g \in G\}$ et comme g parcourant G, $\Psi(g)$ parcourt N... on obtient $\omega(sH) = NsH = sNH$ puisque $sN = Ns$ $(\forall s \in G)$.
Soit $g \in G$ tel que $g.sH = sH$ alors $\Psi(g)sH = sH$. L'élément $\Psi(g)s = \Psi\ g\ e$ appartient à $\Psi(g)sH$, donc à sH : il existe donc $h \in H$ tel que $\Psi(g)s = sh$. On a alors $\Psi(g) = shs^{-1} \in H$ puisque H est distingué dans G. Si $\Psi(g) \in H$ alors

$$\Psi(g)sH = \Psi(g)Hs = Hs = sH$$

G_{sH} le fixateur de sH est donc $\{g \in G/\Psi(g) \in H\}$ soit le sous-groupe de G/H : $\overline{\Psi}^{-1}(H)$.

- L'image par l'isomorphisme $\overline{\Psi}$ du groupe $\overline{\Psi}^{-1}(H)$ -c'est à dire le groupe $\Psi\left(\overline{\Psi}^{-1}(H)\right)$- est, par définition de Ψ et $\overline{\Psi}$, à valeur sur H et incluse dans N : on a donc

  $$\Psi\left(\overline{\Psi}^{-1}(H)\right) \subset H \cap N$$

  .
- Puisque $N = Im\,(\Psi)$ tout élément de $H \cap N$ est image par Ψ d'un élément de $\overline{\Psi}^{-1}(H)$: on a donc $H \cap N \subset \Psi\left(\overline{\Psi}^{-1}(H)\right)$; et de ce qui précède

  $$\Psi\left(\overline{\Psi}^{-1}(H)\right) = H \cap N$$

  .

On a alors l'alternative :

- $H \cap N = \{e\}$: dans ce cas $G = NH$ provient de que G/H et N sont isomorphes. Ψ envoie alors N sur N

et a pour noyau H; c'est le pendant non-commutatif d'un projecteur sur N de direction H.

- $H \cap N \neq \{e\}$ alors comme $\overline{\Psi}$ est à image sur N, $\overline{\Psi}^{-1}(H) = \overline{\Psi}^{-1}(H \cap N)$ et en composant avec $\overline{\Psi}$ on obtient $H = H \cap N$ soit $H \subset N$.

Pour l'alternative $H \subset N$, on définit bien un morphisme par $\Theta \ : \ \begin{cases} G/H \to G/N \\ gH \mapsto gN \end{cases}$ puisque si $g_1 H = g_2 H$ alors $g_2^{-1} g_1 \in N \supset H$ et donc $g_1 N = g_2 N$.
Si kH est un élément du noyau de Θ alors $\forall g \in G$:

$$\begin{aligned} \Theta(kHgH) &= \Theta(kH).\Theta(gH) \\ &= \Theta(gH).\Theta(kH) \\ &= \Theta(gHkH) = gN \end{aligned}$$

soit $\forall g \in G, \ kgN = gkN = gN$ soit $k \in N$ puisque N est distingué dans G.
Si à présent $k \in N$ alors $\Theta(kH) = kN = N$. **Ceci prouve que** $Ker(\Theta) = N/H$**.** En utilisant le premier théorème d'isomorphisme de la théorie des groupes, on a le
Paradoxe du reste constant : Soit G un groupe et H, N deux sous-groupes avec H **distingué** dans G tels que $H \cap N \neq \{0\}$, alors

$$(N \simeq G/H) \ \Rightarrow \ N \supset H \ et \ G/N \simeq (G/H)/(N/H)$$

autrement exprimé si G un groupe et H, N deux sous-groupes dont H est **distingué** dans G tels que $N \simeq G/H$ alors G, M, N vérifient le dit troisième d'isomorphisme de la théorie des groupes avec $G \supset N \supset H$!

Remarquons que **l'isomorphisme de classes**

$$\overline{\Theta} \ : \ \begin{cases} (G/H)/(N/H) \to G/N \\ gH.(N.H) \mapsto gN \end{cases}$$

est l'isomorphisme $\overline{\Theta}$: $\begin{cases} (G/H)/(N/H) \to G/N \\ gH.(N/H) \mapsto gN \end{cases}$
mais **n'est pas l'identité de** G/N **puisque** $(N/H) = \{nH/n \in N\}$ **n'est pas le groupe** N **bien que** $gH.(N/H) = gN$: en effet l'opération de groupe sur N est $n + n' = n''$ tandis que l'opération de groupe sur N/H est $nH+n'H = n''H$. **Il faut donc distinguer** gN **comme classe de** G/N **de** gN **comme classe de** $(G/H)/(N/H)$**!**

L'exemple des nombres réels classiques

Suivant Ross Street (An efficient construction of the real numbers (2004), disponible à http://www.math.mq.edu.au/~EffR.pdf) et Xavier Caruso (Une incarnation peu connue du corps des nombres rels (2008) disponible à http://perso.univ-rennes1.fr/xavier.caruso/articles/R.pdf) $\mathbb{R}$ est constructible comme corps totalement ordonné possédant la propriété de la borne supérieure, **par quasi-endomorphismes sur les entiers et sans recours à l'axiome du choix**. On pourra aussi consulter http://fr.wikipedia.org/wiki/Construction_des_nombres_reels pour les constructions plus classiques par suites de Cauchy et par coupures de Dedekind. Suivant ces trois constructions la **topologie** de $\mathbb{R}$ est métrisable (les boules ouvertes sont les intervalles $I_{a,b} = \{x \in \mathbb{R}/a < x < b\}$ où $a, b \in \mathbb{R}$ et $a < b$) et la propriété de la borne supérieure font de $\mathbb{R}$ un **corps totalement ordonné archimédien, complet, de corps premier** $\mathbb{Q}$ **dense**; De plus ces propriétés supplémentaires, ainsi que le théorème des valeurs intermédiaires sont prouvables sans recours à l'axiome du choix dans la théorie de Street.

Exponentielles discontinues

-Comment avez-vous trouvé mes dates?

$\mathbb{R}$ classique comme espace vectoriel sur $\mathbb{Q}$ classique

*Dans cette partie la théorie des ensembles est la théorie Zermelo-Fraenkel pour laquelle **l'ensemble** $\mathbb{R}$ est un espace vectoriel sur son corps premier $\mathbb{Q}$ comme nous le rappellons dans les classiques.*
En ajoutant l'axiome du choix à la théorie ZF : l'utilisation de logiques non-contradictoires permet de conclure à l'existence de bases pour tout espace vectoriel sur un corps.

Les morphismes $\Phi_{.,.}$

Cette collection se spécialise en une base β du $\mathbb{Q}$-espace vectoriel $\mathbb{R}$ et en un entier l différent de 1 de cette manière : Nous posons $\Phi_{\beta,l}(0) = 1$ et si $x \in \mathbb{R}^*$ alors $\exists n \in \mathbb{N},\ x = \sum_{i=1}^{n} q_i b_i$ avec $q_i \in \mathbb{Q}$ et b_i un vecteur de β alors nous posons

$$\Phi_{\beta,l}(x) = l^{\sum_{i=1}^{n} q_i}$$

Les $\Phi_{\beta,l}$ sont des solutions non continues de

$$f(x+y) = f(x) \times f(y)$$

Si $x = \sum_{i=1}^{n} q_i e_i$ et $y = \sum_{i=1}^{m} r_i e'_i$ avec $q_i, r_i \in \mathbb{Q}$ e_i, e'_i vecteurs de β alors

$$\begin{aligned}\Phi_{\beta,l}(x+y) &= l^{\sum_{i=1}^{n} q_i + \sum_{i=1}^{m} r_i} \\ &= l^{\sum_{i=1}^{n}} \times l^{\sum_{i=1}^{m} r_i} = \Phi_{\beta,l}(x) \times \Phi_{\beta,l}(y)\end{aligned}$$

$\Phi_{\beta,l}$ n'est pas constante, elle prend la valeur 1 et la valeur l sur les vecteurs de bases. $\Phi_{\beta,l}$ est une puissance rationnelle d'un nombre entier ; c'est un nombre algébrique. Comme l'ensemble des nombres algébriques est
dénombrable, comme $\Phi_{\beta,l}(x)$ admet au moins deux valeurs et est toujours algébrique, l'image de $\mathbb{R}$ contient au moins deux valeurs et est au plus dénombrable. Si $\Phi_{\beta,l}$ était continue alors l'image de la partie connexe $\mathbb{R}$ serait connexe : ce serait un singleton ou un intervalle de $\mathbb{R}$ de mesure non nulle. Comme un intervalle de mesure non nulle n'est pas dénombrable et que $\Phi_{\beta,l}$ admet au moins deux valeurs : $\Phi_{\beta,l}$ n'est pas continue et d'après ce qui précède $\Phi_{\beta,l}$ n'est pas continue en tout $x \in \mathbb{R}$.

Quelques propriétés des noyaux G_β et des morphismes $\Phi_{\beta,l}$

Dans ce qui suit on choisit une base β du $\mathbb{Q}$-espace vectoriel $\mathbb{R}$.
Si nous posons $G_\beta = Ker(\Phi_{\beta,l})$ alors

$$G_\beta = \{x \in \mathbb{R}/(x = \sum_{i \in I fini} r_i b_i) \wedge (\sum_{i \in I fini} r_i = 0)\}$$

est un sous-groupe de $\mathbb{R}$ comme noyau d'un morphisme de groupe.
G_β est dense dans $\mathbb{R}$ et n'est pas connexe : Comme $\mathbb{Q}$-espace vectoriel, $\mathbb{R}$ n'est pas de dimension finie - En effet si $dim_{\mathbb{Q}}(\mathbb{R}) = n < +\infty$ alors $\mathbb{R}$ est isomorphe et donc équipotent à $\mathbb{Q}^n$, il est alors dénombrable, or $\mathbb{R}$ n'est pas dénombrable - il suit que pour nombre entier p on peut trouver au moins p éléments distincts dans la base β. En particulier, il n'existe pas de réel $x > 0$ tel que $G_\beta = x\mathbb{Z}$: si c'est le cas alors il

existe des entiers relatifs m et n tels que $a-b=m\times x$ et $c-d=n\times x$, il vient alors

$$x=\frac{1}{m}\times a-\frac{1}{m}\times b=\frac{1}{n}\times c-\frac{1}{n}\times d$$

Cette double égalité signifie que x admet deux décompositions distinctes comme combinaison linéaire d'éléments de β et contredit le fait que β est une $\mathbb{Q}$-base de $\mathbb{R}$. Choisissons à présent les 2 nombres réels a et b $\mathbb{Q}$-libres dans G_β. Comme β est une $\mathbb{Q}$-base de $\mathbb{R}$, les réels $a-b$ ne sont pas nuls et par définition $\Phi_{\beta,l}((a+b)/2)=1$: **le milieu de deux nombres de G_β est toujours dans G_β. Ceci signifie que si G_β est connexe alors** $[a,b]\in G_\beta,\ \forall a,b\in G_\beta$. G_β serait alors un sous-groupe continu de $\mathbb{R}$: il serait $\mathbb{R}$, ce qu'il n'est pas!
G_β non connexe dans $\mathbb{R}$ ne peut pas être ni fermé ni ouvert.
D'après le dit premier théorème d'isomorphisme de la théorie des groupes, il existe pour tout l un isomorphisme $\overline{\Phi}_{\beta,l}$ tel que $\mathbb{R}/G_\beta \overset{\overline{\Phi}_{\beta,l}}{\to} \{l^q/q\in\mathbb{Q}\}$. ln_l : le logarithme à base l est un isomorphisme tel que $ln_l\left(\{l^q/q\in\mathbb{Q}\}\right)=\mathbb{Q}$, de sorte que sur la figure suivante la flèche représente un isomorphisme.

$$(\mathbb{R}/G_\beta,+)\overset{ln_l\circ\overline{\Phi_{\beta,l}}}{\to}(\mathbb{Q},+)$$

Il suit l'alternative :

(i) $G_\beta\subset\mathbb{Q}$.

(ii) $G_\beta\cap\mathbb{Q}=\emptyset$ et $ln_l\circ\overline{\Phi_{\beta,l}}$ envoie $\mathbb{Q}$ sur $\mathbb{Q}$.

dont nous examinons chaque terme :

(i) : **Les groupes G_β sont invariants par toute homothétie de rapport rationnel et donc**

$$G_\beta=\mathbb{Q}=G$$

Soit $x \in G_\beta$ et $r \in \mathbb{Q}$ alors $x = \sum_{i \in Ifini} r_i b_i$ et $r \times x = \sum_{i \in Ifini} (r.r_i) b_i \in r.G_\beta$.
Réciproquement si $y \in r.G_\beta$ alors $\exists r_i \in \mathbb{Q}$ tels que $y = r \times \sum_{i \in Ifini} r_i b_i$, on a donc $y = \sum_{i \in Ifini} (r.r_i) b_i \in G_\beta$ puisque $\forall i,\ r.r_i \in \mathbb{Q}$.

Pour autant G ne parait pas être Lebesgue mesurable! Supposons qu'il le soit : comme $\mathbb{Q} \supset G_\beta$ cela doit entrainer $\mu(G_\beta) = 0$ mais l'existence d'un isomorphisme de groupe de $(\mathbb{R}/G_\beta, +)$ vers $(\mathbb{Q}, +)$ entraîne que $\mathbb{R}$ admet une partition comme union dénombrable de translatés de G_β, qui sont tous de mesure nulle, $\mu(\mathbb{R})$ est alors la somme d'une série, absolument convergente et dont les termes sont les mesures -égales à zéro- de translatés de G_β. La somme d'une telle série est 0 ce qui contredit que $\mu(\mathbb{R}) = \infty$.
Soit $l \in \mathbb{R}$ alors les applications
$\Phi_l \ : \ \begin{cases} (\mathbb{R}, +) \to (\mathbb{R}, \times) \\ x \mapsto \ 1 \ si \ x \in \mathbb{Q}, \ l^x \ si \ x \in \mathbb{R} \backslash \mathbb{Q} \end{cases}$ **ne sont pas des morphismes discontinus** de $(\mathbb{R}, +)$ vers $(\mathbb{R}_+^*, \times)$ de noyaux $\mathbb{Q}$.
$\mathbb{R}$ **semble dénombrable** : puisque l'existence d'un isomorphisme de groupe de $(\mathbb{R}/G_\beta, +)$ vers $(\mathbb{Q}, +)$ fait apparaître $\mathbb{R}$ comme partition dénombrable de translatés des groupes G_β qui apparaissent comme étant $\mathbb{Q}$...Mais si $G_\beta = \mathbb{Q}$ alors nous choisissons $\mu \in \beta$ alors $\forall \nu \neq \mu \in \beta,\ \lambda - \mu \in \mathbb{Q} \supset G_\beta$ de sorte que $\mu + \mathbb{Q} \supset \mathbb{Q}$ et $\mu + \beta = A$ où A est une partie de $\mathbb{Q}$.
Supposons qu'il existe $r \in \mathbb{Q}$ tel que $r \notin A$ alors r s'exprime comme combinaison linéaire

d'éléments de $\mu + A$ c'est à dire que $r = \sum_{i \in I\ fini} r_i(q_i + \mu)$ avec $q_i \in A$, d'où

$$\mu \sum_{i \in I\ fini} r_i = r - \sum_{i \in I\ fini} r_i q_i \in \mathbb{Q}$$

- Si $\sum_{i \in I\ fini} r_i \neq 0$ alors $\mu \in \mathbb{Q}$ ce qui a pour conséquence que $\mathbb{Q} \supset \beta$ et par $\mathbb{Q}$-combinaison linéaire nous obtenons $\mathbb{R} \subset \mathbb{Q}$ ce qui est impossible.
- Si $\sum_{i \in I\ fini} r_i = 0$ alors, par définition de G_β, $r = \sum_{i \in I\ fini} r_i(q_i + \mu) \in G_\beta$, mais comme $G_\beta = \mathbb{Q}$ ceci prouve que tout $r \in \mathbb{Q}$ est combinaison linéaire à somme nulle de coefficients d'éléments de $\mu + \mathbb{Q}$ et, comme il précède $\mathbb{R} \subset \mathbb{Q}$.

Toute $\mathbb{Q}$-base de $\mathbb{R}$ est $\mu + \mathbb{Q}$ avec $\mu \notin \mathbb{Q}$! Mais comme tout réel est $\mathbb{Q}$-combinaison linéaire finie à coefficients rationnels d'éléments de $\mu + \mathbb{Q}$, $\mathbb{R}$ est équipotent à l'ensemble des suites presques nulles à valeur sur $\mathbb{Q}$ c'est à dire à $\mathbb{Q}_1[X]$ qui est dénombrable!

(ii) Appelons $\boldsymbol{l}$ la *forme linéaire*

$$\boldsymbol{l}\ :\ \sum_{i \in I fini} r_i b_i \mapsto \sum_{i \in I fini} r_i \in \mathbb{Q}$$

alors, le shéma d'axiomes de compréhension permet de conclure que $G_\beta = \{x \in \mathbb{R} / \boldsymbol{l}(x) = 0\} = Ker\,(\boldsymbol{l})$ et le shéma d'axiomes de remplacement que $ln_l \circ \overline{\Phi_{\beta,l}}$ est le morphisme $\left\{ \begin{array}{l} \mathbb{R}/Ker\,(\boldsymbol{l}) \to \mathbb{Q} \\ (\boldsymbol{l})^{-1}\,(q) \mapsto q \end{array} \right.$ c'est à dire le morphisme $\{x = \sum_{i \in I\ fini} r_i b_i / \sum_{i \in I\ fini} r_i = q\} \mapsto q$.

L'alternative au paradoxe du reste constant nous dit que $\mathbb{Q} \cap Ker\,(\boldsymbol{l})$ est le groupe réduit à 0 : ceci a pour conséquence que *la droite vectorielle* $\mathbb{Q}$ *est un supplémentaire de l'espace vectoriel* $Ker\,(\boldsymbol{l})$. et donc que toute $\mathbb{Q}$-base de $\mathbb{R}$, on les appelle bases de Hamel, est une partie irrationnelle de $\mathbb{R}$. Nous concluons à l'inconsistance de la théorie ZFC par le lemme

Lemme : *Dans la théorie ZFC des ensembles il existe des bases de Hamel dont* 1 *est vecteur de base (i.e. avec l'axiome du choix on peut choisir* $\mathbb{Q} \subset Ker\,(\boldsymbol{l})$*).*

Soit K un corps, E un K-espace vectoriel non réduit à $\{0\}$ et $e \in E\backslash\{0\}$, nous ordonnons l'ensemble $E(e)$ des parties libres de E qui contiennent e par l'inclusion, nous considérons $\mathcal{L} \subset E(e)$ l'ensemble, défini par les shéma d'axiomes de compréhension et de séparation, des parties libres de $E(e)$. $\mathcal{L}$ n'est pas vide car il contient au moins le singleton $\{e\}$.

Si $\mathcal{C}$ est une partie totalement ordonnée de $\mathcal{L}$ alors $\mathcal{M} = \cup_{c\in\mathcal{C}} c$ est un majorant de $\mathcal{C}$, c'est aussi une partie libre de E qui contient e :

En effet, si $\sum_{i=1}^{n} k_i e_i = 0$ avec $k_i \in K$ et $e_i \in \mathcal{M} = \cup_{c\in\mathcal{C}} c$ alors,

$(\forall i \in \{1,..,n\})(\exists c_i \in \mathcal{C}) e_i \in c_i$: les e_i sont des items d'au plus n parties libres c_i distinctes de $\mathcal{C}$, comme ces n parties sont totalement ordonnées par inclusion, la famille $(c_i)_{1\leq i\leq n}$ admet un plus grand élément c^* dans $\mathcal{C}$: autrement dit $\sum_{i=1}^{n} k_i e_i$ est une combinaison linéaire nulle sur la partie libre c^*, ce qui entraîne que $k_i = 0\ \forall i \in \{1, ..., n\}$.

Ceci étant vrai pour toute combinaison linéaire sur $\mathcal{M}$, il suit que $\mathcal{M}$ **est une partie libre de** E.

$\mathcal{L}$ est donc une partie non vide et inductive de E et, par application du lemme de Zorn, il existe un élément $\mathcal{B}$ de $\mathcal{L}$ qui est maximal pour l'ordre de l'inclusion.

$\mathcal{B}$ **est une base de** E : Soit $x \in E$, si x est un vecteur de $\mathcal{B}$ il est égal à $1.x$ et c'est une combinaison linéaire de vecteurs de $\mathcal{B}$.
Si $x \notin \mathcal{B}$ alors la partie $\mathcal{B}' = \mathcal{B} \cup \{x\}$ n'est pas libre car si elle l'était $\mathcal{B}$ ne serait pas une partie libre maximale. Il existe alors une combinaison linéaire nulle à coefficients non tous nuls de vecteurs de $\mathcal{B}'$, et le coefficient de x, item de $\mathcal{B}'$ n'est pas 0 car alors il existerait une combinaison linéaire nulle à coefficients non tous nuls de vecteurs de la partie libre $\mathcal{B}$. Si $\lambda x + \sum_{i=1}^{n} \lambda_i e_i = 0$ avec $\lambda \neq 0,\ e_i \in \mathcal{B}$ était cette combinaison linéaire alors $x = -\sum_{i=1}^{n} \dfrac{\lambda_i}{\lambda} e_i$ serait combinaison linéaire de vecteurs de $\mathcal{B}$.
On a prouvé que $\mathcal{B}$ est une partie génératrice de E et, comme c'est déjà une partie libre : c'est une base de E et comme $\mathcal{B} \subset \mathcal{L}$ c'est, par définition de $\mathcal{L}$ une partie de E qui contient e.

Comment peut-on choisir?

La conservation du principe de non-contradiction sans lequel toute proposition du langage est simultanément vraie et fausse impose de ne pas recourir à la généralité de l'axiome du choix : *Étant donné un ensemble X d'ensembles non vides mutuellement disjoints, il existe un ensemble y (l'ensemble de choix pour X) contenant exactement un élément pour chaque membre de X*, une version restreinte de cet axiome comme l'axiome du choix dépendant : *si $\mathcal{R}$ est une relation sur un ensemble E qui vérifie $(\forall x \in E)(\exists y \in E\ x\mathcal{R}y)$ alors il existe une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de E telle que $\forall n\ x_n \mathcal{R} x_{n+1}$* sera utile pour le développement de l'analyse réelle.
On appellera les nombres réels classiques, ceux construits

comme corps de nombres totalement ordonné et vérifiant la propriété de la borne supérieure.
L'apparence de non mesurabilité de $\mathbb{Q}$ est alors levée par le fait que la mesure complète de Lebesgue utilise des ensembles non mesurables inclus dans des boréliens de mesures nulles (*les exemples donnés pour des ensembles non mesurables utilisant toujours l'axiome du choix*). L'argument, basé sur l'utilisation de l'axiome du choix, de dénombrabilité de $\mathbb{R}$ n'en est plus un.

Sur les bases de $\mathbb{R}$

Avec l'usage d'une logique admettant le principe du tiers exclus pour prouver l'existence d'un objet, l'axiome du choix est inconsistant dans l'axiomatique Zermelo-Fraenkel de l'arithmétique réelle classique et $\mathbb{R}$ n'est pas un ensemble.

Sur les groupes réels noyaux d'un morphisme discontinu

Il y a deux bouts à ce bout de bois : Raymond Devos.
Dans ce qui suit la possibilité d'une construction des nombres réels sans utiliser l'axiome du choix permet le principe de non-contradiction.
Le noyau G d'un morphisme ϕ discontinu de $(\mathbb{R}, +)$ vers $(\mathbb{R}_+^*, \times)$ est un groupe réel non réduit à $\{0\}$ puisqu'un tel morphisme ne peut pas être injectif. Dans la suite nous considérons un tel morphisme ϕ : nous supposons qu'il en existe au moins un.
Si G était $d\mathbb{Z}$ avec $d \neq 0$ on aurait pour tout q entier impair

$$\phi(\frac{d}{q})^q = \phi(q \times \frac{d}{q}) = \phi(d) = 1$$

et donc $\phi(\frac{d}{q}) = 1$ soit $\frac{d}{q} \in d\mathbb{Z}$ ce qui n'est pas!

Considérons le morphisme de $(\mathbb{R}, +)$ vers lui-même $ln \circ \phi$ où ln est le logarithme népérien. Comme ln est un isomorphisme (de plus continu) de $(\mathbb{R}_*^+, \times)$ vers $(\mathbb{R}, +)$, $ln \circ \phi$ est un morphisme sur $(\mathbb{R}, +)$ dont l'image est un sous-groupe additif de $\mathbb{R}$, **nécessairement dense dans** $\mathbb{R}$.
Soit $y \in \mathbb{R}^*$ tel que $\phi(y) \neq 0$ alors nous posons

$$G(y) = \{x \in \mathbb{R} / ln(\phi(x)) = \frac{x}{y} ln(\phi(y))\}$$

- $ln(\phi(0)) = 0 = \dfrac{0}{y} ln(\phi(y) \Rightarrow 0 \in G(y)$
- Si $x \neq 0 \in G(y)$ alors, puisque $\phi(-x) = 1/\phi(x)$,

$$\begin{aligned} 0 &= ln(\phi(x)\phi(-x)) \\ &= ln(\phi(x)) + ln(\phi(-x)) \\ &= \frac{x}{y} ln(\phi(y)) + ln(\phi(-x)) \end{aligned}$$

$$\Downarrow$$

$$ln(\phi(-x)) = -\frac{x}{y} ln(\phi(y))$$

$$\Downarrow$$

$$-x \in G(y)$$

- Si $x_1, x_2 \in G(y)$ alors

$$\begin{aligned} ln(\phi(x_1 + x_2)) &= ln(\phi(x_1)\phi(x_2)) \\ &= ln(\phi(x_1)) + ln(\phi(x_2)) \\ &= \frac{x_1}{y} ln(\phi(y)) + \frac{x_2}{y} ln(\phi(y)) \\ &= \frac{x_1 + x_2}{y} ln(\phi(y)) \end{aligned}$$

$$\Downarrow$$

$$x_1 + x_2 \in G(y)$$

Il suit que $G(y)$ est un sous-groupe additif de $(\mathbb{R}, +)$, il contient y puisque $ln(\phi(y)) = \frac{y}{y} ln(\phi(y))$.

Propriété :

$$(\forall y, z \in \mathbb{R} \backslash Ker(\phi)) \ G(y) = G(z) \Leftrightarrow \frac{ln(\phi(y))}{y} = \frac{ln(\phi(z))}{z}$$

Preuve :

- Si $G(z) = G(y)$ alors $\left\{ \begin{array}{l} z \in G(y) \\ y \in G(z) \end{array} \right.$

$$\Downarrow$$

$$\left\{ \begin{array}{l} ln(\phi(z)) = \frac{z}{y} ln((\phi(y)) \\ ln(\phi(y)) = \frac{y}{z} ln((\phi(z)) \end{array} \right.$$

$$\Downarrow$$

$$\frac{ln(\phi(y))}{y} = \frac{ln(\phi(z))}{z}$$

- Si $\frac{ln(\phi(y))}{y} = \frac{ln(\phi(z))}{z}$ alors

$$\begin{aligned} x \in G(y) &\Leftrightarrow ln(\phi(x)) = \frac{x}{y} ln(\phi(y)) \\ &\Leftrightarrow ln(\phi(x)) = \frac{x}{z} ln(\phi(z)) \\ &\Leftrightarrow x \in G(z) \end{aligned}$$

Pour tout $y \in \mathbb{R} \backslash Ker(\phi)$, $G(y)$ est le groupe des réels t pour lesquels l'image de la fonction $x \mapsto \frac{ln(\phi(x))}{x}$ est constante et égale à $\frac{ln(\phi(y))}{y}$.

Soit $x \in \mathbb{R}\backslash Ker(\phi)$ alors $x \in G(x)$ et $2x \in G(x)$ puisque $2x = x+x$ et que $G(x)$ est un groupe qui contient x. On en déduit que $\dfrac{ln(\phi(2x))}{x} = \dfrac{ln(\phi(x))}{x}$ soit $2\dfrac{ln(\phi(x))}{x} = \dfrac{ln(\phi(x))}{x}$ soit $\dfrac{ln(\phi(x))}{x} = 0$ soit $(\phi(x)) = 1$ ce qui contredit que $x \notin Ker(\phi)$.

De l'insuffisance d'une définition constructive des nombres réels pour la mathématique

Nous avons établit les résultats suivants : Par l'utilisation du lemme des deux ouverts, dont on a donné une démonstration sans recours à l'axiome du choix et dans l'axiomatique Zermelo-Frankael de la théorie naïve des ensembles l'ajout de l'axiome du choix est inconsistant puisque la propriété de la borne supérieure se déduit de la complétion du groupe topologique $\mathbb{R}$ pour la topologie de la norme.

Une reformulation des nombres réels par axiome du choix dépendant n'est possible que comme groupe commutatif orienté par l'ordre, admettant des sous-groupes denses pour la topologie définie par l'ordre; la classe des solutions à l'équation fonctionnelle

$$f(x+y) = f(y) \times f(y) \ avec \ x, y \in \mathbb{R}$$

est le groupe des exponentielles népairiennes, *la propriété de la borne supérieure n'est pas démontrée par l'article de Street qui utilise pour le faire l'axiome du choix* Ceci est contradictoire avec ces différents points : Dans les disciplines de l'analyse numérique, de l'algèbre et de la mécanique du point matériel, l'utilisation de l'axiome du choix permet, grâce à son équivalent, le lemme de maximalité de Zorn, la démonstration de nombreux résultats en analyse fonctionnelle classique et en algèbre classique, parmi lesquels

- l'existence d'idéaux maximaux dans les anneaux de nombres réels,
- celle de solutions maximales aux équations de la dynamique.

Conclusions

Propriété des réels : Les réels sont constructibles, à partir des nombres entiers, comme corps de classe orienté par axiome du choix dépendant. Le corps de classe des réels est de plus archimédien; son corps premier est le corps des rationnels, dense. Par composition avec le logarithme *népairien* toute application additive est un morphisme de groupe orienté.
La Tronche, Echirolles, Eybens-26 Novembre 2010, 14 Mars 2016-17 Novembre 2017 14h20 heure locale