Sous-groupes de $\mathbb{R}$

Victor Rouanet

5 novembre 2021

1 Rappels et énoncé

La construction de $\mathbb{R}$ par les suites de Cauchy le fait apparaître comme un corps totalement ordonné, muni d'une structure d'espace métrique pour la distance associée à la valeur absolue et complet pour cette métrique. Le sous-groupe (et même sous-corps) $\mathbb{Q}$ y est dense, à la fois pour la métrique évoquée et pour la topologie de l'ordre (entre deux réels il y a toujours un rationnel).

À la manière de ceux de $(\mathbb{Z}, +)$, nous disposons d'un résultat fort qui caractérise les sous-groupes de $\mathbb{R}$. Commençons par un bref rappel des notions mises en jeu.

Définition. Un *sous-groupe de* $(\mathbb{R}, +)$ est une partie $G \subset \mathbb{R}$ telle que :
— G contient 0
— G est stable pour la loi interne : $\forall (x, y) \in G^2, x - y \in G$

Définition. Une partie $A \subset \mathbb{R}$ est dite *dense* si tout intervalle ouvert non-vide de $\mathbb{R}$ contient un élément de A.

Nous pouvons maintenant énoncer le théorème.

Théorème. *Tout sous-groupe de* $(\mathbb{R}, +)$ *est soit monogène soit dense.*

Démonstration. Soit $G \subset \mathbb{R}$ un sous-groupe. Si $G = \{0\}$, le résultat est trivial. Sinon, on pose $H = G \cap \mathbb{R}_+^* = \{x \in G, x > 0\}$ l'ensemble des éléments strictement positifs de G. Il s'agit d'une partie non-vide et minorée de $\mathbb{R}$, qui admet donc une borne inférieure notée α. Les deux alternatives du théorème résultent des deux cas suivants :

— **Si** $\alpha > 0$. On va montrer que $G = \alpha\mathbb{Z}$. D'abord, prouvons que $\alpha \in H$: en supposant le contraire et grâce à la définition de la borne inférieure, on pourrait trouver x et $y \in H$ tels que

$$\alpha < x < 2\alpha$$
$$\alpha < y < x$$

d'où

$$\alpha < x < 2\alpha$$
$$-y < -\alpha$$
$$y < x$$

et enfin

$$0 < x - y < \alpha.$$

Mais comme G est stable, on a $x - y \in G$ donc $x - y \in H$, ce qui contredit le fait qu'α est un minorant de H. Ainsi, $\alpha = \min H$ et $\boxed{\alpha\mathbb{Z} \subset G.}$

Réciproquement, soit $g \in G$. En notant $k = E(\frac{g}{\alpha}) \in \mathbb{Z}$, on a

$$k \leq \tfrac{g}{\alpha} < k + 1$$
$$0 \leq \tfrac{g}{\alpha} - k < 1$$
$$0 \leq g - k\alpha < \alpha = \min H$$

d'où $g - k\alpha = 0$ (puisque G est stable), et donc $\boxed{G \subset \alpha\mathbb{Z}.}$

— **Si** $\alpha = 0$. Intuitivement, G contenant des éléments strictement positifs arbitrairement petits, sa structure de groupe va entraîner sa densité pour la topologie de l'ordre car $\mathbb{R}$ est archimédien. Par symétrie, il suffit de montrer que H est dense dans $\mathbb{R}_+$.
Soit $I =]a; b[$ un intervalle ouvert non vide de $\mathbb{R}_+$. Comme $\inf H = 0$, il existe $\delta \in H$ tel que $\delta < b - a$. $\mathbb{R}$ étant archimédien, il existe $n \in \mathbb{N}$ tel que $a < n\delta$. La partie $\{n \in \mathbb{N}, a < n\delta\}$ de $\mathbb{N}$ est par conséquent non vide, et elle admet un plus petit élément, noté m, qui vérifie $(m-1)\delta \leq a < m\delta$. On a donc d'une part $m\delta \in H$ et de l'autre

$$a < m\delta = (m-1)\delta + \delta \leq a + \delta < a + (b-a) = b$$

Finalement $\boxed{\delta\mathbb{Z} \cap I \neq \emptyset \text{ et } G \text{ est dense.}}$

□

L'intérêt principal de ce théorème réside dans sa capacité à prouver la densité d'un sous-groupe : il suffira de dire que celui-ci n'est pas monogène, ce qui est en général beaucoup plus facile à vérifier.

2 Quelques applications

Corollaire. *Tout sous-groupe de* $(\mathbb{R}, +)$ *est soit fermé soit dense.*

Démonstration. Conséquence immédiate du théorème. □

Remarquons d'ailleurs que grâce aux propriétés des limites, l'adhérence d'un sous-groupe reste un sous-groupe.

Bien que ce résultat suivant soit une des pierres angulaires de la construction des nombres réels, le théorème permet de s'en assurer à nouveau.

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

Les trois propositions suivantes sont basées sur le même raisonnement : pour prouver la densité d'une partie, on l'écrit comme image directe d'un sous-groupe additif de $\mathbb{R}$ par une application continue.

Proposition. *Tout sous-groupe multiplicatif* $(G, \times) \subset (\mathbb{R}_+^*, \times)$ *est soit monogène soit dense.*

Démonstration. L'application

$$\begin{array}{cccc} \ln & : & \mathbb{R}_+^* & \to & \mathbb{R} \\ & & x & \mapsto & \ln(x) \end{array}$$

est continue et bijective. C'est de plus un morphisme du groupe $(\mathbb{R}_+^*, \times)$ dans le groupe $(\mathbb{R}, +)$, c'est à dire qu'elle vérifie pour tout a, b de $\mathbb{R}_+^*$:

$$\ln(a \times b) = \ln(a) + \ln(b)$$

L'image directe $\ln(G)$ est donc un sous-groupe de $(\mathbb{R}, +)$, caractérisé selon le théorème :

— **si** $\ln(G)$ est monogène, il existe $\alpha \in \mathbb{R}$ tel que $\ln(G) = \alpha\mathbb{Z}$, ce qui entraîne que $G = \exp(\alpha\mathbb{Z}) = \{\exp(\alpha)^k, k \in \mathbb{Z}\}$ est le sous-groupe monogène de $(\mathbb{R}_+^*, \times)$ engendré par $\exp(\alpha)$.
— **si** $\ln(G)$ est dense, son image par la bijection continue $x \mapsto \exp(x)$ l'est aussi, donc G est dense dans $\mathbb{R}_+^*$.

□

Proposition. $\cos(\mathbb{N}) = \{\cos(n), n \in \mathbb{N}\}$ *est dense dans* $[-1, 1]$.

Démonstration. La fonction cos étant paire et 2π-périodique, on a $\cos(\mathbb{N}) = \cos(\mathbb{Z}) = \cos(\mathbb{Z} + 2\pi\mathbb{Z})$. Or, comme π est irrationnel, le sous-groupe $\mathbb{Z} + 2\pi\mathbb{Z}$ de $(\mathbb{R}, +)$ n'est pas monogène, il est donc dense, tout son image par la surjection continue $\cos : \mathbb{R} \to [-1, 1]$. □

L'application similaire du théorème à la fonction sin nous permet de déduire que $\sin(\mathbb{Z})$ est dense dans $[-1,1]$ mais ne permet pas directement de conclure pour $\sin(\mathbb{N})$. Nous devons au préalable affiner le résultat de densité.

Lemme. $\mathbb{N}+2\pi\mathbb{Z}$ *est dense dans* $\mathbb{R}$.

Démonstration. On se donne $]u,v[$ un intervalle non vide et l'on note $\epsilon = |v-u|$.

- Si $0 \in]u,v[$, il n'y a rien à faire.
- Si $u > 0$. Puisque $\mathbb{Z}+2\pi\mathbb{Z}$ est dense, il y a une infinité de points s'écrivant comme $p+2q\pi$ dans l'intervalle $]0,\epsilon[$. Si l'un deux admet pour valeur de p un entier naturel, on a fini. Sinon, on choisit $x = p+2q\pi \in]0,\epsilon[$ tel que $p<0$, et l'on a alors grâce à la densité une infinité de points $y = r+2s\pi \in]0,x[$ avec tous $r<0$ d'après ce qui précède. Comme il y en a une infinité, au moins l'un d'entre eux vérifie $r<p<0$, car pour un r fixé il n'y a qu'un nombre fini de $r+2s\pi$ dans $]0,x[$. On a alors $x-y = (p-r)+2(q-s)\pi \in \mathbb{N}+2\pi\mathbb{Z}$ et $0 < x-y < x < \epsilon$.
- Si $v<0$, on applique le raisonnement symétrique sur avec l'intervalle $]-\epsilon, 0[$.

□

De ce lemme découle maintenant la proposition souhaitée :

Proposition. $\sin(\mathbb{N}) = \{\sin(n), n \in \mathbb{N}\}$ *est dense dans* $[-1,1]$.

Enfin, le théorème de classification des sous-groupes fournit un contre-exemple (en dimension 1 !) à l'affirmation « une somme de fermés est un fermé » dans le cadre d'un espace vectoriel topologique.

Proposition. $\mathbb{Z}+\alpha\mathbb{Z}$ *fermé* $\iff \alpha \in \mathbb{Q}$

Démonstration.

- **Si** $\alpha \in \mathbb{Q}$, il admet une forme irréductible $\alpha = \frac{p}{q}$ avec p et q des entiers premiers entre eux. D'une part, on peut écrire pour tous $m,n \in \mathbb{Z}$
$$m+n\alpha = m+n\frac{p}{q} = \frac{1}{q}(mq+pn)$$
d'où $\mathbb{Z}+\alpha\mathbb{Z} \subset \frac{1}{q}\mathbb{Z}$. D'autre part, théorème de Bézout assure l'existence de $(m,n) \in \mathbb{Z}^2$ tels que
$$mq+np=1$$
c'est à dire
$$m+n\frac{p}{q} = m+n\alpha = \frac{1}{q}$$
et ainsi $\frac{1}{q}\mathbb{Z} \subset \mathbb{Z}+\alpha\mathbb{Z}$, donc $\boxed{\mathbb{Z}+\alpha\mathbb{Z} = \frac{1}{q}\mathbb{Z}}$ est discret et fermé.
- **Si** $\mathbb{Z}+\alpha\mathbb{Z}$ **est fermé**, il ne peut être à la fois fermé et dense, car on aurait dans ce cas $\mathbb{R} = \mathbb{Z}+\alpha\mathbb{Z}$, mais le membre de droite est dénombrable alors que le membre de gauche ne l'est pas. Ainsi, $\mathbb{Z}+\alpha\mathbb{Z} = \gamma\mathbb{Z}$, et il existe donc $k,k' \in \mathbb{Z}$ tels que
$$\begin{aligned} \alpha = 0+\alpha\times 1 &= \gamma k \\ 1 = 1+\alpha\times 0 &= \gamma k' \end{aligned}$$
d'où $\boxed{\alpha = \frac{k}{k'} \in \mathbb{Q}}$.

□

En particulier, dès que α est irrationnel et bien que $\mathbb{Z}$ et $\alpha\mathbb{Z}$ soient des fermés, leur somme n'est pas un fermé.

Pour aller plus loin, voir par exemple [2], [1].

Références

[1] Jean-Yves Mérindol : *Nombres et Algèbre.* EDP Sciences, 2006.

[2] Frédéric Testard : *Analyse mathématique : la maîtrise de l'implicite.* Calvage & Mounet, 2012.