

LES SOUS-GROUPES DE $(\mathbb{R}, +)$

Un *sous groupe* (additif) de $(\mathbb{R}, +)$ est un ensemble de nombres réels contenant 0 et stable pour l'addition et la symétrisation. Cela signifie qu'une partie G de $\mathbb{R}$ est un sous-groupe lorsque

- $0 \in G$
- $\forall (x, y) \in G^2 : x + y \in G$
- $\forall x \in G : -x \in G$

Soient A et B deux parties de $\mathbb{R}$. On dit que A est *dense* dans B lorsque

$$\forall b \in B, \forall \varepsilon > 0 :]b - \varepsilon, b + \varepsilon[\cap A \neq \emptyset$$

Soit G un sous groupe de $(\mathbb{R}, +)$, on dira que G est *discret* lorsqu'il existe un réel α *strictement positif* tel que

$$G \cap]0, \alpha[= \emptyset$$

L'objet de ce problème est d'étudier les sous-groupes additifs de $\mathbb{R}$.

Dans toute la suite, G désigne un tel sous-groupe.

1. Formuler une proposition traduisant que G n'est pas discret. Montrer que si G n'est pas discret alors :

$$\forall x \in \mathbb{R}, \forall \alpha > 0, G \cap [x, x + \alpha[\neq \emptyset$$

2. Dans cette question, on suppose que G est discret et contient un élément autre que 0. Il existe alors un réel α strictement positif tel que $G \cap]0, \alpha[= \emptyset$.

- (a) Soit I un intervalle de longueur $\frac{\alpha}{2}$. Montrer que $G \cap I$ contient au plus un élément. Que peut-on en déduire pour l'intersection de G avec un intervalle quelconque de longueur finie ?
- (b) Montrer que $G \cap \mathbb{R}_+^*$ admet un plus petit élément que l'on notera m .
- (c) Montrer que $G = \{km, k \in \mathbb{Z}\}$. Un tel ensemble sera noté $\mathbb{Z}m$

3. Soit x et y deux réels strictement positifs, on pose

$$X = \mathbb{Z}x = \{kx, k \in \mathbb{Z}\}, Y = \mathbb{Z}y = \{ky, k \in \mathbb{Z}\}, S = \{mx + ny, (m, n) \in \mathbb{Z}^2\}$$

- (a) Vérifier que X , Y et S sont des sous-groupes de $(\mathbb{R}, +)$. On dira que X est le sous-groupe *engendré* par x , que Y est le sous-groupe engendré par y et que S est le sous-groupe engendré par x et y .
- (b) Montrer que S est discret si et seulement si $\frac{x}{y} \in \mathbb{Q}$.
4. On suppose ici que $\frac{x}{y}$ est irrationnel. Définissons des parties A et B

$$A = \{kx, k \in \mathbb{Z}^*\}, B = \{ky, k \in \mathbb{Z}^*\}$$

- (a) Montrer que $A \cap B = \emptyset$
- (b) Montrer que

$$\inf\{|a - b|, (a, b) \in A \times B\} = 0$$

5. En considérant un certain sous-groupe additif et en admettant que π est irrationnel, montrer que $\{\cos n, n \in \mathbb{Z}\}$ est dense dans $[-1, 1]$.

LES SOUS-GROUPES DE $(\mathbb{R}, +)$

1. Le sous-groupe G n'est pas discret si et seulement si

$$\forall \alpha > 0, G \cap]0, \alpha[\neq \emptyset$$

Supposons que G ne soit pas discret. Considérons un réel x quelconque et un $\alpha > 0$. Il existe un élément $g \in G \cap]0, \alpha[$. Appelons n la partie entière de $\frac{x}{g}$. On a alors

$$\begin{aligned} ng &\leq x < ng + g \\ ng + g &< ng + \alpha \leq x + \alpha \end{aligned}$$

donc $(n+1)g \in G \cap]x, x+\alpha[$ car G est stable.

2. (a) Si x et y sont dans I :

$$|x - y| \leq \frac{\alpha}{2} < \alpha$$

En particulier, si x et y sont deux éléments distincts de $G \cap I$, un des deux réels $x - y$ ou $y - x$ est un élément de $G \cap]0, \alpha[$ ce qui est impossible.

Un intervalle quelconque de longueur finie est toujours inclus dans l'union d'un nombre fini d'intervalles de longueur $\frac{\alpha}{2}$ et chacun de ces (petits) intervalles ne peut contenir qu'au plus un élément de G . Par conséquent, l'intersection de G avec un tel intervalle borné quelconque est toujours soit vide soit finie.

- (b) Comme G n'est pas réduit à 0, il existe un g non nul dans G . Comme $-g \in G$ on peut supposer $g > 0$.

Considérons alors l'ensemble $G \cap]0, g]$.

Il est non vide (il contient g) et fini d'après la question précédente. Il admet donc un plus petit élément que l'on note m .

Montrons que $m = \min G \cap \mathbb{R}_+^*$.

On sait déjà que

$$m \in G \cap]0, g] \subset \mathbb{R}_+^*$$

D'autre part, si $k \in G \cap \mathbb{R}_+^*$ deux cas sont possibles

- $k \leq g$ alors $k \in G \cap]0, g]$ donc $m \leq k$
- $g < k$ alors $m < k$ car $m \leq g$.

Ceci montre bien que m est un minorant de $G \cap]0, g]$ donc le plus petit élément de cet ensemble.

- (c) D'après la définition d'un sous-groupe (stabilité) $\mathbb{Z}m \subset G$.

Réciproquement, soit $g \in G \cap \mathbb{R}_+^*$. Notons k la partie entière de $\frac{g}{m}$. On a alors

$$k \leq \frac{g}{m} < k+1 \Rightarrow km \leq g < (k+1)m \Rightarrow 0 \leq g - km < m$$

À cause des propriétés de stabilité de G , on a $-km \in G$ et $g - km \in G \cap [0, m]$. D'après la définition de m , il est impossible que $g - km \in G \cap \mathbb{R}_+^*$. Ceci entraîne $g - km = 0$. C'est à dire $g = km$ donc $g \in \mathbb{Z}m$.

3. (a) Vérification facile des propriétés de stabilité.

- (b) Si S est discret, d'après la question 2., il existe $m > 0$ tel que $S = \mathbb{Z}m$.

Comme $x = 1 \times x + 0 \times y \in S$, il existe $p \in \mathbb{Z}$ tel que $x = pm$. De même, $y = 0 \times 1 + 1 \times y \in S$ il existe donc $q \in \mathbb{Z}^*$ tel que $y = qm$. On en déduit

$$m = \frac{x}{p} = \frac{y}{q} \Rightarrow \frac{x}{y} = \frac{p}{q} \in \mathbb{Q}$$

Réciproquement, si on suppose que $\frac{x}{y}$ est rationnel, il existe des entiers p et q tels que

$$\frac{x}{y} = \frac{p}{q} \in \mathbb{Q} \Rightarrow \frac{x}{p} = \frac{y}{q}$$

Notons m ce nombre réel. On a $x = pm$ et $y = qm$ donc x et y sont dans $\mathbb{Z}m$. De plus, pour tous les entiers i et j ,

$$ix + jy = (ip + jq)m \in \mathbb{Z}m$$

donc $S \subset \mathbb{Z}m$ Ceci entraîne que $S \cap]0, m[$ est vide donc que S est discret.

LES SOUS-GROUPES DE $(\mathbb{R}, +)$

4. (a) Si $A \cap B$ était non vide, il existerait des entiers non nuls p et q tels que $px = qy$. On aurait alors

$$\frac{x}{y} = \frac{p}{q} \in \mathbb{Q}$$

- (b) D'après 3., S est un sous-groupe qui n'est pas discret. Pour tout $\alpha > 0$, il existe donc des entiers m et n tels que $mx + ny \in]0, \alpha[$.

Lorsque $\alpha < \min(x, y)$, les entiers m et n sont tous les deux non nuls. Posons $a = mx$, $b = -ny$, alors $a \in A$ et $b \in B$ donc

$$\forall \alpha < \min(x, y), \inf\{|a - b|, (a, b) \in A \times B\} \leq \alpha$$

On en déduit que cette borne inférieure est nulle.

5. Considérons un intervalle quelconque $[u, v]$ dans $[-1, 1]$, on doit montrer qu'il existe un entier n tel que $\cos n \in [u, v]$.

Posons $\alpha = \arccos v$, $\beta = \arccos u$ et formons l'intervalle $[\alpha, \beta]$ de $\mathbb{R}$.

Comme 2π est irrationnel, le sous-groupe additif $\mathbb{Z} + 2\pi\mathbb{Z}$ engendré par 1 et $2\pi i$ est dense dans $\mathbb{R}$. Il existe donc des entiers m et n tels que $m + 2\pi n \in [\alpha, \beta]$. On en déduit que $\cos m \in [u, v]$ ce qu'il fallait montrer.