Sous-groupes de $(\mathbb{Z}, +)$

On a vu en cours que $(\mathbb{Z}, +)$ forme un groupe. On s'intéresse maintenant aux **sous-groupes** de $(\mathbb{Z}, +)$: un **sous-groupe de $(\mathbb{Z}, +)$** est une partie G de $\mathbb{Z}$ vérifiant :

i/ stabilité par zéro : $0 \in G$;

ii/ stabilité par opposé : $\forall x \in G,\ -x \in G$;

iii/ stabilité par somme : $\forall x \in G,\ \forall y \in G,\ x + y \in G$.

Le point suivant est assez immédiat : si G est un sous-groupe de $(\mathbb{Z}, +)$ alors $(G, +)$ est un groupe.

I Les sous-groupes de $(\mathbb{Z}, +)$

Dans cette partie, on montre le résultat suivant : Les sous-groupes de $(\mathbb{Z}, +)$ sont les $a\mathbb{Z}$, pour un certain $a \in \mathbb{N}$.

1. Montrer que, pour tout $a \in \mathbb{N}$, $a\mathbb{Z}$ est bien un sous groupe de $(\mathbb{Z}, +)$.
2. On veut maintenant montrer que tous les sous-groupes de $(\mathbb{Z}, +)$ sont bien de cette forme.
   On se donne donc un sous-groupe G de $(\mathbb{Z}, +)$.
   a. Si $G = \{0\}$, justifier qu'il existe $a \in \mathbb{N}$ tel qu'on ait bien $G = a\mathbb{Z}$.
   b. On suppose maintenant $G \neq \{0\}$.
      i. Justifier que l'ensemble $G_+^* = \{g \in G,\ g > 0\}$ est non vide.
      ii. En déduire que G_+^* possède un plus petit élément que l'on notera a.
      iii. Finalement, conclure qu'on a $G = a\mathbb{Z}$.
3. Conclure.

II Formulation moderne du théorème d'Eudoxe

Pour A, $B \subset \mathbb{R}$ on note $A + B = \{a + b,\ (a, b) \in A \times B\}$.

4. Soient G_1 et G_2 deux sous groupes de $(\mathbb{Z}, +)$. Montrer que $G_1 + G_2$ est un sous groupes de $(\mathbb{Z}, +)$.
5. Soient a, b, $d \in \mathbb{N}$. Montrer qu'on a $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ si et seulement si et d est un PGCD de a et b.

Sous-groupes de $(\mathbb{Z}, +)$

1 Soit $a \in \mathbb{N}$.

Mq $a\mathbb{Z} \subset \mathbb{Z}$

Soit $x \in a\mathbb{Z}$ ie $x \in \{ak,\ k \in \mathbb{Z}\} =$
ie il existe $k \in \mathbb{Z}$, $x = \underbrace{ak}_{\in a\mathbb{Z}}$.

Mq $\forall x, y \in a\mathbb{Z}$, $x + y \in \mathbb{Z}$

Soit $x, y \in a\mathbb{Z}$ ainsi il existe $k' \in \mathbb{Z}$ tq $x = ak'$
$k \in \mathbb{Z}$, tq $y = ak$

$$x + y = a(\underbrace{k + k'}_{\in \mathbb{Z}})$$

ie $x + y \in a\mathbb{Z}$

Mq $0 \in a\mathbb{Z}$.

Posons $k = 0$. $a0 = 0 \in a\mathbb{Z}$

Mq $\forall x \in a\mathbb{Z}, -x \in a\mathbb{Z}$
Soit $x \in a\mathbb{Z}$ il existe $k \in \mathbb{Z}$, $x = ak$

$$\text{ie } -x = -ak$$
$$= a\underbrace{(-k)}_{\mathbb{Z}}$$

le $-x \in a\mathbb{Z}$

2/a Posons $a = 0 \in \mathbb{N}$. $a\mathbb{Z} = \{0k,\ k \in \mathbb{Z}\} = \{0\} = G$

2/b/i Supp $G \neq \{0\}$. Alors il existe $a \in \mathbb{N}^*$, $G = a\mathbb{Z} = \{ak,\ k \in \mathbb{Z}\}$.

$$G_+^* = \{g \in G,\ g > 0\}$$
$$= \{g \in \{ak,\ k \in \mathbb{Z}\},\ g > 0\}$$

G est un sous-groupe de $(\mathbb{Z}, +)$

donc $\forall g \in G,\ -g \in G$

On a $G \neq \{0\}$

Mais $0 \in G$

Ainsi il existe $g \in G \setminus \{0\}$

Deux cas :

- $g > 0$ alors $g \in G_+^*$
- $g < 0$ alors $-g > 0$ et $-g \in G_+^*$

donc $G_+^* \neq \emptyset$

2/b/ii

$$\begin{cases} G_+^* \subset \mathbb{N} \\ G_+^* \neq \emptyset \end{cases}$$

car $\begin{cases} \forall g \in G_+^*,\ g \geqslant 0 \\ \forall g \in G_+^*,\ g \in \mathbb{Z} \end{cases}$

d'ap. la ppte du bon ordre, $\min_{(G, \geqslant)} G_+^* =: a$ existe.

2/b/iii

5 Mq $G \supset a\mathbb{Z}$

Procédons par récurrence. Mq $aℕ \subset G$ ie $\forall k \in ℕ,\ ak \in G$

(I) Pour $k = 0$

$0 \in G$ car G est un sous-groupe de $(ℤ, +)$ et donc G est stable par neutre.

(H) Soit $k \in ℕ$ et supp $ak \in G$. Mq $a(k+1) \in G$

$a(k+1) = ak + a$

or $\begin{cases} ak \in G \\ a \in G \end{cases}$

par stabilité de la somme sur $(G, +)$

ccl $aℕ \subset G$

De plus, $(G, +)$ est stable par opposé, donc $aℤ \subset G$

$\boxed{\subset}$ Mq $G \subset aℤ$

Soit $g \in G$. $\begin{cases} G \subset ℤ \\ a \in ℤ \end{cases}$ donc il existe $(q, r) \in ℤ^2$ tel que :

$$\begin{cases} a > r \geqslant 0 \\ g = aq + r \end{cases}$$

Mq $g = aq$. Procédons par l'absurde. Supp $r \neq 0$.

$r = g - aq$

et $-aq \in aℤ \subset G$

donc $\begin{cases} -aq \in G \\ g \in G \end{cases}$

donc $r \in G$

et $r < a$

mais $a = \min_{(a, \geqslant)} G_+^*$ donc $r \notin G_+^*$ donc $r \in G \setminus G_+^*$ donc $r \in \{0\}$ donc $r = 0$

CMB

donc $g = aq$

$\Rightarrow y \in a\mathbb{Z}$

$\Rightarrow \forall g \in G,\ g \in a\mathbb{Z}$

$\Rightarrow G \subset a\mathbb{Z}$

3 On a montré que tout les $a\mathbb{Z}$, $a \in \mathbb{N}$ sont des sous-groupes de $(\mathbb{Z}, +)$ dans

On a également mtq tt les sous-groupes de $(\mathbb{Z}, +)$ sont les $a\mathbb{Z}$, $a \in \mathbb{N}$.

Donc sous-groupes de $(\mathbb{Z}, +) = \{a\mathbb{Z},\ a \in \mathbb{N}\}$