Sous-groupes de $\mathbb{Z}$

73.1 **Pté** Soit $a \in \mathbb{N}$. $a\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$

Preuve : $\cdot\ 0 = a \times 0 \in a\mathbb{Z}$

$\cdot$ Soit $(x,y) \in (a\mathbb{Z})^2$. Il existe $(u,v) \in \mathbb{Z}^2$ tq $\begin{cases} x = au \\ y = av \end{cases}$

$x - y = au - av = a(u-v)$ or $(u-v) \in \mathbb{Z}$ donc $x-y \in a\mathbb{Z}$.

D'où $a\mathbb{Z}$ est sous groupe de $\mathbb{Z}$

73.2 **Pté** Soit G un sous-groupe de $\mathbb{Z}$

Il existe un unique $a \in \mathbb{N}$ tel que $G = a\mathbb{Z}$

Preuve Soit $G < \mathbb{Z}$ (sous groupe de $\mathbb{Z}$).

$\cdot$ Si $G = \{0\}$ $\quad G = 0\mathbb{Z}$.

$\cdot$ Sinon il existe $x \in G \setminus \{0\}$. $-x \in G \setminus \{0\}$ aussi.

On pose $A = G \cap \mathbb{N}^*$, x ou $-x \in A$ donc $A \neq \emptyset$

Ainsi A est une partie non vide de $\mathbb{N}$, elle admet donc un plus petit élément que l'on note a. $a \in A \subset \mathbb{N}^*$ donc $a > 0$.

↳ *Montrons que $a\mathbb{Z} \subset G$.*

$\cdot\ a0 = 0 \in G$

$\cdot$ Soit $n \in \mathbb{N}$. on suppose que $an \in G$.

$a(n+1) = \underbrace{an}_{\in G} + \underbrace{a}_{\in A \subset G} \in G$. Donc la pté est vraie au rg $n+1$.

Par récurrence on a donc $a\mathbb{N} \subset G$.

Or G stable par passage à l'opposé. Donc $a\mathbb{Z} \subset G$.

↳ *Montrons que $G \subset a\mathbb{Z}$.* Soit $y \in \mathbb{Z} \setminus a\mathbb{Z}$

D'après 72.1, il existe $(q,r) \in \mathbb{Z} \times [0..a[$ tq $y = aq + r$ (DE)

Si $y \in G$, $r = \underbrace{y}_{\in G} - \underbrace{aq}_{\in G} \in G$. Donc $r \in (\mathbb{N}^* \cap G) = A$ or $r < a = \min(A)$.

IMPOSSIBLE. donc $y \notin G$. Soit $a\mathbb{Z}^c \subset G^c$,

d'où $G \subset a\mathbb{Z}$

Ainsi par double inclusion on a bien $G = a\mathbb{Z}$, d'où l'existence

· Si $(a,b) \in \mathbb{N}^2$ tels que $a\mathbb{Z} = b\mathbb{Z} = G$.

↳ soit $G = \{0\}$ alors $a = b = 0$

↳ soit $G \neq \{0\}$ alors $a = \min(a\mathbb{Z} \cap \mathbb{N}^*)$ et $b = \min(b\mathbb{Z} \cap \mathbb{N}^*)$

or $a\mathbb{Z} \cap \mathbb{N}^* = G = b\mathbb{Z} \cap \mathbb{N}^*$ donc $a = b$ en tant qu'unique minimum du même ensemble non vide de $\mathbb{N}$.