

Cette proposition dit qu'il n'existe, à un isomorphisme près, qu'un seul groupe cyclique d'ordre $n \in \mathbb{N}^*$, et qu'un seul groupe monogène.

Prop.3: Tout groupe cyclique d'ordre $n \in \mathbb{N}^*$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
Tout groupe monogène infini est isomorphe à $\mathbb{Z}$.

I. Développement

Supposons tout d'abord que G soit fini d'ordre n , on traitera le cas G monogène infini dans le dernier paragraphe.

A. Mise en place du morphisme ($\sim$ exponentielle) qui permettra de quotienter, étude de $\text{Ker}\Psi$.

Soit $G = \langle a \rangle = \{e; a; \dots; a^{n-1}\}$, on a: $o(a) = n > 0$ et $a \neq 0$.

Considérons $\psi: \begin{cases} (\mathbb{Z}, +) \rightarrow (G, \times) \\ k \mapsto a^k \end{cases}$.

Ψ est un morphisme: $\forall k, k' \in \mathbb{Z}, \psi(k + k') = a^{k+k'} = a^k \cdot a^{k'} = \psi(k) \times \psi(k')$.

Par définition de $G = \langle a \rangle$, Ψ est surjective. (tout élément de $(G, \times)$ admet un antécédent par Ψ).

$\text{Ker}\psi = \{k \in \mathbb{Z} / a^k = e\}$ est un sous-groupe de $(\mathbb{Z}, +)$.

Par ailleurs, $\text{Ker}\Psi \neq \{0\}$ car $n \in \text{Ker}\Psi$.

B. "Lemme": Montrons que tous les sg H de $(\mathbb{Z}, +)$ non réduits à $\{0\}$ sont de la forme $k\mathbb{Z}$, $k \in \mathbb{N}^*$.

a) Détermination d'un candidat $k \in \mathbb{N}^*$ pour que $H = k\mathbb{Z}$

Soit H un sg de $(\mathbb{Z}, +)$, $H \neq \{0\}$. $\exists a \in H$ tq. $a \neq 0$.

- Ou bien $a > 0$, et $H \cap \mathbb{N}^* \neq \emptyset$
- Ou bien $a < 0$, et comme H est un groupe, $-a > 0$ appartient à H , et donc $H \cap \mathbb{N}^* \neq \emptyset$.

Ainsi, dans tous les cas, $H \cap \mathbb{N}^* \neq \emptyset$, donc H contient une partie non vide de $\mathbb{N}^*$, qui admet un plus petit élément.

Soit $k \in \mathbb{N}^*$ ce plus petit élément.

b) Montrons que $k\mathbb{Z} \subset H$.

On a $k \in H$ et H est un groupe additif, donc $\forall n \in \mathbb{N}, kn \in H$. Comme H est un groupe additif, $-kn \in H$, donc $k\mathbb{Z} \subset H$.

c) Montrons que $H \subset k\mathbb{Z}$.

Rappelons que H est un sg de $(\mathbb{Z}, +)$, $H \neq \{0\}$. Soit $x \in H \subset \mathbb{Z}$. On fait la division euclidienne de x par k , il vient:

$$\underset{\substack{x \\ \in H}}{x} = \underset{\substack{qk \\ \in H}}{kq} + r, \text{ où } q \in \mathbb{Z}, r \in \mathbb{N} \text{ et } 0 \leq r < k. \text{ Or } k \in H \text{ groupe additif, donc } qk \in H. \text{ Par conséquent (H sg additif) } r = x - kq \in H.$$

Donc $r \in H \cap \mathbb{N}$, et comme $r < k$, $r = 0$ par définition de k comme plus petit élément.

Finalement, $x = kq$, avec $q \in \mathbb{Z}$, donc $H \subset k\mathbb{Z}$.

C. Application à $\text{Ker}\Psi$, où l'on montre que $\text{Ker}\Psi = n\mathbb{Z}$, où $n = o(a)$.

Ainsi, en considérant l'application Ψ déterminée au A., $\exists k \in \mathbb{N}^*$ tq $\text{Ker}\Psi = k\mathbb{Z}$ (car $\text{Ker}\Psi$ sg de $(\mathbb{Z}, +)$ non réduit à $\{0\}$).

On sait que $o(a) = n$, donc $a^n = 1$, donc $n \in \text{Ker}\Psi$, et par conséquent $\exists q \in \mathbb{Z}$ tq. $n = kq$.

Il vient donc $a^{kq} = a^n = 1$. Or $\text{Ker}\Psi = k\mathbb{Z}$, donc $k \in \text{Ker}\Psi$ et par suite $a^k = 1$.

Mais n est le plus petit entier tq $a^n = 1$, donc $k = n$, et $q = 1$.

Donc $\text{Ker}\psi = n\mathbb{Z}$, où $n = o(a)$.

D. Conclusion grâce au premier théorème d'isomorphisme.

Or d'après le premier théorème d'isomorphisme, le morphisme Ψ se décompose comme suit (diagramme commutatif):

$$\begin{array}{ccc} (\mathbb{Z}, +) & \xrightarrow{\Psi} & (G, \times) \\ \downarrow & & \uparrow \\ \mathbb{Z} / \text{Ker}\psi & \xrightarrow{\sim} & \text{Im}(\psi) \end{array} \quad \text{où } \text{Im}(\Psi) = \langle a \rangle$$

Donc $\mathbb{Z} / \text{Ker}\Psi \simeq \langle a \rangle$

i.e. d'après ce qui précède $\mathbb{Z} / n\mathbb{Z} \simeq \langle a \rangle$, où $n = o(a)$.

Ainsi $G \simeq \mathbb{Z} / n\mathbb{Z}$, où $n \in \mathbb{N}^*$ est l'ordre de G .

E. Cas où l'ordre de G est infini.

$$\psi : \begin{cases} (\mathbb{Z}, +) \rightarrow (G, \times) \\ k \mapsto a^k \end{cases} \text{ est un morphisme surjectif.}$$

Afin de montrer que Ψ est bien l'isomorphisme recherché, raisonnons par l'absurde en supposant Ψ non injectif.

Si $\text{Ker}\Psi \neq \{0\}$, alors $\text{Ker}\Psi$ est un sous-groupe de $\mathbb{Z}$ non réduit à $\{0\}$, et $\exists n \in \mathbb{Z}$ tq. $\text{Ker}\Psi = n\mathbb{Z}$.

Donc, en appliquant le premier théorème d'isomorphisme comme ci-dessus, on a $\mathbb{Z}/n\mathbb{Z} \simeq \langle a \rangle$, et par conséquent ces groupes sont de même ordre, i.e. $o(\mathbb{Z}/n\mathbb{Z}) = n = o(a)$, ce qui contredit l'hypothèse $n = \infty$.

Donc Ψ est injective, et $G \simeq \mathbb{Z}$.

II. Commentaires.

Si c'est trop long, on peut considérer comme acquis la forme des sg. de $(\mathbb{Z}, +)$. A voir selon timing.

Il peut être aussi judicieux de le présenter comme un "Lemme" en début de démonstration.