Théorème : Tous les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $(n\mathbb{Z}, +)$ pour un $n \in \mathbb{Z}$.

Preuve : Soit H un sous groupe de $(\mathbb{Z}, +)$. Si $H = 0$, alors $H = 0.\mathbb{Z}$. Sinon $H \cap \mathbb{N}^*$ est non-vide et donc admet un plus petit élément, que nous allons noter n. D'où $n\mathbb{Z} \subseteq H$. Montrons que $H \subseteq n\mathbb{Z}$. Soit $a \in H$, effectuons la division euclidienne de a par n : $a = qn + r$ avec $0 \leq r < n$
Alors $a - qn = r \in H$ donc $r = 0$ par minimalité de n. Donc $a = nq$.

Sous-groupe engendré par une partie

Proposition : Soit $\{H_i\}_{i \in I}$ une famille quelconque de sous-groupes d'un groupe G. Alors leur intersection est encore un sous-groupe de G.

Proposition : Soit A une partie de G. On considère l'intersection des sous groupes de G contenant A :

$$\langle A \rangle := \bigcap_{\substack{H \leq G \\ H \supseteq A}} H$$

Alors $\langle A \rangle$ est un sous-groupe de G contenant A et c'est le plus petit sous-groupe possédant cette propriété.
On dit que c'est le sous-groupe engendré par A.

Preuve :

La proposition précédente montre que $\langle A \rangle$ est un sous-groupe de G. Il contient A car c'est l'intersection de sous-ensembles contenants A. Réciproquement, soit H_0 un sous-groupe de G contenant A, alors $\bigcap_{\substack{H \leq G \\ H \supseteq A}} H \subseteq H_0$ par définition de l'intersection. Donc $\langle A \rangle \subseteq H_0$. ∎

Proposition : Soit A une partie d'un groupe G. Alors

$$\langle A \rangle = \{ g_1 \cdots g_n \mid n \geq 1,\ g_i \in A \text{ ou } g_i^{-1} \in A \}$$

Preuve : On note $K = \{ g_1 \cdots g_n \mid n \geq 1,\ g_i \in A \text{ ou } g_i^{-1} \in A \}$. On a successivement :

- K est un sous-groupe de G contenant A, donc $\langle A \rangle \subseteq K$
- Comme $\langle A \rangle$ est un sous-groupe de G contenant A, il contient les inverses des éléments de A et leurs produits donc il contient K.

Ainsi : $\langle A \rangle = K$. ∎

Morphismes de groupes

Définition :

Soient $(G, *)$ et $(H, \heartsuit)$ deux groupes. Un morphisme de groupes de $(G, *)$ vers $(H, \heartsuit)$ est une application $\varphi : G \to H$ telle que

$\forall\, x, y \in G, \qquad \varphi(x * y) = \varphi(x) \heartsuit \varphi(y)$

Exemple :

- exp est un morphisme de $(\mathbb{R}, +)$ vers $(\mathbb{R}^*, \times)$
- $x \longmapsto \sqrt{x}$ est un morphisme de $(\mathbb{R}_+^*, \times)$ vers $(\mathbb{R}_+^*, \times)$.
- $x \longmapsto ax$ pour $a \in \mathbb{R}$ est un morphisme de $(\mathbb{R}, +)$ vers $(\mathbb{R}, +)$.

Proposition :

Soit φ un morphisme d'un groupe $(G, .)$ vers un groupe $(H, .)$.

Alors :

1) $\varphi(1_G) = 1_H$

2) $\forall\, x \in G, \quad \varphi(x^{-1}) = \varphi(x)^{-1}$

3) $\forall\, x \in G, n \in \mathbb{Z}, \quad \varphi(x^n) = \varphi(x)^n$.

Preuve : 1) $\varphi(1_G) = \varphi(1_G \times 1_G) = \varphi(1_G) \times \varphi(1_G)$.

L'élément $a = \varphi(1_G)$ vérifie donc $a \times a = a$. Donc $a = a \times a^{-1} = 1_H$

2) Soit $x \in G$, alors $\varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(1_G) = 1_H$

de même $\varphi(x)\varphi(x^{-1}) = 1_H$. Donc $\varphi(x^{-1}) = \varphi(x)^{-1}$.

3) Montrons par récurrence que $\forall\, n \in \mathbb{N}, \quad \varphi(x^n) = \varphi(x)^n$:

pour $n = 0$, $\varphi(x^0) = \varphi(1_G) = 1_H = \varphi(x)^0$

Soit $n \geq 0$, supposons que $\varphi(x^n) = \varphi(x)^n$.

alors $\varphi(x^{n+1}) = \varphi(x^n \cdot x) = \varphi(x^n x) = \varphi(x^n) \cdot \varphi(x)$

$= \varphi(x)^n \cdot \varphi(x)$

$= \varphi(x)^{n+1}$

On passe aux n négatifs avec le 2).

■

Noyau et image d'un morphisme :

Définition/Proposition :

Soit φ un morphisme d'un groupe $(G, \cdot)$ vers un groupe $(H, \cdot)$

L'image de φ, notée $\mathrm{Im}\,\varphi$, c'est $\varphi(G) = \{\varphi(x) ; x \in G\}$. Alors $\mathrm{Im}\,\varphi$ est un sous-groupe de H.

Preuve :

$\mathrm{Im}\,\varphi$ contient 1_H car $1_H = \varphi(1_G)$.

De plus, soient $u, v \in \mathrm{Im}(\varphi)$, alors on peut écrire : $u = \varphi(x)$, $v = \varphi(y)$

donc $uv^{-1} = \varphi(x)\,\varphi(y)^{-1} = \varphi(x)\,\varphi(y^{-1}) = \varphi(xy^{-1})$

donc $uv^{-1} \in \mathrm{Im}\,\varphi$ aussi $\mathrm{Im}\,\varphi$ est un sous groupe de H.

■

Définition/Proposition :

Soit φ un morphisme d'un groupe $(G, \cdot)$ vers un groupe $(H, \cdot)$. Le noyau de φ noté $\ker\varphi$ est par définition :

$$\ker(\varphi) = \{x \in G ; \ \varphi(x) = 1_H\}$$

C'est un sous-groupe de G.

Preuve :

On a $1_G \in \ker\varphi$ car $\varphi(1_G) = 1_H$

et pour $x, y \in \ker\varphi$ on a $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = 1_H \cdot 1_H^{-1} = 1_H$.

donc $\ker\varphi$ est un sous-groupe de G.

Proposition :

Soit φ un morphisme d'un groupe $(G, \cdot)$ vers un groupe $(H, \cdot)$.

Alors :

1) $\forall x, y \in G$, $\varphi(x) = \varphi(y) \iff xy^{-1} \in G$

2) φ est injective si et seulement si $\ker\varphi = \{1_G\}$.

Preuve :

On a les équivalences :

$$\varphi(x) = \varphi(y) \iff \varphi(x)\varphi(y)^{-1} = 1_H$$
$$\iff \varphi(x)\varphi(y^{-1}) = 1_H$$
$$\iff \varphi(xy^{-1}) = 1_H.$$
$$\iff xy^{-1} \in \ker\varphi.$$

Supposons que φ est injective.

Soit $x \in \ker\varphi$, alors $\varphi(x) = 1_H = \varphi(1_G)$ donc $x = 1_G$.

Ainsi $\ker \varphi = \{1_G\}$.

Réciproquement supposons que $\ker \varphi = \{1_G\}$

alors par 1) si $\varphi(x) = \varphi(y)$ alors $xy^{-1} \in \ker \varphi$ donc $xy^{-1} = 1_G$ donc $x = y$. Ainsi φ est injective.

■

Composition de morphismes et isomorphismes :

Proposition : Soient $(G, \cdot)$, $(H, \circ)$ et $(I, *)$ trois groupes et $\varphi : G \to H$, $\phi : H \to I$ deux morphismes de groupes. Alors la composée $\phi \circ \varphi : G \to I$ est un morphisme de groupes.

Preuve :

Soient $x, y \in G$, alors :

$$\begin{aligned} \phi \circ \varphi(xy) &= \phi(\varphi(x) \circ \varphi(y)) \\ &= \phi(\varphi(x)) * \phi(\varphi(y)) \\ &= (\phi \circ \varphi)(x) * (\phi \circ \varphi)(y) \end{aligned}$$

■

Proposition / Définition :

Soit φ un morphisme bijectif de $(G, \cdot)$ vers $(H, \cdot)$ alors φ^{-1} est un morphisme bijectif de $(H, \cdot)$ vers $(G, \cdot)$

On dit que φ est un isomorphisme.

Preuve : Soient $u, v \in G$ tels que $u = \varphi(x)$, $v = \varphi(y)$.

alors $\varphi^{-1}(u \cdot v) = \varphi^{-1}(\varphi(x) \cdot \varphi(y))$

$= \varphi^{-1}(\varphi(xy))$

$= xy = \varphi^{-1}(x) \cdot \varphi^{-1}(y)$

d'où φ^{-1} est un morphisme de groupes. ●