

GROUPES MONOGÈNES

1.1. Définition

On appelle groupe monogène, tout groupe de la forme :

$$G = \{a^n, n \in \mathbb{Z}\}$$

On dit alors que a est un **générateur** de G et on note $G = \langle a \rangle$

On dit qu'un groupe est **cyclique** s'il est monogène et fini.

Exemples :

Typiquement : $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique (d'ordre n)

$(\mathbb{Z}, +)$ est un groupe monogène (infini)

1.2. Théorème

Tout groupe monogène $\langle a \rangle$ est soit infini et isomorphe à $(\mathbb{Z}, +)$, soit fini et isomorphe à $(\mathbb{Z}/m\mathbb{Z}, +)$, $m \in \mathbb{N}^*$.

Démonstration :

On considère l'application :

$$\begin{aligned} \varphi_a : \mathbb{Z} &\rightarrow \langle a \rangle \\ n &\mapsto a^n \end{aligned}$$

- $\text{Im}(\varphi_a) = \langle a \rangle$ donc φ_a est **surjectif**.
- $\varphi_a(n + n') = a^{n+n'} = a^n \times a^{n'} = \varphi_a(n) \times \varphi_a(n')$ donc φ_a est un **morphisme de groupes**.

On sait que le noyau d'un morphisme de groupe est un sous-groupe, donc :

$$\text{Ker}(\varphi_a) = \{n \in \mathbb{Z} \mid a^n = 1\} \text{ est un sous-groupe de } \mathbb{Z}$$

Par conséquent, il existe $m \in \mathbb{N}$ tel que : $\text{Ker}(\varphi_a) = m\mathbb{Z}$

Deux cas se présentent alors :

$m = 0$: et alors $\text{Ker}(\varphi_a) = \{0\}$, φ_a est injective et donc bijective. Donc $\langle a \rangle$ est infini et isomorphe à $(\mathbb{Z}, +)$.

$m \in \mathbb{N}^*$: dans ce cas, φ_a n'est pas injective. Mais :

$$\varphi_a(n) = \varphi_a(n') \Rightarrow a^n = a^{n'} \Rightarrow a^{n-n'} = 1 \Rightarrow n - n' \in \text{Ker}(\varphi_a) \Rightarrow n - n' \in m\mathbb{Z} \Rightarrow n = n' + m$$

$\varphi_a(n)$ ne dépend donc que de la classe \bar{n} de n modulo m .

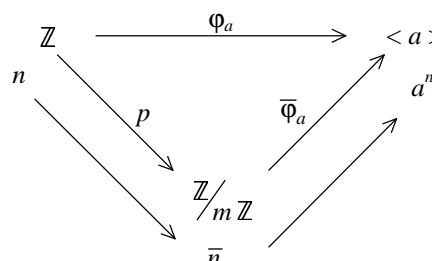
Définissons alors :

$$\begin{aligned} \bar{\varphi}_a : \mathbb{Z}/\text{Ker}(\varphi_a) &= \mathbb{Z}/m\mathbb{Z} \rightarrow \langle a \rangle \\ \bar{n} &\mapsto a^n \end{aligned}$$

Ainsi, ce nouveau morphisme $\bar{\varphi}_a$ est injectif (puisque $\bar{\varphi}_a(\bar{n}) = \bar{\varphi}_a(\bar{n}') \Rightarrow \bar{n} = \bar{n}'$) et surjectif.

Donc $\langle a \rangle$ est isomorphe à $\mathbb{Z}/m\mathbb{Z}$.

On dit que l'on a **factorisé** le morphisme φ_a :



L'entier $m \in \mathbb{N}^*$ vérifie donc $a^m = 1$ et c'est le plus petit. (En effet : $a^k = 1 \Rightarrow k \in \text{Ker}(\varphi_a) \Rightarrow k \in m\mathbb{Z}$)

Cet entier m s'appelle **l'ordre de l'élément a** .

1.3. Théorème

Soit G un groupe monogène : $G = \langle a \rangle$

- 1) Si G est infini, alors ses seuls générateurs sont a et a^{-1} .
- 2) Si G est fini d'ordre n , alors ses générateurs sont d'ordre n et sont les a^k où $(k, n) = 1$.

Démonstration :

- 1) Puisque a est générateur, a^{-1} l'est également :

$$\forall g \in G, \exists n \in \mathbb{Z}, g = a^n = (a^{-1})^{-n}$$

Soit b un générateur de G .

Comme a est générateur : $\exists u \in \mathbb{Z}, b = a^u$

Comme b est générateur : $\exists v \in \mathbb{Z}, a = b^v$

On a donc : $b = b^{uv}$
 $b^{1-uv} = 1$

Or, b n'est pas d'ordre fini. (S'il l'était, il ne pourrait pas être générateur)

Donc : $1 - uv = 0$
 $uv = 1$

Et comme u et v sont des entiers : $u = 1$ ou $u = -1$

D'où : $b = a$ ou $b = a^{-1}$

- 2) Soit b un générateur de G . Montrons que b est d'ordre n .

D'après le théorème de Lagrange, on sait que l'ordre de b divise n .

S'il le divisait strictement, b ne pourrait pas engendrer G , donc b est d'ordre n .

Soit maintenant un entier k tel que $b = a^k$ soit générateur.

Comme b est générateur : $\exists u \in \mathbb{Z}, a = b^u$

On a donc : $b = b^{ku}$
 $b^{1-ku} = 1$

Or, l'ordre de b est égal à n (car b est générateur), donc :

$$\exists v \in \mathbb{Z}, 1 - ku = vn$$

D'après le théorème de Bézout, on déduit : $(k, n) = 1$

Réciproquement, supposons $(k, n) = 1$ et montrons que $b = a^k$ est générateur :

D'après le théorème de Bézout : $\exists (u, v) \in \mathbb{Z}^2, uk + vn = 1$

Comme a est d'ordre n , on a alors :

$$(a^k)^u = a^{uk} = a^{1-vn} = a \times (a^n)^{-v} = a$$

Ce qui prouve que a est une puissance de a^k , donc $G = \langle a^k \rangle$.