

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 $G = \langle a^k \rangle$.