

3.1 Définitions

Un groupe G est *monogène* ssi il existe un élément a de G qui engendre G .

On a alors $G = \{a^n / n \in \mathbb{Z}\}$ en notation multiplicative et $G = \{na / n \in \mathbb{Z}\}$ en notation additive.

Un groupe fini et monogène est dit *cyclique*.

Remarques :

un groupe d'ordre n est cyclique ssi il admet au moins un élément d'ordre n ;

un groupe monogène est commutatif.

Exemples :

$\mathbb{Z}$ est monogène (ses générateurs sont 1 ou -1);

$\mathbb{Z}/n\mathbb{Z}$ est cyclique; $\bar{p}$ engendre $\mathbb{Z}/n\mathbb{Z}$ ssi p est premier avec n ;

si $n \geq 3$, S_n n'est pas cyclique car non commutatif.

Exercice 24

Un produit de deux groupes cycliques est cyclique ssi leurs ordres sont premiers entre eux.

Exercice 25

Montrer que les sous-groupes finis de $O^+(\mathbb{R}^2)$ (rotations vectorielles de $\mathbb{R}^2$) sont cycliques. Plus précisément $O^+(\mathbb{R}^2)$ a un unique sous-groupe de cardinal n , isomorphe au groupe des isométries affines du plan qui invarie un polygone régulier à n côtés.

Exercice 26

Un groupe fini d'ordre premier est cyclique (donc commutatif).

(Indication : considérer le sous-groupe engendré par $x \neq e$).

Proposition : Soit G un groupe fini d'ordre n . Alors pour tout élément x de G :

$$x^n = e.$$

Démonstration : si $x \in G$ le sous-groupe $\langle x \rangle$ engendré par x est d'ordre q diviseur de n (théorème de Lagrange, Exercice 17) donc $n = qq'$; comme x est d'ordre q on a $x^q = e$ donc $x^n = (x^q)^{q'} = e^{q'} = e$.

Remarque : en bref, dans un groupe fini, tout élément est « racine de l'unité » et tout élément est d'ordre fini.