03.03.2021

Chapitre 2 : Élément de la théorie des groupes

Définition :
Soit G un ensemble $\neq \emptyset$

Soit $\cdot : G \times G \to G$

On dit que $(G, \cdot)$ est un groupe si :

1) $\cdot$ est associative : $\forall x, y, z \in G \quad x.(y.z) = (x.y).z$

2) il existe un élément neutre : $\exists e \in G$ tq $\forall x \in G \quad e.x = x.e = x$

3) tous les éléments sont inversibles : $\forall x \in G, \exists y \in G$ tq $x.y = y.x = e$

Exemples :

a) $(\mathbb{Z}, +)$ est un groupe
→ neutre $= 0$
→ $\forall x, y \in \mathbb{Z} \quad x + (y + z) = (x + y) + z$
→ $\forall x \in \mathbb{Z} \quad x + (-x) = 0$

b) $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe
→ élément neutre $= \bar{0}$
→ inverse de $\bar{a} = \overline{-a}$

c) $((\mathbb{Z}/n\mathbb{Z})^{\times}, \times)$ est un groupe
→ neutre $\bar{1}$
→ inverse : inverse modulo n
→ le produit de 2 éléments inversibles est inversible.

Tous ces ex sont commutatif

Ex non commutatif :
l'ensemble des matrices inversibles.

On dit que G est commutatif (ou abélien) si $\forall x, y \in G \quad x.y = y.x$

On appelle $\cdot$ la loi de composition de G.

Remarque :
Qd on parle d'un groupe abstrait, on note tjs la loi multiplicativement.
On note $x^k = x.x.x \dots x$

Lemme : L'élément neutre d'un groupe est unique.
$\forall x \in G$, l'inverse de x est unique et on le note x^{-1}.

Preuve : Soient e, e' deux éléments neutres
$$\left.\begin{array}{l} e.e' = e \\ e.e' = e' \end{array}\right\} \text{donc } e = e'$$

Soient y, y' deux inverses de x
$x.y = e$
$x.y' = e \quad y'.x = e$
$y'.x.y = y'.e$
$e.y = y'.e$
donc $y = y'$

Définition Soit $H \subset G$. On dit que H est un sous-groupe de G si :
1) $\forall x, y \in H \quad x.y \in H$
2) $\forall x \in H \quad x^{-1} \in H$
$\Rightarrow e \in H$
↳ H est lui-même un groupe

Ex : Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$.

Ex 2 : $(\{\bar{0}, \bar{2}\}, +)$ est un sous-groupe de $(\mathbb{Z}/4\mathbb{Z}, +)$.

Définition : On appelle ordre d'un groupe son cardinal.

Définition : On appelle groupe fini un groupe d'ordre fini.

Définition : Soit $\mathcal{S} = \{x_1, \dots, x_n\}$ un ensemble d'éléments d'un groupe G.

On appelle sous-groupe engendré par $\mathcal{S}$, noté $<\mathcal{S}>$, l'ensemble de tous les produits des x_i et de leurs inverses.

Exemple : dans $\mathbb{Z}/6\mathbb{Z}$ $\quad <\bar{2}> = \{\underbrace{\bar{0}}_{\bar{2}+\overline{-2}}, \bar{2}, \underbrace{\bar{4}}_{\bar{2}+\bar{2}}\}$ est le sous-groupe engendré par $\mathcal{S} = \{\bar{2}\}$

Définition On dit que G est engendré par $\mathcal{S}$ si $G = <\mathcal{S}>$

Exemple : $\mathbb{Z}/n\mathbb{Z} = <\bar{1}>$

Théorème de Lagrange :

Soit G un groupe fini et H un sous-groupe de G.

Alors l'ordre de H divise l'ordre de G.