

Définition:

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

Soit  $\cdot : G \times G \rightarrow G$

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

- 1)  $\cdot$  est associative :  $\forall x, y, z \in G \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- 2) il existe un élément neutre :  $\exists e \in G \text{ tq } \forall x \in G \quad e \cdot x = x \cdot e = x$
- 3) tous les éléments sont inversibles :  $\forall x \in G, \exists y \in G \text{ tq } x \cdot y = y \cdot x = e$

Exemples:

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

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

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

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

Tous ces ex sont commutatif

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

Ex non commutatif:

l'ensemble des matrices inversibles.

Remarque:

Qd on parle d'un groupe abstrait, on note tjrs la loi multiplicativement.

On note  $x^k = x \cdot x \cdot x \dots x$

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

$$\left. \begin{array}{l} e \cdot e' = e \\ e \cdot e' = e' \end{array} \right\} \text{ donc } e = e'$$

Soient  $y, y'$  deux inverses de  $x$

$$\left( \begin{array}{l} x \cdot y = e \\ x \cdot y' = e \quad y' \cdot x = e \end{array} \right. \rightarrow \left. \begin{array}{l} y' \cdot x \cdot y = y' \cdot e \\ e \cdot y = y' \cdot e \\ \text{donc } y = y' \end{array} \right)$$

Définition Soit  $H \subset G$ . On dit que  $H$  est un sous-groupe de  $G$  si:

- 1)  $\forall x, y \in H \quad x \cdot y \in H$
  - 2)  $\forall x \in H \quad x^{-1} \in H$
- $\Rightarrow e \in H$   $\hookrightarrow H$  est lui-même un groupe

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

Ex 2:  $(\{\bar{0}, \bar{1}\}, +)$  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  $\mathcal{Y} = \{x_1, \dots, x_n\}$  un ensemble d'éléments d'un groupe  $G$ .

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

Exemple: dans  $\mathbb{Z}/6\mathbb{Z}$   $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}\}$  et le sous-groupe engendré par  $\mathcal{Y} = \{\bar{2}\}$

$\begin{array}{c} \uparrow \quad \uparrow \\ \bar{2} + \bar{-2} \quad \bar{2} + \bar{2} \end{array}$

Définition On dit que  $G$  est engendré par  $\mathcal{Y}$  si  $G = \langle \mathcal{Y} \rangle$

Def.  $G$  est cyclique si il existe un ensemble  $\mathcal{Y}$  qui ne contient qu'un seul élément tel que  $G = \langle \mathcal{Y} \rangle$

Prop:  $\mathbb{Z}/n\mathbb{Z}$  engendré par  $k \Leftrightarrow \text{PGCD}(k, n) = 1$

Théorème de Lagrange:

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

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

Exemple:  $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$  est cyclique

car  $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ ,  $\bar{k} = \underbrace{\bar{1} + \bar{1} + \dots + \bar{1}}_{k \text{ fois}}$

Exemple:  $\mathbb{Z}/30\mathbb{Z}$  engendré par  $\bar{1}$

engendré aussi par  $\{\bar{2}, \bar{3}\}$

↳  $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \dots, \bar{28}\}$

↳  $\langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \dots, \bar{27}\}$

↳ Il manque des éléments qui sont une combinaison linéaire de  $\bar{3}$  et  $\bar{2}$

↳ ex  $\bar{5} = \bar{3} + \bar{2}$

$\bar{1} = \bar{3} - \bar{2}$

$\bar{10} = \bar{2} + \bar{3} + \bar{2} + \bar{3}$

..