

Algèbre Générale : Structure de groupes

Partie 1 : Structure de Groupe & Sous-groupes

Définition : Un groupe est un couple $(G, \cdot)$ où $\cdot$ est une loi interne associative, admettant un élément neutre e_G , et où tout élément $x \in G$ possède un symétrique x^{-1} .

Caractérisation d'un sous-groupe : $H \subset G$ est un sous-groupe de $(G, \cdot)$ ssi :

- ☞ $e_G \in H$ (donc $H \neq \emptyset$)
- ☞ $\forall x, y \in H, \quad x \cdot y^{-1} \in H$

Propriétés des sous-groupes :

- ☞ L'intersection de toute famille de sous-groupes de G est un sous-groupe de G .
- ☞ $H_1 \cup H_2$ est un sous-groupe ssi $H_1 \subset H_2$ ou $H_2 \subset H_1$.

Sous-groupes spéciaux

- ☞ Tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$.
- ☞ Tout sous-groupe de $(\mathbb{R}, +)$ est de la forme $n\mathbb{Z}$ avec $n \in \mathbb{R}^+$, ou bien dense dans $\mathbb{R}$.

Morphisme de groupes : $f : G \rightarrow G'$ vérifie $f(x \cdot y) = f(x) \cdot f(y)$.

- ☞ $\text{Ker}(f) = \{x \in G \mid f(x) = e_{G'}\}$ sgr de G .
- ☞ $\text{Im}(f) = \{f(x) \mid x \in G\}$ sous groupe de G' .
- ☞ f injectif $\iff \text{Ker}(f) = \{e_G\}$.

Partie 2 : Ordre d'un Élément

Sous-groupe engendré : $\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$ est le plus petit sous-groupe de G contenant x .

Ordre : L'ordre de $x \in G$, noté $\text{ord}(x)$, est la cardinalité du sous-groupe $\langle x \rangle$.

- ☞ **Cas infini :** Si $\forall k \in \mathbb{N}^*, x^k \neq e$, alors $\text{ord}(x) = +\infty$ et $\langle x \rangle \simeq \mathbb{Z}$.
- ☞ **Cas fini :** C'est le plus petit $n \in \mathbb{N}^*$ tel que $x^n = e$. Alors $\langle x \rangle = \{e, x, \dots, x^{n-1}\}$ et $\langle x \rangle \simeq \mathbb{Z}/n\mathbb{Z}$.

Propriétés fondamentales :

- ☞ $x^k = e \iff \text{ord}(x) \mid k$.
- ☞ $x^k = x^l \iff k \equiv l \pmod{\text{ord}(x)}$.
- ☞ $\text{ord}(x^k) = \frac{n}{n \wedge k}$, où $n = \text{ord}(x)$.
- ☞ $\text{ord}(x^{-1}) = \text{ord}(x)$, $\text{ord}(xy) = \text{ord}(yx)$.
- ☞ $\text{ord}(gxg^{-1}) = \text{ord}(x)$ pour tout $g \in G$.
- ☞ Si $xy = yx$ et $\text{ord}(x) \wedge \text{ord}(y) = 1$, alors $\text{ord}(xy) = \text{ord}(x)\text{ord}(y)$.

Théorème de Lagrange : Si G est un groupe fini et H sgr de G , alors $|H|$ divise $|G|$.

Conséquences directes :

- ☞ Pour tout $x \in G$, $\text{ord}(x)$ divise $|G|$.
- ☞ Pour tout $x \in G$, $x^{|G|} = e_G$.

Partie 3 : Groupes Monogènes et Cycliques

Définitions :

- ☞ G est **monogène** ssi $\exists a \in G$ tel que $G = \langle a \rangle$.
- ☞ G est **cyclique** s'il est monogène et **fini**.
Dans ce cas $G = \langle a \rangle = \{e_G, a, \dots, a^{n-1}\}$, où $n = \text{ord}(x) = \text{card}(G)$.

Classification isomorphe :

- ☞ Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$.
- ☞ Tout groupe cyclique d'ordre n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$ ou à $(\mathbb{U}_n, \times)$.

Générateurs d'un groupe cyclique : Soit $G = \langle a \rangle$ un groupe cyclique d'ordre n .

- ☞ a^k est un générateur de $G \iff k \wedge n = 1$.
- ☞ Le nombre de générateurs de G est égal à $\varphi(n)$ (l'indicatrice d'Euler).

Sous-groupes d'un groupe cyclique : Soit G un groupe cyclique d'ordre n .

- ☞ Tout sous-groupe de G est lui-même cyclique.
- ☞ Pour chaque diviseur d de n , il existe un unique sous-groupe de G d'ordre d , engendré par $a^{n/d}$.
- ☞ Tout groupe d'ordre premier p est cyclique et n'admet que $\{e_G\}$ et G comme sous-groupes.