

GROUPES

 : Définition.  : Résultat de cours.  : Résultat pratique.  : Astuce.  : Démarche.  : Exemple classique.  : Attention.  : Information

GROUPES



Groupe

On appelle groupe tout ensemble G muni d’une loi de composition interne \star vérifiant :

- la loi \star est associative: $\forall x, y, z \in G : \quad (x \star y) \star z = x \star (y \star z)$
- G possède un élément neutre: $\exists e \in G$ tel que: $\forall x \in G, \quad x \star e = e \star x = e$
- Tout élément x de G admet un symétrique, c’est-à-dire $\forall x \in G, \quad \exists x' \in G$ tel que $x \star x' = x' \star x = e$

Si de plus $\forall x, y \in G: x \star y = y \star x$, on dit que la loi \star est commutative, et que le groupe est abélien.



Groupe produit

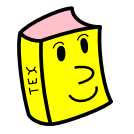
Soit $(G_1, \star_1), \dots, (G_n, \star_n)$ des groupes.
En définissant dans $G = G_1 \times \dots \times G_n$ la loi \star par:
 $\forall (x_1, \dots, x_n), (y_1, \dots, y_n) \in G:$

$$(x_1, \dots, x_n) \star (y_1, \dots, y_n) = (x_1 \star_1 y_1, \dots, x_n \star_n y_n)$$

Alors (G, \star) est un groupe d’élément neutre $(e_{G_1}, \dots, e_{G_n})$ et pour tout $(x_1, \dots, x_n) \in G_1 \times \dots \times G_n$, on a

$$(x_1, \dots, x_n)^{-1} = (x_1^{-1}, \dots, x_n^{-1})$$

Un tel groupe est appelé le groupe produit.
Il est abélien si, et seulement, si les G_i le sont



Sous-groupe

Soit $(G, .)$ un groupe. Une partie $H \subset G$ est un sous-groupe de G

$$\begin{aligned} \Longleftrightarrow \quad & \begin{cases} H \neq \emptyset; \\ \forall x, y \in H : x.y \in H; & (x + y \in H) \\ \forall x \in H : x^{-1} \in H & (-x \in H) \end{cases} \\ \Longleftrightarrow \quad & \begin{cases} H \neq \emptyset; \\ \forall x, y \in H : x.y^{-1} \in H. & (x - y \in H) \end{cases} \end{aligned}$$



Théorème

Un sous-groupe d’un groupe est un groupe.



Les sous-groupes de $(\mathbb{Z}, +)$

Soit H un sous groupe de \mathbb{Z} , alors il existe un unique entier $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$



Sous-groupe engendré

- L’intersection d’une famille non vide de sous-groupes est un sous-groupe
- Soit $S \subset G$. L’ensemble $\text{gr}(S)$ intersection de tous les sous-groupes de G contenant S est le plus petit sous-groupe de $(G, .)$, au sens de l’inclusion, contenant S , dit le sous-groupe engendré par S

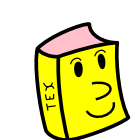


Exemple

Pour $a \in G, \text{gr}(a) = \{a^k, k \in \mathbb{Z}\}$.
En notation additive $\text{gr}(a) = \{ka, k \in \mathbb{Z}\}$

MORPHISMES DE GROUPES

Soit $(G, .), (G', \star)$ deux groupes de neutres respectifs e et e' .



Morphismes de groupes

Une application $f : G \longrightarrow G'$ est dite morphisme de groupes si:

$$\forall x, y \in G, \quad f(x.y) = f(x) \star f(y)$$

Si de plus f est bijectif, on dit que f est un isomorphisme de groupes



Opérations de morphismes

- La composée de deux morphismes est un morphisme;
- L’application réciproque d’un isomorphisme est un isomorphisme



Propriétés de morphismes

Soit $f : (G, .) \rightarrow (G', \star)$ un morphisme de groupes.
Alors $\forall x, y \in G$ et $n \in \mathbb{Z}$:

- $f(e) = e'$
- $f(x^{-1}) = f(x)^{-1}$
- $f(xy^{-1}) = f(x) \star f(y)^{-1}$
- $f(x^n) = f(x)^n$



Images de sous-groupes

Soit $f : (G, .) \rightarrow (G', \star)$ un morphisme de groupes. Alors

- Si H est un sous-groupe de G , alors $f(H)$ est un sous-groupe de G' .
- Si H' est un sous-groupe de G' , alors $f^{-1}(H')$ est un sous-groupe de G .

En particulier

- $\text{Ker}(f) = f^{-1}(\{e'\})$, le noyau de f , est un sous-groupe de G .
- $\text{Im}(f) = f(G)$, l’image de f , est un sous-groupe de G' .



Injectivité et surjectivité

Un morphisme de groupe $f : (G, .) \rightarrow (G', \star)$ est

- injectif si, et seulement, si $\text{Ker} f = \{e_G\}$
- surjective si, et seulement, si $\text{Im} f = G'$

ORDRES



Caractérisation de l’ordre

Un élément $a \in G$ est d’ordre fini s’il existe $k \in \mathbb{Z}^*$ tel que $a^k = e$. Au quel cas $\circ(a) = \min\{k \in \mathbb{N}^* \mid a^k = e\}$ est appelé l’ordre de a et aussi l’unique entier n de \mathbb{N}^* tel que l’on ait : $\forall k \in \mathbb{Z}, \quad a^k = e \iff n \mid k$



Ordre des itérés

Si $a \in G$ est d’ordre fini n et $r \in \mathbb{Z}$, alors $\circ(a^r) = \frac{n}{n \wedge r}$

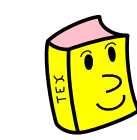


Ordre et cardinal

Si a est d’ordre n , alors

- Le groupe $\text{gr}(a)$ est de cardinal n et $\text{gr}(a) := \{e, a, \dots, a^{n-1}\}$
- $\text{gr}(a)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$

GROUPES MONOGÈNE, CYCLIQUE



Groupe monogène, groupe cyclique

- S’il existe $a \in G$ tel que $G = \text{gr}(a)$, le groupe est dit *monogène*.
- Un groupe cyclique est un groupe monogène fini.



Propriété

- Tout groupe monogène est abélien
- Un sous-groupe d’un groupe monogène est monogène
- Un sous-groupe d’un groupe cyclique est cyclique



Classification de groupes monogènes

Soit $G = \text{gr}(a)$ un groupe monogène, alors

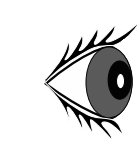
- Si G est infini, il est isomorphe à \mathbb{Z}
- Si G est d’ordre n , il est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$



Générateurs d’un groupe monogène

Soit $G = \text{gr}(a)$ un groupe monogène

- Si G est infini, alors a et a^{-1} sont les seuls générateurs de $\text{gr}(a)$
- Si G est cyclique d’ordre n , alors les générateurs de G sont exactement a^r avec $r \in \llbracket 0, n - 1 \rrbracket$ et $r \wedge n = 1$



Générateurs de $\mathbb{Z}/n\mathbb{Z}$ et de \mathbb{U}_n

Soit $k \in \llbracket 0, n - 1 \rrbracket$ et $\omega = e^{i\frac{2\pi}{n}}$

- \bar{k} engendre $(\mathbb{Z}/n\mathbb{Z}, +) \iff n \wedge k = 1$
- ω^k engendre $(\mathbb{U}_n, \times) \iff n \wedge k = 1$

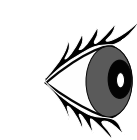
THÉORÈME DE LAGRANGE



Théorème de Lagrange

Soit G un groupe fini. Alors:

- Tout élément de G est d’ordre fini;
- l’ordre de tout élément de G divise le cardinal G .
En particulier: $\forall a \in G, \quad a^{\text{Card} G} = e_G$



Exemple: Groupe d’ordre premier

Soit G un groupe fini d’ordre premier p . Alors G est cyclique.

CONTACT INFORMATION

Web: www.elamdaoui.com
Email: elamdaoui@gmail.com
Phone: 06 62 30 38 81