Synthèse de cours PanaMaths
→ Groupes - Généralités

Généralités

Définitions

Soit G un ensemble et $*$ une loi de composition interne (LCI) sur G.
On dit que « $(G,*)$ est un groupe » (ou, s'il n'y a pas d'ambiguïté, que « G est un groupe ») si la loi $*$ vérifie :

1. $*$ est <u>associative</u> :

$$\forall (x,y,z)\in G^3, (x*y)*z = x*(y*z)$$

2. $*$ possède un <u>élément neutre</u> e :

$$\forall x\in G,\ x*e = e*x = x$$

3. Tout élément de G possède un <u>symétrique</u> pour $*$:

$$\forall x\in G, \exists x'\in G / x*x' = x'*x = e$$

Si la loi $*$ est commutative, on dit que « G est commutatif » ou que « G est abélien ».

Remarques :

❶ Dans un groupe, le symétrique d'un élément x donné est classiquement noté x^{-1} (c'est systématiquement le cas lorsque la loi est notée multiplicativement). Si la loi est note additivement (« + »), le symétrique de x est traditionnellement noté « $-x$ »).

❷ La combinaison de l'associativité et de la commutativité permet dans un groupe de s'affranchir des parenthèses, de traiter les calculs dans l'ordre que l'on veut et de regrouper les éléments à notre guise. C'est ce que nous pratiquons, parfois sans en avoir pleinement conscience, lorsque nous effectuons des calculs dans $\mathbb{R}$.

Quelques exemples fondamentaux

$(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes additifs. Ils sont abéliens.
$(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$ et $(\mathbb{C}^*,\times)$ sont des groupes multiplicatifs. Ils sont abéliens.
L'ensemble des bijections d'un ensemble dans lui-même muni de la composition des applications est un groupe. Il n'est, en général, pas abélien.
Pour tout ensemble E, $(\mathscr{P}(E),\cap)$ (ensemble des parties de E muni de l'intersection) est un groupe abélien.

Propriétés

- Un groupe est non vide (il contient son élément neutre).
- L'élément neutre est unique.
- Tout élément d'un groupe admet un unique symétrique.
- Tout élément d'un groupe est régulier :

$$\forall (a,b,c) \in (\mathrm{G},*)^3,\ a*b = a*c \Rightarrow b = c \text{ et } b*a = c*a \Rightarrow b = c$$

- $\forall (a,b) \in (\mathrm{G},*)^2, (a*b)^{-1} = b^{-1}*a^{-1}$.

Remarques :

❶ L'unicité du symétrique découle (résultat général) du fait que la loi de composition interne admet un élément neutre et est associative.

❷ Si un ensemble E est muni d'une loi de composition interne et si on a :
$\forall (a,b,c) \in (\mathrm{E},*)^3,\ a*b = a*c \Rightarrow b = c$ (respectivement $b*a = c*a \Rightarrow b = c$), on dit que « l'élément *a* de E est régulier à gauche » (respectivement « à droite »).

Sous-groupe

Définition

Soit $(\mathrm{G},*)$ un groupe et soit H une partie de G.
On dit que « $(\mathrm{H},*)$ est un sous-groupe de $(\mathrm{G},*)$ » (ou, s'il n'y a pas d'ambiguïté, que « H est un sous-groupe de G ») si :

1. H est stable pour $*$ ($\forall (x,y) \in \mathrm{H}^2,\ x*y \in \mathrm{H}$).
2. H muni de la loi induite par $*$ est encore un groupe.

Remarque : la loi induite par $*$ sur H est traditionnellement encore notée $*$.

Un exemple fondamental

Les sous-groupes de $(\mathbb{Z},+)$ sont les ensembles $(n\mathbb{Z},+)$, où *n* est un entier relatif.

Caractérisation

Soit $(G,*)$ un groupe et soit H une partie de G.
H est un sous-groupe de G si, et seulement si, on a :

- $H \neq \varnothing$;
- $\forall (x, y) \in H^2, x * y^{-1} \in H$.

Sous-groupe engendré par une partie

Définition

Soit $(G,*)$ un groupe et soit A une partie de G.
On appelle « sous-groupe de G engendré par A », classiquement noté $\langle A \rangle$, le plus petit sous-groupe (au sens de l'inclusion) contenant A.

Exemple

On considère deux entiers *m* et *n* et $p = \text{PGCD}(m, n)$.
$(p\mathbb{Z},+)$ est le sous-groupe de $(\mathbb{Z},+)$ engendré par $m\mathbb{Z} \cup n\mathbb{Z}$ (c'est-à-dire : le plus petit sous-groupe de $(\mathbb{Z},+)$ contenant tous les multiples de *m* et tous les multiples de *n*) :

$$p\mathbb{Z} = \langle m\mathbb{Z} \cup n\mathbb{Z} \rangle$$

Théorème

Soit $(G,*)$ un groupe et soit A une partie de G.
$\langle A \rangle$ est l'intersection de tous les sous-groupes de G contenant A.

Morphisme de groupe

Dans cette partie, on considère deux groupes $(G,*)$ et $(G',\top)$ d'éléments neutres e et e' respectivement.

Définitions

Soit φ une application de G dans G'.

On dit que « φ est un morphisme de groupe » (ou, s'il n'y a pas d'ambiguïté, « un morphisme ») si on a :

$$\forall (x, y) \in G^2, \varphi(x * y) = \varphi(x) \top \varphi(y)$$

Si le morphisme de groupe est bijectif on dit qu'il s'agit d'un « isomorphisme ».

Un morphisme (resp. morphisme bijectif) d'un groupe dans lui-même est un « endomorphisme » (resp. un « automorphisme »).

Propriétés

Morphismes

- Si φ est un isomorphisme de $(G,*)$ dans $(G',\top)$ alors l'application réciproque φ^{-1} est un isomorphisme de $(G',\top)$ dans $(G,*)$.
- Si φ est un morphisme de $(G,*)$ dans $(G',\top)$ et si ϕ est un morphisme de $(G',\top)$ dans $(G'',\perp)$ alors $\phi \circ \varphi$ est un morphisme de $(G,*)$ dans $(G'',\perp)$.

Morphismes et structure

Dans ce qui suit, φ est un morphisme de $(G,*)$ dans $(G',\top)$.

- $\varphi(e)=e'$.
  (l'image par φ de l'élément neutre de G est l'élément neutre de G')
- Pour tout élément x de G : $\varphi\left(x^{-1}\right)=\left(\varphi(x)\right)^{-1}$.
  (l'image par φ de l'inverse d'un élément de G est l'inverse dans G' de l'image de cet élément par φ)
- Si H est un sous-groupe de G alors $H'=\varphi(H)$ est un sous-groupe de G'.
- Si H' est un sous-groupe de G' alors $H=\varphi^{-1}(H')$ est un sous-groupe de G.

Noyau et image

Dans ce qui suit, φ est un morphisme de $(G,*)$ dans $(G',\top)$.

Définitions

L'image réciproque, $\varphi^{-1}(\{e'\})$, par φ de l'élément neutre e' de H' est appelé « noyau de φ » et noté : $\boxed{\ker\varphi}$ (ou $\boxed{\text{Ker}\,\varphi}$).

L'image, $\varphi(G)$, par φ du groupe G est appelée « image de φ » et notée : $\boxed{\text{Im}\,\varphi}$.

Propriétés

- $\ker\varphi$ est un sous-groupe de G.
- $\text{Im}\,\varphi$ est un sous-groupe de G'.
- φ est injective si, et seulement si, $\ker\varphi=\{e\}$.
- φ est surjective si, et seulement si, $\text{Im}\,\varphi=G'$.