La structure algébrique de groupe

DÉFINITION ***La structure algébrique de groupe***

Si $\left[\begin{array}{lccc} *: & G\times G & \to & G \\ & (x,x') & \mapsto & x*x' \end{array}\right]$ est une loi de composition interne sur l'ensemble G (càd une application de $G\times G$ dans G)

vérifiant : -la loi $*$ est associative : $\forall (x,x',x'')\in G^3,\quad (x*x')*x''=x*(x'*x'')$

-la loi $*$ possède un élément neutre : $\exists 0_G\in G, \forall x\in G,\quad x*0_G=0_G*x=x$

-tout élément de G possède un symétrique pour cette loi : $\forall x\in G,\exists x'\in G,\quad x*x'=x'*x=0_G$

alors on dit que $(G,*)$ est un groupe.

Si, de plus la loi $*$ est commutative : $\forall (x,x')\in G^2,\quad x*x'=x'*x$

alors on dit que $(G,*)$ est un groupe abélien (du nom d'Abel...) ou encore un groupe commutatif.

Exemples :

- $(\mathbb{Z},+)$ est un groupe commutatif où la loi $+$ est l'addition usuelle entre les entiers.
  L'addition est bien associative et commutative, elle possède un élément neutre qui est l'entier 0
  et, pour tout entier relatif n, le symétrique de n pour $+$ est l'entier $-n$

- $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont aussi des groupes abéliens.
  L'addition a été construite sur ces ensembles en conservant les propriétés d'associativité et de commutativité.
  L'élément neutre est toujours 0 (qu'on voit soit comme un rationnel, soit comme un réel soit comme un complexe selon les cas)
  Le symétrique de $r\in\mathbb{Q}$ est $-r\in\mathbb{Q}$, celui de $x\in\mathbb{R}$ est $-x\in\mathbb{R}$ et enfin celui de $z\in\mathbb{C}$ est $-z\in\mathbb{C}$.

- $(\mathbb{Q}^*,\times)$ est aussi un groupe abélien où $\times$ est la multiplication usuelle.
  $\times$ est bien une loi de composition interne sur $\mathbb{Q}^*$ car : $(r\in\mathbb{Q}^* \text{ et } r'\in\mathbb{Q}^*)\Rightarrow rr'\in\mathbb{Q}^*$
  La multiplication est bien associative et commutative. Son élément neutre est $1\in\mathbb{Q}^*$
  et le symétrique pour $\times$ du rationnel non nul r est le rationnel non nul $\frac{1}{r}$

- $(\mathbb{R}^*,\times)$ et $(\mathbb{C}^*,\times)$ sont aussi des groupes abéliens mais $(\mathbb{Z}^*,\times)$ **n'est pas un groupe**
  En effet, il existe des éléments dans $\mathbb{Z}^*$ qui n'ont pas de symétrique pour $\times$
  Par exemple, puisque l'équation $2x=1$ n'a pas de solution dans $\mathbb{Z}^*$, 2 n'a pas de symétrique pour $\times$ dans $(\mathbb{Z}^*,\times)$

Quelques propriétés à retenir sur les groupes :

- **Dans un groupe, l'élément neutre est unique !**

Démonstration Comme toute démonstration d'unicité, elle se fait par l'absurde.
S'il y a deux éléments neutre qu'on note 0_G et $0_G{}'$
alors, d'une part, $0_G+0_G{}'=0_G$ car 0_G est élément neutre
et, d'autre part, $0_G+0_G{}'=0_G{}'$ car $0_G{}'$ est élément neutre
donc on a : $0_G=0_G+0_G{}'=0_G{}'$ soit $0_G=0_G{}'$ L'élément neutre est bien unique. ∎

- **Dans un groupe, tout élément x possède un unique symétrique !**

Démonstration Supposons qu'il y a deux symétriques à l'élément x de G qu'on note $sym_1(x)$ et $sym_2(x)$
alors $x+sym_1(x)=sym_1(x)+x=0_G$ et $x+sym_2(x)=sym_2(x)+x=0_G$
Mais alors, en utilisant l'associativité, on a :

$$\big(sym_1(x)+x\big)+sym_2(x)=sym_1(x)+\big(x+sym_2(x)\big) \quad\Leftrightarrow\quad 0_G+sym_2(x)=sym_1(x)+0_G$$
$$\Leftrightarrow\quad sym_2(x)=sym_1(x)$$

Le symétrique de x est donc unique.∎

Le symétrique de x est noté $-x$ lorsque la loi est additive (loi $+$) et x^{-1} lorsqu'elle est multiplicative (loi $\times$ ou $\circ$)

DÉFINITION **_Notion de sous-groupe_**

Si $(G,*)$ est un groupe et si H est une partie de G alors on dit que H est un sous-grope de G lorsque
- H est non-vide
- H est stable pour la loi $*$: $\forall (x,y)\in H^2, \quad x*y\in H$
- H est stable pour le passage au symétrique : $\forall x\in H, \quad sym(x)\in H$

De façon évidente, si H est un sous-groupe de $(G,*)$ alors $(H,*)$ est lui même un groupe.

Remarques : En général, pour prouver $H\neq\emptyset$ on montre que $0_G\in H$...

Exemples :
- $(\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{Q},+)$ qui est lui même un sous-groupe de $(\mathbb{R},+)$, lui même un sous groupe de $(\mathbb{C},+)$
- $(\mathbb{Q}^*,\times)$ est un sous-groupe de $(\mathbb{R}^*,\times)$ qui est lui même un sous-groupe de $(\mathbb{C}^*,\times)$
- $]0,+\infty[$ est un sous-groupe de $(\mathbb{R}^*,\times)$ (et donc aussi de $(\mathbb{C}^*,\times)$)
  En effet, $]0,+\infty[\neq\emptyset$ car $1\in]0,+\infty[$. Si $x>0$ et $x'>0$ alors $xx'>0$. Si $x>0$ alors $\frac{1}{x}>0$

DÉFINITIONS **_Morphisme de groupe_**

Morphisme Si $(G,+)$ et $(H,*)$ sont des groupes et si $\varphi: G\to H$ est une application vérifiant
$\forall (x,x')\in G, \varphi(x+x')=\varphi(x)*\varphi(x')$
alors on dit que φ est un morphisme de groupe

Si $\varphi:(G,+)\to(H,*)$ est un morphisme de groupe, on définit :
Image -l'image de φ notée Imφ par $\text{Im}\varphi=\{\varphi(x)|x\in G\}\subset H$
Noyau -le noyau de φ notée Kerφ par $\text{Ker}\varphi=\{x\in G|\varphi(x)=0_H\}$

Exemples :
- Le module $[z\mapsto|z|]$ est un morphisme du groupe $(C^*,\times)$ vers $(]0,+\infty[,\times)$ car $\forall (z,z')\in(\mathbb{C}^*)^2, \quad |zz'|=|z|\times|z|'$
  Son noyau est $\mathbb{U}=\{z\in\mathbb{C}\mid |z|=1\}=\{z\in\mathbb{C}^*\mid |z|=1\}$ et son image est $]0,+\infty[$
  Ce n'est pas un morphisme sur $(\mathbb{C},+)$ car $|z+z'|\neq|z|+|z'|$ en général...

• **On a nécessairement $\varphi(0_G)=0_H$!**

Démonstration : Notons $u=\varphi(0_G)$ et $sym_H(u)$ le symétrique de u dans le groupe H pour $*$
alors $u=\varphi(0_G+0_G)=\varphi(0_G)*\varphi(0_G)=u*u$
aussi $0_H=sym_H(u)*u=sym_H(u)*(u*u)=(sym_H(u)*u)*u=0_H*u=u$
et donc on a prouvé que $u=\varphi(0_G)=0_H$ ■

• **(Im$\varphi,*$) est un sous-groupe de H !**

Démonstration :
- >$*$ est stable sur Imφ : si on prend deux éléments de Imφ qu'on peut écrire $\varphi(x)$ et $\varphi(x')$ avec $(x,x')\in G^2$ alors $\varphi(x)*\varphi(x')=\varphi(x+x')\in\text{Im}\varphi$
- >$*$ est associative sur Imφ car elle l'est sur H
- >$*$ admet l'élément neutre $1_H=\varphi(0_G)\in\text{Im}\varphi$: pour tout élément $\varphi(x)$ avec $x\in G$ de Imφ alors $\varphi(x)*1_H=\varphi(x)*\varphi(0_G)=\varphi(x+0_G)=\varphi(x)$ et $1_H*\varphi(x)=\varphi(0_G)*\varphi(x)=\varphi(x)$
- >tout élément $\varphi(x)$ avec $x\in G$ de Imφ possède un symétrique pour $*$ qui est $\varphi(-x)$ car $\varphi(x)*\varphi(-x)=\varphi(x-x)=\varphi(0_G)=1_H$ et aussi $\varphi(-x)*\varphi(x)=\varphi(0_G)=1_H$ ■

On note que, par unicité du symétrique dans le groupe H, on a $\boxed{\varphi\big(sym_G(x)\big)=sym_H\big(\varphi(x)\big)}$

• **(Ker$\varphi,+$) est un sous-groupe de G !**

Démonstration :
- >$+$ est stable sur Kerφ : si on prend deux éléments x et x' de Kerφ, alors $\varphi(x)=\varphi(x')=0_H$ aussi $\varphi(x+x')=\varphi(x)*\varphi(x')=0_H*0_H=0_H$ donc $x+x'\in\text{Ker}\varphi$
- >$+$ est associative sur Kerφ car elle l'est sur G
- >$+$ admet l'élément neutre 0_G car $\varphi(0_G)=0_H$ entraîne que $0_G\in\text{Ker}\varphi$
- >tout élément de Kerφ possède un symétrique pour $+$ car si $x\in\text{Ker}\varphi$ alors $\varphi\big(sym_G(x)\big)=sym_H\big(\varphi(x)\big)=sym_H(0_H)$ puisque $\varphi(x)=0_H$.
  Or $sym_H(0_H)=0_H$ donc $\varphi\big(sym_G(x)\big)=0_H$ et $sym_G(x)\in\text{Ker}\varphi$ ■