Sous-Groupe

Définition	Soit (E, o) un groupe. Un sous ensemble H de E est appelé sous groupe de E lorsque • L'élément neutre de E appartient à H • $\forall (x,y) \in H^2, xoy \in H$ (H est stable pour la loi o) • $\forall x \in H, x^{-1} \in H$ (Le symétrique de tout élément de H est dans H)
Exemples	• $(\mathbb{Z}, +)$ est un sous groupe de $(\mathbb{R}, +)$ • $(\mathbb{Q}^*, *)$ est un sous groupe de $(\mathbb{R}^*, *)$
Propriété	Un sous-groupe est un groupe.

Preuve

Soit H un sous groupe de (E, o). Considérons (H, o)

- o est associative dans E, elle l'est donc aussi dans H
- H est stable pour la loi o donc la loi o est une loi de composition interne pour H
- L'élément neutre de E appartient à H. Donc H admet un élément neutre
- $\forall x \in H, x^{-1} \in H$ (Le symétrique de tout élément de H est dans H).

Remarque	Lorsqu'il vous est demandé de prouver qu'un ensemble est un groupe, vous pouvez bien sûr le faire directement en prouvant les axiomes fondateurs d'un groupe. Mais vous pouvez aussi grâce à la propriété précédente montrer que cet ensemble est un sous groupe d'un groupe existant. Cela va souvent beaucoup plus vite …
Propriété	Une manière équivalente (à la définition) de caractériser un sous groupe est la suivante : H est un sous groupe de (E, o) lorsque : 1. H est non vide 2. $\forall (x,y) \in H^2\ xoy^{-1} \in H$

Preuve

Montrons que la définition d'un sous groupe et la propriété précédente sont équivalentes.

- Soit H un sous groupe. L'élément neutre de E appartient à H. Donc H est non vide.
  Soient x et y dans H. $y^{-1} \in H$ puisque H est un sous groupe. De plus $xoy^{-1} \in H$ car H est stable pour o
  Donc être un sous groupe implique la propriété précédente.
- Réciproquement. Supposons la propriété précédente vraie.
  D'après le premier point H est non vide. $\exists x \in H$. D'après le deuxième point $xox^{-1} \in H \Longrightarrow e \in H$
  L'élément neutre de E appartient à H
  D'après le deuxième point $\forall x \in H$, $eox^{-1} \in H \Longrightarrow x^{-1} \in H$ Donc :
  le symétrique de tout élément de H est dans H.
  $\forall (x,y) \in H^2$, $xoy = xo(y^{-1})^{-1}$. x et y^{-1} sont dans H donc d'après le deuxième point :
  $xo(y^{-1})^{-1} \in H \Longrightarrow xoy \in H$. **$H$ est stable pour la loi o**

La définition et la propriété sont donc équivalentes.

Remarque	La propriété est souvent plus rapide à démontrer que la définition. Ne vous en privez pas.
Propriété	Soit (G, o) un groupe. Alors $(\{e_g\}, o)$ et (G, o) sont des sous groupes de G

Preuve

Evidente

Propriété	$(\mathbb{U}_n, *)$ est un sous groupe de $(\mathbb{U}, *)$. L'ensemble des racines n –ièmes de l'unité muni de la multiplication est un sous groupe de l'ensemble des nombres complexes de module 1 muni de la multiplication.

Preuve

Bien sur $\mathbb{U}_n \subset \mathbb{U}$

- $1 \in \mathbb{U}_n$ donc $\mathbb{U}_n$ est non vide.
- $\forall (x,y) \in {\mathbb{U}_n}^2\ \exists (k,k') \in \mathbb{Z}^2$ tels que $x = e^{\frac{2i\pi k}{n}}$ et $y = e^{\frac{2i\pi k'}{n}}$. $y^{-1} = e^{-\frac{2i\pi k'}{n}}$ et $xy^{-1} = e^{\frac{2i\pi(k-k')}{n}}$ donc $xy^{-1} \in \mathbb{U}_n$

$\mathbb{U}_n$ est donc bien un sous groupe de $(\mathbb{U}, *)$.

Propriété	Les sous groupes additifs de $(\mathbb{Z},+)$ sont les groupes de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$

Preuve

- Montrons tout d'abord que les groupes de la forme $n\mathbb{Z}$ sont des sous groupes de $(\mathbb{Z},+)$

Soit $n \in \mathbb{N}$ et $G = n\mathbb{Z}$
Si $n = 0$ alors $G = \{0\}$ et bien entendu $(\{0\},+)$ est un sous groupe de $(\mathbb{Z},+)$
Si $n \neq 0$ nous savons que $G \subset \mathbb{Z}$ et que $(\mathbb{Z},+)$ est un groupe.
G est non vide puisque $0 \in G$
Soit $(x,y) \in G^2$. $\exists(p,q) \in \mathbb{Z}^2$ tels que $x = np$ et $y = nq$. Donc $x - y = n(p-q) \Rightarrow x - y \in G$
G est donc bien un sous groupe.

- Montrons maintenant qu'un sous-groupe de $(\mathbb{Z},+)$ est forcément de la forme $n\mathbb{Z}$

Soit G un sous-groupe de $(\mathbb{Z},+)$. G est non vide.
Si $G = \{0\}$ alors $n = 0 * \mathbb{Z}$ et c'est réglé.
Sinon appelons $G^+ = \{g \in G\ tq\ g > 0\}$. G^+ est non vide. (En effet si $x \in G$ et $x \neq 0$ alors $-x \in G$). Donc si G est non vide, G^+ l'est aussi.
G^+ est une sous-partie de $\mathbb{N}$. Il admet donc un plus petit élément n.
Soit $y \in G. y \in \mathbb{Z}$. La division euclidienne de y par n dans $\mathbb{Z}$ nous donne :

$$y = qn + r \text{ avec } q \in \mathbb{Z},\ r \in \mathbb{Z} \text{ et } 0 \leq r < n.$$

$n \in G \Rightarrow qn \in G$. Donc $y - qn \in G \Rightarrow r \in G$.
$r > 0$ donc $r \in G^+ \Rightarrow n$ ne peut plus être le plus petit élément. Nous avons donc une contradiction.
Donc $r = 0 \Rightarrow y = qn$. Tout élément de G est donc bien de la forme $n\mathbb{Z}$.