1. Groupes

1.1. Définition

un ensemble $G \neq \emptyset$ muni d'une loi de composition interne $\star$ est un groupe si cette loi est associative, s'il existe un élément neutre et si tout élément de G a un symétrique pour la loi $\star$ dans G. Si de plus $\star$ est commutative, le groupe est dit commutatif ou abélien.

1.2. Exemples

$(\mathbb{K}, +)$ est un groupe abélien si $\mathbb{K} = \mathbb{Z},\ \mathbb{Q},\ \mathbb{R}$ ou $\mathbb{C}$.

$(\mathbb{K}^*, \times)$ est un groupe abélien si $\mathbb{K} = \mathbb{Q},\ \mathbb{R},\ \mathbb{C},\ \mathbb{Q}_+, \mathbb{R}_+, \mathbb{U}, \mathbb{U}_n$.

$(\mathfrak{S}(E), \circ)$ est le groupe des permutations (bijections) de l'ensemble E.

$(\mathfrak{S}_n, \circ)$: groupe des permutations de $[\![1, n]\!]$ est le groupe symétrique d'ordre n.

1.3. Propriétés

- Dans un groupe, l'élément neutre est unique.
- Dans un groupe, le symétrique de tout élément est unique.
- Si a, b sont deux éléments d'un groupe $(G, .)$, alors $(a.b)^{-1} = b^{-1}.a^{-1}$.

2. Produit de groupes

2.1. Théorème et définition

Si G_1 et G_2 sont deux groupes, alors $G_1 \times G_2$ est muni d'une loi de composition interne notée :

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2) \text{ en notation additive,}$$

$$(x_1, x_2) \times (y_1, y_2) = (x_1 \cdot y_1, x_2 \cdot y_2) \text{ en notation multiplicative.}$$

Muni de cette loi $G_1 \times G_2$ a une structure de groupe.

2.2. Exemples

Si $\mathbb{K} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ alors, pour $n \geqslant 2$, $(\mathbb{K}^n, +)$ est un groupe abélien.

3. Sous-groupes

3.1.Définition

Une partie non vide H de G est un sous-groupe de $(G, \star)$ si elle est stable par $\star$ et si, munie de la loi induite, elle a une structure de groupe.

3.2. Caractérisations

Soit $(G, \star)$ un groupe. H est un sous-groupe de $(G, \star)$ si l'une des assertions équivalentes suivantes est vraie.

(1) $\big(H \subset G\big), \big(H \neq \emptyset\big)$ et $\big(\forall (x, y) \in H^2, x \star y' \in H\big)$ où y' est le symétrique de y dans G.

(2) $\big(H \subset G\big), \big(H \neq \emptyset\big), \big(\forall (x, y) \in H^2, x \star y \in H$ et $y' \in H\big)$ où y' est le symétrique de y dans G.

3.3. Exemples

- $\{-1, 1\}$ est un sous-groupe de $(\mathbb{R}^*, \times)$.

• $\mathbb{Z}[i] = \{z \in \mathbb{C} \mid \exists (a,b) \in \mathbb{Z}^2, z = a + ib\}$ est un sous-groupe de $(\mathbb{C}, +)$.

• $\mathbb{K}^{(I)} = \{x = (x_i) \in \mathbb{K}^I |\ x_i = 0$ sauf sur une partie finie de $I\}$ est un sous-groupe additif de $\mathbb{K}^I$.

• Si G est un groupe additif (*resp.* multiplicatif), le sous-groupe
$\mathrm{gr}(a) = \{ka \mid k \in \mathbb{Z}\}$ (*resp.* $\{a^k \mid k \in \mathbb{Z}\}$) est le sous-groupe de G engendré par l'élément a de G.

4. Morphismes de groupes

1. Définition

Si (G,T) et (G',T') sont deux groupes, une application f de G dans G' est un morphisme de groupes si, pour tout $(x,y) \in G^2$, $f(x\,T\,y) = f(x)T'f(y)$.

2. Propriétés

On conserve les notations de la définition précédente.

a) L'image par f du neutre de (G,T) est le neutre de (G',T').

b) L'image par f du symétrique de $x \in G$ pour la loi T est le symétrique de $f(x) \in G'$ pour la loi T'.

c) $f(G)$ est un sous groupe de (G',T').

d) L'image réciproque de l'élément neutre e' de (G',T'), appelée le ***noyau*** du morphisme f et notée $\mathrm{Ker}(f)$, est un sous-groupe de (G,T).

e) f est injective si, et seulement si, $\mathrm{Ker}(f)$ est réduit à l'élément neutre de (G,T).

f) Si f est un ***isomorphisme*** de groupes *ie.* si f est un morphisme bijectif de groupes, il en est de même de f^{-1}.

3. Exemples

• ln est un isomorphisme du groupe $(\mathbb{R}_+^\star, \times)$ sur le groupe $(\mathbb{R}, +)$.

• det est un morphisme du groupe $(\mathrm{GL}_n(\mathbb{C}), \times)$ dans le groupe $(\mathbb{C}^\star, .)$.
• L'application $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}, \sigma \mapsto \varepsilon(\sigma)$, la signature de la permutation σ, est un morphisme de groupes.

5. Anneaux

1. Définition

$(A, +, \star)$ est un anneau si $(A, +)$ est un groupe abélien, la loi $\star$ est asociative et distributive par rapport à la loi $+$ et si A admet un élément neutre 1_A pour la loi $\star$.
Si la loi $\star$ est commutative, l'anneau est dit commutatif.

Exemples

Si $\mathbb{K}$ est l'un des ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, les ensembles $\mathbb{K}$, $\mathbb{K}[X], \mathcal{F}(A, \mathbb{K})$, $\mathbb{K}^{\mathbb{N}}$ sont munis d'une structure d'anneau commutatif et $\mathfrak{M}_n(\mathbb{K})$ d'une structure d'anneau non commutatif.

Si $(E, +, .)$ est un $\mathbb{K}$ espace vectoriel, $(\mathcal{L}(E), +, \circ)$ est un anneau.

2. Définition : sous-anneaux

Soit $(A, +, \star)$ un anneau. Une partie A' de A est un sous-anneau de $(A, +, \star)$ si $1_A \in A'$, si A' est stable par les lois $+$ et $\star$ et si, muni des lois induites, c'est un anneau.

On en déduit immédiatement, comme pour les sous-groupes, la

3. Caractérisation

Soit $(A, +, \star)$ un anneau. Une partie A' de A est un sous-anneau de $(A, +, \star)$ si, et seulement si, $1_A \in A'$ et $\big(\forall (x, y) \in A'^2,\ x - y \in A' \text{ et } x \star y \in A'\big)$.

Exemples

- $\mathbb{Z}[i] = \{p + iq \,|\, (p, q) \in \mathbb{Z}^2\}$ est un sous-anneau de $(\mathbb{C}, +, .)$.
- $\mathcal{C}(\mathbb{R}, \mathbb{C})$ est un sous-anneau de $(\mathcal{F}(\mathbb{R}, \mathbb{C}), +, .)$.

4. Définition

*$(\mathbb{K}, +, \star)$ est un **corps** si $(\mathbb{K}, +, \star)$ est un anneau commutatif et si tout élément non nul de $\mathbb{K}$ est inversible dans $\mathbb{K}$ (pour la loi $\star$).*

Exemples

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{Q}[i] = \{p + iq \,|\, (p, q) \in \mathbb{Q}^2\}$ sont des corps.

5. Définition

*On appelle **sous-corps** d'un corps $(\mathbb{K}, +, .)$ tout sous-anneau $\mathbb{K}'$ qui, pour les lois induites, est un corps.*

6. Définition : anneau produit

Si A_1 et A_2 sont des anneaux, $A_1 \times A_2$ est muni de deux lois de composition internes notées :

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2),$$
$$(x_1, x_2) \times (y_1, y_2) = (x_1 \cdot y_1, x_2 \cdot y_2).$$

Muni de ces lois, $A_1 \times A_2$ a une structure d'anneau.

Quelques propriétés des anneaux

Règles de calcul : soit $(A, +, \star)$ un anneau.

a) Règles de calcul dans un groupe abélien $(A, +)$.

b) (i) $\forall x \in A,\ x \star 0_A = 0_A \star x = 0_A$.
(ii) $\forall (x, y) \in A^2, x \star (-y) = (-x) \star y = -(x \star y)$.

c) **Binôme de Newton**

Si $a \star b = b \star a$ alors : $\forall n \in \mathbb{N}, (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \star b^{n-k}$.

d) Applications du binôme de Newton.

$\forall p \in [\![0, n]\!], \binom{n}{p} = \dfrac{n(n-1)\cdots(n-p+1)}{p!} = \dfrac{n!}{p!(n-p)!}$.

$\forall p \in [\![1, n]\!], \binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p}$,

$\forall p \in [\![1, n]\!], p\binom{n}{p} = n\binom{n-1}{p-1}$.

$\forall n \in \mathbb{N}, \sum_{k=0}^{n} \binom{n}{k} = 2^n$.

$\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} = \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2k+1} = 2^{n-1}$.

e) Si $a \star b = b \star a$, alors : $\forall n \in \mathbb{N}, n \geqslant 2, a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^{n-1-k} \star b^k$.

$\forall n \in \mathbb{N}, n \geqslant 2, \forall a \in A$,
$a^n - 1_A = (a - 1_A) \star (1_A + a + \cdots + a^{n-1}) = (1_A + a + \cdots + a^{n-1}) \star (a - 1_A)$.