

Structures algébriques usuelles

Résumé

I - Groupes :

1) Loi de composition interne (LCI)

⚡!

Pour montrer que T est une loi de composition interne sur G , on montre que :

$$\forall x, y \in G, xTy \in G$$

Exemples usuels de LCI (à savoir)

1) L'addition "+" dans $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{N}$

2) Le produit "x" dans $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{N}$

3) Le produit "x" est une LCI aussi sur :
 $\mathbb{R}^{+*} =]0, \infty[$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{I}$, $\mathbb{I}_n$ (où $n \geq 1$)

Vocabulaire :

Soit E un ensemble non vide.

Une bijection de E sur E s'appelle **permutation** de E .

Notation :

S_E : l'ensemble des permutations dans E .

Exemples usuels de LCI

(à savoir)

1) E étant un ensemble non vide.

la composition " $\circ$ " est une LCI sur $E^E = \mathcal{F}(E, E)$.

2) " $\circ$ " est aussi une LCI sur S_E .

Exemples usuels de LCI

(à savoir)

1) X un ensemble non vide quelconque.

$\mathcal{R}^X = \mathcal{F}(X, \mathbb{R})$, l'ens des appls de X vers $\mathbb{R}$.

" $+$ " et " $\times$ " sont aussi deux LCI sur $\mathcal{F}(X, \mathbb{R})$.

2) " $+$ " et " $\times$ " sont deux LCI sur $\mathcal{F}(\mathbb{N}, \mathbb{R}) = \mathbb{R}^{\mathbb{N}}$

et $\mathbb{C}^{\mathbb{N}}$: l'ensemble des suites réelles et complexes.

Def 2. Soit $*$ une LCI sur E .

1) Commutativité :

$*$ est dite commutative si et ssi $(\forall x, y \in E, x * y = y * x)$

2) Associativité :

$*$ est dite associative si et ssi $(\forall x, y, z \in E, (x * y) * z = x * (y * z))$

3) Element neutre :

Soit $e \in E$

e est dite element neutre si et ssi :

$$\forall x \in E, \begin{cases} x * e = x \\ e * x = x \end{cases}$$

4) Élément inversible :

Soit $a \in E$, Soit e l'élément neutre.

a est dit **inversible** si et ssi : $\exists b \in E$ $\left\{ \begin{array}{l} a * b = e \\ \text{et} \\ b * a = e \end{array} \right.$

Vocab et notation :

Dans ce cas, b s'appelle **l'inverse** de a et se note a^{-1} .

5) Distributivité

$*$ et T deux LCI sur E .

On dit que $*$ est **distributive** par rapport à T .

si et ssi :

$$\forall x, y, z \in E, x * (y T z) = (x * y) T (x * z)$$

NB :

1) Supp a est inversible, on a : $\left\{ \begin{array}{l} a * a^{-1} = e \\ a^{-1} * a = e \end{array} \right.$

2) e inversible et $e^{-1} = e$

$\rightarrow$ car $e * e = e$.

Prop 3 : Supp que a et b sont **inversibles**.

$*$ étant associative

Alors $(a * b)$ est aussi **inversible** et on a

$$(a * b)^{-1} = b^{-1} * a^{-1}$$

Def 4: (Partie stable par *)

Soit $*$ une LCI sur E .

Soit H une partie de E .

H est dite **stable par $*$** si et ssi

$$(\forall x, y \in H, x * y \in H)$$

2° Groupes :

Def 1: Soit $*$ une LCI sur l'ensemble non vide G .

$(G, *)$ est dit **groupe** si et ssi :

1 $*$ est **associative**

2 $*$ admet un **élément neutre**.

3 Tout élément de G est **inversible**.

Vocabulaire :

Si $(G, *)$ est un **groupe** et que $*$ est **commutative**,
on dit que $(G, *)$ est un groupe **commutatif** ou
abelien.

Prop 2 :

X un ensemble non vide (q.l.q).

$IK = \mathbb{R}$ ou $\mathbb{C}$.

$(IK^X, +)$ est un **groupe abélien** d'élément neutre la
fonction nulle.

Prop 3 :

E est un ensemble non vide.

$(S_E, \circ)$ est un groupe d'élément neutre I_E .

NB₁ : $(S_E, \circ)$ n'est en général pas commutatif.

NB₂ : S_E s'appelle le groupe symétrique sur E .
d'où la notation S_E .

Notation :

1) Si $(G, \times)$ groupe d'élément neutre 1.

Soit $a \in G$, soit $n \in \mathbb{N}^*$.

$\underbrace{a \times \dots \times a}_{n \text{ fois}}$ se note a^n , et $a^0 = 1$ par convention.

2) Si $(G, +)$ groupe d'élément neutre 0.

Soient $a \in G$ et $n \in \mathbb{N}^*$.

$\underbrace{a + \dots + a}_{n \text{ fois}}$ se note na ; et $0.a = 0$ par convention.

3°) Sous-groupes

Def 1 :

Soient $(G, *)$ un groupe d'élément neutre e , et $H \subset G$.
 H est dit sous groupe de G si et si

1) $e \in H$

2) $\forall x, y \in H, x * y \in H$

3) $\forall x \in H, x^{-1} \in H$

NB₁ : Ici $(G, +)$ est un groupe d'élément neutre 0 ,
 et $H \subset G$; H est dit un **sous-groupe** de G si et si
1 $0 \in H$
2 $\forall x, y \in H, x + y \in H$
3 $\forall x \in H, (-x) \in H$

Prop 2 :

$(G, *)$ est un groupe et $H \subset G$, on a :

H **sous-groupe** de $G \Leftrightarrow \begin{cases} \text{i) } e \in H \\ \text{ii) } \forall x, y \in H, x * y^{-1} \in H \end{cases}$

NB₁ : Ici $(G, +)$ groupe d'élément neutre 0 et
 $H \subset G$, on a :

H est **s-groupe** de $G \Leftrightarrow \begin{cases} \text{i) } 0 \in H \\ \text{ii) } \forall x, y \in H, x - y \in H \end{cases}$

NB : $\{e\}$ et G sont deux sous groupes de $(G, *)$.

Prop 3 :

Si H est un **s-groupe** du groupe $(G, *)$
 alors $(H, *)$ est aussi **un groupe**.

Remarque pratique :

Pour montrer qu'un ensemble est un groupe, des fois
 il est plus facile de procéder en montrant que
 c'est un sous groupe.

Prop 4 (Intersection de s-gr)

Soit $(G, *)$ un groupe.

Toute intersection de sous-groupes de G est un sous-groupe de G .

Cà d : Si $(H_i)_{i \in I}$ est une famille de s-gr de G
alors $\bigcap_{i \in I} H_i$ est un s-gr de G .

Attention

La réunion de deux s-gr n'est en général pas un s-gr.

II - Anneaux :

1) Déf et exemples :

Déf 1

Soit A un ensemble non vide muni de deux LCI "+" et "x".

On dit que $(A, +, x)$ est un anneau si et ssi :

- 1) $(A, +)$ est un groupe commutatif (avec la 1^{ère} loi).
- 2) x est associative et admet un élément neutre (2^{ème} loi).
- 3) x est distributive par rapport à $+$

Vocabulaire Si la loi x est commutative on dit que l'anneau $(A, +, x)$ est commutatif.

Exemples usuels d'anneaux (à retenir)

Exemple 1 :

- 1) $(\mathbb{Z}, +, \times)$ anneau commutatif
- 2) Idem pour $\mathbb{R}, \mathbb{Q}, \mathbb{C}$.

Exemple 2 :

$K = \mathbb{R}$ ou $\mathbb{C}$. X ensemble non vide qlque.

$(K^X, +, \times)$ est un anneau commutatif d'éléments neutres respectifs la fonction nulle 0 et la fonction constante 1 .

Exemple 3 :

Cas particulier de l'exemple 2 avec $N = X$.
L'ensemble des suites $\mathbb{R}^{\mathbb{N}}$ (resp complexes $\mathbb{C}^{\mathbb{N}}$)
est un anneau commutatif d'éléments neutres resp
la suite nulle et la suite constante 1 .

2) Anneau intègre

Def : Soit $(A, +, \times)$ un anneau.

A est dit anneau intègre si et ssi :

$$\forall a, b \in A, ab = 0 \Rightarrow (a = 0 \text{ ou } b = 0)$$

NB : Dans un anneau intègre on a :

$$ab = 0 \Leftrightarrow (a = 0 \text{ ou } b = 0)$$

NB₂ : Si A intègre on a :

$$ab \neq 0 \Leftrightarrow (a \neq 0 \text{ et } b \neq 0)$$

Exemples d'anneaux intègres :

$(\mathbb{Z}, +, \times)$; $(\mathbb{Q}, +, \times)$; $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$
sont des anneaux intègres.

39 Calculs dans un anneau

prop 1 :

Soit $(A, +, \times)$ anneau. On a :

$$\forall a \in A, 0 \times a = 0 \text{ et } a \times 0 = 0$$

Prop 2 :

$(A, +, \times)$ anneau.

Soient a et $b \in A$ tq $ab = ba$. on a :

1) $\forall n \in \mathbb{N}, (ab)^n = a^n b^n$

2) $\forall n \in \mathbb{N}, (a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$

Formule de binôme de Newton

3) $\forall n \in \mathbb{N}, a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^{n-1-k} b^k$

Égalité de Bernoulli

4) Éléments inversibles d'un anneau.

Déf 1 :

Soit $(A, +, \times)$ un anneau.

Les éléments inversibles de A sont les inversibles pour la 2^{ème} loi $\times$.

NB : Pour la 1^{ère} loi $+$, tous les éléments sont inversibles puisque $(A, +)$ est un groupe.

Notation :

$\mathcal{U}(A)$ désignera l'ensemble des éléments inversibles de A .

Prop 2 :

Soit $(A, +, \times)$ un anneau.

$(\mathcal{U}(A), \times)$ est un groupe.

R/R : $(\mathcal{U}(A), \times)$ est le groupe des éléments inversibles de A .

NB

$\mathcal{U}(A)$ se note aussi $A^\times$

5) Corps

Déf 1

Soit $(K, +, \times)$ un anneau commutatif, non réduit à $\{0\}$.
 $(K, +, \times)$ est un Corps si et seulement si tout élément non nul de K est inversible.

Exemples usuels de Corps

$(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des Corps.

$(\mathbb{Z}, +, \times)$ est un anneau intègre mais n'est pas un Corps.

NB 1

- 1) Si $(K, +, \times)$ est un Corps, alors $U(K) = K^*$.
- 2) Un Corps est par définition commutatif.

NB 2

- 1) Tout Corps est un anneau intègre.
- 2) La réciproque est en général fausse.

Morphisme de groupes

Déf :

On appelle morphisme du groupe (G_1, T_1) vers le groupe (G_2, T_2) toute application f définie de G_1 vers G_2 vérifiant

$$\forall x, y \in G_1, f(x T_1 y) = f(x) T_2 f(y)$$

Vocabulaire :

- i) Si f est un morphisme de G vers lui-même, on dit que f est un endomorphisme de G .
- ii) Un morphisme bijectif est dit isomorphisme.
- iii) Un endomorphisme bijectif de G est dit automorphisme de G .
- iv) Deux groupes sont dits isomorphes s'il existe un isomorphisme entre eux.

Prop :

- 1) La composée de deux morphismes (resp. endomorphismes) (resp. isomorphismes) est un morphisme (resp. endomorphisme) (resp. isomorphisme)
- 2) La réciproque d'un isomorphisme est un isomorphisme.

NB $(\text{Aut}(G), \circ)$ est un groupe ; où $\text{Aut}(G)$ est l'ensemble des automorphismes de G .

Prop

Soit f un morphisme du groupe G vers G' . Soient e et e' les éléments neutres respectifs. On a :

- 1) $f(e) = e'$
- 2) $\forall x \in G, f(x^{-1}) = f(x)^{-1}$
- 3) $\forall x \in G, \forall m \in \mathbb{Z}, f(x^m) = f(x)^m$

Prop :

L'image directe (resp. réciproque) d'un sous-groupe par un morphisme de groupes est un sous-groupe.

Autrement dit :

Soit $f: (G, \cdot) \rightarrow (G', \cdot)$ un morphisme de groupes

1) Si F est un s-gr de G alors $f(F)$ est un s-gr de G' .

2) Si H est un s-gr de G' alors $f^{-1}(H)$ est un s-gr de G .



Rappel

$$x \in f(F) \Leftrightarrow (\exists t \in F, x = f(t))$$

oublié ?! $x \in f^{-1}(H) \Leftrightarrow f(x) \in H$

Définition et proposition : (Noyau et image d'un morphisme)

Soit f un morphisme du groupe G vers G' . Soit e' l'élément neutre de G' .

1) Le *noyau* de f est

$$\ker(f) = f^{-1}(\{e'\}) = \{x \in G / f(x) = e'\}$$

2) L'*image* de f est

$$\text{Im}(f) = f(G) = \{f(x) / x \in G\}$$

3) $\text{Ker}(f)$ et $\text{Im}(f)$ sont des sous-groupes resp de G et G' .

Prop : Soit f un morphisme du groupe G vers G' . Soit e le neutre de G .

1) f est injectif $\Leftrightarrow \ker(f) = \{e\}$

2) f est surjectif $\Leftrightarrow \text{Im}(f) = G'$

À retenir :

Dans la rédaction, pour montrer qu'un morphisme de groupes f est injectif, on peut rédiger comme suit :

$$\begin{aligned} \text{Supp } f(x) &= e' \\ \text{On a } x &= e \end{aligned}$$

Sous-anneaux

Déf :

Soit $(A, +, \times)$ un anneau. Soit B une partie de A .

B est dite *sous-anneau* de A si et ssi

$$\left\{ \begin{array}{l} a) 1 \in B \\ b) \forall x, y \in B, x - y \in B \\ c) \forall x, y \in B, x \times y \in B \end{array} \right.$$

NB :

- Il faut vérifier que 1 qui est dans B , non pas 0 ;
- *un sous-anneau contient par définition 1.*

Prop : Un sous-anneau est à son tour un anneau.

Morphisme d'anneaux

Déf :

Soit f une application définie d'un anneau A vers un anneau B .
 f est dite *morphisme d'anneaux* si et ssi

- 1) $f(1)=1$
- 2) $\forall x, y \in A, f(x + y) = f(x) + f(y)$
- 3) $\forall x, y \in A, f(x \times y) = f(x) \times f(y)$

Vocabulaire :

- 1) Un morphisme d'anneaux *bijectif* est dit *isomorphisme* d'anneaux.
- 2) Deux anneaux sont dits *isomorphes* s'il existe un ^{iso}morphisme d'anneaux entre eux.

Prop :

- 1) La *composée* de deux morphismes d'anneaux est un morphisme d'anneaux.
- 2) La *composée* de deux isomorphismes d'anneaux est un isomorphisme d'anneaux.
- 3) La *reciproque* d'un isomorphisme d'anneaux est un isomorphisme d'anneaux.

Prop :

Soit f un morphisme d'anneaux de A vers B . On a :

- 1) $f(0)=0$
- 2) $\forall x \in A, \forall n \in \mathbb{N}, f(x^n) = (f(x))^n$
- 3) $\forall x \in A, \forall m \in \mathbb{Z}, f(mx) = mf(x)$
- 4) Si $x \in A$ est inversible alors son image $f(x)$ l'est aussi, et on a $(f(x))^{-1} = f(x^{-1})$

Noyau et image d'un morphisme d'anneaux

Déf :(noyau et image)³

Soit f un morphisme d'anneaux de A vers B .

- 1) *Le noyau* de f :

$$\ker(f) = \{x \in A / f(x) = 0\} = f^{-1}\{0\}$$

- 2) *L'image* de f :

$$\operatorname{Im}(f) = \{f(x)/x \in A\} = f(A)$$

Prop : Soit f un morphisme d'anneaux de A vers B . On a :

- 1) $\operatorname{Im}(f)$ est un sous-anneau de B
- 2) f est injective $\Leftrightarrow \ker(f) = \{0\}$
- 3) f est surjective $\Leftrightarrow \operatorname{Im}(f) = B$

NB : $\ker(f)$ n'est en général pas un sous-anneau de A

⌞ Il est en fait un idéal ; voir deuxième année ⌞

FIN