

STRUCTURES ALGÈBRIQUES USUELLES

I) Loi de composition interne

Définition: Soit E un ensemble. On appelle **loi de composition interne**, une application f de $E \times E$ vers E .

Notation: Si f est une loi de composition interne sur E et (a,b) est un couple d'éléments de E , on notera plutôt $f(a,b)$ sous la forme : $a \top b$, $a \perp b$, $a+b$, $a \Delta b$, $a * b$, $a \times b$, $a \cdot b$ ou ab . La loi $+$ est appelée **l'addition** (à réserver aux lois commutatives), la loi \times est la **multiplication** (il en est de même de $*$). Dans le cas général, on travaillera avec la loi \top .

On va ici donner le vocabulaire associé aux lois de composition interne.

Associativité

Définition: La loi \top est dite **associative** $\Leftrightarrow \forall (a,b,c) \in E^3$, $(a \top b) \top c = a \top (b \top c)$.

Notation: On note alors $(a \top b) \top c = a \top b \top c$.

Exemple: L'addition dans \mathbb{R} , la composition dans l'ensemble des applications de E dans E sont associatives. Par contre la soustraction dans \mathbb{Z} n'est pas associative.

Remarque: Si la loi \top est associative, $a_1 \top a_2 \top \dots \top a_n$ est définie de manière explicite et on peut faire des calculs intermédiaires en regroupant, dans l'ordre, certains termes consécutifs.

On note $\bigtop_{i=1}^n (a_i)$ cet élément de E . Par exemple, on note $\sum_{i=1}^n a_i$ pour une somme et $\prod_{i=1}^n a_i$ pour un produit.

Commutativité

Définition: La loi \top est dite **commutative** $\Leftrightarrow \forall (a,b) \in E^2$, $a \top b = b \top a$.

Exemple: L'addition de \mathbb{R} est commutative. Par contre la composition dans l'ensemble des applications de E dans E et la soustraction dans \mathbb{Z} ne sont pas commutatives.

Élément neutre

Définition: $e \in E$ est un **élément neutre** dans E pour la loi $\top \Leftrightarrow \forall a \in E$, $a \top e = e \top a = a$

Exemple: 0 est élément neutre dans \mathbb{N} pour $+$ et 1 l'est pour la multiplication.

Propriété: Soit E un ensemble et \top une l.c.i. associative sur E . Si e est un élément neutre de (E, \top) , e est unique

Dem : On suppose que l'on a deux éléments neutres e et e' pour \top dans E .

Comme e est neutre, on a : $e' \top e = e \top e' = e'$. Comme e' est neutre, on a : $e \top e' = e' \top e = e$.

En regroupant les deux égalités, on obtient $e = e'$.

Notation: L'élément neutre pour $+$ (\times) est noté 0_E (1_E).

Éléments symétrisables (ou inversibles)

Définition: Soit E un ensemble, \top une l.c.i. associative sur E et admettant un élément neutre e . Soit $x \in E$.

On dit que x est un **élément inversible** dans E pour la loi $\top \Leftrightarrow \exists y \in E \mid x \top y = y \top x = e$

Proposition: Soit E un ensemble, \top une l.c.i. associative sur E et admettant un élément neutre e . Soit x un élément inversible. Alors on a l'unicité de l'élément y de E tel que $x \top y = y \top x = e$.

Définition: Cet unique élément y est appelé **symétrique de x**

Dem: On suppose que l'on a deux symétriques y et z de x . On a, par associativité : $(y \top x) \top z = y \top (x \top z)$ Or y et z sont des inverses de x . Donc l'égalité écrite devient : $e \top z = y \top e$. Comme e est élément neutre, on a : $z = y$

Notation, Définition: Le symétrique pour $+$ est appelé opposé et est noté $-x$

Le symétrique pour \times est appelé inverse et est noté x^{-1} ou $\frac{1}{x}$ si la loi est commutative.

Proposition: Soit E un ensemble, \top une l.c.i. associative sur E et admettant un élément neutre e . Soient a et b deux éléments inversibles d'inverses a^{-1} et b^{-1} . Alors $a \top b$ est inversible d'inverse $b^{-1} \top a^{-1}$.

Dem: On a : $(a \top b) \top (b^{-1} \top a^{-1}) = a \top (b \top b^{-1}) \top a^{-1} = a \top e \top a^{-1} = a \top a^{-1} = e$. De même à droite

Exemple: La bijection réciproque de $f : \mathbb{R}^+ \rightarrow [1, +\infty[$, $x \rightarrow \exp(\sqrt{x})$ est $f^{-1} : [1, +\infty[\rightarrow \mathbb{R}^+$, $t \rightarrow (\ln t)^2$

Distributivité

Définition: Soit E un ensemble, \top et Δ deux l.c.i. sur E . On dit que **Δ est distributive à droite et à gauche par rapport à la loi \top** $\Leftrightarrow \forall (x,y,z) \in E^3$, $x \Delta (y \top z) = (x \Delta y) \top (x \Delta z)$ et $(x \top y) \Delta z = (x \Delta z) \top (y \Delta z)$

Partie stable

Définition: Soit E un ensemble, T une l.c.i. sur E. Soit H une partie de E.

On dit que **H est stable par la loi T** $\Leftrightarrow \forall (x,y) \in H^2, x T y \in H$

On dit que **H est stable par passage à l'inverse** $\Leftrightarrow \forall x \in H, x^{-1} \in H$

II) Groupe

Groupe

Définition: Soit un ensemble G muni d'une loi de composition interne T. On dit que **(G,T) est un groupe** si T vérifie les trois axiomes suivants :

- T est associative : $\forall (x,y,z) \in G^3, x T (y T z) = (x T y) T z$
- G possède un élément neutre e pour la loi T : $\exists e \in G \mid \forall x \in G, x T e = e T x = x$
- Tout élément de G est symétrisable pour T : $\forall x \in G, \exists x' \in G \mid x T x' = x' T x = e$

Exemple: (R,+), (C,+), (U,×), (Z,+), (R*,×), (U₃,×), (U_n,×) sont des groupes.

Exercice: Si (G, T) et (G',Δ) sont deux groupes, G × G' est un groupe pour la loi * définie par : (x,y)* (x',y') = (x T x', y Δ y'). Ce groupe est appelé groupe produit de (G, T) et (G',Δ)

Définition: Un groupe est dit **commutatif (ou abélien)** si de plus la loi T est commutative sur G.

Propriété: Soit (G,T) un groupe. Alors tout élément de G est régulier à gauche et à droite pour T i.e. $\forall a \in G, \forall (x,y) \in G^2, x T a = y T a \Leftrightarrow x = y$ (régulier à droite)

**** $\forall a \in G, \forall (x,y) \in G^2, a T x = a T y \Leftrightarrow x = y$**

Dem: Soit a ∈ G. Soit (x,y) ∈ G² | x T a = y T a. Appelons b le symétrique de a pour T. On a :

$$(x T a) T b = (y T a) T b \Leftrightarrow x T (a T b) = y T (a T b) \Leftrightarrow x = y : a \text{ est régulier à gauche. De même à droite.}$$

Propriété: Soit X un ensemble. L'ensemble des permutations S_X de l'ensemble X est, avec la composition, un groupe

Dem: S_X est non vide (contient Id_X).

La loi o est une loi interne dans S_X car la composée de deux permutations de X est une permutation de X.

La loi o est associative car : f o (g o h) = (f o g) o h

Id_X est élément neutre pour o dans S_X.

Enfin, si f et g sont dans S_X, f o g est une permutation de X de réciproque g⁻¹ o f⁻¹

Donc (S_X, o) est bien un groupe

Définition: Soit n ∈ ℕ*, on appelle **groupe symétrique d'ordre n** et on note S_n, le groupe des permutations de $\llbracket 1, n \rrbracket$.

Sous-groupe

Définition: Soit (G,T) un groupe. On appelle **sous-groupe de (G,T)** toute partie H non vide de G telle que la restriction de T à H confère à H une structure de groupe, i.e., si (H,T) est un groupe avec H partie de G.

Propriété: Soit (G,T) un groupe et H un sous-groupe de G. Alors :

- (i) L'élément neutre de T dans G est l'élément neutre de T dans H.
- (ii) Si x ∈ H, son symétrique pour T dans G est son symétrique pour T dans H.

Dem: (i) Soit e et e' les éléments neutres respectifs de T dans G et dans H. Comme e est l'élément neutre de T dans G et que e' est dans H donc dans G, on a : e T e' = e'. Or e' est l'élément neutre de T dans H donc vérifie e' T e' = e'. Mais alors e' T e' = e T e' donc e = e' car e' est régulier.

(ii) Soit x ∈ H. Soit y son symétrique dans G et y' son symétrique dans H. On a x T y = e car y symétrique de x dans G. On a également x T y' = e' = e d'après le (i). Mais alors par régularité de x à droite, on a y = y'.

Propriété: caractérisation des sous-groupes. Soit (G,T) un groupe. Soit H ∈ P(G).

H est un sous-groupe de (G,T) \Leftrightarrow H est non vide, H est stable par T et par passage au symétrique $\Leftrightarrow H \neq \emptyset, \forall (x,y) \in H^2, x T y \in H$ et $\forall x \in H, x' \in H$ avec x' le symétrique de x

Dem: \Rightarrow Si H est un sous-groupe de G alors H est bien non vide (car il contient l'élément neutre e de G), il est stable par T (car T est une loi interne dans H) et il est stable par passage au symétrique d'après la propriété précédente.

\Leftarrow Si H est une partie non vide de G stable par T et par passage au symétrique.

La loi T est alors une loi interne dans H. Cette loi est encore associative.

Soit $x \in H$. Soit x' son symétrique. Par stabilité, on a $x' \in H$ et donc $xTx' \in H$. Ainsi $e \in H$: H possède un élément neutre pour la loi T , cet élément neutre étant celui de G .

Enfin tout élément de H admet, dans H , un élément symétrique : celui qu'il possède dans G .

Aussi (H, T) est un groupe.

Exercice: Soit (G, T) un groupe. Soit $H \in P(G)$. Montrer que :

H est un sous-groupe de $(G, T) \Leftrightarrow H \neq \emptyset, \forall (x, y) \in H^2, xTy' \in H$ avec y' le symétrique de y .

III) Anneau - Corps

1) Anneau

Définition: Soit un ensemble non vide A muni de deux lois de composition interne T et Δ . On dit que **(A, T, Δ) est un anneau** ssi il vérifie les axiomes suivants :

- (A, T) est un groupe commutatif. L'élément neutre est noté 0_A et appelé zéro de A
- Δ est associative
- Δ possède un élément neutre dans A noté 1_A et appelé unité de A ou élément unité de A
- Δ est distributive à gauche et à droite par rapport à la loi T i.e. $\forall (x, y, z) \in A^3,$
 $x \Delta (y T z) = (x \Delta y) T (x \Delta z)$ et $(x T y) \Delta z = (x \Delta z) T (y \Delta z)$

Définition: **(A, T, Δ) est un anneau commutatif** ssi (A, T, Δ) est un anneau avec Δ commutative.

Exemple: $(\mathbb{R}, +, \times), (\mathbb{C}, +, \times), (\mathbb{Z}, +, \times), (\mathbb{Q}, +, \times), (\mathcal{A}(\mathbb{R}, \mathbb{R}), +, \times)$ sont des anneaux.

Propriété : Si $(A, +, \times)$ est un anneau et si A^\times est l'ensemble des éléments inversibles pour \times , alors (A^\times, \times) est un groupe.

Dem: On vérifie aisément les axiomes de groupe

2) Calcul dans un anneau

Distributivité du produit par rapport au signe Σ

Propriété : Soit $(A, +, \times)$ un anneau. Soit $(x_i)_{1 \leq i \leq n}$ une famille de n éléments de l'anneau A .

Soit $a \in A$. Alors : $a \times \left(\sum_{i=1}^n x_i \right) = \left(\sum_{i=1}^n a \times x_i \right)$ et $\left(\sum_{i=1}^n x_i \right) \times a = \left(\sum_{i=1}^n x_i \times a \right)$

Dem: Par récurrence sur n . Soit P_n : " Pour toute famille (x_i) de n éléments de A et pour tout $a \in A$; on a :

$$a \times \left(\sum_{i=1}^n x_i \right) = \left(\sum_{i=1}^n a \times x_i \right) \text{ et } \left(\sum_{i=1}^n x_i \right) \times a = \left(\sum_{i=1}^n x_i \times a \right) "$$

✓ P_1 est évidemment vraie.

✓ Si P_n est vraie. Soit $(x_i)_{1 \leq i \leq n+1}$ une famille de $n+1$ éléments de A et a un autre élément de A . On pose : $y = \sum_{i=1}^n x_i$ On a : $a \times \sum_{i=1}^{n+1} x_i = a \times$

$$(y + x_{n+1}) = a \times y + a \times x_{n+1} = \left(\sum_{i=1}^n a \times x_i \right) + a \times x_{n+1} = \sum_{i=1}^{n+1} a \times x_i.$$

De même pour la multiplication à gauche. Ainsi P_{n+1} est vraie.

Par théorème de récurrence on a bien montré que la propriété est vraie pour tout n

Multiplication par 0 et règle de signes

Propriété : Soit $(A, +, \times)$ un anneau. Soit 0_A l'élément neutre de l'addition. Alors 0_A est absorbant pour la multiplication i.e. $\forall x \in A, x \times 0_A = 0_A = 0_A \times x$

Dem: $x \times 0_A = x \times (0_A + 0_A) = x \times 0_A + x \times 0_A$. D'où par régularité de $x \times 0_A$ pour l'addition, $x \times 0_A = 0_A$

Propriété : Soit $(A, +, \times)$ un anneau. (i) $\forall (x, y) \in A^2, (-x) \times y = x \times (-y) = -(x \times y)$.

(ii) $\forall (x, y) \in A^2, (-x) \times (-y) = x \times y$ (iii) $\forall (x, y, z) \in A^2, x \times (y - z) = x \times y - x \times z$

Dem: (i) $(x + (-x)) \times y = (x \times y) + (-x) \times y = 0_A$. D'où $(-x) \times y = -(x \times y)$

De même, $x \times (y + (-y)) = x \times y + x \times (-y) = 0_A$. D'où $x \times (-y) = -(x \times y)$

(ii) On applique (i) en remplaçant x par $-x$

(iii) $x \times (y - z) = x \times (y + (-z)) = x \times y + x \times (-z) = x \times y - x \times z$

Formule du binôme

Propriété : Soit $(A, +, \times)$ un anneau commutatif. Soit $(a, b) \in A^2$ et $n \in \mathbb{N}^*$. Alors :

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} \quad \text{avec la convention : } a^0 = 1_A = b^0$$

Ce résultat reste vrai si $(A, +, \times)$ est un anneau non commutatif mais avec $a \times b = b \times a$

Dem: On procède par récurrence sur n. On constate d'abord que si $a \times b = b \times a$, alors $(a^n \times b^q) \times a = a^{n+1} \times b^q$

Soit P_n : " $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$ "

♦ P_1 est clairement vraie

♦ Si P_n est vraie. On a : $(a + b)^{n+1} = (a + b)^n \times (a + b) = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} (a + b)$

$$= \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} a + \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} b = \sum_{k=0}^n \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^n \binom{n}{k} a^k b^{n+1-k}$$

$$= a^{n+1} + \sum_{k=0}^{n-1} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=1}^n \binom{n}{k} a^k b^{n+1-k} + b^{n+1}$$

$$= a^{n+1} + \sum_{k=1}^n \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=1}^n \binom{n}{k} a^k b^{n+1-k} + b^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}$$

Donc P_{n+1} est vraie

Aussi $\forall n \in \mathbb{N}^*$, P_n vraie

Identité remarquable

Propriété : Soit $(A, +, \times)$ un anneau commutatif. Soit $(a, b) \in A^2$ et $n \in \mathbb{N}$. Alors :

$$a^{n+1} - b^{n+1} = (a - b) \times \sum_{k=0}^n a^k b^{n-k} = \sum_{k=0}^n a^k b^{n-k} \times (a - b)$$

Ce résultat reste vrai si $(A, +, \times)$ est un anneau non commutatif mais avec $a \times b = b \times a$

Dem: On développe le produit $(a - b) \times \sum_{k=0}^n a^k b^{n-k}$

On a : $(a - b) \times \sum_{k=0}^n a^k b^{n-k} = \sum_{k=0}^n a a^k b^{n-k} - \sum_{k=0}^n b a^k b^{n-k} = \sum_{k=0}^n a^{k+1} b^{n-k} - \sum_{k=0}^n a^k b^{n+1-k} = a^{n+1} - b^{n+1}$

De même on a : $a^{n+1} - b^{n+1} = \sum_{k=0}^n a^k b^{n-k} \times (a - b)$

Exercice: Si $(u_n)_{n \in \mathbb{N}}$ est une suite géométrique de K où $(K, +, \times)$ est un corps, de raison $q \neq 1_K$. Déterminer la somme des n premiers termes de la suite $(u_n)_{n \in \mathbb{N}}$.

3) Corps

Corps

Définition: On dit que $(K, +, \times)$ est un corps ssi c'est un anneau commutatif non réduit à un point tel que $(K \setminus \{0_K\}, \times)$ soit un groupe i.e. ssi tout élément non nul de K est inversible.

Exemple: $(\mathbb{R}, +, \times)$ est un corps alors que $(\mathbb{Z}, +, \times)$ ne l'est pas.

Définition: Soit $(K, +, \times)$ un corps non réduit à un point. On appelle sous-corps de $(K, +, \times)$ toute partie L non vide de K telle que les restrictions de $+$ et de \times à L confèrent à L une structure de corps, i.e., si $(L, +, \times)$ est un corps avec L partie de K .