

Chapitre 15

Structures algébriques

Sommaire

I	Lois de composition interne	140
1)	Définitions	140
2)	Élément neutre	141
II	Structure de groupe	141
1)	Définitions	141
2)	Sous-groupes d'un groupe	142
III	Anneaux et corps	143
1)	Anneaux	143
2)	Corps	145

I LOIS DE COMPOSITION INTERNE

1) Définitions



Définition 15.1 (loi de composition interne)

Soit E un ensemble non vide. On appelle loi de composition interne (ou lci) dans E toute application de $E \times E$ vers E . L'image d'un couple $(x, y) \in E^2$ par une telle application est en général noté sous la forme d'une opération avec un symbole : $x + y$ ou $x \times y$ ou $x * y$ ou $x.y$ ou xTy , ... Et on écrira $(E, *)$ pour dire que l'ensemble E est muni d'une lci notée $*$.

Exemples :

- L'addition et la multiplication des nombres sont des lci dans \mathbb{N} , dans \mathbb{Z} , dans \mathbb{Q} , dans \mathbb{R} , dans \mathbb{C} mais pas dans $[-2; 2]$ par exemple.
- L'addition et la multiplication des fonctions dans $(\mathcal{F}(A, \mathbb{C}))$ sont des lci (A étant un ensemble non vide). En particulier l'addition et la multiplication des suites sont des lci dans $\mathcal{F}(\mathbb{N}, \mathbb{C})$.
- Soit E un ensemble non vide, dans $\mathcal{F}(E, E)$, la composition des applications (dite loi \circ) est une lci.

★Exercice 15.1 Soit $E =]-1; 1[$. Pour $x, y \in E$, on pose $x * y = \frac{x+y}{1+xy}$. Montrer que l'on définit ainsi une lci dans E .



Définition 15.2 (associativité, commutativité)

Soit $(E, *)$ un ensemble muni d'une lci.

- On dit que la loi est associative lorsque : $\forall x, y, z \in E, x * (y * z) = (x * y) * z$.
- On dit que deux éléments x et y de E commutent lorsque $x * y = y * x$. Si tous les éléments commutent deux à deux, on dit que la lci est commutative.

Exemples :

- L'addition et la multiplication des nombres dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, sont associatives et commutatives.
- L'addition et la multiplication des fonctions dans $\mathcal{F}(A, \mathbb{C})$ (A étant un ensemble non vide) sont associatives et commutatives.
- Dans $(\mathcal{F}(E, E), \circ)$, la loi est associative mais non commutative en général.

- Dans $(\mathbb{R}, *)$ avec $x * y = x - y$ pour tout $x, y \in \mathbb{R}$, la loi est une lci non commutative ($2 * 3 = -1$ mais $3 * 2 = 1$) et non associative ($(1 * 2) * 3 = (-1) * 3 = -4$ et $1 * (2 * 3) = 1 * (-1) = 2$).

★ **Exercice 15.2** Soit $E =]-1; 1[$. Pour $x, y \in E$, on pose $x * y = \frac{x+y}{1+xy}$. Montrer que l'opération $*$ est associative et commutative.

2) Élément neutre

Définition 15.3

Soit $(E, *)$ un ensemble muni d'une lci et soit $e \in E$, on dit que e est un élément neutre pour la loi $*$ lorsque $\forall x \in E, x * e = e * x = x$. Dans le cas où l'opération est notée additivement, l'élément neutre (s'il existe) est appelé noté en général 0_E (zéro de E). Dans le cas où l'opération est notée multiplicativement, l'élément neutre (s'il existe) est noté en général 1_E (un de E).

Exemples :

- L'élément neutre de l'addition des nombres est 0. Celui de la multiplication des nombres est 1.
- L'élément neutre de l'addition des fonctions dans $(\mathcal{F}(A, \mathbb{C}))$ est la fonction constamment nulle. Celui de la multiplication est la fonction constante $x \mapsto 1$.
- Dans $(\mathcal{F}(E, E), \circ)$, id_E est élément neutre.
- Dans $(\mathbb{R}, *)$ avec $x * y = x - y$ il y a un élément neutre à droite qui est 0 car $\forall x \in \mathbb{R}, x - 0 = x$, mais il n'y a pas d'élément neutre à gauche.

★ **Exercice 15.3** Soit $E =]-1; 1[$. Pour $x, y \in E$, on pose $x * y = \frac{x+y}{1+xy}$. Montrer qu'il y a un élément neutre pour cette opération.

Remarque 15.1 – Si $(E, *)$ possède un élément neutre, alors celui-ci est unique. En effet, si on a deux éléments neutre e et e' , alors $e * e' = e$ car e' est neutre, et $e * e' = e'$ car e est neutre, d'où $e = e'$.

Définition 15.4

Soit $(E, *)$ un ensemble muni d'une lci possédant un élément neutre e . On dit que $x \in E$ est symétrisable lorsqu'il existe $x' \in E$ tel que $x * x' = x' * x = e$. Si c'est le cas, on dit que x' est un symétrique de x . Dans le cas où l'opération est notée additivement, le symétrique de x est appelé opposé de x et noté $-x$. Dans le cas où l'opération est notée multiplicativement, le symétrique de x est appelé inverse de x et noté x^{-1} .

Exemples :

- Dans $(\mathbb{C}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$ et $(\mathbb{Z}, +)$, chaque élément possède un opposé, mais pas dans $(\mathbb{N}, +)$.
- Dans (\mathbb{C}^*, \times) , (\mathbb{R}^*, \times) , (\mathbb{Q}^*, \times) , chaque élément possède un inverse, mais pas dans (\mathbb{Z}^*, \times) .
- Dans $(\mathcal{F}(A, \mathbb{C}), +)$ chaque fonction possède un opposé.
- Dans $(\mathcal{F}(A, \mathbb{C}), \times)$, seules les fonctions qui ne s'annulent jamais ont un inverse.
- Dans $(\mathcal{F}(E, E), \circ)$, un élément f de $\mathcal{F}(E, E)$ a un symétrique si et seulement si il existe g dans $\mathcal{F}(E, E)$ telle que $f \circ g = g \circ f = \text{id}_E$, ce qui équivaut à dire que f est une bijection, auquel cas le symétrique de f est la bijection réciproque f^{-1} .

Théorème 15.1

Soit $(E, *)$ un ensemble muni d'une lci associative et possédant un élément neutre e . Si un élément x possède un symétrique x' dans E , alors celui-ci est unique.

Preuve : Si x' et x'' sont deux symétriques de x , alors $x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''$. \square

★ **Exercice 15.4** Soit $E =]-1; 1[$. Pour $x, y \in E$, on pose $x * y = \frac{x+y}{1+xy}$. Montrer que chaque élément a un symétrique dans E .

II STRUCTURE DE GROUPE

1) Définitions

Définition 15.5

Un groupe est un ensemble non vide G muni d'une opération $*$ (ou loi de composition) qui vérifie les propriétés suivantes :

- elle doit être interne : $\forall x, y \in G, x * y \in G$.
- elle doit être associative : $\forall x, y, z \in G, x * (y * z) = (x * y) * z$.
- elle doit posséder un élément neutre : $\exists e \in G, \forall x \in G, e * x = x * e = x$. Si la loi est une addition l'élément neutre sera noté 0_G et on parlera de groupe additif. Si la loi est une multiplication, l'élément neutre sera noté 1_G et on parlera de groupe multiplicatif. Dans le cas général l'élément neutre est souvent noté e_G .
- tout élément de G doit avoir un symétrique dans G : $\forall x \in G, \exists x' \in G, x * x' = x' * x = e_G$. En notation additive, le symétrique de x est appelé **opposé de x** et noté $-x$, en notation multiplicative on l'appelle **inverse de x** et on le note x^{-1} .

Lorsque toutes ces conditions sont remplies, on dit $(G, *)$ est un groupe. Si en plus la loi $*$ est commutative ($\forall x, y \in G, x * y = y * x$), alors on dit que $(G, *)$ est un **groupe abélien** (ou groupe commutatif).

Exemples :

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, (\mathbb{Q}^*, \times) , (\mathbb{R}^*, \times) , (\mathbb{C}^*, \times) sont des groupes abéliens.
- $(\mathbb{N}, +)$ et (\mathbb{Z}^*, \times) ne sont pas des groupes.
- $(\mathcal{F}(I, \mathbb{C}), +)$ est un groupe abélien pour l'addition des fonctions (ou des suites si $I = \mathbb{N}$).
- Si E est un ensemble non vide, on note $S_E = \{f : E \rightarrow E \mid f \text{ est bijective}\}$, alors (S_E, \circ) est un groupe (non abélien en général), on l'appelle groupe des permutations de E .

À retenir : Règles de calculs

Soit $(G, *)$ un groupe :

- Soient $x, y \in G$, le symétrique de $x * y$ est : $(x * y)' = y' * x'$.
- Soient $a, b \in G$, l'équation $a * x = b$ admet comme unique solution dans G , $x = a' * b$.
- Soient $a, b, c \in G$, si $a * b = a * c$ alors $b = c$ (régularité à gauche).
- Soient $a, b, c \in G$, si $b * a = c * a$ alors $b = c$ (régularité à droite).

★ **Exercice 15.5** Soit $n \geq 2$, dans \mathbb{K}^n ($\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$) on définit l'addition :

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n).$$

Montrer que $(\mathbb{K}^n, +)$ est un groupe abélien.

2) Sous-groupes d'un groupe

Définition 15.6

Soit $(G, .)$ un groupe et H un ensemble, on dit que H est un sous-groupe de $(G, .)$ lorsque :

$$H \subset G; \quad H \neq \emptyset \quad \text{et} \quad \forall x, y \in H, x \cdot y \in H, x^{-1} \in H.$$

Exemples :

- $\{e\}$ et G sont des sous-groupes de $(G, .)$, ils sont appelés sous-groupes triviaux de $(G, .)$.
- Si $(H, .)$ est un groupe inclus dans un groupe $(G, .)$ pour la même loi, alors H est un sous-groupe de G , car on vérifie facilement que l'élément neutre de G est forcément égal à l'élément neutre de H , ce qui entraîne pour $x \in H$, que son symétrique dans G et son symétrique dans H sont les mêmes.
- (\mathbb{U}, \times) et (\mathbb{U}_n, \times) sont des sous-groupes de (\mathbb{C}^*, \times) .
- L'ensemble des fonctions définies sur \mathbb{R} et 2π -périodiques est un groupe additif, car c'est un sous-groupe de $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +)$.
- L'ensemble des entiers pairs est un groupe additif, car c'est un sous-groupe de $(\mathbb{Z}, +)$.
- $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{C}, +)$.

Remarque 15.2 – Si H est un sous-groupe de $(G, .)$ alors $(H, .)$ lui-même est un groupe (de même élément neutre que G). Ceci est souvent utilisé dans la pratique pour montrer qu'un ensemble est un groupe pour une loi, on essaie de montrer (quand c'est possible) que c'est un sous-groupe d'un groupe connu pour cette même loi.

**Théorème 15.2 (sous-groupes de $(\mathbb{Z}, +)$)**

H est un sous-groupe de $(\mathbb{Z}, +)$ si et seulement si il existe un entier n tel que $H = n\mathbb{Z}$ (ensemble des multiples entiers de n). L'entier n est unique au signe près et si $H \neq \{0\}$, alors $n = \min H^{*+}$.

Preuve : Il est facile de vérifier que pour $n \in \mathbb{Z}$, $n\mathbb{Z}$ est un sous-groupe de \mathbb{Z} . Si $H = \{0\}$, alors on peut prendre $n = 0$ et c'est le seul entier qui convienne. Si $H \neq \{0\}$, posons, $n = \min H^{*+}$ (n existe dans \mathbb{N} , c'est la propriété fondamentale de \mathbb{N}), on a $n \in H$, comme H est un sous-groupe de $(\mathbb{Z}, +)$, tout multiple de n est dans H , i.e. $n\mathbb{Z} \subset H$. Soit $k \in H$ effectuons la division euclidienne de k par n ($n \neq 0$) : $k = nq + r$ avec $0 \leq r < n$. On a donc $r = k - nq \in H$, si $r \neq 0$ alors $r \geq n$ ce qui est absurde, donc $r = 0$ ce qui donne $k = nq \in n\mathbb{Z}$, finalement $H = n\mathbb{Z}$. Si on a aussi $H = m\mathbb{Z}$ avec $m \in \mathbb{N}$, alors $n\mathbb{Z} = m\mathbb{Z}$, donc n et m se divisent mutuellement dans \mathbb{N} , donc $n = m$. \square

**Théorème 15.3 (sous-groupes de $(\mathbb{R}, +)$)**

Soit G un sous-groupe de $(\mathbb{R}, +)$ non réduit à $\{0\}$, alors soit G est dense dans \mathbb{R} , soit G est de la forme $G = \alpha\mathbb{Z}$ avec $\alpha > 0$ réel.

Preuve : Il existe $x \in G$ non nul, on a donc x et $-x$ dans G , par conséquent G_+^* est non vide (et minoré par 0), soit $\alpha = \inf G_+^*$.

- Si $\alpha \neq 0$, alors $\alpha > 0$: supposons $\alpha \notin G$, alors on peut trouver deux éléments de G , g_1 et g_2 tels que $\alpha < g_1 < g_2 < 2\alpha$, mais alors $0 < g_2 - g_1 < \alpha$ avec $g_2 - g_1 \in G_+^*$: absurde, donc $\alpha \in G$. On en déduit alors que $\alpha\mathbb{Z} \subset G$. Soit $g \in G$ et $n = \lfloor \frac{g}{\alpha} \rfloor$, alors $n\alpha \leq g < (n+1)\alpha$ et donc $0 \leq g - n\alpha < \alpha$, on en déduit que $g - n\alpha$ est nul car c'est un élément positif de G , d'où $G = \alpha\mathbb{Z}$.
- Si $\alpha = 0$: soit $x \in \mathbb{R}$ et $\varepsilon > 0$, il existe $g \in G$ tel que $0 < g < \varepsilon$, soit $n = \lfloor \frac{x}{g} \rfloor$ alors $ng \leq x < ng + g < ng + \varepsilon$, donc $|x - ng| < \varepsilon$ avec $ng \in G$, donc G est dense dans \mathbb{R} . \square

★ **Exercice 15.6** Soient $a, b \in \mathbb{R}^*$, montrer que $G = a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$ dense dans \mathbb{R} si et seulement si $\frac{a}{b}$ est irrationnel. En déduire que $\{\cos(n) \mid n \in \mathbb{N}\}$ est dense dans $[-1; 1]$.

**Théorème 15.4 (propriétés des sous-groupes)**

- Soit $H \subset (G, *)$ non vide, alors H est un sous-groupe de $(G, *)$ si et seulement si $\forall x, y \in H, x * y^{-1} \in H$.
- Une intersection quelconque de sous-groupes de $(G, *)$, est un sous-groupe de $(G, *)$, mais ceci n'est pas vrai pour la réunion.

Preuve : Le premier point est laissé en exercice.

Soit $(H_i)_{i \in I}$ une famille de sous-groupes de $(G, *)$, posons $K = \bigcap_{i \in I} H_i$, ce sont des parties de G donc l'intersection aussi : $K \subset G$. Tous les sous-groupes H_i contiennent l'élément neutre e de G , donc l'intersection aussi et par conséquent K est non vide. Si $x, y \in K$, alors x, y sont dans tous les sous-groupes H_i , donc $x * y^{-1}$ aussi, par conséquent $x * y^{-1}$ est dans l'intersection, i.e. $x * y^{-1} \in K$, K est donc un sous-groupe de $(G, *)$.

Donnons un contre-exemple pour la réunion : $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe de $(\mathbb{Z}, +)$, car 2 et 3 sont dans la réunion, mais pas $2 + 3 = 5$, cet ensemble n'est donc pas stable pour l'addition (les autres conditions sont néanmoins remplies). \square

III ANNEAUX ET CORPS

1) Anneaux

**Définition 15.7**

Un anneau est un ensemble A muni de deux lois de composition internes : une addition et une multiplication, qui vérifient :

- $(A, +)$ est un groupe abélien.
- La multiplication :
 - est associative,
 - admet un élément neutre (noté 1).
 - est distributive sur l'addition.

Si de plus la multiplication est commutative, on dit que $(A, +, \times)$ est un anneau commutatif.

☞ **Exemples :**

- $(\mathbb{Z}, +, \times)$ est un anneau commutatif mais ce n'est pas un corps.
- $(\mathcal{F}(\mathbb{N}, \mathbb{C}), +, \times)$ est un anneau commutatif.
- Si E est un ensemble non vide, l'ensemble des fonctions de E dans \mathbb{C} muni des opérations usuelles sur les fonctions, est un anneau commutatif, *i.e.* $(\mathcal{F}(E, \mathbb{C}), +, \times)$ est un anneau commutatif.
- Plus généralement, si $(A, +, \times)$ est un anneau et E est un ensemble non vide, alors $(\mathcal{F}(E, A), +, \times)$ est un anneau.

À retenir : Règles de calculs dans un anneau

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

- $\forall x \in A, x \times 0 = 0 \times x = 0$.
- $\forall x, y \in A, -(x \times y) = (-x) \times y = x \times (-y)$.
- $\forall x, y \in A$, si x et y sont inversibles (pour la multiplication), alors $x \times y$ est inversible est $(x \times y)^{-1} = y^{-1} \times x^{-1}$.
- Si $x \in A$ et $p \in \mathbb{Z}$ alors on note $p \cdot x = 0$ si $p = 0$, $p \cdot x = x + \dots + x$, p fois si $p > 0$, et $p \cdot x = (-x) + \dots + (-x)$, $-p$ fois si $p < 0$. On note également $x^p = 1_A$ si $p = 0$, $x^p = x \times \dots \times x$, p fois si $p > 0$, et $x^p = x^{-1} \times \dots \times x^{-1}$, $-p$ fois si $p < 0$ **et x inversible**.
- $\forall x, y \in A$, si x et y commutent ($x \times y = y \times x$), alors on peut utiliser la formule du binôme, c'est à dire : $\forall n \in \mathbb{N}, (x + y)^n = \sum_{k=0}^n \binom{n}{k} \cdot x^k \times y^{n-k} = \sum_{k=0}^n \binom{n}{k} \cdot x^{n-k} \times y^k$.
- Si $x, y \in A$ avec $x \times y = y \times x$ alors $\forall n \in \mathbb{N}^* : x^n - y^n = (x - y) \sum_{k=0}^{n-1} a^k b^{n-1-k}$.

★ **Exercice 15.7** Si $x \in A$, simplifier $(1 - x) \sum_{k=0}^n x^k$ et $(1 + x) \sum_{k=0}^n (-1)^k x^k$.

Théorème 15.5 (groupe des inversibles)

Soit $(A, +, \times)$ un anneau, l'ensemble des inversibles de A est noté $U(A)$, cet ensemble est un **groupe multiplicatif**. $(U(A), \times)$ est appelé **groupe des unités** de A .

Preuve : Celle-ci est simple et laissée en exercice. □

☞ **Exemples** :

- $U(\mathbb{Z}) = \{\pm 1\}$.
- Si A est l'anneau des suites complexes, alors $U(A)$ est l'ensemble des suites complexes qui ne s'annulent pas.

Définition 15.8 (anneau intègre)

Soit $(A, +, \times)$ un anneau. On dit que A est un anneau intègre lorsque le produit de deux éléments non nuls est toujours non nul, sinon on dit que A est un anneau non intègre.

Remarque 15.3 –

- Dans un anneau intègre, un produit de facteurs est nul si et seulement si au moins un des facteurs est nul.
- $(\mathbb{Z}, +, \times)$ est un anneau intègre.
- L'ensemble des suites complexes est un anneau non intègre.

Définition 15.9 (sous-anneaux d'un anneau)

Soit $(A, +, \times)$ un anneau, et soit H un ensemble, on dit que H est un sous-anneau de A lorsque :

- $H \subset A$.
- $1_A \in H$.
- $\forall x, y \in H, x + y \in H, x \times y \in H$ et $-x \in H$.

Si c'est le cas, alors $(H, +, \times)$ est lui-même un anneau.

☞ **Exemple** : $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.

Théorème 15.6

Une intersection de sous-anneaux de $(A, +, \times)$ est un sous-anneau de A .

Preuve : Celle-ci est simple et laissée en exercice. □

2) Corps

 **Définition 15.10**

Un corps est un ensemble E muni de deux opérations (ou deux lois de composition), une addition et une multiplication. Ces deux opérations doivent vérifier les propriétés suivantes :


- $(E, +, \times)$ est un anneau.
- $U(E) = E \setminus \{0\}$, i.e. : $\forall x \in E \setminus \{0\}, x$ a un inverse dans E . Si de plus la multiplication est commutative, on dit que $(E, +, \times)$ est un corps commutatif.

 **Exemples :**

- $(\mathbb{R}, +, \times), (\mathbb{Q}, +, \times), (\mathbb{C}, +, \times)$ sont des corps commutatifs, mais $(\mathbb{Z}, +, \times)$ n'est pas un corps.
- Il existe des corps non commutatifs (corps des quaternions).

Remarque 15.4 –

- Un corps est toujours intègre.
- Les règles de calculs sont les mêmes que dans un anneau.

 **Définition 15.11 (sous-corps d'un corps)**

Soit $(K, +, \times)$ un corps et soit H un ensemble, on dit que H est un sous-corps de K lorsque :

- $H \subset K$.
- $1_K \in H$.
- $\forall x, y \in H, x + y \in H, -x \in H$ et $x \times y \in H$.
- $\forall x \in H \setminus \{0\}, x^{-1} \in H$.

Si c'est le cas alors $(H, +, \times)$ est lui-même un corps.

 **Exemples :**

- \mathbb{Q} est un sous-corps de \mathbb{R} qui est lui-même un sous-corps de \mathbb{C} .
- $\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\}$ est un sous-corps de $(\mathbb{C}, +, \times)$.
- $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ est un sous-corps de \mathbb{R} .