Chapitre 5 : Les structures algébriques

Introduction : En mathématiques, plus précisément en algèbre générale et en algèbre universelle, une structure algébrique est un type particulier de structure. Sa spécificité par rapport aux autres types de structure est d'être formée d'un ensemble combiné à une ou plusieurs lois de composition, éventuellement complétées par un ordre ou une topologie, le tout satisfaisant un certain nombre d'axiomes.

En algèbre générale, les structures algébriques sont définies une à une et leurs propriétés sont étudiées séparément.

En algèbre universelle, les structures algébriques sont étudiées de façon globale de façon à

obtenir un modèle unifié, d'où l'adjectif « universel ». Par exemple, qu'y a-t-il en commun entre la théorie des groupes, la théorie des anneaux et la théorie des corps ?

L'objectif de ce chapitre est de dresser une liste des structures algébriques usuelles et de les classer.

Définition : Soit E un ensemble non vide,

On appelle loi de composition interne de E dans E notée $\star$, toute application de $E \times E$ vers E et on écrit :

$\star : E \times E \longrightarrow E$

$$(x, y) \longmapsto \star\big((x, y)\big) = x \star y$$

$x \star y$ est une notation de $\star\big((x, y)\big)$

Si E est muni d'une loi de composition interne notée $\star$ c'est-à-dire $\star : E \times E \longrightarrow E$ est une application alors $(E,\star)$ est dit Magma. Et on peut dire que $\star$ est une loi de composition interne définie dans E.

Autrement dit : $\star$ est une loi de composition interne de l'ensemble E dans l'ensemble E

si et seulement si $\forall\, x \in E, \forall\, y \in E,$ donc $x \star y \in E$.

Remarque : $\star$ est une loi de composition interne dans E c'est-à-dire $\star$ est une loi de composition interne de E dans E.

Propriétés : Soient E un ensemble non vide et $\star, T$ deux lois de compositions internes dans E, on définit quelques propriétés des lois $\star$ et T comme suit :

1) $\star$ est commutative $\Leftrightarrow \forall\, x, y \in E,\ x \star y = y \star x$
2) $\star$ est associative $\Leftrightarrow \forall\, x, y, z \in E,\ x \star (y \star z) = (x \star y) \star z$
3) $\star$ admet un élément neutre à droite de $E \Leftrightarrow \exists\, e_d \in E$, tel que
$$\forall\, x \in E : e_d \star x = x$$

Et on dit que e_d est l'élément neutre à droite de E pour la loi $\star$ c'est-à-dire

$\forall\, x \in E : e_d \star x = x$

Remarque : L'élément e_d est unique.

4) $\star$ admet un élément neutre à gauche de $E \Leftrightarrow \exists\, e_g \in E$, tel que

$$\forall\, x \in E : x \star e_g = x$$

Et on dit que e_g est l'élément neutre à gauche de E pour la loi $\star$ c'est-à-dire

$\forall\, x \in E : x \star e_g = x$

Remarque : L'élément e_g est unique.

5) $\star$ admet un élément neutre de $E \Leftrightarrow \exists\, e \in E$, tel que

$$\forall\, x \in E : x \star e = e \star x = x$$

Et on dit que e est l'élément neutre de E pour la loi $\star$ c'est-à-dire

$\forall\, x \in E : x \star e = e \star x = x$

Remarque : L'élément e est unique.

6) Supposons que la loi précédente $\star$ admet un élément neutre à droite de E notée e_d

Un élément $x \in E$ admet un élément symétrique à droite pour $\star \Leftrightarrow \exists x'_d \in E$, tel que,

$$x'_d \star x = e_d$$

Et on dit que x'_d est l'élément symétrique à droite de l'élément x pour $\star$ c'est-à-dire

$$x'_d \star x = e_d$$

Remarque : L'élément x'_d est unique.

7) Supposons que la loi précédente $\star$ admet un élément neutre à gauche de E notée e_g

Un élément $x \in E$ admet un élément symétrique à gauche pour $\star \Leftrightarrow \exists\, x'_g \in E$, tel que,

$$x \star x'_g = e_g$$

Et on dit que x'_g est l'élément symétrique à gauche de l'élément x pour $\star$ c'est-à-dire

$$x \star x'_g = e_g$$

Remarque : L'élément x'_g est unique.

8) Supposons que la loi précédente $\star$ admet un élément neutre de E noté e

Un élément $x \in E$ admet un élément symétrique pour $\star \Leftrightarrow \exists\, x' \in E$, tel que,

$$x \star x' = x' \star x = e$$

Et on dit que x' est l'élément symétrique de l'élément x pour $\star$ c'est-à-dire

$x \star x' = x' \star x = e$

Remarque : L'élément x' est unique.

9) T est distributive sur $\star \Leftrightarrow \forall\, x, y, z \in E$:

$$\begin{cases} (x \star y)Tz = (xTz) \star (yTz) \\ xT(y \star z) = (xTy) \star (xTz) \end{cases}$$

10) On dit que l'élément $a \in E$ est régulier ou bien l'élément a est simplifiable pour la loi $\star$ si et seulement si : $\forall\, x \in E$, $\forall\, y \in E$, on a :

$a \star x = a \star y \Longrightarrow x = y$

Et

$x \star a = y \star a \Longrightarrow x = y$

Remarques concernant l'élément symétrique d'un élément :

1) On dit que l'élément x est inversible ou bien l'élément x admet un inverse.
2) On dit l'inverse de l'élément x ou bien le symétrique de l'élément x.

Remarques des propriétés précédentes :

Soit E un ensemble non vide et $\star$ une loi de composition interne dans E alors :

- Si la loi $\star$ est commutative alors pour démontrer que $\star$ admet un élément neutre, il suffit de démontrer que $\star$ admet un élément neutre à droite noté e_d ou bien $\star$ admet un élément neutre à gauche noté e_g et dans ce cas (le cas de la commutativité) et si $\star$ admet un élément neutre à droite e_d ou bien $\star$ admet un élément neutre à gauche e_g alors l'élément neutre de E pour $\star = e_d = e_g$
- Si la loi $\star$ n'est pas commutative alors si l'élément neutre à droite de E pour $\star$ noté e_d existe dans E et différent de l'élément neutre à gauche de E pour $\star$ noté e_g qui existe dans E, on dit alors que $\star$ n'admet pas un élément neutre, mais $\star$ admet un élément neutre à droite et $\star$ admet un élément neutre à gauche, mais si l'élément $e_d =$ l'élément e_g donc $\star$ admet un élément neutre $= e_d = e_g$
- Si la loi $\star$ admet un élément neutre e donc l'élément neutre à droite de E pour $\star =$ l'élément neutre à gauche de E pour $\star = e$
- Si la loi $\star$ est commutative alors pour démontrer qu'un élément $x \in E$ admet un élément symétrique pour $\star$ il suffit de montrer que x admet un élément symétrique à droite pour $\star$ noté x'_d ou bien x admet un élément symétrique à gauche pour $\star$ noté x'_g et dans ce cas (le cas de la commutativité) et si le x admet un élément symétrique à droite pour $\star$ noté x'_d ou bien si le x admet un élément symétrique à gauche pour $\star$ noté x'_g donc l'élément symétrique de x pour $\star = x'_d = x'_g$
- Si la loi $\star$ n'est pas commutative alors si l'élément symétrique à droite d'un élément $x \in E$ pour $\star$ noté x'_d existe dans E et différent de l'élément symétrique à gauche de l'élément x pour $\star$ noté x'_g qui existe dans E, on dit

alors que x n'admet pas un élément symétrique pour $\star$ mais x admet un élément symétrique à droite pour $\star$ noté x'_d et x admet un élément symétrique à gauche pour $\star$ noté x'_g mais si l'élément $x'_d =$ l'élément x'_g donc l'élément symétrique de x pour $\star = x'_d = x'_g$

- Soit x' l'élément symétrique d'un élément $x \in E$ pour la loi $\star$ donc l'élément symétrique à droite de x pour $\star$ noté $x'_d =$ l'élément symétrique à gauche de x pour $\star$ noté $x'_g = x'$

On s'intéresse maintenant à l'étude de la première structure algébrique.

Définition : Soit G un ensemble muni d'une loi de composition interne notée $\star$

On dit que $(G,\star)$ est un groupe si et seulement si :

1) $\star$ est associative.
2) $\star$ admet un élément neutre de G (l'élément neutre est dans G)
3) Tout élément de G admet un élément symétrique pour la loi $\star$

Si de plus $\star$ est commutative, on dit que $(G,\star)$ est un groupe abélien ou bien on dit que $(G,\star)$ est un groupe commutatif.

Remarques :

1) Lorsque on dit que e est l'élément neutre d'un ensemble G pour une loi de composition interne $\star$ c'est-à-dire que l'ensemble G admet un élément neutre e pour cette loi $\star$
2) On écrit $(G,\star)$ est un groupe commutatif ou bien simplement G est un groupe commutatif.

Définition : Soit $(G,\star)$ un groupe, si le nombre d'élément de G est fini, $(\text{card}\, G = n)$, on dit alors que G est un groupe fini d'ordre n (bien sûr le $n \neq 0$).

Définition : Soient $(G,\star)$ un groupe et H un sous ensemble non vide de G,

On dit que H est un sous-groupe de G si et seulement si $(H,\star)$ est un groupe.

Et on peut écrire : $(H,\star)$ est un sous-groupe de $(G,\star)$.

Exemples :

1) Si G est un groupe d'élément neutre e, alors $\{e\}$ et G sont des sous-groupes de G dont $\{e\}$ est le plus petit sous-groupe, et G est le plus grand sous-groupe.
2) Pour tout $n \in \mathbb{N}$, l'ensemble $n\mathbb{Z} = \{nx,\ x \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$ ($+$ c'est l'addition).

Proposition : Soient $(G,\star)$ un groupe d'élément neutre e et H est un sous ensemble non vide de G et x^{-1} est le symétrique de $x \in G$ pour la loi $\star$, alors :

$$H \text{ est un sous-groupe de } G \Leftrightarrow \begin{cases} e \in H \\ \forall\, x, y \in H,\ \ x \star y \in H \\ \forall\, x \in H,\ x^{-1} \in H \end{cases}$$

Caractérisation d'un sous-groupe : Soit $(G,\star)$ un groupe d'élément neutre e et soit H un sous ensemble non vide de G, et y^{-1} est le symétrique de $y \in G$ pour la loi $\star$, alors :

H est un sous-groupe de $G \Leftrightarrow \begin{cases} e \in H \\ \forall\, x, y \in H,\ \ x \star y^{-1} \in \mathrm{H} \end{cases}$

Proposition : Soient G un groupe et $(H_i)_{i\in I}$ une famille de sous-groupes de G alors

$H_1 \cap H_2 \cap \cdots\cdots\cdots \cap H_n$ est un sous-groupe de G avec $I = \{1,2,\cdots\cdots\cdots,n\}$

(n est un entier naturel non nul).

Remarque : En général la réunion des sous-groupes n'est pas un sous-groupe

Preuve : Pour $G = \mathbb{Z}$, $H_1 = 2\mathbb{Z}$ et $H_2 = 3\mathbb{Z}$

$(\mathbb{Z}, +)$ est un groupe, mais $(H_1 \cup H_2, +)$ n'est pas un sous-groupe de $(\mathbb{Z}, +)$ car

$2 \in H_1 = 2\mathbb{Z}$ et $3 \in H_2 = 3\mathbb{Z}$ mais $2 + 3 \notin H_1 \cup H_2 = 2\mathbb{Z} \cup 3\mathbb{Z}$

Définition : Soient $(G,\star)$ un groupe et A un sous ensemble non vide de G, alors l'intersection de tous les sous-groupes de G contenant A est un sous-groupe de G appelé le sous-groupe engendré par A et noté $< A >$

Proposition : Soient $(G,\star)$ un groupe et A un sous ensemble de G alors $< A >$ est le plus petit sous-groupe de G contenant A (au sens de l'inclusion).

Morphismes de groupes :

Définition : Soient $(G,\star), (G', T)$ deux groupes, on appelle morphisme de groupes ou bien homomorphisme de groupes toute application f :

$f : (G,\star) \longrightarrow (G', T)$ telle que :

$\forall\, x, y \in G : f(x \star y) = f(x)\ T\ f(y)$

Remarques :

1) Un endomorphisme de groupes est un morphisme de groupes tel que l'ensemble de départ de ce morphisme = l'ensemble d'arrivé de ce morphisme.
2) Un isomorphisme de groupes est un morphisme de groupes bijectif.
3) Un automorphisme de groupes est un endomorphisme de groupes bijectif.

Proposition : Soient $(G,\star)$ un groupe d'élément neutre e et (G', T) un groupe d'élément neutre e'

Soit $f : (G,\star) \longrightarrow (G', T)$ un morphisme de groupes alors :

1) $f(e) = e'$
2) $\forall\, x \in G,\ \ f(x^{-1}) = \big(f(x)\big)^{-1}$

$x^{-1} =$ L'élément symétrique de x pour $\star$

$\big(f(x)\big)^{-1} =$ L'élément symétrique de $f(x)$ pour T

Proposition : Soient $(G,\star)$, (G',T) et (G'',Δ) trois groupes

Soient $f:(G,\star) \longrightarrow (G',T)$ et $g:(G',T) \longrightarrow (G'',\Delta)$ deux morphismes de groupes alors :

$g \circ f:(G,\star) \longrightarrow (G'',\Delta)$ est aussi un morphisme de groupes.

Proposition : Soient $(G,\star)$, (G',T) deux groupes et $f:(G,\star) \longrightarrow (G',T)$ un morphisme de groupes.

Si f est bijective alors f^{-1} existe et f^{-1} est aussi un morphisme de groupes.

La théorie des applications permet de définir :

Noyau d'un morphisme de groupes :

Définition : Soit $f:(G,\star) \longrightarrow (G',T)$ un morphisme de groupes, on désigne par e' l'élément neutre de G' , alors l'image réciproque de $\{e'\}$ par l'application f est dite noyau de f et il est noté $Kerf$, c'est-à-dire

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

Proposition : Soit $f:(G,\star) \longrightarrow (G',T)$ un morphisme de groupes, alors le $Kerf$ est un sous-groupe de G.

Image d'un morphisme de groupes :

Définition : Soit $f:(G,\star) \longrightarrow (G',T)$ un morphisme de groupes, alors l'ensemble $f(G) = \{f(x), x \in G\}$ est appelé image de f notée Imf

Proposition : Soit $f:(G,\star) \longrightarrow (G',T)$ un morphisme de groupes, alors Imf est un sous-groupe de G'.

La structure de groupe permet de définir une deuxième structure algébrique.

Définition : Soit A un ensemble muni de deux lois de compositions internes $\star$ et T

On dit que $(A,\star,T)$ est un anneau si et seulement si :

1) $(A,\star)$ est un groupe abélien.
2) T est associative.
3) T est distributive sur $\star$

Définition : Soit $(A,\star,T)$ un anneau alors :

1) Si T est commutative donc l'anneau $(A,\star,T)$ est dit anneau commutatif ou bien anneau abélien.
2) Si T admet un élément neutre donc l'anneau $(A,\star,T)$ est dit anneau unitaire.

Exemples : $(\mathbb{Z},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des anneaux commutatifs unitaires.

($+$ est l'addition et $\times$ est la multiplication).

Définition d'un sous-anneau : Soit $(A,\star,T)$ un anneau, B une partie de A, on dit que B est un sous-anneau de A si et seulement si $(B,\star,T)$ est un anneau.

Proposition : Soit $(A,\star,T)$ un anneau, B une partie de A, on dit que B est un sous-anneau de A si et seulement si :

1) $(B,\star)$ est un sous-groupe de $(A,\star)$
2) B est stable pour la loi T c'est-à-dire : $\forall\ x, y \in B, x\ T\ y \in B$

Exemple : $(\mathbb{Z},+,\times)$ est un sous-anneau de $(\mathbb{R},+,\times)$

($+$ est l'addition et $\times$ est la multiplication).

Morphisme d'anneaux :

Définition : Soient $(A,\star,T)$ et $(A',\Delta,\perp)$ deux anneaux, on appelle morphisme d'anneaux ou homomorphisme d'anneaux toute application $f : (A,\star,T) \longrightarrow (A',\Delta,\perp)$

Telle que : $\forall\ x, y \in A : f(x \star y) = f(x)\ \Delta\ f(y)$

Et

$$f(x\ T\ y) = f(x) \perp f(y)$$

En utilisant la structure d'un anneau nous définissons un corps.

Définition : Soit K un ensemble muni de deux lois de compositions internes $\star$ et T

On dit que $(K,\star,T)$ est un corps si et seulement si :

1) $(K,\star,T)$ est un anneau unitaire.
2) Tout élément de $K-\{0_K\}$ admet un inverse pour la loi T

$0_K =$ L'élément neutre de K pour la première loi $\star$

Si de plus la loi T est commutative, on dit que K est un corps commutatif.

Exemples :

1) $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des corps commutatifs.
2) $(\mathbb{Z},+,\times)$ n'est pas un corps car les seuls éléments de $\mathbb{Z}-\{0\}$ qui admettent un inverse pour la loi $\times$ sont -1 et 1

Remarque : Dans les exemples précédents $+$ est l'addition et $\times$ est la multiplication.

Exercice 1 :

On définit sur $G=\mathbb{R}$ une loi de composition notée $\ast$ par :

$x \ast y = x + y$

Montrer que $(G,\ast)$ est un groupe commutatif ?

La réponse :

$\ast$ est interne $\Leftrightarrow \forall\ x, y \in G, x \ast y \in G$

Soient x et y deux éléments de G :

$x \divideontimes y = x + y \in \mathbb{R}$

Conclusion : $\divideontimes$ est interne.

$\divideontimes$ est commutative $\Leftrightarrow \forall\, x, y \in G, x \divideontimes y = y \divideontimes x$

Soient x et y deux éléments de G :

$x \divideontimes y = x + y = y + x = y \divideontimes x$

Conclusion : $\divideontimes$ est commutative.

$\divideontimes$ est associative $\Leftrightarrow \forall\, x, y, z \in G :\ (x \divideontimes y) \divideontimes z = x \divideontimes (y \divideontimes z)$

Soient x, y et z trois éléments de G :

$(x \divideontimes y) \divideontimes z = (x + y) \divideontimes z = (x + y) + z = x + y + z$

$x \divideontimes (y \divideontimes z) = x \divideontimes (y + z) = x + (y + z) = x + y + z$

Donc on peut déduire que $(x \divideontimes y) \divideontimes z = x \divideontimes (y \divideontimes z)$

Conclusion : $\divideontimes$ est associative.

Puisque $\divideontimes$ est commutative donc il suffit de chercher l'élément neutre de G pour $\divideontimes$ à droite ou bien à gauche alors :

G admet un élément neutre pour $\divideontimes$ noté $e \Leftrightarrow \forall\, x \in G, e \divideontimes x = x$

Soit x un élément de G,

$e \divideontimes x = x \Longrightarrow e + x = x$

$\Longrightarrow e = x - x$

$\Longrightarrow e = 0 \in \mathbb{R}$

Conclusion : G admet un élément neutre $e = 0$ pour la loi $\divideontimes$

Puisque $\divideontimes$ est commutative donc il suffit de chercher l'élément symétrique d'un élément $x \in G$ pour $\divideontimes$ à droite ou bien à gauche alors :

Soit $x \in G$:

x' est l'élément symétrique de $x \in G$ pour $\divideontimes \Leftrightarrow x' \divideontimes x = 0$

$x' \divideontimes x = 0 \Longrightarrow x' + x = 0$

$\Longrightarrow x' = -x \in \mathbb{R}$

Conclusion : Chaque élément x de G admet un élément symétrique pour la loi $\divideontimes$

Conclusion finale : $(G,\divideontimes)$ est un groupe commutatif.

Exercice 2 :

On définit sur $G = \mathbb{R} - \{0\}$ une loi de composition notée $\triangle$ par :

$x \triangle y = x \times y$

($\times$ est la multiplication)

Montrer que $(G,\triangle)$ est un groupe commutatif.

Solution :

$\triangle$ est interne $\Leftrightarrow \forall\, x, y \in G, x \triangle y \in G$

Soient x et y deux éléments de $G = \mathbb{R} - \{0\}$

$x \triangle y = x \times y \in \mathbb{R} - \{0\}$

Car pour $x, y \in \mathbb{R}$, on a l'implication suivante :

$x \times y = 0 \Longrightarrow x = 0$ ou bien $y = 0$

En utilisant la contraposée de l'implication, on obtient l'implication suivante :

$x \neq 0$ et $y \neq 0 \Longrightarrow x \times y \neq 0$

Conclusion : $\triangle$ est interne

$\triangle$ est commutative $\Leftrightarrow \forall\, x, y \in G, x \triangle y = y \triangle x$

Soient x et y deux éléments de $G = \mathbb{R} - \{0\}$

$x \triangle y = x \times y = y \times x = y \triangle x$

Conclusion : $\triangle$ est commutative.

$\triangle$ est associative $\Leftrightarrow \forall x, y, z \in G,\ (x \triangle y) \triangle z = x \triangle (y \triangle z)$

Soient x, y et z trois éléments de G

$(x \triangle y) \triangle z = (x \times y) \triangle z = (x \times y) \times z = x \times y \times z$

$x \triangle (y \triangle z) = x \triangle (y \times z) = x \times (y \times z) = x \times y \times z$

Donc on peut déduire que $(x \triangle y) \triangle z = x \triangle (y \triangle z)$

Conclusion : $\triangle$ est associative.

Puisque $\triangle$ est commutative donc il suffit de chercher l'élément neutre de G pour $\triangle$ à droite ou bien à gauche alors :

G admet un élément neutre pour $\triangle$ notée $e \Leftrightarrow \forall\, x \in G,\ e \triangle x = x$

Soit x un élément de $\mathbb{R} - \{0\}$

$e \triangle x = x \Longrightarrow e \times x = x$

$\Longrightarrow (e \times x) - x = 0$

$$\Longrightarrow x(e-1)=0$$

et puisque $x \neq 0$ donc $e = 1$

Conclusion : G admet un élément neutre $e = 1$ pour la loi $\triangle$

Puisque $\triangle$ est commutative donc il suffit de chercher l'élément symétrique d'un élément $x \in G$ pour $\triangle$ à droite ou bien à gauche alors :

Soit $x \in G$

x' est l'élément symétrique de $x \in G$ pour $\triangle \Leftrightarrow x' \triangle x = 1$

$x' \triangle x = 1 \Longrightarrow x' \times x = 1$

$$\Longrightarrow x' = \frac{1}{x} \in \mathbb{R} - \{0\}$$

Conclusion : Chaque élément $x \in G$ admet un élément symétrique $x' = \frac{1}{x}$ pour la loi $\triangle$

Conclusion finale : $(G,\triangle)$ est un groupe commutatif.

Remarques : Dans l'exercice 2 précédent , on a :

1) L'expression $x \triangle y = x \times y$ permet de dire que $\triangle = \times$
2) Le groupe $(\mathbb{R} - \{0\},\times)$ est appelé le groupe multiplicatif pour la multiplication usuelle de $\mathbb{R}$.