Chapitre 13

Structures algébriques et exemples

Dans ce chapitre, nous allons étudier les différentes structures algébriques élémentaires (au sens "particules élémentaires") que vous allez rencontrer. Il faudra apprendre à reconnaître ces structures dans les situations pratiques courantes. Les théorèmes généraux que vous démontrerez pendant votre scolarité pourront alors être appliqués aux différentes situations concrètes.

Les termes "groupes", "anneaux" et "corps" sont à prendre au sens "groupe de personnes", "cercle des poètes disparus" (et **pas** "seigneur des anneaux"), "corps de métier". Le terme "anneau" est en fait la traduction de l'allemand "ring", qui a le double-sens des deux films énoncés ci-dessus.

1 Loi de composition interne

Dans ce paragraphe, on fixe un ensemble X non vide.

1.1 Définitions

Définition 1.1 (Loi de composition interne)

Une *loi de composition interne* sur X est une application de $X \times X$ dans X.

Remarques.

1. L'ensemble $X \times X$ (aussi X^2) est le produit cartésien de X avec lui-même, *i.e.* l'ensemble des couples d'éléments de X.
2. On note souvent avec un symbole ($\star$, ou $+$, ou $\times$) une loi de composition interne, et si $(x, y) \in X \times X$, on note $x \star y$ (ou $x + y$ ou $x \times y$) l'image de (x, y) par la fonction $\star$ (plutôt que $\star(x, y)$).

Remarque.

On voit que le même symbole peut être utiliser pour des lois de composition interne différentes (par exemple "$+$" pour les réels et pour les fonctions). C'est le contexte qui permettra de déterminer à quelle loi de composition interne on a affaires.

Définition 1.2

Soit $\star$ une loi de composition interne sur X. Alors :

1. $\star$ est *associative* si pour tous $x, y, z \in X$, on a $x \star (y \star z) = (x \star y) \star z$.
2. $\star$ est *commutative* si pour tout $x, y \in X$, on a $x \star y = y \star x$.

Définition 1.3 (Élément neutre)

Soit $\star$ une loi de composition interne sur X. La loi $\star$ admet un élément neutre s'il existe un élément $e \in X$ tel que

$$\forall\, x \in X,\ x \star e = e \star x = x.$$

Remarque.

Notez bien que pour l'existence d'un élément neutre, il faut les deux relations $x \star e = x$ et $e \star x = x$. Dans le cas où la loi est commutative, comme $x \star e = e \star x$, une seule des relations doit être vérifiée.

Proposition 1.4

Soit $\star$ une loi de composition interne sur X. Si $\star$ admet un élément neutre, celui-ci est unique.

Méthode 1.5 (Montrer qu'une lci admet un élément neutre)

On suppose qu'on a une lci $\star$ associative sur un ensemble X. On veut vérifier si elle admet un élément neutre, et le cas échéant, le déterminer. Pour cela, on fixe $x \in X$, et on résout les équations $x \star e = e \star x = x$ d'inconnue $e \in X$. On cherche une solution indépendante de x.

1.2 Éléments réguliers et symétrisables

Définition 1.6 (Élément régulier)

Soit $\star$ une loi de composition interne sur X. Un élément $a \in X$ est

1. *régulier à gauche* si : $\forall\, (x, y) \in X^2,\ a \star x = a \star y \Longrightarrow x = y$.
2. *régulier à droite* si : $\forall\, (x, y) \in X^2,\ x \star a = y \star a \Longrightarrow x = y$.
3. *régulier* s'il est régulier à gauche et à droite, *i.e.* si

$$\forall\, (x, y) \in X^2,\ \Big(a \star x = a \star y \Longrightarrow x = y \text{ et } x \star a = y \star a \Longrightarrow x = y\Big).$$

Méthode 1.7 (Simplification par un élément régulier)

Si $a \in X$ est régulier, on peut simplifier par a : par exemple, et on résout une équation $a \star x = a \star b$ d'inconnue $x \in X$ (et où $b \in X$, alors elle admet comme unique solution $x = b$.

Définition 1.8 (Élément symétrisable)

Soit $\star$ une loi de composition interne sur X qui admet un élément neutre noté e. Un élément $x \in X$ est *symétrisable* (ou *inversible*) s'il existe $y \in X$ tel que $x \star y = y \star x = e$. L'élément y est alors un *symétrique* de x.

Remarque.
Comme pour l'élément neutre, notez bien que l'existence d'un symétrique pour $x \in X$ impose deux conditions : $x \star y = e$ et $y \star x = e$. Lorque la loi est commutative, ces deux conditions n'en deviennent qu'une seule.

Proposition 1.9

Soit $\star$ une loi de composition interne associative sur X qui admet un élément neutre. Soit $x \in X$ un élément symétrisable. Alors x admet un unique symétrique.

Méthode 1.10 (Montrer qu'un élément est symétrisable)

Comment montrer qu'un élément $x \in X$ est symétrisable, ou pas ? On résout les équations $x \star y = y \star x = e$ d'inconnue $y \in X$. S'il y a une solution, x est symétrisable, et y est son symétrique. Sinon, x n'est pas symétrisable.

Proposition 1.11 (Symétrique du symétrique)

Soit $\star$ une loi de composition interne associative sur X qui admet un élément neutre. Soit $x \in X$ un élément symétrisable et x' son symétrique. Alors x' est symétrisable et son symétrique est x.

Proposition 1.12 (Produit d'éléments symétrisables)

Soit $\star$ une loi de composition interne associative sur X qui admet un élément neutre. Soient $x, y \in X$ deux éléments symétrisables, et x', y' leurs symétriques respectifs. Alors $x \star y$ est symétrisable et son symétrique est $y' \star x'$.

Proposition 1.13 (Un élément symétrisable est régulier)

Soit $\star$ une loi de composition interne associative sur X qui admet un élément neutre. Alors tout élément symétrisable est régulier.

Remarque.
On peut donc simplifier par un éléménet symétrisable.

1.3 Notations particulières

On suppose que X est muni d'une lci $\star$ associative.

1. Souvent, on note xy au lieu de $x \star y$. On note aussi x^n (si $n \in \mathbb{N}^*$) pour $x \star \cdots \star x$ n-fois. On a bien sûr $x^n x^m = x^{n+m}$ si $n, m \in \mathbb{N}^*$ (mais attention : pas $x^n y^n = (xy)^n$ si la lci n'est pas commutative).

2. Si $\star$ admet un élément neutre, on définit x^0 comme étant l'élément neutre.

3. Si $\star$ admet un élément neutre, et x est symétrisable, on note alors en général x^{-1} son symétyrique. Attention, en général, cette notation n'a rien à voir avec l'inverse d'un réel, ou la fonction réciproque d'une fonction bijective, sauf si on est dans un des exemples ci-dessus. Seul le contexte nous permet de savoir.

4. Si $\star$ admet un élément neutre, et x est symétrisable, et $n \in \mathbb{Z}$, $n < 0$, on définit $x^n = \left(x^{-1}\right)^{-n}$. On a alors une définition de x^n pour tout $n \in \mathbb{Z}$, et $x^n x^m = x^{n+m}$.

On suppose que X est muni d'une lci $\star$ associative et commutative.

1. Souvent, on note $x + y$ au lieu de $x * y$. On note aussi nx (si $n \in \mathbb{N}^*$) pour $x * \cdots * x$ n-fois. On a bien sûr $nx + mx = (n+m)x$ si $n, m \in \mathbb{N}^*$, et aussi $nx + ny = n(x+y)$ car lci est commutative.

2. Si $\star$ admet un élément neutre, on le note alors 0 (qui n'a rien à voir en général avec le "0" usuel). On définit aussi $0x$ comme étant l'élément neutre.

3. Si $\star$ admet un élément neutre, et x est symétrisable, son symétrique est appelé l'opposé de x et est noté $-x$. En notant 0 l'élément neutre, on a $x + (-x) = 0$ (*i.e.* $x * x^{-1} = e$).

4. Si $\star$ admet un élément neutre, et x est symétrisable, et $n \in \mathbb{Z}$, $n < 0$, on définit $nx = -n(-x)$. On a alors une définition de nx pour tout $n \in \mathbb{Z}$, et $nx + mx = (n+m)x$.

1.4 Parties stables et loi induite

On suppose que X est muni d'une lci $\star$.

Définition 1.14 (Partie stable)

Soit Y un sous-ensemble de X.

1. La partie Y est stable par $\star$ si
$$\forall\, y, y' \in Y,\ y * y' \in Y.$$

2. La partie Y est stable par passage au symétrique si pour tout $y \in Y$, y est symétrisable, et son symétrique est dans Y.

Proposition 1.15 (Loi induite)

Soit $Y \subset X$ une partie stable par $\star$. Alors $\star$ définie une loi de composition interne sur Y.

2 Groupes

2.1 Définition

Définition 2.1 (Groupe)

Un *groupe* est un couple $(G, *)$ où G est un ensemble non vide, $\star$ une loi de composition interne associative sur G, munie d'un élément neutre, et pour laquelle tout élément de G est symétrisable, *i.e.*

1. $\forall\, x, y, z \in G,\ x * (y * z) = (x * y) * z.$

2. $\exists\, e \in G,\ \forall\, x \in G,\ x * e = e * x = x.$

3. $\forall\, x \in G,\ \exists\, x' \in G,\ x * x' = x' * x = e.$

Un *groupe commutatif* est un groupe $(G, *)$ dont la loi $*$ est commutative, *i.e.*

$$\forall\, x, y \in G,\ x * y = y * x.$$

Proposition 2.2

Soit $(G, *)$ un groupe, e un élément neutre. Alors

1. $(G, *)$ admet un unique élément neutre.
2. Tout élément est régulier.
3. Tout élément $x \in G$ admet un unique symétrique.
4. Soit $x \in G$ et x' son symétrique. Alors x est le symétrique de x'.
5. Si $x \in G$ et $y \in G$ vérifient $x * y = e$, alors y est le symétrique de x.

Remarques.

1. Le symétrique de l'élément neutre est lui-même.
2. Le point 5 de cette proposition est délicat : il suppose déjà que x admet un symétrique. En particulier, si on sait juste que $x \star y = e$, en général, x n'est pas symétrisable.

2.2 Sous-groupes

À partir d'ici, on notera x^{-1} le symétrique d'un élément x d'un groupe.

Définition 2.3

Soit $(G, \star)$ un groupe. Un *sous-groupe* de G est un sous-ensemble H non vide de G, stable par $\star$ et par passage au symétrique, *i.e.* tel que

1. Si $x \in H$, alors $x^{-1} \in H$.
2. Si $x, y \in H$, alors $x \star y \in H$.

Proposition 2.4 (Sous-groupes triviaux)

Soit $(G, \star)$ un groupe et e son élément neutre. Alors $\{e\}$ et G sont des sous-groupes de $(G, \star)$, appelés sous-groupes triviaux de G.

Proposition 2.5

Soit H un sous-groupe d'un groupe $(G, \star)$. L'élément neutre de G est dans H.

Méthode 2.6

Souvent, pour montrer qu'un candidat H à être un sous-groupe est non vide, on montre qu'il contient l'élément neutre.

Proposition 2.7 (Intersection de sous-groupes)

L'intersection de sous-groupes d'un même groupe $(G, \star)$ est un sous-goupe de $(G, \star)$.

Proposition 2.8

Un sous-groupe H d'un groupe $(G, \star)$ est un groupe pour la loi induite.

Méthode 2.9 (Montrer que $(G, \star)$ est un groupe)

- Soit on le montre directement, en montrant qu'on a une lci associative, un élément neutre (méthode 1.5) et que tout élément est symétrisable (méthode 1.10).
- Mais en général, on montre que G est un sous-groupe d'un groupe connu. Cela évite de montrer l'associativité, de trouver l'élément nutre, et de montrer que tout élément est symétrisable. Il y a juste un problème de stabilité par $\star$ et par passage au symétrique.

Proposition 2.10

Soit $(G, \star)$ un groupe et $H \subset G$. Alors H est un sous-groupe de $(G, \star)$ si et seulement si

1. $H \neq \emptyset$
2. $\forall\, x, y \in H,\ xy^{-1} \in H$.

3 Anneaux

3.1 Définitions

Définition 3.1 (Anneau)

Un anneau est un triplet $(A, +, \times)$ tel que :

1. $(A, +)$ est un groupe commutatif.
2. $\times$ une loi de composition interne associative sur A admettant un élément neutre.
3. La loi $\times$ est distributive sur $+$, *i.e.* pour tous $x, y, z \in A$, on a $x \times (y + z) = x \times y + x \times z$ et $(y + z) \times x = y \times x + z \times x$.

Remarques.

1. La première loi de composition interne d'un anneau est appelé "addition", et la deuxième "multiplication", par analogie avec $\mathbb{R}$. Mais bien entendu, ces opérations n'ont en général rien à voir avec les opérations dans $\mathbb{R}$ si A n'est pas l'ensemble des réels.
2. L'élément neutre de la loi "$+$" est noté 0, et l'élément neutre de la loi "$\times$" est noté 1. Encore une fois, ce ne sont pas en général le 0 et le 1 réels. Cela peut-être des fonctions par exemple. Le contexte permet de savoir.
3. Le symétrique d'un élément x pour la loi "$+$" (l'addition) est appelé *opposé*, et est noté $-x$.
4. Pour alléger les notations, on note en général $xy = x \times y$ et $x - y = x + (-y)$.

Définition 3.2 (Anneau commutatif)

Un anneau $(A,+,\times)$ est commutatif si la loi $\times$ est commutative.

Définition 3.3 (Élément régulier)

Un élément x d'un anneau $(A,+,\times)$ est régulier s'il est régulier pour la lci $\times$.

Définition 3.4 (Diviseur de zéro)

Un élément x d'un anneau $(A,+,\times)$ est un *diviseur de zéro* s'il est non nul, et s'il existe $y \neq 0$ tel que

$$xy = 0 \quad \text{ou} \quad yx = 0.$$

Définition 3.5 (Anneau intègre)

Un anneau $(A,+,\times)$ est *intègre* si $A \neq \{0\}$, si A commutatif, et s'il n'admet pas de diviseur de 0, ou encore si pour tous $x, y \in A$,

$$xy = 0 \Longrightarrow \big(x = 0 \quad \text{ou} \quad y = 0\big).$$

Définition 3.6 (Élément inversible, ensemble A^*)

Un élément x d'un anneau $(A,+,\times)$ est *inversible* s'il est symétrisable pour la loi $\times$. On note A^* l'ensemble des éléments inversibles de A.

Remarques.

1. Un élément n'admet pas nécessairement de symétrique pour $\times$. En particulier, 0 n'a jamais de symétrique pour $\times$, sauf si $A = \{0\}$.
2. Si un élément $x \in A$ est inversible, son symétrique s'apelle l'inverse, et est noté x^{-1}.

Proposition 3.7

Soit $(A,+,\times)$ un anneau. Tout élément inversible est régulier.

Méthode 3.8

Comme dans un groupe, on peut simplifier par un élément régulier, et en particulier par un élément inversible : si $ax = ay$ et a est régulier, alors $x = y$.

Remarque.

C'est bien entendu aussi vrai pour l'addition, puisque $(A,+)$ est un groupe : si $a + x = a + y$, alors $x = y$, pour tout $a \in A$.

3.2 Propriétés

Proposition 3.9

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

1. Pour tout $x \in A$, $0 \times x = x \times 0 = 0$.

2. Tout élément de A admet un unique opposé et tout élément inversible de A admet un unique inverse.

3. Soit $x \in A$. Alors $-(-x) = x$ et si x est inversible, x^{-1} l'est également, et $(x^{-1})^{-1} = x$.

Proposition 3.10 (Produit d'éléments inversibles)

Soit $(A, +, \times)$ un anneau, et $x, y \in A^*$. Alors $xy \in A^*$ et $(xy)^{-1} = y^{-1}x^{-1}$.

Remarque.

Attention à l'ordre ! C'est $y^{-1}x^{-1}$, et pas dans l'autre sens.

Proposition 3.11

Soit $(A, +, \times)$ un anneau. Alors $(A^*, \times)$ est un groupe.

Proposition 3.12 (Calculs dans un anneau)

Soient $(A, +, \times)$ un anneau, et $a, b \in A$ tels que $ab = ba$. Soit $n \in \mathbb{N}$. Alors

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

2. $a^n - b^n = (a-b) \displaystyle\sum_{k=0}^{n-1} a^k b^{n-1-k}$.

Remarque.

Ces égalités sont en particulier vraies dans un anneau commutatif. Mais attention : si a et b ne commutent pas, les résultats tombent en défaut. Par exemple, $(a+b)^2 = a^2+ab+ba+b^2 \neq a^2+2ab+b^2$ si $ab \neq ba$.

Méthode 3.13

Soit $(A, +, \times)$ un anneau, et $x \in A^*$. Alors

1. x et x^{-1} commutent, donc $(x + x^{-1})^n = \cdots$ et $(x - x^{-1})^n = \cdots$.

2. x et 1 commutent, donc $(x+1)^n = \cdots$ et $(x-1)^n = \cdots$.

3.3 Sous-anneaux

Définition 3.14 (Sous-anneau)

Un *sous-anneau* d'un anneau $(A, +, \times)$ est un sous-groupe B de $(A, +)$, contenant 1, et stable par multiplication, *i.e.*

1. $B \subset A$.

2. $B \neq \emptyset$.

3. $\forall\, x, y \in B$, $x + y \in B$.

4. $\forall\, x \in B$, $-x \in B$.

5. $1 \in B$.

6. $\forall\, x, y \in B$, $xy \in B$.

Proposition 3.15

Un sous-anneau d'un anneau $(A, +, \times)$ est un anneau pour les lois induites.

Méthode 3.16

Cette proposition est très utile pour montrer qu'un ensemble est un anneau, en montrant que c'est un sous-anneau d'un anneau connu. Cela évite en particulier de redémontrer l'associativité, la distributivité,... Par exemple, l'ensemble des suites convergentes est un anneau pour les lois usuelles, puisque c'est un sous-anneau de l'anneau des suites.

Proposition 3.17 (Sous-anneau d'un anneau intègre)

Un sous-anneau d'un anneau intègre est un anneau intègre.

Méthode 3.18

Pour montrer qu'un ensemble est un anneau intègre, souvent on montre que c'est un sous-anneau d'un anneau intègre connu, *cf* en particulier les sous-anneaux d'un corps.

4 Corps

Définition 4.1 (corps)

Un *corps* est un anneau $(K, +, \times)$ commutatif, tel que K contienne au moins deux éléments, et dont tous les éléments sauf 0 (élément neutre de l'addition) sont inversibles.

Remarques.

1. On utilise les mêmes notations que pour les anneaux : 0, 1, $xy = x \times y$ et $x - y = x + (-y)$.
2. La distributivité à gauche est équivalente à celle à droite puisque l'addition et la multiplication sont commutatives.
3. On parle souvent d'un corps K lorsque les deux lois sont implicites.

Proposition 4.2

Soit $(K, +, \times)$ un corps. Alors

1. Pour tout $x \in K$, $0 \times x = 0$.

2. $0 \neq 1_K$.

3. Tout élément de K admet un unique opposé et tout élément non nul de K admet un unique inverse.

4. Soit $x \in K$. Alors $-(-x) = x$ et si $x \neq 0_K$, $(x^{-1})^{-1} = x$.

5. Soient $x, y \in K$. Alors
$$xy = 0_K \iff x = 0 \text{ ou } y = 0.$$

Autrement dit, un corps est un anneau intègre.

Remarque.
C'est évidemment une redite de la proposition 3.9, sauf en ce qui concerne l'intégrité.

Méthode 4.3 (Simplification dans un corps)

Dans un corps, on peut donc simplifier par tout élément non nul. Autrement dit, si $x, y, z \in K$, et $x \neq 0$, alors $xy = xz \Longrightarrow y = z$.

Proposition 4.4

Soit $(K, +, \times)$ est un corps.

1. $(K, +)$ est un groupe commutatif. commutatif.

2. Soit $K^* = K \setminus \{0\}$. Alors $(K^*, \times)$ est un groupe commutatif dont l'élément neutre est 1.

Définition 4.5

Soit $(K, +, \times)$ un corps. Un sous-corps de K est un sous-anneau de K stable par passage à l'inverse, *i.e.* un sous-anneau C de K tel que, si $x \in C$ et $x \neq 0$, alors $x^{-1} \in C$.

Proposition 4.6

Un sous-corps d'un corps est un corps pour les lois induites.

5 Exemples fondamentaux

5.1 Groupes

Proposition 5.1 (Nombres complexes de module 1)

1. L'ensemble $\mathcal{U}$ des nombres complexes de module 1 est un sous-groupe de $(\mathbb{C}^*, \times)$.

2. Pour tout $n \in \mathbb{N}^*$, l'ensemble $\mathcal{U}_n$ des racines n-ème de l'unité est un sous-groupe de $(\mathcal{U}, \times)$

Proposition 5.2 (Groupe des permutations d'un ensemble)

Soit E un ensemble non vide. L'ensemble $\mathcal{S}(E)$ des permutations de E muni de la composition des fonctions est un groupe (non commutatif en général).

5.2 Ensembles de fonctions

Dans tout ce paragraphe, on fixe un ensemble non vide X, et un corps K (généralement $\mathbb{R}$ ou $\mathbb{C}$).

On rappelle que K^X et $\mathcal{F}(X, K)$ désigne l'ensemble des fonctions de X vers K.

Définition 5.3

Soient $f, g \in K^X$, et $\lambda \in K$.

1. La somme $f + g$ est la fonction de X vers K définie par :

$$\forall\, x \in X,\ (f + g)(x) = f(x) + g(x).$$

2. La fonction λf est la fonction de X vers K définie par :

$$\forall\, x \in X,\ (\lambda f)(x) = \lambda f(x).$$

3. Le produit fg est la fonction de X vers K définie par :

$$\forall\, x \in X,\ (fg)(x) = f(x)g(x).$$

Remarques.

1. Ici, il est très important de bien savoir quelles sont ces opérations "+", "$\times$", "$\cdot$" qu'on utilise : c'est dans K ? Dans K^X ? Cela demande un peu travail pour que la réponse vienne facilement.
2. Les opérations que l'on vient de définir sont les "lois usuelles" sur K^X. Ce sont les additions et multiplications "point par point".

Proposition 5.4

L'ensemble K^X muni des lois usuelles est un anneau commutatif. L'élément neutre pour l'addition est la fonction identiquement nulle, et l'élément neutre pour la multiplication est la fonction constante égale à 1.

Proposition 5.5

Les éléments inversibles de l'anneau K^X sont les fonctions qui ne s'annulent pas, et les diviseurs de 0 sont les fonctions non nulles, qui s'annulent.

Il est temps de faire des exemples d'exemples...

5.3 Suites réelles et complexes

Dans tout ce paragraphe, on fixe un corps K ($\mathbb{R}$ ou $\mathbb{C}$).

On rappelle que $K^{\mathbb{N}}$ désigne l'ensemble des suites à valeurs dans K.

Définition 5.6

Soient $(u_n), (v_n) \in K^{\mathbb{N}}$

1. La somme $(u_n)_{n\in\mathbb{N}} + (v_n)_{n\in\mathbb{N}}$ est la suite de terme général $u_n + v_n$

2. Le produit $(u_n)_{n\in\mathbb{N}}(v_n)_{n\in\mathbb{N}}$ est la suite de terme général $u_n v_n$

Remarques.

1. Ici, il est très important de bien savoir quelles sont ces opérations "$+$", "$\times$", "$\cdot$" qu'on utilise : c'est dans K ? Dans $K^{\mathbb{N}}$?
2. Les opérations que l'on vient de définir sont les "lois usuelles" sur $K^{\mathbb{N}}$. Ce sont les additions et multiplications "terme à terme".

Proposition 5.7

L'ensemble $K^{\mathbb{N}}$ muni des lois usuelles est un anneau. L'élément neutre pour l'addition est la suite constante égale à 0, et l'élément neutre pour la multiplication est la suite constante égale à 1.

6 Compétences

1. Savoir reconnaître dans les ensembles que vous rencontrer les structures algébriques élémentaires.

2. Savoir montrer qu'un ensemble est muni d'une structure de groupe (resp. anneau, corps), en montrant que c'est un sous-groupe (resp. sous anneau, sous-corps) d'un groupe (resp. anneau, corps) connu, en particulier dans les cas d'ensembles de fonctions.