Chapitre 4

Structures algébriques

4.1 Lois de composition internes et ses propriétés

4.1.1 Lois de composition internes

Définition 4.1 *Soit E un ensemble. Une loi de composition interne $*$ sur E est une application de $E \times E$ vers E*

$$\begin{array}{rccc} * : & E \times E & \longrightarrow & E \\ & (x, y) & \mapsto & x * y \end{array}$$

Notations

1. Plutôt que loi de composition interne, on dit aussi opération de composition interne, ou plus simplement opération interne ;
2. On note souvent $(E, *)$ pour désigner un ensemble E muni d'une opération interne $*$.

Exemple 4.1 .

1. *Les lois $\cup$ (union), $\cap$ (intersection) et $\triangle$ (différence symétrique) sur $\mathcal{P}(E)$;*
2. *La loi $\circ$ (la composition) sur $\mathcal{F}(E)$ (l'ensemble des applications de E vers E).*
3. *Les lois $+$ et $\times$ sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$.*
4. *Soit $*$ définie sur $\mathbb{R}$ par : $x * y = \frac{1}{x+y}$. Alors $*$ n'est pas une opération interne, car $(-1, 1)$ n'admet pas une image.*

Définition 4.2 (Partie stable pour une loi) *Soit E un ensemble muni par une loi de composition interne $*$ et F une partie de E. On dit que F est stable pour la loi $*$ si*

$$\forall (x, y) \in F \times F : x * y \ \in F.$$

Exemple 4.2 .

1. *$\mathbb{R}^+$ et $\mathbb{R}^-$ sont deux partie stable de $\mathbb{R}$ pour la loi $+$.*
2. *Pour la loi $\times$, $\mathbb{R}^+$ est encore une partie stable, mais ce n'est pas le cas de $\mathbb{R}^-$.*

4.1.2 Propriétés des lois de composition internes

Définition 4.3 (Commutativité et associativité) *Soit E un ensemble muni par une loi de composition interne $*$*

On dit que $*$ est commutative si $\forall(x,y) \in E^2 : x * y = y * x$.

On dit que $*$ est associative si $\forall(x,y,z) \in E^3 : (x * y) * z = x * (y * z)$.

Exemple 4.3 .

1. *Les lois $+$ et $\times$ sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont commutative et associative ;*
2. *Aussi, les lois $\cup$, $\cap$ et $\triangle$ sur $\mathcal{P}(E)$ sont commutative et associative ;*
3. *La loi $\circ$ sur $\mathcal{F}(E)$ est associative mais pas commutative, car $f \circ g \neq g \circ f$ en général ;*
4. *Soit la loi $*$ définie sur $\mathbb{Q}$ par : $x * y = \frac{x+y}{2}$. Alors $*$ est commutative, car $x * y = \frac{x+y}{2} = \frac{y+x}{2} = y * x$ mais n'est pas associative, car $(-1 * 0) * 1 = \frac{1}{4} \neq -1 * (0 * 1) = \frac{-1}{4}$.*

Définition 4.4 (Element neutre) *Soit E un ensemble muni d'une loi de composition interne $*$. Soit e un élément de E. On dit que e est élément neutre pour la loi $*$, si*

$$\forall x \in E : x * e = e * x = x.$$

Remarque 4.1 *Si la loi $*$ est commutative, l'égalité $x * e = e * x$ est automatiquement réalisée.*

Exemple 4.4 .

1. *Dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$, 0 est neutre pour la lois $+$, et 1 est neutre pour la loi $\times$;*
2. *Dans $\mathcal{P}(E)$, $\emptyset$ est neutre pour la lois $\cup$, et E est neutre pour la loi $\cap$;*
3. *Soit la loi $*$ définie sur $\mathbb{R}$ par : $x * y = x + y - 1$. Alors $e = 1$ est un élément neutre, car $x * e = x \Rightarrow x + e - 1 = x$. Donc $e = 1$.*

Proposition 4.1 (Unicité de l'élement neutre) *L'élement neutre de E pour la loi $*$ s'il existe, est unique.*

Preuve: En effet, soit e' un autre élément neutre pour $*$ alors $e' = e' * e = e * e' = e$. Donc, l'élement neutre est unique. ■

Définition 4.5 (Element symétrique) *Soit E un ensemble muni d'une loi de composition interne $*$ ait un élément neutre e. On dit que l'élément x de E admet un élément symétrique (inversible) x' de E, si $\forall x \in E : x * x' = x' * x = e$.*

Exemple 4.5 .

1. *Dans $\mathbb{R}$, les éléments inversibles pour la lois $\times$, sont les éléments non nuls ;*
2. *Soit la loi $*$ définie sur $\mathbb{R}$ par : $x * y = x + y - 1$. Alors $x \in \mathbb{R}$ admet un élément symétrique $x' = 2 - x$, car $x * x' = 1 \Rightarrow x + x' - 1 = 1$. Donc $x' = 2 - x$.*

Proposition 4.2 *Soit E un ensemble muni d'une loi de composition interne $*$ qui est associative et admet un élément neutre.*

1. *L'élement symétrique x' de x pour la loi $*$ dans E, s'il existe, est unique ;*
2. *Si $x, y \in E$ sont symétrisables alors $x * y$ est symétrisable et son symétrique donné par $(x * y)' = y' * x'$.*

Définition 4.6 (Distributivité) *Soit E un ensemble muni par deux lois de composition internes $*$ et $\top$*

On dit que $*$ est distributive à gauche par rapport a $\top$ si $\forall(x,y,z) \in E^3 : x*(y\top z) = (x*y)\top(x*z)$.

On dit que $*$ est distributive à droite par rapport à $\top$ si $\forall(x,y,z) \in E^3 : (x\top y)*z = (x*z)\top(y*z)$.

Remarque 4.2 *Si la loi $*$ est commutative, alors l'une de ces deux propriétés implique l'autre.*

Exemple 4.6 .

1. *Dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$, la loi $\times$ est distributive par rapport à la loi $+$;*
2. *Dans $\mathcal{P}(E)$, les lois $\cup$, $\cap$ sont distributives l'une par rapport à l'autre ;*
3. *Soit la loi $*$ définie sur $\mathbb{R}$ par : $x*y = x+y-xy$ et la loi $\top$ définie sur $\mathbb{R}$ par : $x\top y = x+y-1$. Comme la loi $*$ est commutative donc il suffit de démontrer la distributivité à gauche par rapport à $\top$.*

$$x*(y\top z) = x*(x+y-1) = 2x+y+z-xy-xz-1......(1)$$

$$(x*y)\top(x*z) = (x+y-xy)\top(x+z-xz) = 2x+y+z-xy-xz-1.....(2)$$

$(1) = (2)$, *donc la loi $*$ est distributive par rapport à la loi $\top$.*

4.2 Structures algebriques

4.2.1 Groupes

Définitions et exemples

Définition 4.7 (Groupe) *Un groupe est un ensemble non vide muni d'une loi de composition interne $(G,*)$ tels que :*
- *$*$ est associative ;*
- *$*$ admet un élément neutre e ;*
- *tout élément de G est symétrisable (admet un symétrique) pour $*$.*

Remarque 4.3 *Si $*$ est commutative, on dit que $(G,*)$ est commutatif, ou abélien.*

Exemple 4.7 .

1. *$(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes abéliens ;*
2. *L'ensemble $\mathcal{P}(E)$ muni de la différence symétrique $\triangle$ est un groupe abélien ;*
3. *$(\mathbb{N},+)$, $(\mathbb{R},\times)$, $(\mathcal{P}(E),\cap)$ et $(\mathcal{P}(E),\cup)$ ne sont pas des groupes.*

Définition 4.8 (Sous-groupe) *Soit $(G,*)$ un groupe et soit H une partie non vide de G. On dit que H est un sous-groupe de G si :*

1. *H est stable pour la lois $*$: $\forall(x,y) \in H^2, x*y \in H$;*
2. *H est stable pour le passage à l'inverse $\forall x \in H, x' \in H$.*

Exemple 4.8 .

1. *Soit* $(G, *)$ *un groupe, alors* e_G *et* G *sont des sous-groupes (dits triviaux) ;*
2. *Soit* $(\mathbb{Z}, +)$ *un groupe. Alors* $3\mathbb{Z}$ *est un sous groupe de* $\mathbb{Z}$ *avec*

$$3\mathbb{Z} = \{3z : \ z \in \mathbb{Z}\} = \{..., -6, -3, 0, 3, 6, ...\}$$

3. *Soit* $(G, \cdot)$ *un groupe, alors l'ensemble* $Z(G) = \{x \in G : \forall y \in G, xy = yx\}$ *est un sous groupe de* G *appelé* ***centre*** *de* G.

Théorème 4.1 (Caractérisation des sous-groupes) *Soit* $(G, *)$ *un groupe et soit* H *une partie non vide de* G. *Alors* H *est un sous-groupe de* G *si et seulement si :*

$$\forall (x, y) \in H^2, x * y' \in H$$

Proposition 4.3 (Intersection de sous-groupes) *Soit* $(G, *)$ *un groupe et soit* $\{H_i\}_{i \in I}$ *une famille de sous groupe de* G. *Alors* $\bigcap\limits_{i \in I} H_i$ *est un sous-groupe de* G.

Remarque 4.4 *La réunion de deux sous-groupes de* G *n'est pas nécessairement un sous-groupe de* G. *Par exemple* $2\mathbb{Z}$ *et* $3\mathbb{Z}$ *sont deux sous-groupes de* $(\mathbb{Z}, +)$, *mais la réunion ne l'est pas puisque* 2 *et* 3 *sont dans* $2\mathbb{Z} \cup 3\mathbb{Z}$ *alors que* $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

Homomorphisme de groupes

Définition 4.9 *Soient* $(G_1, *)$ *et* $(G_2, \perp)$ *deux groupes. On appelle homomorphisme (ou morphisme) de groupes de* G_1 *dans* G_2, *une application* $f : G_1 \longrightarrow G_2$ *telle que,*

$$\forall x, y \in G_1, \ f(x * y) = f(x) \perp f(y).$$

Exemple 4.9 *Soit l'application* f *donnée par :* $\begin{array}{rccc} f : & \mathbb{R} & \longrightarrow & \mathbb{R}^* \\ & x & \mapsto & f(x) = 2^x \end{array}$ f *est un homomorphisme de* $(\mathbb{R}, +)$ *dans* $(\mathbb{R}, \times)$ *car :*

$$\forall x, y \in \mathbb{R}, f(x + y) = 2^{x+y} = 2^x \times 2^y = f(x) \times f(y).$$

Remarque 4.5 *Soient* $(G_1, *)$ *et* $(G_2, \perp)$ *deux groupes et* f *un homomorphisme de* G_1 *dans* G_2. *Alors*

1. *Si* f *est bijective, alors on dit que* f *est isomorphisme ;*
2. *Si* f *est définie dans* $(G_1, *)$ *dans lui mème, alors on dit que* f *est endomorphisme ;*
3. *Si* f *est endomorphisme bijective, alors on dit que* f *est automorphisme.*

Exemple 4.10 .

1. *La fonction exponentielle est un isomorphisme des groupes de* $(\mathbb{R}, +)$ *dans* $(\mathbb{R}_+^*, \times)$;
2. *La fonction logarithme népérien est un isomorphisme de groupes de* $(\mathbb{R}_+^*, \times)$ *dans* $(\mathbb{R}, +)$;

Proposition 4.4 *Soient* $(G_1, *)$ *et* $(G_2, \perp)$ *deux groupes d'éléments neutres* e_1 *et* e_2 *et soit* f *un homomorphisme de* G_1 *dans* G_2. *Alors*

1. $f(e_1) = e_2$ *;*
2. $\forall x \in G_1, \ (f(x))' = f(x')$.

Proposition 4.5 *Soient $(G_1, *)$ et $(G_2, \perp)$ deux groupes d'éléments neutres e_1 et e_2 et soit f un homomorphisme de G_1 dans G_2. Alors*

1. *Si H est un sous-groupe de G_1, alors $f(H)$ est un sous-groupe de G_2 ;*
2. *Si H' est un sous-groupe de G_2, alors $f^{-1}(H)$ est un sous-groupe de G_1.*

Définition 4.10 (Le noyau et l'image d'un homomorphisme) *Soient $(G_1, *)$ et $(G_2, \perp)$ deux groupes et f un homomorphisme de G_1 dans G_2. Alors*

1. *On appelle noyau de f l'ensemble*

$$Ker(f) = f^{-1}(e) = \{x \in G_1 : \ f(x) = e_2\}.$$

2. *On appelle image de f l'ensemble*

$$Im(f) = f(G_1) = \{f(x) \in G_2 : \ x \in G_1\}.$$

Exemple 4.11 *Soit f un homomorphisme donné dans l'exemple4.9, alors*

$$Ker(f) = \{x \in \mathbb{R}, \ f(x) = 1\} = \{x \in \mathbb{R}, \ 2^x = 1\} = \{0\}$$

et $Im(f) = \{f(x) : \ x \in \mathbb{R}\}$. On a $f(x) = y$, alors $2^x = y$ ceci implique que $xln2 = lny$, donc $x = \frac{lny}{ln2}$. D'où, $Im(f) = \mathbb{R}_+^*$.

Théorème 4.2 *Soit f un homomorphisme de $(G_1, *)$ dans $(G_2, \perp)$. Alors*

1. *$Ker(f)$ est un sous-groupe de G_1 ;*
2. *$Im(f)$ est un sous-groupe de G_2 ;*
3. *f est injective si et seulement si $Ker(f) = \{e_1\}$;*
4. *f est surjective si et seulement si $Im(f) = G_2$.*

4.2.2 Anneaux

Définitions

Définition 4.11 (Anneau) *Soit A un ensemble muni de deux lois de composition, $*$ et $\perp$. On dit que $(A, *, \perp)$ est un **anneau** si :*

1. *$(A, *)$ est un groupe commutatif;*
2. *la loi $\perp$ est associative ;*
3. *la loi $\perp$ distributive par rapport à la loi $*$.*

Remarque 4.6 .

1. *Si $\perp$ est commutative, on dit que $(A, *, \perp)$ est un anneau commutatif.*
2. *Si $\perp$ admet un élément neutre, on dit que $(A, *, \perp)$ est un anneau unitaire.*

Exemple 4.12 .

1. *$(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs ;*
2. *Soit E un ensemble, $(\mathcal{P}(E), \triangle, \cap)$ est un anneau commutatif ;*
3. *Soit A l'ensemble des applications de $\mathbb{C}$ dans $\mathbb{C}$, de la forme $z \mapsto \alpha z + \beta \overline{z}$.*
   $(A, +, \circ)$ est un anneau non commutatif.

Définition 4.12 (Sous-anneau) *Soit $(A,+,\cdot)$ un anneau et soit B une partie de A. On dit que B est un* ***sous-anneau*** *de $(A,+,\cdot)$ si et seulement si :*

1. *$B \neq \emptyset$ ($0_A \in B$) ;*
2. *$(B,+)$ est un sous-groupe de A ;*
3. *B stable pour la loi $\cdot$*

Ce qui équivaut à

1. *$0_A \in B$;*
2. *$\forall a,b \in B,\ a-b \in B$;*
3. *$\forall a,b \in B,\ a \cdot b \in B$.*

Exemple 4.13 .

1. *$(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$, chacun est un sous-anneau du suivant ;*
2. *l'ensemble, $\{r+s\sqrt{2},\ (r,s) \in \mathbb{Q}^2\}$ est un sous-anneau de $(\mathbb{R},+,\times)$.*

Définition 4.13 (Homomorphisme d'anneaux) *Soient $(A,+,\cdot)$ et $(B,+,\cdot)$ deux anneaux. On dit qu'une application f de A vers B est un* ***homomorphisme*** *(ou* ***morphisme****) si :*

1. *$f(1_A) = 1_B$;*
2. *$\forall a,b \in A,\ f(a+b) = f(a)+f(b)$;*
3. *$\forall a,b \in A,\ f(a\cdot b) = f(a)\cdot f(b)$.*

Remarque 4.7 *En particulier, f est un homomorphisme de groupes, de $(A,+)$ vers $(A,+)$;*

Définition 4.14 (L'élément inversible) *Un élément d'un anneau $(A,+,\cdot)$ est dit* ***inversible*** *si et seulement s'il est symétrisable pour la seconde opération (s'il admet un symétrique pour la loi $\cdot$).*

Définition 4.15 (Diviseur de zéro) *Un élément non nul x d'un anneau A est un* ***diviseur de zéro*** *si et seulement si son produit avec un autre élément non nul vaut zéro :*

$$\exists y \neq 0 \mid xy = 0 \quad ou \quad yx = 0.$$

Exemple 4.14 .

1. *Dans $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ et $(\mathbb{C},+,\cdot)$, tous les éléments non nuls sont inversibles ;*
2. *Dans l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, toute fonction f qui s'annulle est diviseur de 0 et les éléments inversibles sont les fonctions qui ne s'annullent pas.*

Ideal dans un anneau

Définition 4.16 (Idéal) *Soit $(A,+,\cdot)$ un anneau. Une partie I non vide de A est dite un* ***idéal*** *de A si et seulement si*

1. *I est un sous-groupe de $(A,+,\cdot)$;*
2. *pour $x \in I$ et $a \in A$ on a : $x\cdot a \in I$ et $a \cdot x \in I$*

Exemple 4.15 . *L'ensemble $\mathbb{Z}$ n'est pas un idéal de $(\mathbb{R},+,\times)$, car $\frac{1}{5} \in \mathbb{R}$ et $3 \in \mathbb{Z}$ alors que $\frac{3}{5} \notin \mathbb{Z}$.*

Remarque 4.8 *Il est facile de vérifier que*

1. *L'intersection des idéaux de A est un idéal de A.*
2. *L'image directe d'un idéal par un morphisme d'anneau surjective est un idéal.*
3. *Le noyau d'un morphisme d'anneaux est un idéal.*

Règles de calculs dans un anneau

On rappelle la formule du binôme de Newton, qui s'étend de $\mathbb{Z}$ aux anneaux commutatifs, mais aussi dans un anneau quelconque.

Proposition 4.6 *Soient $(A, +, \cdot)$ un anneau et $a, b \in A$, avec $a \cdot b = b \cdot a$, et $n \in \mathbb{N}^*$. Alors :*

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

Preuve: Récurrence sur $\mathbb{N}$ et formule du triangle de Pascal. ■

Remarque 4.9 *Soient $x, y \in A$ et $n \in \mathbb{N}^*$, alors $x - y \mid x^n - y^n$ et plus précisément :*

$$x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^k y^{n-1-k}.$$

• Cas particulier de ce qui précède : si $1 - x$ est inversible, on peut calculer $\sum_{k=0}^{n-1} x^k$ grâce à la formule :

$$1 - x^n = (1-x)\sum_{k=0}^{n-1} x^k.$$

4.2.3 Corps

Définition 4.17 (Corps) *Un corps est un anneau commutatif dans lequel tout élément non nul est inversible pour la deuxième loi.*

Remarque 4.10 *Si de plus la deuxième loi est commutative, le corps $(K, +, \cdot)$ est dit corps commutatif.*

Exemple 4.16 .
$\mathbb{Q}$, $\mathbb{R}$ *et* $\mathbb{C}$, *sont des corps, mais pas* $\mathbb{Z}$ *(2 n'est pas inversible).*

Définition 4.18 (Sous-corps) *Soit $(K, +, \cdot)$ un corps, un sous-corps de K est une partie K_1 de K telle que $(K_1, +, \cdot)$ soit un corps, c'est-à-dire, pour tous x, y de K_1, on a*

$$x - y \in K_1 \quad \text{et} \quad xy^{-1} \in K_1.$$

Exemple 4.17 .

1. $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ *et* $(\mathbb{C}, +, \times)$, *chacun est un sous-corps du suivant ;*
2. *L'ensemble* $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Q}\}$ *est un corps commutatif qui admet* $\mathbb{Q}$ *comme sous-corps.*