Chapitre 8 : Structures algébriques

Table des matières

1 Loi de composition interne

1.1 Généralités

Définition: Loi de composition interne
Soit E un ensemble. On *loi de composition interne sur E*, toute application :

$$\star : E \times E \to E$$

La donnée $(E, \star)$ d'un ensemble E et une loi de composition interne $\star$ sur E est appelé un *magma*.

Exemple
- L'opération $+$ sur $\mathbb{N}$ définie une loi de composition interne. En effet, pour tout $n, m \in \mathbb{N}$, $n + m \in \mathbb{N}$.
- L'opération $+$ sur $\mathbb{R} \setminus \mathbb{Q}$ ne définit pas une loi de composition interne. En effet, $\pi \in \mathbb{R} \setminus \mathbb{Q}$ et $-\pi \in \mathbb{R} \setminus \mathbb{Q}$ pourtant $0 = \pi - \pi \notin \mathbb{R} \setminus \mathbb{Q}$.

Lorsque l'on compose plusieurs éléments dans un magma, il est possible dans la plupart des cas (sinon c'est vraiment embêtant) de réaliser les opérations en mettant les parenthèses dans l'ordre que l'on veut. On appelle cette propriété l'associativité.

Définition: Associativité
Soit $(E, \star)$ un magma. On dit que la loi de composition interne $\star$ est *associative* si pour tout $(x, y, z) \in E \times E \times E$:

$$x \star (y \star z) = (x \star y) \star z.$$

Remarque 1 *Historiquement, un des premiers exemples d'ensemble muni d'une loi de composition interne non associative porte le nom d'une super-méchant de séries à juste titre : l'algèbre des octonions notée $\mathbb{O}$. Elle est trop difficile à décrire au niveau des classes préparatoires.*

Exemple
L'opération $+$ sur $\mathbb{N}$ est une loi de composition interne associative. En effet, pour tout $n, m, k \in \mathbb{N}$, $n + (m + k) = (n + m) + k$.

Définition: Élément neutre
Pour $(E, \star)$, ensemble E muni d'une loi de composition interne $\star$, on dit que $e \in E$ est un *élément neutre* pour E si pour tout $x \in E$:

$$x \star e = e \star x = x.$$

Théorème: Unicité du neutre
Si $(E, \star)$ admet un élément neutre alors il est unique.

Démonstration :

Définition: Partie stable pour une loi de composition interne
Soit $(E, \star)$ un ensemble muni d'une loi de composition interne et F une sous-partie de E. On dit que F est *stable* pour la loi $\star$ si pour tous $x, y \in F$, $x \star y \in F$.

Exemple
On a la loi $\times$ qui définit une loi de composition interne sur $\mathbb{R}$ et $\mathbb{Q} \subset \mathbb{R}$ telle que pour tout $q, q' \in \mathbb{Q}$, $q \times q' \in \mathbb{Q}$. En effet, si $q = \dfrac{a}{b}$ et $q' = \dfrac{a'}{b'}$ où $a, a', b, b' \in \mathbb{Z}$ alors $q \times q' = \dfrac{aa'}{bb'} \in \mathbb{Q}$.
On en déduit que $\mathbb{Q}$ est stable pour la loi $\times$.

Définition: Symétrique d'un élément
Soit $(E, \star)$ un magma admettant un élément neutre e. On dit que $x \in E$ admet pour symétrique (ou inverse) l'élément noté $\bar{x}$ (ou x^{-1}) si $x \star \bar{x} = \bar{x} \star x = e$.
On dit dans ce cas que x est symétrisable ou inversible.

1.2 Méthodes d'étude

Étudier une loi de composition interne consiste à d'abord s'assurer que la loi en définit bien une puis à détecter si elle est associative, commutative, exhiber l'élément neutre s'il existe et déterminer les éléments admettant un symétrique dans E (inversibles).

Méthode: Comment étudier une loi de composition interne sur un ensemble E
Soit $\star : E \times E \to E$ une loi de composition interne sur E.

1. On s'assure que pour deux éléments arbitraires $x, y \in E$, $x \star y$ appartient bien à E.
2. Vérifier si la loi $\star$ est associative.
3. Vérifier si la loi $\star$ est commutative.
4. Vérifier l'existence d'un élément neutre $e \in E$ qui satisfait donc pour tout $x \in E$, $x = x \star e = e \star x$.
5. Déterminer l'ensemble des éléments $x \in E$ admettant un symétrique dans E, c'est-à-dire tel qu'il existe $y \in E$ satisfaisant $e = x \star y = y \star x$.

Exemple
Soit $E = \mathbb{Z}$ et $\star = +$. On a pour tout $(n, m, k) \in \mathbb{Z}^3$:

1. $n + m$ qui est entier donc $+$ définit une loi de composition interne sur $\mathbb{Z}$.
2. $(n + m) + k = n + (m + k)$ donc la loi $+$ est associative sur $\mathbb{Z}$.
3. $n + m = m + n$ donc la loi $+$ est commutative sur $\mathbb{Z}$.
4. $n + 0 = 0 + n = n$.
5. On a $n + (-n) = 0 = (-n) + n$.

On en déduit que tous les entiers sont inversibles dans $\mathbb{Z}$ pour la loi $+$.

Exercice 1 *Pour chaque couple $(E, \star)$ suivant, vérifier que $\star$ est une loi de composition interne sur E puis étudier ses propriétés : associativité, commutativité, élément neutre, éléments inversibles. Enfin, on exprimera le plus simplement possible les itérés $x^{\star n} = x \star x \star \cdots \star x$ en fonction de $x \in E$ et $n \in \mathbb{N}$.*

1. *$\star$ est définie dans $E = \mathbb{R}^\star \times \mathbb{R}$ et pour $(x, y) \in E, (x', y') \in E$, $(x, y) \star (x', y') = (xx', xy' + y)$.*
2. *$\star$ est définie dans $E =]0, +\infty[$ et pour $x, y' \in E$, $x \star y = \sqrt{x^2 + y^2}$.*
3. *$\star$ est définie dans $E =]-1, 1[$ et pour $x, y' \in E$, $x \star y = \dfrac{x + y}{1 + xy}$.*

2 Structure de groupe

Un groupe est un magma $(G, \star)$ pour lequel la loi de composition interne $\star$ est associative et dont l'ensemble des éléments sont inversibles. Cette notion apparait de façon omniprésente dans de multiples domaines des mathématiques.

2.1 Groupes et sous-groupes.

Définition: Groupe

Soit G un ensemble et $\star$ une loi de composition interne sur G. On dit que $(G, \star)$ est un *groupe* si :

- la loi $\star$ est associative.
- la loi $\star$ possède un élément neutre e.
- tout élément possède un symétrique.

Si de plus la loi $\star$ est commutative alors on dit que le groupe $(G, \star)$ est *abélien*.

Exemple

L'ensemble $\mathbb{Z}$ muni de la loi $+$ est un groupe abélien d'élément neutre 0. (cf exemple précédent).

Exercice 2 *Montrer que $(\mathbb{C}^\star, \times)$ est un groupe abélien.*
Est-ce que $(\mathbb{C}, \star)$ est un groupe ?

Exemple

Les deux familles suivantes sont des groupes abéliens de référence :

- les groupes additifs : $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$,$(\mathbb{Q}_+, +)$ $(\mathbb{R}, +)$ $(\mathbb{R}_+, +)$et $(\mathbb{C}, +)$.
- les groupes mutiplicatifs : $(\mathbb{Z}^\star, \times)$, $(\mathbb{Q}^\star, \times)$, $(\mathbb{R}^\star, \times)$ et $(\mathbb{C}^\star, \times)$.

Vocabulaire 1 *Soit x un élément d'un groupe G et $n \in \mathbb{N}$.*

— *Si G est un groupe additif on notera $n.x$ la n-ième itérée de l'élément x.*
— *Si G est un groupe multiplicatif on notera x^n la n-ième itérée de l'élément x.*

Exercice 3 *Montrer que $(\mathbb{U}, \times)$ et pour $n \in \mathbb{N}^\star$, $(\mathbb{U}_n, \times)$ sont des groupes multiplicatifs.*

Définition: Groupe de permutations

Soit X un ensemble. L'ensemble $S_X = \{\sigma : X \to X | \sigma \text{ bijective } \}$ est un groupe pour la loi de composition des applications notée $\circ$.

L'élément neutre de $(S_X, \circ)$ est l'identité $\begin{array}{rccc} Id : & X & \longrightarrow & X \\ & x & \longmapsto & x \end{array}$.

Exemple

Si $X = \{1; 2\}$ on a S_X qui est composée de deux bijections : l'identité et l'application qui permute 1 avec 2.

Nous étuiderons en profondeur cette famille de groupe pour $X = [\![1, n]\!]$ lorsque nous aborderons la notion de *déterminant* au second semestre en algèbre linéaire.

Pour $(G, \star)$ un groupe, il est naturel de se demander si une sous-partie $H \subset G$ induit sur H une structure de groupe, c'est-à-dire : Est-ce que $(H, \star)$ est un groupe ?

On introduit la notion de sous-groupe d'un groupe pour répondre à cette question.

Définition: Sous-groupe

Soit $(G, \star)$ un groupe et H un sous-ensemble de G. On dit que H est un *sous-groupe* de G, et on note $H < G$, si :

- H est stable pour la loi $\star$, c'est-à-dire pour tout $x, y \in H$, $x \star y \in H$.
- $(H, \star)$ forme un groupe.

Exemple

Pour $n \in \mathbb{Z}$, l'ensemble des multiples de n noté $n.Z = \{n.k | k \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$.

Théorème: Caractérisation des sous-groupes

Soit $(G, \star)$ un groupe. L'ensemble non vide $H \subset G$ est un sous-groupe de G si et seulement si :

1. $\forall x, y \in H$, $x \star y \in H$.
2. Pour tout $x \in H$, $x^{-1} \in H$ où x^{-1} désigne l'inverse de x dans G.

Exercice 4 *1. Montrer que $(\mathbb{C}^\star, \times)$ est un groupe.*

2. Montrer que $\mathbb{U}$ est un sous-groupe de $\mathbb{C}^\star$.

Théorème: Intersection de sous-groupes

Soit H et K deux sous-groupes de G. Alors $H \cap K$ est un sous-groupe de G.

Exemple

On a $3\mathbb{Z} \cap 5Z$ qui est un sous-groupe de $(\mathbb{Z}, +)$.

Risque d'erreur

Le théorème précédent est en général faux pour les réunions de sous-groupes. En effet, on a par exemple $3\mathbb{Z} \cup 5Z$ qui n'est pas un sous-groupe de $(\mathbb{Z}, +)$.

Théorème: Groupes produits

Soit H et K deux sous-groupes de $(G, \star)$. L'ensemble $HK = \{x \star y | x \in H, y \in K\}$ est un sous-groupe de G si et seulement si $HK = KH$.

Démonstration :admlse.

2.2 Morphismes de groupes

Définition: Morphisme de groupes

Soit $(G_1, \star)$ et $(G_2, \square)$ deux groupes. On dit que $\phi : G_1 \to G_2$ est un *morphisme de groupes* entre G_1 et G_2 si pour tout $x, y \in G_1$:

$$\phi(x \star y) = \phi(x) \square \phi(y).$$

Lorsque $G_1 = G_2$ et que leurs lois sont identiques on dit que ϕ est un *endomorphisme*. Un endomorphisme bijectif prend le nom d'*automorphisme*.

Théorème: Propriétés remarquables des morphismes

Soit $\phi : G \to G'$ un morphisme de groupes. Notons e le neutre de G et e le neutre de G'. Alors :

1. $\phi(e) = e'$.
2. $\forall x \in G$, $\phi(x^{-1}) = (\phi(x))^{-1}$.
3. Si H est un sous-groupe de G alors $f(H)$ est un sous-groupe de G'.
4. Si H' est un sous-groupe de G' alors $f^{-1}(H')$ est un sous-groupe de G.

Démonstration :

La composition, lorsqu'elle est compatible, fait de la composée de deux morphismes de groupes un morphisme de groupe.

Théorème: Composée de morphismes de groupes

Si $\varphi : G \to H$ et $\psi : H \to K$ sont des morphismes de groupes, alors la composée $\psi \circ \varphi : G \to K$ est un morphisme de groupes.

Démonstration :admise

Le théorème suivant fournit un critère pour déterminer si un morphisme de groupes est surjectif ou injectif.

Théorème: Critères d'injectivité et de surjectivité

Soit $\phi : G \to G'$ un morphisme de groupes. Alors :

- ϕ est surjectif si et seulement si $Im(\phi) = G'$.
- phi est injectif si et seulement si $Ker(\phi) = \phi^{-1}(\{e'\}) = \{e\}$.

Démonstration :

3 Structures d'anneau et de corps

On voit dans Z par exemple que l'on peut additionner des entiers mais aussi les multiplier. Dans cette partie on ajoute une seconde loi à un groupe de manière à dégager des propriétés algèbriques intéressantes sur le plan mathématique.

Définition: Distributivité
Soit E un ensemble muni de deux lois, $\star$ et $\square$. On dit que $\star$ est distributive sur $\square$ si pour tout $x, y, z \in E$:
$$x \star (y \square z) = (x \star y) \square (x \star z) \quad et \quad (x \square y) \star z = (x \star z) \square (y \star z).$$

3.1 Anneaux

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

1. $(A, +)$ est un groupe abélien. On note 0_A son élément neutre.
2. la loi $\times$ est associative.
3. la loi $\times$ est distributive par arpport à la loi $+$.
4. la loi $\times$ possède un élément neutre, noté 1_A.

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

Exemple
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des anneaux usuels pour les lois $+$ et $\times$.

Définition: Éléments inversibles d'un anneau
Soit $(A, \times)$ un anneau. On note $A^\star$ l'ensemble des éléments inversible pour la loi $\times$ dans A.

Proposition
Soit un anneau $(A, +, \times)$, le magma $(A^\star, \times)$ forme un groupe.

Les anneaux bénéficient de plus de souplesse que les groupes généraux pour faire des calculs :

Théorème: Formules dans les anneaux
Soit $n \in \mathbb{N}$ et $a, b \in A$ un anneau. On a alors :

1. $a^n - b^n = (b - a) \times \left(\sum_{k=0}^{n-1} a^k b^{n-1-k} \right)$.
2. (Binôme de Newton) $(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

Démonstration :admise.

3.2 Corps

Définition: Corps
Soit $(A, +\times)$ un anneau unitaire. On dit que A est un *corps* si tout élément différent de 0_A dans A admet un symétrique pour la loi $\times$.

Exemple
Les anneaux R et $\mathbb{Q}$ sont des corps mais $\mathbb{Z}$ n'en est pas un.

Proposition
Un corps est commutatif

3.3 Morphismes d'anneaux

Définition: Morphisme d'anneaux
Soit A et B deux anneaux. On dit que $f : A \to B$ est un *morphisme d'anneaux* si :

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