COURS D'ALGÈBRE 1

Docteur Cédric K. SOME

29 août 2022

Chapitre 3

Les structures algébriques

Sommaire

3.1 Loi de composition

3.1.1 Définitions

Définition 3.1.1 *Soit E un ensemble. On appelle loi de composition interne sur E ou opération dans E toute application de $E \times E$ vers E. L'image d'un couple (x, y) est appelée composée de x et y. Nous ne noterons de telles applications sous la forme $f(x, y)$ mais à l'aide de l'un des symboles : $*$, $\perp$, $\bullet, \cdots$*
Un ensemble E muni d'une loi de composition interne est noté $(E, *), (E, \perp), (E, \bullet), ...$

Définition 3.1.2 *Soit $(E, *)$ un ensemble muni d'une loi de composition interne et A une partie de E. On dit que A est stable par la loi $*$ si :*

$$\forall x, y \in A,\ x * y \in A.$$

Dans ce cas, la restriction de la loi$*$ - à A est appelée loi induite.

Exemple 3.1.1

- *L' addition et la multiplication sont des lois de composition internes sur $\mathbb{R}$.*
- *L'union et l'intersection sont des lois de composition internes dans $\mathcal{P}(E)$.*
- *Dans $\mathbb{N}^*$, la loi $\perp$ définie par $x \perp y = x^y + 1$ est une loi de composition interne.*

3.1.2 Lois particulières, éléments particuliers

Définition 3.1.3 *Soient $(E, *)$ une loi de composition interne.*
- *On dit que $*$ est associative si : $\forall x, y, z \in E, x * (y * z) = (x * y) * z$.*
- *On dit que $*$ est commutative si : $\forall x, y \in E,\ x * y = y * x$.*
- *On dit que deux éléments x et y commutent si $x * y = y * x$.*
- *Un élément e de E est dit neutre si : $\forall x \in E,\ x * e = e * x = x$.*
- *Un élément x de E est dit symétrisable à gauche (respectivement à droite) s'il existe x' dans E tel que $x' * x = e$ (respectivement $x * x' = e$).*
- *On dit que x est symétrisable si x est symétrisable à gauche et à droite ; dans ce cas on dit que x et x' sont symétriques.*
- *Un élément a de E est dit régulier ou simplifiable à gauche (respectivement à droite) si $\forall x, y \in E, a * x = a * y \Longrightarrow x = y$ (respectivement $x * a = y * a \Longrightarrow x = y$).*

Exemple 3.1.2
- *L'addition et la multiplication sont des lois de composition interne, commutatives et associatives de $\mathbb{R}$.*
- *Dans $\mathbb{N}^*$, la loi $\perp$ définie par $x \perp y = x^y + 1$ n'est pas commutative car :*
  $3 \perp 4 = 3^4 + 1 = 81 + 1 = 82$ *et* $4 \perp 3 = 4^3 + 1 = 48 + 1 = 49$. $82 \neq 49 \Longleftarrow 3 \perp 4 \neq 4 \perp 3$.
  Par conséquent, la loi $\perp$ n'est pas commutative dans $\mathbb{R}$.

Remarque 3.1.1
- *Le symétrique d'un élément est unique s'il existe.*
- *Lorsque la loi est notée additivement son élément neutre sera 0 et le symétrique d'un élément x est noté $-x$ et est appelé opposé de x.*
- *Lorsque la loi est notée multiplicativement son élément neutre sera noté 1 et le symétrique d'un élément x est noté x^{-1} et appelé inverse de x.*
- *L'élément neutre est unique s'il existe et son symétrique est lui même.*
- *Le symétrique.*
- *le symétrique de $x * y$ s'il existe est $y^{-1} * x^{-1}$.*

Définition 3.1.4 *Soient $(E, *)$ un ensemble muni d'une loi de composition interne et $\mathcal{R}$ une relation sur E.*
- *On dit que $*$ est compatible avec $\mathcal{R}$:*

$$\forall x, x', y, y' \in E,\ (x \mathcal{R} x' \text{ et } y \mathcal{R} y' \Longrightarrow x * y \mathcal{R} x' * y').$$

- *Si $\mathcal{R}$ est une relation d'équivalence sur E et E/R l'ensemble des classes d'équivalence alors on définit sur E/R la loi $\overline{*0}$:*

$$\forall x, y \in E/R,\ x \overline{*} y = \overline{x * y}$$

*La loi $\overline{*}$ est appelé **loi quotient** de la loi $*$.*

Exemple 3.1.3
L'addition et l'égalité sont compatibles dans $\mathbb{R}$ car

$$\forall x, x', y, y' \in \mathbb{R}, (x = x' \text{ et } y = y') \Longrightarrow (x + x\prime = y + y').$$

Exercice 3.1.1 *On définit sur* $\mathbb{R}$ *la loi* $*$ *par :*

$$x * yxy - x - y + 2$$

1. Montrer que $*$ *est une loi de composition interne, associative et commutative.*
2. Montrer que $*$ *admet un élément neutre que l'on déterminera.*
3. En déduire l'ensemble des éléments inversibles de $\mathbb{R}$ *par rapport à* $*$*.*

3.2 Groupes et morphismes de groupes

3.2.1 Groupes

Définition 3.2.1
Un groupe est un ensemble non vide muni d'une loi de composition interne, associative, admettant un élément neutre et tout élément est symétrisable. Si de plus la loi est commutative on dit qu'on a un groupe commutatif ou groupe abélien.

Exemple 3.2.1
- $(\mathbb{R}, +)$, $(\mathbb{R}^*, \times)$ *et* $(\mathbb{Z}, +)$ *sont des groupes abéliens.*
- *L'ensemble des vecteurs du plan muni de l'addition est un groupe abélien.*
- $(N, +)$ *et* $(\mathbb{R}, \times)$ *ne sont pas des groupes.*

Théorème 3.2.1 *Dans un groupe tout élément est régulier.*

Exercice 3.2.1 *Faire la table de multiplication d'un groupe à trois éléments.*

Exercice 3.2.2 *Soit* $(G, *)$ *un groupe d'élément neutre* e *tel que*

$$\forall x \in G, x^2 = x * x = e$$

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

3.2.2 Sous-groupe

Définition 3.2.2 *Un sous groupe d'un groupe* $(G, *)$ *est une partie non vide* H *de* G *telle que* H *muni de la loi induite* $*$ *soit un groupe.*

Exemple 3.2.2 $(\mathbb{Z}, +)$ *est un sous groupe de* $(\mathbb{R}, +)$*.*

Théorème 3.2.2 ***(Théorème de caractérisation)***
Soit $(G, *)$ *un groupe et* H *une partie de* G*. Les propriétés suivantes sont équivalentes :*

(i) H *est un sous groupe de* G*.*

(ii) $H \neq \emptyset$; $\forall x, y \in H, x * y \in H$ *et* $\forall x \in H,\ x^{-1} \in H$ *où* x^{-1} *est le symétrique de* x*.*

(iii) $H \neq \emptyset$ *et* $\forall x, y \in H,\ x * y^{-1} \in H$ *où* y^{-1} *est le symétrique de* y*.*

Remarque 3.2.1
Si $(G, *)$ *est un groupe d'élément neutre* e *alors* $\{e\}$ *et* G *sont des sous-groupes de* G*.*

Théorème 3.2.3 *L'intersection de deux sous groupes d'un groupe G est un sous groupe de G.*

Définition 3.2.3 *Soient $(G, *)$ un groupe et A une partie non vide de G.*
- *On appelle sous-groupe engendré par A le plus petit sous-groupe de G contenant A. On le note $\langle A \rangle$.*
- *On dira que A est une partie génératrice de G si le sous-groupe engendré par A est G.*
- *On dira que $(G, *)$ est un groupe monogène si G est engendré par un seul élément.*
- *Un groupe cyclique est un groupe monogène fini.*

Exercice 3.2.3
Soit $(G, *)$ un groupe d'élément neutre e. Un élément a de G est dit élément de torsion si, et seulement si, il existe $n \in \mathbb{N}$ tel que $a^n = e$. Montrer que les éléments de torsion d'un groupe abélien est un sous groupe abélien.

3.3 Morphismes de groupes

Définition 3.3.1
Soient $(G, *)$ et $(G', \perp)$ deux groupes.On appelle morphisme de groupes de G dans G' toute application f de G dans G' vérifiant :

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

Si de plus l'application f est bijective on dit que f est un isomorphisme. Dans ce cas, on dit que G et G^* sont isomorphes et on note $G \cong G^*$.
Un endomorphisme est un morphisme d'un groupe dans lui même et un automorphisme est un endomorphisme bijectif.

Exemple 3.3.1 *La fonction* ln *est un morphisme de groupes de $(\mathbb{R}_+^*, \times)$ vers $(\mathbb{R}, +)$.*

Remarque 3.3.1
L'ensemble des morphismes de G dans G' est noté $Hom(G; G')$.
L'ensemble des endomorphismes de G est noté $End(G)$.
L'ensemble des automorphismes de G est noté $Aut(G)$.

Proposition 3.3.1
Soient $(G, *)$ et $(G', \perp)$ deux groupes d'élément neutre respectif e et e' et f un morphisme de G dans G'. On a les résultats suivants :
- *$f(e) = e'$*
- *$\forall x \in G,\ f(x^{-1}) = (f(x))^{-1}$.*
- *Si H est un sous-groupe de G alors $f(H)$ est un sous-groupe de G'.*
- *Si H' est un sous-groupe de G' alors $f^{-1}(H)$ est un sous-groupe de G.*

Définition 3.3.2
Soient $(G, *)$ et $(G', \perp)$ deux groupes d'élément neutre respectif e et e' et f un morphisme de G dans G'.
On appelle noyau de f noté $ker\,(f)$, le sous-groupe de G défini par

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

Proposition 3.3.2 *Soit $f \in Hom(G, G')$. f est injectif si, et seulement si, $ker(f) = \{e\}$.*

Exercice 3.3.1
Soit $(G, *)$ un groupe, a un élément de G et a' le symétrique de a. On définit une loi de composition interne $\perp$ sur G par :

$$x \perp y = x * a * y.$$

1. Montrer que $(G, \perp)$ est un groupe.
2. Montrer que l'application $f : x \longmapsto x * a'$ est un isomorphisme de $(G, *)$ vers $(G, \perp)$.

3.3.1 Groupes symétriques

Définition 3.3.3 *Soit E un ensemble fini. On appelle permutation de E toute bijection de E dans E. L'ensemble des permutations de E est noté $\mathcal{S}(E)$.*

Remarque 3.3.2 *$(\mathcal{S}(E), \circ)$ est un groupe commutatif.*
Si $E = \{1, 2, \cdots, n\}$ alors $(\mathcal{S}(E), \circ)$ est noté $\mathcal{S}_n$ et est appelé groupe symétrique d'ordre n.
Pour toute permutation $\sigma \in \mathcal{S}_n$, on note :

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

pour signifier que σ est la bijection $\sigma : k \longmapsto \sigma(k)$.
Avec cette notation, on calcule facilement la composition et l'inverse de toute permutation de $\mathcal{S}_n$.

Exemple 3.3.2

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 2 & 1 \end{pmatrix}$$

et

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 2 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 1 & 3 \end{pmatrix}$$

Définition 3.3.4 *Soit r un entier compris entre 2 et $card(E)$. On appelle cycle d'ordre r ou $r-$cycle toute permutation $\sigma \in \mathcal{S}(E)$ qui permute circulairement r éléments de E et laisse fixe les autres éléments de E ; c'est-à-dire qu'il existe une partie $\{x_1, x_2, \cdots, x_r\}$ de E telle que*

$$\begin{cases} \forall k \in \{1, 2, \cdots, r\}, \sigma(x_k) &= x_{k+1} \\ \sigma(x_r) &= x_1 \\ \forall x \notin \{x_1, x_2, \cdots, x_r\} \text{ et } x \in E, \ \sigma(x) &= x \end{cases}$$

On note $\sigma = (x_1, x_2, \cdots, x_r)$ un tel cycle et $\{x_1, x_2, \cdots, x_r\}$ est appelé le support de σ. Ce support se note $supp(\sigma)$.

Exemple 3.3.3 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}$ *permute circulairement* $\{1,3,4\}$ *et laisse fixe* $\{2,5\}$. *Donc* $\sigma = (134)$ *est un cycle d'ordre 3 et* $supp(\sigma) = \{1,2,3\}$.

Remarque 3.3.3
Les r permutations $(x_1, x_2, \cdots, x_r), (x_2, \cdots, x_r, x_1), (x_3, x_4, \cdots, x_r, x_1, x_2), \cdots, (x_r, x_1, \cdots, x_{r-1})$ *définissent le même* $r-$*cycle.*
Le produit de deux cycles de supports disjoints est commutatif.
Si σ *est un r-cycle alors pour tout entier naturel n,* $\sigma^n = \sigma^i$ *où* $n = qr + i$ *avec* $0 \leq i \leq r-1$.

Définition 3.3.5 *On appelle transposition un cycle d'ordre deux.*

Exemple 3.3.4 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix} = (1\ 3)$ *est une transposition.*

Théorème 3.3.1 *Soient* σ *une permutation de* E *et* $x \in E$. *On appelle* $\sigma-$*orbite de* x, *l'ensemble* $Orb_\sigma(x) = \{y \in E \mid \exists k \in \mathbb{N},\ y = \sigma^k(x)\}$.

Exemple 3.3.5 *Soit* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}$. *On a,* $Orb_\sigma(x) = \{3,4,1\}$.

Théorème 3.3.2 *Toute permutation* $\sigma \in \mathcal{S}(E)$ *se décompose en produit de cycles deux à deux disjoints (c'est-à-dire de supports disjoints). Cette décomposition est unique à l'ordre près.*

Théorème 3.3.3 *Tout* $r-$*cycle se décompose en produit de* $r-1$ *transpositions.*

Exemple 3.3.6 *Soit* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 5 & 9 & 7 & 6 & 3 & 8 & 2 \end{pmatrix}$. *On a :*

$$\sigma = \begin{pmatrix} 1 & 4 & 9 & 2 \end{pmatrix} \circ \begin{pmatrix} 3 & 5 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 4 & 9 \end{pmatrix} \circ \begin{pmatrix} 9 & 2 \end{pmatrix} \circ \begin{pmatrix} 3 & 5 \end{pmatrix} \circ \begin{pmatrix} 5 & 7 \end{pmatrix}$$

Définition 3.3.6 *Soit* $\sigma \in \mathcal{S}(E)$. *On appelle signature de* σ *le nombre* $\varepsilon(\sigma) \in \{-1,1\}$ *défini par :*

$$\varepsilon(\sigma) = (-1)^{n-\mu(\sigma)}$$

où $\mu(\sigma) = p + \varphi(\sigma)$ *avec* p *le nombre de* $\sigma-$*orbite non réduite(s) à un point et* $\varphi(\sigma)$ *est le nombre de point(s) fixe(s) de* σ.

Exemple 3.3.7 *Soit* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 5 & 9 & 7 & 6 & 3 & 8 & 2 \end{pmatrix}$
$\varepsilon(\sigma) = (-1)^{9-\mu(\sigma)}$ *avec* $\mu(\sigma) = 2 + 2 = 4$. *Donc* $\varphi(\sigma) = -1$.

Exercice 3.3.2 *Soit* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 5 & 7 & 4 & 1 & 10 & 3 & 8 & 6 & 9 \end{pmatrix}$ *une permutation de* $\mathcal{S}_{10}$.
1. Décomposer σ *en produit de cycles.*
2. Décomposer σ *en produit de transpositions.*
3) Donner la signature de σ.

3.4 Anneaux et corps

3.4.1 Anneaux

Définition 3.4.1 *Soit A un ensemble muni d'une loi additive notée $+$ et d'une loi multiplicative notée $\times$. $(A, +, \cdot)$ est un anneau si :*

- *si $(A, +)$ est un groupe abélien ;*
- *la multiplication est associative*

$$\forall x, y, z \in A \, , x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

- *la multiplication est distributive par rapport à l'addition :*

$$\forall x, y, z \in A, \; x \cdot (y + z) = x \cdot y + x \cdot z \;\; et \;\; (y + z).x = y.x + z.x$$

Si de plus la multiplication est commutative, on dit que A est un anneau commutatif. Lorsque la multiplication possède un élément neutre, on dit que l'anneau A est unitaire.

Exemple 3.4.1 $(\mathbb{Z}, +, \cdots), (\mathbb{R}, +, \cdots)$ *sont des anneaux commutatifs unitaires.*

Remarque 3.4.1 *Dans un anneau, tout élément admet un symétrique par rapport à la première loi $+$ mais n'admet pas nécessairement de symétrique par rapport à la deuxième loi $\cdot$.*

Proposition 3.4.1
Soient $(A, +, \cdot)$ un anneau unitaire, $a, b \in A$ et $n \in \mathbb{Z}$. Soient 0_A l'élément neutre pour la loi additive et 1_A l'élément neutre pour la loi multiplicative. On les propriétés suivantes :

- $0_A.a = a.0_A = 0_A$ *; on dit que 0_A est un élément absorbant.*
- *si $card(A) > 1$ alors $0_A \neq 1_A$, on dit que A est non nul.*
- $a.(-b) = (-a).b = -(ab)$.
- $1_A.a = a.1_A = a$.
- $(-a).(-b) = ab$.
- $(na).b = n(a.b)$.

Proposition 3.4.2
Soit $(A, +, \cdot)$ un anneau commutatif. Soient $x, y, y_i \in A$ avec $i = 1, \cdots, n$. On a :

- $x \left(\sum_{i=1}^{n} y_i \right) = \sum_{i=1}^{n} x y_i \quad et \quad \left(\sum_{i=1}^{n} y_i \right) x = \sum_{i=1}^{n} y_i x$.
- *Formule de binôme de Newton :*

$$(x + y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k} \;\; et \;\; x^n - y^n = (x - y) \left(\sum_{k=0}^{n-1} x^{n-k-1} y^k \right)$$

Définition 3.4.2
Soient $(A, +, \cdot)$ un anneau non nul et $a_i n A^* = A \setminus \{0_A\}$.

- *On dit que a est un diviseur de zéro à gauche (respectivement à droite) s'il existe $b \in A^*$ tel que $a.b = 0_A$ (respectivement $b.a = 0_A$).*
- *On dit que A est un anneau intègre si A est un anneau non nul, commutatif et sans diviseur de zéro c'est-à-dire :*

$$\forall x, y \in A, \; x.y = 0_A \implies x = 0_A \; ou \; y = 0_A.$$

- *On dit qu'un élément $a \in A^*$ est nilpotent s'il existe $k \in \mathbb{N}$ tel que $a^k = 0_A$.*
  Le plus petit entier k_0 tel que $a^{k_0} = 0_A$ est appelé indice de nilpotence de a.

Définition 3.4.3 *Soient $(A, +, \cdot)$ un anneau et B une partie de A. On dit que B est un sous-anneau de A si $(B, +; \cdot)$ a une structure d'anneau.*

Théorème 3.4.1 ***(Caractérisation)***
Soient $(A, +, \cdot)$ un anneau et B une partie non vide de A. Les propriétés suivantes sont équivalentes :
- *B est un sous anneau de A.*
- *$\forall x, y \in B, x + y \in B, -x \in B, x.y \in B$.*
- *$\forall x, y \in B, x - y \in B, -x.y \in B$.*

Remarque 3.4.2 *$(\mathbb{Z}, +, \cdot)$ est un sous-anneau de $(\mathbb{R}, +, \cdot)$.*

Définition 3.4.4 *Soient $(A, +, \cdot)$ un anneau et I une partie de A*
- *On dit que I est un idéal à gauche de A si et seulement si : $(I, +)$ est un sous-groupe de $(A, +)$ et $I.A \subset I$ c'est-à-dire ; $\forall x \in I, \forall a \in A, x.a \in I$.*
- *On dit que I est un idéal à droite de A si et seulement si : $(I, +)$ est un sous-groupe de $(A, +)$ et $A.I \subset I$ c'est-à-dire ; $\forall x \in I, \forall a \in A, a.x \in I$.*
- *On dit que I est un idéal si I est un idéal à gauche et à droite de A.*

Remarque 3.4.3 *Si $(A, +, \cdot)$ un anneau, alors :*
- *$\{0_A\}$ et A sont des idéaux triviaux de A. Tout autre idéal de A est appelé idéal propre de A.*
- *Tout idéal de A contenant 1_A est confondu à A.*
- *L'intersection de deux idéaux de A est un idéal de A.*

Exemple 3.4.2 *$\forall \in \mathbb{N}$, $n\mathbb{Z}$ est un idéal de $(\mathbb{Z}, +, \cdot)$.*

Définition 3.4.5 *Soit $(A, +, \cdot)$ un anneau.*
- *On appelle idéal engendré par une partie H de A le plus petit idéal contenant H.*
- *Un idéal principal est un idéal engendré par un élément et un anneau principal est un anneau intègre dans lequel tout idéal est principal.*

Définition 3.4.6 *Soient $(A, +, \cdot)$ et $(A', *, \perp)$ deux anneaux.*
Une application f de A vers A' est un morphisme d'anneaux si :
- *f est un morphisme de groupes de $(A, +)$ vers $(A', *)$;*
- *$f(x.y) = f(x) \perp f(y)$, $\forall x, y \in A$.*

Proposition 3.4.3 *Soient f un morphisme d'anneaux de $(A, +, \cdot)$ vers $(A', *, \perp)$ et $a \in A$. On a :*
- *$f(0_A) = 0_{A'}$ et $f(-a) = -f(a)$.*
- *$f(na) = nf(a)$ et $f(a^n) = (f(a))^n$, $\forall n \in \mathbb{N}$.*
- *$\ker(f)$ est un idéal de A.*
- *Si I est un idéal de A alors $f(I)$ est un idéal de A'.*
- *Si I' est un idéal de A' alors $f^{-1}(I')$ est un idéal de A.*

3.4.2 Corps

Définition 3.4.7 *Un corps A est un anneau non nul dont tout élément non nul soit symétrisable par rapport à la deuxième loi ; c'est-à-dire :*

$$\forall x \in A^*, \exists x^{-1} \in A^* \mid x.x^{-1} = x^{-1}.x = 1_A.$$

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