Complément 5

Structures algébriques

Introduction

Ce complément de cours a pour but d'introduire le vocabulaire associé aux structures algébriques rencontrées durant l'année. Les notions de groupes, anneaux, corps, algèbres sont hors programme en PCSI. On se contente ici de donner les principales définitions et de nombreux exemples tirés du cours de première année.

Mathieu Mansuy - Professeur de Mathématiques en supérieures PCSI au Lycée Saint Louis (Paris)
mansuy.mathieu@hotmail.fr

1 Groupes

1.1 Définition

Définition.

Soit G un ensemble non vide pour lequel on définit $*$ une **loi de composition interne** (LCI), c'est à une relation binaire telle que :

$$* : (x, y) \in G \times G \mapsto x * y \in G$$

On dit que $(G, *)$ est un **groupe pour la loi** $*$ si :

- cette loi est **associative** : $\forall\, x, y, z \in G,\ x * (y * z) = (x * y) * z$
- cette loi possède un **élément neutre** : $\exists\, e \in G,\ \forall\, x \in G,\ x * e = e * x = x$
- tout élément admet un **symétrique** par cette loi : $\forall\, x \in G,\ \exists\, sym(x) \in G,\ x * sym(x) = sym(x) * x = e$

Si la loi $*$ est **commutative**, c'est à dire : $\forall\, x, y \in G,\ x * y = y * x$, on pourra dire que $(G, *)$ est un **groupe commutatif** ou **abélien**.

Propriété 1 (unicité des éléments remarquables)

Soit $(G, *)$ un groupe. Alors,

(1) l'élément neutre e associé est unique.

(2) pour tout élément $x \in G$, le symétrique de x est unique.

Preuve.

(1) Si e, e' sont des éléments neutres pour $(G, *)$, on a :

$$e = e * e' = e'$$

(2) Soit $x \in G$, et y, y' des symétriques de x dans $(G, *)$. Alors :

$$y = y * e = y * (x * y') = (y * x) * y' = e * y' = y'.$$

□

Notation. Étant donné un groupe, sa loi de composition interne sera souvent notée :

- $+$ si celle-ci est commutative et dans ce cas, $e = 0_G$ et $sym(x) = -x$ appelé **opposé de** x.
- $.$ si on n'a pas d'information sur sa commutativité et dans ce cas, $e = 1_G$ et $sym(x) = x^{-1}$ appelé **inverse de** x.

Exemples. De nombreux exemples de groupes ont été rencontrés durant l'année. En voici une liste non exhaustive :

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sont des groupes commutatifs, l'élément neutre est $e = 0$.
- $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ sont des groupes commutatifs, l'élément neutre est $e = 1$.
- $(\mathbb{N}, +)$, $(\{-1, 0, 1\}, +)$, $(\{-1, 0, 1\}, \times)$ ne sont pas des groupes puisque :

- ▷ 1 n'a pas de symétrique dans $(\mathbb{N}, +)$;
- ▷ $1 + 1 = 2 \notin \{-1, 0, 1\}$ ($+$ n'est pas une LCI de $\{-1, 0, 1\}$) ;
- ▷ 0 n'a pas d'inverse dans $(\{-1, 0, 1\}, \times)$.

- Soit E un ensemble fini de cardinal $n \geq 2$. Notons $S(E)$ l'ensemble des bijections (ou **permutations**) de E dans E. Alors $(S(E), \circ)$ est un groupe (non commutatif si $n \geq 3$) appelé **groupe symétrique** de E (où $\circ$ désigne la composition des applications). L'élément neutre est l'application identité $e = Id_E$.

  Vous avez rencontré ce groupe en informatique, et on l'a évoqué dans les chapitres de dénombrement et déterminants. Rappelons que si $Card(E) = n$, alors on connait le cardinal de $S(E)$:

  $$Card(S(E)) = n!$$

- Soit $n \geq 2$. L'ensemble $GL_n(\mathbb{K})$ des matrices inversibles à coefficients dans $\mathbb{K}$ est un groupe non commutatif pour le produit matriciel (ce n'est pas un groupe pour l'addition matricielle !). L'élément neutre est $e = I_n$.

1.2 Sous-groupes

Définition.

Soit G un groupe, et $H \subset G$. On dit que H est un sous groupe de G si

$$\begin{cases} e \in H \text{ (élément neutre)} \\ \forall\, x, y \in H,\ x * y \in H \text{ (stabilité pour la loi induite)} \\ \forall\, x \in H,\ sym(x) \in H \text{ (stabilité par passage aux symériques)} \end{cases}$$

Remarque. $\{e\}$, G sont des sous groupes de $(G, *)$.

Exemples.

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

  Pour tout $n \geq 2$, l'ensemble $\mathbb{U}_n$ des racines n-ièmes de l'unité est un sous-groupe de $(\mathbb{C}^*, \times)$ (et de $(\mathbb{U}, \times)$ aussi).
- Soit $n \geq 2$. L'ensemble $O_n(\mathbb{R})$ des matrices orthogonales de taille $n \times n$ est un sous groupe de $GL_n(\mathbb{R})$.

  L'ensemble $SO_n(\mathbb{R})$ des matrices orthogonales directes est un sous-groupe de $O_n(\mathbb{R})$.
- Notons $\mathcal{D}_n^*(\mathbb{K})$ (resp. $(\mathcal{T}_n^{\pm})^*(\mathbb{K})$) l'ensemble des matrices diagonales inversibles (resp. triangulaires supérieures/inférieures inversibles). Alors $D_n^*(\mathbb{K}), (\mathcal{T}_n^{\pm})^*(\mathbb{K})$ sont des sous groupes de $GL_n(\mathbb{K})$.

Exercice. On montre dans cet exercice que les sous-groupes de $(\mathbb{Z}, +)$ sont les ensembles de la forme $n\mathbb{Z} = \{kn, k \in \mathbb{Z}\}$ avec $n \geq 0$.

a) Montrer que pour tout $n \geq 0$, nZ est un sous groupe de Z.

b) Soit H un sous groupe de $(\mathbb{Z}, +)$, $H \neq \{0\}$.

(i) Montrer que la partie $H \cap \mathbb{N}^*$ possède un plus petit élément. On note a cet élément.

(ii) Montrer que $a\mathbb{Z} \subset H$.

(iii) Montrer que $H \subset a\mathbb{Z}$ (penser à utiliser la division euclidienne).

Solution.

a) On montre les différents points définissant un sous-groupe de $(\mathbb{Z}, +)$:

- $0 = 0 \times n \in n\mathbb{Z}$;
- Soient $a, b \in n\mathbb{Z}$, il existe $k, l \in \mathbb{Z}$ tels que $a = kn$ et $b = ln$. Alors $a+b = kn+ln = (k+l)n \in n\mathbb{Z}$;
- Soit $a \in n\mathbb{Z}$, il existe $k \in \mathbb{Z}$ tel que $a = kn$. Alors $sym(a) = -a = -kn = (-k)n \in n\mathbb{Z}$.

Ainsi $n\mathbb{Z}$ est bien un sous groupe de $\mathbb{Z}$.

b) (i) Par hypothèse $H \neq \{0\}$, donc il existe $h \in H$ tel que $h \neq 0$. Si $h > 0$, c'est bon. Sinon, comme H est un groupe, on a $sym(h) = -h \in H$ et $-h > 0$. Dans tous les cas on a donc que $H \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}^*$. Elle possède donc un plus petit élément a.

(ii) Puisque $a \in H$ et que H est un sous groupe, on a aussi $sym(a) = -a \in H$. On montre alors par une récurrence (à faire) que pour tout $k \in \mathbb{N}$, ka et $-ka$ appartiennent à H. Ainsi $a\mathbb{Z} \subset H$.

(iii) Soit $h \in H$. Montrons que $h \in a\mathbb{Z}$. Faisons la division euclidienne de h par a : il existe $q, r \in \mathbb{Z}$ tels que :

$$h = qa + r \text{ et } 0 \leq r < a.$$

On a $h \in H$, $qa \in a\mathbb{Z} \subset H$. Puisque H est un sous groupe, on en déduit que $r = h - qa$ appartient à H. Par minimalité de a, on en déduit que $r = 0$. Ainsi on a bien $h = qa$, et donc $h \in a\mathbb{Z}$.

On a ainsi montré que tout sous groupe de $(\mathbb{Z}, +)$ est de la forme $n\mathbb{Z}$ avec $n \geq 0$ (résultat qu'il est intéressant de retenir).

1.3 Morphismes de groupes

Définition.

Soient $(G_1, *)$ et $(G_2, \perp)$ deux groupes et une application $f : G_1 \to G_2$. On dit que f est un **morphisme de groupes** si elle respecte les lois associées, c'est à dire :

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

En particulier,

- on dit que f est un **isomorphisme** s'il s'agit d'un morphisme bijectif ;
- on dit que f est un **endomorphisme** si $G_1 = G_2$;
- on dit que f est un **automorphisme** s'il s'agit d'un endomorphisme bijectif.

Propriété 2 (images des éléments remarquables)

Soient $(G_1, .)$ et $(G_2, *)$ deux groupes et un morphisme $f : G_1 \to G_2$. Alors, en notant e_1, e_2 les éléments neutres associés aux lois . et $*$:

(1) $f(e_1) = e_2$

(2) pour tout $x \in G_1$, $f(x^{-1}) = [f(x)]^{-1}$

Preuve.

(1) On a $f(e_1) = f(e_1 * e_1) = f(e_1) \perp f(e_1)$. D'où en multipliant à gauche par $f(e_1)^{-1}$:

$$f(e_1) = e_2$$

(2) Soit $x \in G_1$. On a :

$$f(x^{-1}) \perp f(x) = f(x^{-1} * x) = f(e_1) = e_2.$$

De même, on a $f(x) \perp f(x^{-1}) = e_2$. Par unicité du symétrique de $f(x)$, on a bien $f(x)^{-1} = f(x^{-1})$.

□

Exemples. Là aussi, de nombreux exemples ont été rencontrés au cours de cette année :

- Le logarithme ln est un morphisme de groupes de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$ puisque :

  $$\forall a, b \in \mathbb{R}_+^*, \quad ln(ab) = ln(a) + ln(b).$$

  De même, l'exponentielle est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$.

  Il s'agit en fait d'isomorphismes, réciproques l'un de l'autre.

- L'application $\theta \in \mathbb{R} \to e^{i\theta} \in \mathbb{U}$ est un morphisme de groupes surjectif de $(\mathbb{R}, +)$ dans $(\mathbb{U}, \times)$.
- L'application déterminant det : $GL_n(\mathbb{K}) \to \mathbb{K}^*$ est un morphisme de groupes surjectif de $(GL_n(\mathbb{K}), \times)$ dans $(\mathbb{K}^*, \times)$.

2 Anneaux

2.1 Définition

Définition.

Soit A un ensemble non vide pour lequel on définit $+$ et $\times$ deux lois de composition interne.
On dit que $(A, +, \times)$ est un **anneau** si :

- $(A, +)$ est un groupe commutatif, d'élément neutre noté 0_A ;
- la loi $\times$ est **associative**: $\forall\, x, y, z \in A,\ x \times (y \times z) = (x \times y) \times z$;
- la loi $\times$ possède un **élément neutre** noté 1_A : $\forall\, x \in A,\ x \times 1_A = 1_A \times x = x$;
- la loi $\times$ est **distributive** par rapport à $+$: $\forall\, x, y, z \in A,\ x \times (y + z) = x \times y + x \times z$ et $(y + z) \times x = y \times x + z \times x$.

Si de plus la loi $\times$ est **commutative**, c'est à dire si $\forall\, x, y \in A,\ x \times y = y \times x$, on dira que $(A, +, \times)$ est un **anneau commutatif**.

Exemples. Voici des exemples d'anneaux rencontrés pendant l'année.

- $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs.
- $(\mathbb{K}[X], +, \times)$ est un anneaux commutatif.
- $(\mathbb{K}^{\mathbb{N}}, +, \times)$ est un anneau commutatif, où :

  $$u \times v = (u_n \times v_n)_{n \in \mathbb{N}}.$$

  Ici on a $0_A = (0)_{n \in \mathbb{N}}$ et $1_A = (1)_{n \in \mathbb{N}}$.

- $(\mathcal{F}(I,\mathbb{K}),+,\times)$ est un anneau commutatif, où I qui désigne un intervalle de $\mathbb{R}$ et :

$$\forall x \in I, (f \times g)(x) = f(x) \times g(x).$$

  Ici 0_A est l'application identiquement nulle et 1_A l'application constante égale à 1.

- $(\mathcal{M}_n(\mathbb{K}),+,\times)$ est un anneau non commutatif si $n \geq 2$.

Définition.

On dit que l'anneau $(A,+,\times)$ est **intègre** si :

$$\forall\, x,y \in A,\ x \times y = 0_A \Leftrightarrow x = 0_A \text{ ou } y = 0_A.$$

Remarque. L'anneau des matrices $(\mathcal{M}_n(\mathbb{K}),+,\times)$ n'est pas intègre, tout comme $(\mathcal{F}(I,\mathbb{K}),+,\times)$ et $(\mathbb{K}^{\mathbb{N}},+,\times)$. Les autres anneaux cités plus haut sont tous intègres.

2.2 Sous-anneaux

Définition.

Soient $(A,+,\times)$ un anneau et $B \subset A$. On dit que B est un **sous-anneau de** A si

$$\begin{cases} 1_A \in B \\ \forall\, x,y \in B,\ x - y \in B & ((B,+) \text{ est un sous groupe de } (A,+)) \\ \forall\, x,y \in B,\ x \times y \in B & \text{(stabilité pour la loi } \times) \end{cases}$$

Exemples.

- $(\mathbb{Z},+,\times)$ est un sous anneau de $(\mathbb{Q},+,\times)$.
- L'ensemble des suites bornées est un sous-anneau de $(\mathbb{K}^{\mathbb{N}},+,\times)$.
- $\mathcal{C}^0(I,\mathbb{K})$, $\mathcal{C}^1(I,\mathbb{K})$, ... sont des sous anneaux de $(\mathcal{F}(I,\mathbb{K}),+,\times)$.
- $\mathcal{D}_n(\mathbb{K}), \mathcal{T}_n^{\pm}(\mathbb{K})$ sont des sous-anneaux de $\mathcal{M}_n(\mathbb{K})$.

2.3 Morphismes d'anneaux

Définition.

Soient $(A_1,+,\times)$ et $(A_2,+,\times)$ deux anneaux et une application $f : A_1 \to A_2$. On dit que f est un **morphisme d'anneaux** si elle respecte les lois associées, c'est à dire :

$$\forall\, x,y \in A_1,\ f(x+y) = f(x) + f(y)\ ,\ \forall\, x,y \in A_1,\ f(x \times y) = f(x) \times f(y)\ ,\ f(1_{A_1}) = 1_{A_2}$$

En particulier,

- on dit encore que f est un **isomorphisme** s'il s'agit d'un morphisme bijectif.
- on dit encore que f est un **endomorphisme** s'il s'agit d'un morphisme de A_1 dans lui-même.
- on dit encore que f est un **automorphisme** s'il s'agit d'un endomorphisme bijectif.

2.4 Eléments inversibles et corps

Définition.

Soit $(A, +, .)$ un anneau. On dit qu'un élément $a \in A^*$ est **inversible** s'il admet un inverse par la loi $\times$, c'est à dire s'il existe $y \in A$ tel que :

$$x \times y = y \times x = 1_A$$

L'inverse de x est unique, noté x^{-1}.

Remarque. On note en général $U(A)$ l'ensemble des éléments inversibles de A. On peut montrer que $(U(A), \times)$ est un groupe, appelé **groupe des éléments inversibles**.

Exemples.

- $U(\mathbb{Z}) = \{1, -1\}$, $U(\mathbb{R}) = \mathbb{R}^*$, $U(\mathbb{C}) = \mathbb{C}^*$.
- $U(\mathcal{M}_n(\mathbb{K})) = GL_n(\mathbb{K})$.
- $U(\mathbb{K}[X]) = \mathbb{K}^*$.

La démonstration de ces différents points a été effectuée durant l'année dans les chapitres correspondants.

Définition.

On appelle **corps** tout anneau commutatif $(A, +, .)$ non réduit à $\{0_A\}$ et dans lequel $U(A) = A^*$, c'est à dire un anneau dont tous les éléments non nuls sont inversibles.

Exemples.

- $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des corps.
- $(\mathbb{Z}, +, \times)$ n'est pas un corps, de même que $\mathcal{M}_n(\mathbb{K})$ ou $\mathbb{K}[X]$.

Remarque. Si A est un corps, alors A est intègre. La réciproque est fausse en général ($\mathbb{Z}$, $\mathbb{K}[X]$).

3 Algèbres

Définition.

Soit A un ensemble non vide muni de deux lois de composition interne $+$ et $\times$, et d'une loi de composition externe $\cdot : \mathbb{K} \times A \to A$.
On dit que $(A, +, \times, \cdot)$ est une **algèbre** (ou $\mathbb{K}$-algèbre) si

- $(A, +, \times)$ est un anneau ;
- $(A, +, \cdot)$ est un espace vectoriel ;
- pour tout $\lambda \in \mathbb{K}$, $a, b \in A$, on a :

$$\lambda \cdot (a \times b) = (\lambda \cdot a) \times b = a \times (\lambda \cdot b).$$

Si de plus la loi $\times$ est commutative, on dira que $(A, +, \times, \cdot)$ est une **algèbre commutative**.

Exemples.

- $(\mathbb{K}[X], +, \times, \cdot)$, $(\mathbb{K}^{\mathbb{N}}, +, \times, \cdot)$, $(\mathcal{F}(I, \mathbb{K}), +, \times, \cdot)$ sont des algèbres commutatives.

- Si on note $\mathcal{P}_{\mathbb{K}}$ l'ensemble des applications polynomiales à coefficients dans $\mathbb{K}$, alors $(\mathcal{P}_{\mathbb{K}}, +, \times, \cdot)$ est une algèbre commutative (c'est une sous-algèbre de $(\mathcal{F}(I, \mathbb{K}), +, \times, \cdot)$, c'est à dire à la fois un sous anneau et un sous espace vectoriel).
- Soit E un espace vectoriel. Alors $(\mathcal{L}(E), +, \circ, \cdot)$ est une algèbre, non commutative en général.
- $(\mathcal{M}_n(\mathbb{K}), +, \times, \cdot)$ est une algèbre non commutative si $n \geq 2$.

Définition.

Soient $(A_1, +, \times, \cdot)$ et $(A_2, +, \times, \cdot)$ deux algèbres et une application $f : A_1 \to A_2$. On dit que φ est un **morphisme d'algèbres** si φ est à la fois une application linéaire et un morphisme d'anneaux.

Exemples.

- L'application φ qui à un polynôme P associe sa fonction polynomiale associée $\tilde{P}$, est un isomorphisme d'algèbres de $(\mathbb{K}[X], +, \times, \cdot)$ dans $(\mathcal{P}_{\mathbb{K}}, +, \times, \cdot)$.
- Soit E un espace vectoriel de dimension finie $n \geq 1$, et $\mathcal{B}$ une base de E. L'application φ qui à $f \in \mathcal{L}(E)$ associe sa matrice $M_{\mathcal{B}}(f)$ dans la base $\mathcal{B}$ est un isomorphisme d'algèbres de $(\mathcal{L}(E), +, \times, \cdot)$ dans $(\mathcal{M}_n(\mathbb{K}), +, \times, \cdot)$.