Structures algébriques élémentaires

AVERTISSEMENT. Selon le programme, les structures algébriques ne doivent pas être étudiées pour elles-mêmes en toute généralité. Voici néanmoins un survol rapide des notions algébriques élémentaires.

Lois de composition

Soient E et K deux ensembles.

DÉFINITIONS. Toute application de $E \times E$ dans E s'appelle une *loi de composition interne sur E* ou *loi interne sur E*. Toute application de $K \times E$ dans E s'appelle une *loi externe de domaine K sur E* ou *loi d'action de K sur E*. On note ces applications à l'aide d'un symbole, $*$ par exemple, que l'on place entre les deux variables :

$$E \times E \to E,\ (x,y) \mapsto x * y,$$
$$K \times E \to E,\ (\lambda,x) \mapsto \lambda * x.$$

Pour désigner une loi abstraite, on utilise souvent les symboles $*$ (*étoile*), $\star$ (*star*), $\top$ (*truc*) ou $\perp$ (*antitruc*). Il arrive que le même symbole désigne des lois différentes, mais le contexte permet alors de les distinguer.

Désormais, $*$ désigne une loi interne sur E.

STABILITÉ. Une partie F de E est *stable pour* la loi $*$ si

$$\forall (x,y) \in F^2,\ x * y \in F.$$

L'application $F \times F \to F,\ (x,y) \mapsto x * y$ s'appelle la *loi induite par $*$ sur F*, que l'on note encore $*$ abusivement.

ASSOCIATIVITÉ. La loi $*$ est *associative* si

$$\forall (x,y,z) \in E^3,\ (x * y) * z = x * (y * z).$$

COMMUTATIVITÉ. Deux éléments x et y de E *commutent* si $x * y = y * x$. La loi $*$ est *commutative* si tous les éléments de E commutent, c'est-à-dire si

$$\forall (x,y) \in E^2,\ x * y = y * x.$$

Certaines des notions qui suivent sont définies à droite et à gauche, et il convient de distinguer les deux côtés si la loi n'est pas commutative. Naturellement, si elle l'est, les notions à droite et à gauche se confondent.

ÉLÉMENT NEUTRE. Un élément e de E est un *élément neutre* pour la loi $*$ si

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

Désormais, on suppose que la loi $*$ admet un élément neutre e.

ÉLÉMENTS SYMÉTRISABLES. Un élément x de E est *symétrisable* s'il existe un élément x' de E tel que $x * x' = x' * x = e$; l'élément x' s'appelle *un symétrique de x*. Si la loi $*$ n'est pas commutative, il arrive qu'un élément soit symétrisable d'un seul côté.

DISTRIBUTIVITÉ. Soit une autre loi interne $\top$ sur E. Elle est *distributive par rapport à* la loi $*$ si

$$\forall (x,y,z) \in E^3,\ (x * y) \top z = (x \top z) * (y \top z),$$
$$x \top (y * z) = (x \top y) * (x \top z).$$

ÉLÉMENT ABSORBANT. Un élément a de E est *absorbant* pour la loi $*$ si

$$\forall x \in E,\ x * a = a * x = a.$$

NOTATION ADDITIVE. On désigne souvent une loi interne par le symbole $+$ (*plus*, en prononçant le *s*). La loi s'appelle alors la *somme* ou l'*addition* et l'on dit qu'elle est notée *additivement*.

La notation additive s'utilise *exclusivement* pour des lois commutatives. Alors, dans les définitions précédentes, on se contente de la moitié des égalités. Nous supposons maintenant que $+$ est commutative. S'il existe, le neutre de $+$ se note souvent 0_E ou 0 :

$$\forall x \in E,\ x + 0 = 0 + x = x.$$

Supposons que le neutre existe. Si un élément x de E est symétrisable, son symétrique s'appelle son *opposé* et se note $-x$: on a donc

$$x + (-x) = (-x) + x = 0,$$

ce que l'on écrit

$$x - x = -x + x = 0.$$

NOTATION MULTIPLICATIVE. Si l'on emploie le symbole $\cdot$ (*point*) ou $\times$ (*fois*), la loi s'appelle le *produit* ou la *multiplication* et l'on parle de notation *multiplicative*. Dans ce cas, on omet souvent le symbole et l'on écrit

$$x \cdot y = x \times y = xy.$$

La notation multiplicative s'emploie souvent pour des lois non commutatives. Il faudra donc bien prendre garde de respecter toutes les égalités dans les définitions précédentes. S'il existe, le neutre de $\cdot$ est souvent noté 1_E ou 1 :

$$\forall x \in E,\ x1 = 1x = x.$$

Supposons que le neutre existe. Si un élément x de E est symétrisable, on dit qu'il est *inversible*, son symétrique s'appelle son *inverse* et se note x^{-1} :

$$x x^{-1} = x^{-1} x = 1.$$

Monoïdes

Définition. Un *monoïde* est un couple $(M, *)$ constitué d'un ensemble M et d'une loi interne $*$ sur M, associative et qui admet un élément neutre $e \in M$. Si la loi est de plus commutative, le monoïde est *commutatif*.

Désormais, $(M, *)$ est un monoïde commutatif.

Calculs et notations. Puisque la loi $*$ est à la fois associative et commutative, étant donnés un entier $n \in \mathbb{N}^*$ et des éléments $x_1, \dots, x_n$ dans M, la composée de ces éléments par $*$ ne dépend ni de l'ordre des opérations (grâce à l'associativité) ni de l'ordre des termes (grâce à la commutativité). Alors, on adopte les notations suivantes :

$$x_1 * \cdots * x_n = \mathop{*}_{i=1}^{n} x_i = \mathop{*}_{i \in [\![1,n]\!]} x_i = \mathop{*}_{1 \leqslant i \leqslant n} x_i.$$

Plus généralement, on pose

$$\mathop{*}_{i \in \varnothing} x_i = e,$$

et si $I = \{a, b, \dots\}$ est un ensemble d'indices *fini non vide* et $(x_i)_{i \in I}$ sont des éléments de M, on écrit

$$\mathop{*}_{i \in I} x_i = x_a * x_b * \cdots$$

Soit $x \in M$. On pose $x^{*0} = e$ et pour $n \in \mathbb{N}^*$,

$$\underbrace{x * \cdots * x}_{n \text{ fois}} = x^{*n}.$$

Si x est symétrisable de symétrique x', on pose

$$\underbrace{x' * \cdots * x'}_{n \text{ fois}} = x^{*-n}.$$

Si la loi $*$ est notée additivement, ces notations deviennent

$$x_1 + \cdots + x_n = \sum_{i=1}^{n} x_i = \sum_{i \in [\![1,n]\!]} x_i = \sum_{1 \leqslant i \leqslant n} x_i,$$
$$\underbrace{x + \cdots + x}_{n \text{ fois}} = n\,x,$$
$$\underbrace{(-x) + \cdots + (-x)}_{n \text{ fois}} = -n\,x.$$

Si la loi $*$ est notée multiplicativement, les notations deviennent

$$x_1 \cdots x_n = \prod_{i=1}^{n} x_i = \prod_{i \in [\![1,n]\!]} x_i = \prod_{1 \leqslant i \leqslant n} x_i,$$
$$\underbrace{x \cdots x}_{n \text{ fois}} = x^n,$$
$$\underbrace{x^{-1} \cdots x^{-1}}_{n \text{ fois}} = x^{-n}.$$

Groupes

Dans ce paragraphe, toutes les lois internes sont notées multiplicativement.

Définition. Un *groupe* est un couple $(G, \cdot)$ constitué d'un ensemble G et d'une loi interne $\cdot$ sur G qui est associative, qui admet un élément neutre et pour laquelle tout élément est symétrisable. Si la loi est commutative, le groupe $(G, \cdot)$ est *commutatif* ou *abélien*. Par abus, on parle du groupe G au lieu de $(G, \cdot)$.

Désormais, G est un groupe dont le neutre est e.

Sous-groupes. Une partie *non vide* H de G est un sous-groupe de G si H est stable par la loi $\cdot$ et H est un groupe pour la loi induite.

Soit $H \subset G$. Il est équivalent de dire

— H est un sous-groupe de G ;

— H est non vide et
$$\forall (x, y) \in H^2,\ x\,y^{-1} \in H\,;$$

— H est non vide, H est stable par la loi $\cdot$ et
$$\forall x \in H,\ x^{-1} \in H.$$

Dans la pratique, la première chose à vérifier, c'est que H est bien une partie de G. Un sous-groupe de G contient forcément le neutre de G : c'est pourquoi on montre souvent que H n'est pas vide en prouvant qu'il contient e.

Morphismes de groupes. Soient G et H deux groupes dont les éléments neutres sont e_G et e_H. Un *morphisme* ou *homomorphisme de groupes* de G dans H est une application $f : G \to H$ telle que

$$\forall (x, y) \in G^2,\ f(xy) = f(x)\,f(y).$$

Alors $f(e_G) = e_H$ et

$$\forall x \in G,\ (f(x))^{-1} = f(x^{-1}).$$

Un morphisme de G dans lui-même s'appelle un *endomorphisme* de G. Un *isomorphisme* de G sur H est une bijection $f : G \to H$ telle que les applications f et f^{-1} soient des morphismes. S'il en existe, on dit que G et H sont *isomorphes*. Un isomorphisme de G sur lui-même s'appelle un *automorphisme* de G.

Noyaux & images. Soit f un morphisme de groupes de G dans H.

Le *noyau* de f est l'image réciproque par f de $\{e_H\}$ et se note $\mathrm{Ker}(f)$ ou $\mathrm{Ker}\, f$:

$$\mathrm{Ker}(f) = f^{-1}(\{e_H\}) = \{x \in G \mid f(x) = e_H\}.$$

C'est un sous-groupe de G. Le morphisme f est injectif si et seulement si son noyau est réduit à $\{e_G\}$.

L'*image* de f est l'image directe par f de G et se note $\mathrm{Im}(f)$ ou $\mathrm{Im}\, f$:

$$\mathrm{Im}(f) = f(G) = \{y \in H \mid \exists x \in G,\ f(x) = y\}.$$

C'est un sous-groupe de H. Le morphisme f est surjectif si et seulement si son image est H tout entier.

Anneaux

Définition. Un *anneau* est un triplet $(A, +, \times)$ constitué d'un ensemble A et de deux lois internes sur A telles que

- $(A, +)$ est un groupe abélien dont le neutre est noté 0 et appelé *élément nul* de A ;
- $(A, \times)$ est un monoïde, c'est-à-dire que $\times$ est associative et admet un élément neutre noté 1 et appelé *élément unité* de A ;
- la loi $\times$ est distributive par rapport à la loi $+$.

Si la loi $\times$ est commutative, A est un anneau *commutatif*.

Si A est un singleton, on a forcément $0 = 1$, et A s'appelle l'anneau nul. Sinon, $0 \neq 1$ et l'anneau est non nul.

L'élément nul de A est absorbant pour $\times$:

$$\forall x \in A,\ x0 = 0x = 0.$$

Désormais, $(A, +, \times)$ est un anneau, pas forcément commutatif.

Intégrité. Un élément $x \in A$ est un diviseur de 0 à gauche (resp. à droite) s'il existe un élément *non nul* $y \in A$ tel que $xy = 0$ (resp. $yx = 0$).

Dire que A n'admet pas de diviseur de 0 (à gauche ou à droite) signifie donc que

$$\forall (x, y) \in A^2,\ xy = 0 \iff (x = 0 \text{ ou } y = 0).$$

Un anneau A commutatif et sans diviseur de 0 est un anneau *intègre*.

Éléments inversibles. Puisque la loi $\times$ est notée multiplicativement, on parle d'inversibilité (éventuellement à droite ou à gauche).

Morphismes d'anneaux. Soient A et B deux anneaux dont les éléments neutres sont 0_A, 0_B, 1_A et 1_B. Un *morphisme* ou *homomorphisme d'anneaux* de A dans B est une application $f : A \to B$ telle que $f(1_A) = 1_B$ et

$$\forall (x, y) \in A^2,\ f(x + y) = f(x) + f(y),$$
$$f(xy) = f(x)f(y).$$

En particulier, f est un morphisme de groupes de $(A, +)$ dans $(B, +)$. On définit donc de même un *endomorphisme*, un *isomorphisme* et un *automorphisme*. Le noyau et l'image gardent leur sens :

$$\operatorname{Ker}(f) = \{x \in A \mid f(x) = 0_B\}.$$
$$\operatorname{Im}(f) = \{y \in B \mid \exists x \in A,\ f(x) = y\}.$$

Corps

Un *corps* est un anneau $(K, +, \times)$ où tout élément non nul est inversible. Si la loi $\times$ est commutative, le corps est *commutatif*. S'il ne l'est pas, on l'appelle parfois une *algèbre à division*.

Le programme nous impose de ne considérer que les corps commutatifs.

Espaces vectoriels

Soit K un corps.

Définition. Un *espace vectoriel sur K*, ou *K-espace vectoriel*, est un triplet $(E, +, \cdot)$ constitué d'un ensemble E muni d'une loi de composition interne $+$ et d'une loi de composition externe $\cdot$ de domaine K telles que

- $(E, +)$ est un groupe abélien ;
- $\forall (x, y) \in E^2, \forall (\lambda, \mu) \in K^2,$
$$(\lambda + \mu)x = \lambda x + \mu x,$$
$$\lambda(x + y) = \lambda x + \lambda y,$$
$$(\lambda\mu)x = \lambda(\mu x),$$
$$1x = x.$$

Les éléments de E sont des *vecteurs*. Le corps K est le *corps de base* de E et ses éléments sont des *scalaires*.

Sous-espaces vectoriels. Une partie *non vide* F de E est un *sous-espace vectoriel* de E si elle est stable par les lois $+$ et $\cdot$ et si F est un K-espace vectoriel pour les lois induites.

Soit F une partie de E. Il est équivalent de dire :

- F est un sous-espace vectoriel de E ;
- F est non vide et stable par les lois $+$ et $\cdot$;
- F est non vide et
$$\forall (x, y) \in F^2, \forall \lambda \in K,\ x + \lambda y \in F.$$

Dans la pratique, la première chose à vérifier, c'est que F est bien une partie de E. Un sous-espace vectoriel contient forcément le vecteur nul de E : c'est pourquoi, on montre souvent que F n'est pas vide en prouvant qu'il contient 0.

Applications linéaires. Soient E et F deux K-espaces vectoriels de vecteurs nuls 0_E et 0_F.

Une *application linéaire* de E dans F est une application $u : E \to F$ telle que

$$\forall (x, y) \in E^2, \forall \lambda \in K,\ u(x + y) = u(x) + u(y),$$
$$u(\lambda x) = \lambda u(x).$$

ou, de manière équivalente,

$$\forall (x, y) \in E^2, \forall \lambda \in K,\ u(x + \lambda y) = u(x) + \lambda u(y).$$

En particulier, u est un morphisme de groupes de $(E, +)$ dans $(F, +)$. On définit donc aussi un *endomorphisme*, un *isomorphisme* et un *automorphisme*.

L'ensemble des applications linéaires de E dans F se note $\mathfrak{L}(E, F)$, l'ensemble des endomorphismes de E se note $\mathfrak{L}(E)$ et l'ensemble des automorphismes de E s'appelle le *groupe linéaire* de E et se note $\mathrm{GL}(E)$.

Étant donnée une application linéaire $u \in \mathfrak{L}(E, F)$, son noyau est

$$\operatorname{Ker}(u) = \{x \in E \mid u(x) = 0_F\}.$$

C'est un sous-espace vectoriel de E. Son image est

$$\operatorname{Im}(u) = \{y \in F \mid \exists x \in E,\ y = u(x)\}.$$

C'est un sous-espace vectoriel de F. L'application linéaire u est

- injective si et seulement si $\operatorname{Ker}(u) = \{0_E\}$;
- surjective si et seulement si $\operatorname{Im}(u) = F$.

Exemples

Premier exemple. Dans les ensembles de nombres usuels, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, on considère la somme $(+)$ et le produit $(\times)$ usuels.

- $(\mathbb{N}, +)$ est un monoïde commutatif. Seul 0 y admet un opposé.
- $(\mathbb{Z}, +, \times)$ est un anneau commutatif et intègre. Seuls 1 et -1 y sont inversibles.
- $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des corps (commutatifs).

Deuxième exemple. Dans l'ensemble $E = \mathbb{R}^{\mathbb{R}}$ des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, on considère les opérations usuelles somme $(+)$, produit $(\times)$, composition $(\circ)$ des fonctions, et produit $(\cdot)$ d'une fonction par un réel.

- $(E, +, \cdot)$ est un $\mathbb{R}$-espace vectoriel.
- $(E, +, \times)$ est un anneau commutatif non intègre.
- $(E, +, \circ)$ est un anneau ni commutatif ni intègre.

Troisième exemple. Soit E un espace vectoriel sur un corps K. En notant $+$ et $\circ$ la somme et la composition des endomorphismes de E, et $\cdot$ le produit d'un endomorphisme par un scalaire,

- $(\mathfrak{L}(E), +, \cdot)$ est un K-espace vectoriel.
- $(\mathfrak{L}(E), +, \circ)$ est un anneau ni commutatif ni intègre.
- $(\mathrm{GL}(E), \circ)$ est un groupe non abélien.

De même, si n est un entier naturel non nul, en notant $+$ et $\times$ la somme et le produit des matrices carrées, et $\cdot$ le produit d'une matrice par un scalaire,

- $(\mathfrak{M}_n(K), +, \cdot)$ est un K-espace vectoriel.
- $(\mathfrak{M}_n(K), +, \times)$ est un anneau ni commutatif ni intègre.
- $(\mathrm{GL}_n(K), \times)$ est un groupe non abélien.

Quatrième exemple. Soit K un corps. On considère les espaces usuels $K[X]$ et $K(X)$, respectivement des polynômes et des fractions rationnelles à coefficients dans K, munis de leurs lois usuelles.

- $(K[X], +, \cdot)$ et $(K(X), +, \cdot)$ sont des K-espaces vectoriels.
- $(K[X], +, \times)$ est un anneau commutatif et intègre.
- $(K(X), +, \times)$ est un corps.