STRUCTURES ALGÉBRIQUES EN ALGÈBRE LINÉAIRE

Contents

1. Groupes, anneaux, corps

Definition 1.1. Un corps est un ensemble K muni de deux applications de $K \times K$ dans K, appelées addition et multiplication et notées respectivement

$$\begin{cases} K \times K \to K \\ (x, y) \mapsto x + y \end{cases} \quad \text{et} \quad \begin{cases} K \times K \to K \\ (x, y) \mapsto xy \, , \end{cases}$$

satisfaisant les propriétés suivantes:

(A1) Pour tous $x, y, z \in K$, $(x + y) + z = x + (y + z)$.
(A2) Il existe $0_K \in K$ tel que pour tout $x \in K$, $0_K + x = x + 0_K = x$.
(A3) Pour tout $x \in K$, il existe $-x \in K$ tel que $x + (-x) = (-x) + x = 0_K$.
(A4) Pour tous $x, y \in K$, $x + y = y + x$.
(M1) Pour tous $x, y, z \in K$, $(xy)z = x(yz)$.
(M2) Il existe $1_K \in K$ tel que $1_K \neq 0_K$ et tel que pour tout $x \in K$, $1_K x = x 1_K = x$.
(M3) Pour tout $x \in K \setminus \{0_K\}$, il existe $x^{-1} \in K$ tel que $xx^{-1} = x^{-1}x = 1_K$.
(M4) Pour tous $x, y \in K$, $xy = yx$.
(D) Pour tous $x, y, z \in K$, $x(y + z) = xy + xz$.

Les propriétés (A1)–(A4) concernent l'addition. Un ensemble E muni d'une application $E \times E \to E$ satisfaisant (A1)–(A3) s'appelle un groupe, abélien (ou commutatif) si de plus (A4) est vérifiée. Noter qu'un tel E n'est pas vide par (A2). De plus, l'élément 0_E, appelé élément neutre, est unique, et pour tout $x \in E$, l'élément $-x$ de la propriété (A3) est unique. La propriété (A1) signifie que l'on peut effectuer les additions dans l'ordre que l'on veut, ce qui permet d'écrire $x_1 + \ldots + x_n$ sans ambiguïté pour n éléments de E. La propriété (A4) signifie que l'on peut permuter les éléments d'une somme, ce qui permet d'écrire $\sum_{k \in \{1,\ldots,n\}} x_k$ sans ambiguïté. Pour $x, y \in E$, on note $x - y = x + (-y)$.

Les propriétés (M1)–(M4) concernent la multiplication. Elles impliquent que le produit de deux éléments différents de 0_K est différent de 0_K, et que l'ensemble $K^\times = K \setminus \{0_K\}$ muni de l'application $K^\times \times K^\times \to K^\times$, $(x, y) \mapsto xy$, est un groupe abélien. Noter que (M2) implique qu'un corps K contient au moins deux éléments, à savoir les deux éléments neutres 0_K et 1_K.

La propriété (D) exprime la compatibilité (ou distributivité) de la multiplication par rapport à l'addition. Elle implique que pour tout $x \in K$, $0_K x = 0_K$ et $(-1_K)x = -x$. Plus généralement, elle implique avec les autres propriétés que dans un corps on a les mêmes règles de calcul que dans $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

Un ensemble R qui vérifie toutes les propriétes d'un corps sauf (M3) et (M4) s'appelle un anneau. Un ensemble A qui vérifie toutes les propriétes d'un corps sauf (M3) s'appelle un anneau commutatif.

Example 1.2. Les ensembles $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de l'addition et de la multiplication usuelles sont des corps. Les ensembles $\mathbb{N}$ et $\mathbb{Z}$ munis de l'addition et de la multiplication ne sont pas des corps ; cependant, $\mathbb{Z}$ est un anneau commutatif, alors que $\mathbb{N}$ n'est pas un groupe. L'ensemble $\mathbb{R}_+ = [0, +\infty[$ muni de l'addition n'est pas un groupe. L'ensemble des nombres décimaux est un anneau commutatif mais n'est pas un corps. L'ensemble des nombres complexes purement imaginaires est un groupe abélien mais n'est pas un anneau. L'ensemble $\{0\}$ est un anneau commutatif mais n'est pas un corps. L'ensemble $\mathbb{Q}(i) = \{a + ib \,;\, a, b \in \mathbb{Q}\}$ est un corps, avec $i \in \mathbb{C}$ tel que $i^2 = -1$.

Example 1.3. Soit p un nombre premier. Pour tout $n \in \mathbb{Z}$, soit $r_p(n) \in \{0, \dots, p-1\}$ le reste de la division euclidienne de n par p, c'est-à-dire $n = pk + r_p(n)$ avec $k, r_p(n) \in \mathbb{Z}$ et $0 \leq r_p(n) \leq p-1$. Soient $F_p = \{0, \dots, p-1\}$ et

$$\begin{cases} F_p \times F_p \to F_p \\ (x, y) \mapsto r_p(x + y) \underset{\text{def}}{=} x + y \end{cases}, \quad \begin{cases} F_p \times F_p \to F_p \\ (x, y) \mapsto r_p(xy) \underset{\text{def}}{=} x.y \,. \end{cases}$$

L'ensemble F_p muni de ces deux applications est un corps, appelé corps fini à p éléments. Les deux éléments neutres sont respectivement 0 et 1. En particulier avec $p = 2$ on obtient un corps de cardinalité minimale. L'addition et la multiplication dans $F_2 = \{0, 1\}$ sont données par

$$0 + 0 = 1 + 1 = 0, \quad 0 + 1 = 1 + 0 = 1, \quad 0.0 = 0.1 = 1.0 = 0, \quad 1.1 = 1 \,.$$

Ceci traduit les règles de parité de la somme et du produit de deux entiers n et m : $n + m$ est pair (0) si n et m ont la même parité, impair (1) sinon ; et nm est pair si n ou m est pair, impair sinon. De même l'addition et la multiplication dans F_p traduisent les règles de congruence modulo p. Noter que si l'on remplace p par un entier n non nul quelconque on obtient un anneau commutatif à n éléments, qui est un corps si et seulement si n est premier. (Cet anneau s'identifie à l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$.)

Dans les sections suivantes, partant d'un corps K (par exemple $\mathbb{Q}$, $\mathbb{R}$, ou $\mathbb{C}$), on construit des anneaux en utilisant l'addition et la multiplication de K. Ces anneaux ne sont pas des corps, à moins que la construction ne redonne K lui-même. On note $0_K = 0$ et $1_K = 1$ les deux éléments neutres de K.

2. Anneau produit de corps

Soient K un corps (par exemple $\mathbb{Q}$, $\mathbb{R}$, ou $\mathbb{C}$) et $n \geq 1$ un entier. On note $K^n = K \times \ldots \times K$ (n fois) l'ensemble produit de n copies de K. On a donc $K^1 = K$, $K^2 = K \times K$, $K^3 = K \times K \times K$, et ainsi de suite ; lorsque $K = \mathbb{R}$ on retrouve la notation habituelle $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ et $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$. Les éléments de K^n sont notés $(a_1, \ldots, a_n) = (a_k)_{1 \leq k \leq n}$ avec $a_k \in K$ pour tout $1 \leq k \leq n$. L'élément a_k s'appelle la k-ième composante de $(a_k)_{1 \leq k \leq n}$, ou bien encore, par analogie avec $\mathbb{R}^2$ et $\mathbb{R}^3$, la k-ième coordonnée.

On utilise l'addition et la multiplication de K pour définir celles de K^n de la façon suivante. Pour $(a_k)_{1 \leq k \leq n}$ et $(b_k)_{1 \leq k \leq n}$ dans K^n on pose

$$(a_k)_{1 \leq k \leq n} + (b_k)_{1 \leq k \leq n} \underset{\text{def}}{=} (a_k + b_k)_{1 \leq k \leq n} \quad \text{et} \quad (a_k)_{1 \leq k \leq n} \cdot (b_k)_{1 \leq k \leq n} \underset{\text{def}}{=} (a_k b_k)_{1 \leq k \leq n}.$$

Cela signifie que l'on effectue les deux opérations composante par composante. L'ensemble K^n muni de cette addition et multiplication est un anneau commutatif. Cela découle du fait que K lui-même en est un ; les deux éléments neutres de K^n sont respectivement $0_{K^n} = (0, \ldots, 0)$ et $1_{K^n} = (1, \ldots, 1)$, et l'on a $-(a_k)_{1 \leq k \leq n} = (-a_k)_{1 \leq k \leq n}$. Cependant dès que $n \geq 2$ l'anneau K^n n'est pas un corps. En effet, lorsque $n \geq 2$ les éléments $(1, 0, \ldots, 0)$ et $(0, \ldots, 0, 1)$ sont tous deux différents de 0_{K^n} et leur produit est 0_{K^n} ; or dans un corps le produit de deux éléments non nuls est non nul, donc K^n n'est pas un corps.

3. Anneau de polynômes à coefficients dans un corps

Soit K un corps (par exemple $\mathbb{Q}$, $\mathbb{R}$, ou $\mathbb{C}$). Un polynôme à coefficients dans K est une somme formelle

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$$

avec $n \in \mathbb{N}$ et $a_k \in K$ pour tout $0 \leq k \leq n$. L'élément a_k s'appelle le k-ième coefficient de $P(X)$. On convient de ne pas écrire les termes $a_k X^k$ lorsque $a_k = 0$, sauf si tous les a_k sont nuls, auquel cas on écrit $P(X) = 0$. Alors pour tout $m \in \mathbb{N}$ on a

$$P(X) = 0X^{n+m} + 0X^{n+m-1} + \ldots + 0X^{n+1} + a_n X^n + \ldots + a_1 X + a_0.$$

Avec cette convention, deux polynômes $P(X) = a_n X^n + \ldots + a_1 X + a_0$ et $Q(X) = b_m X^m + \ldots + b_1 X + b_0$ sont égaux si et seulement si $a_k = b_k$ pour tout $k \in \mathbb{N}$. En particulier, on a $P(X) = 0$ si et seulement si tous les a_k sont nuls. Si $P(X) \neq 0$ il existe donc un plus grand $d \in \mathbb{N}$ tel que $a_d \neq 0$, appelé degré de P et noté $d = \deg(P)$; alors $P(X) = a_d X^d + a_{d-1} X^{d-1} + \ldots + a_1 X + a_0$.

On note $K[X]$ l'ensemble des polynômes à coefficients dans K. On utilise l'addition et la multiplication de K pour définir celles de $K[X]$ de la façon suivante. Pour $P(X) = a_n X^n + \ldots + a_1 X + a_0$ et $Q(X) = b_m X^m + \ldots + b_1 X + b_0$ dans $K[X]$ on pose

$$P(X) + Q(X) \underset{\text{def}}{=} (a_N + b_N) X^N + \ldots + (a_1 + b_1) X + (a_0 + b_0) \quad \text{avec } N = \max(n, m),$$

$$P(X)Q(X) \underset{\text{def}}{=} c_{n+m} X^{n+m} + \ldots + c_1 X + c_0 \quad \text{avec } c_k = \sum_{i+j=k} a_i b_j \text{ pour } 0 \leq k \leq n+m.$$

Cela signifie que l'on effectue l'addition coefficient par coefficient, alors que le k-ième coefficient du produit $P(X)Q(X)$ est obtenu en sommant sur $0 \leq i \leq k$ les produits du i-ième coefficient de $P(X)$ avec le $(k-i)$-ième coefficient de $Q(X)$.

L'ensemble $K[X]$ muni de cette addition et multiplication est un anneau commutatif. Cela découle du fait que K lui-même en est un ; les deux éléments neutres de $K[X]$ sont ceux de K, et $-P(X) = -a_nX^n - \ldots - a_1X - a_0$. Cependant $K[X]$ n'est pas un corps. Plus précisément, soient $P(X), Q(X) \in K[X]\setminus\{0\}$ avec $\deg(P) = n$ et $\deg(Q) = m$. Alors $P(X) = a_nX^n + \ldots + a_1X + a_0$ avec $a_n \neq 0$, $Q(X) = b_mX^m + \ldots + b_1X + b_0$ avec $b_m \neq 0$, d'où

$$P(X)Q(X) = a_nb_mX^{n+m} + \ldots + (a_0b_1 + a_1b_0)X + a_0b_0$$

avec $a_nb_m \neq 0$ puisque K est un corps. Donc $P(X)Q(X) \neq 0$ et

$$\deg(PQ) = \deg(P) + \deg(Q).$$

En particulier, si $P(X)Q(X) = 1$ alors $\deg(PQ) = \deg(P) + \deg(Q) = \deg(1) = 0$, ce qui implique $\deg(P) = \deg(Q) = 0$ puisque $\deg(P), \deg(Q) \in \mathbb{N}$. Par conséquent un élément $P(X) \in K[X] \setminus \{0\}$ satisfait la propriété (M3) si et seulement si $\deg(P) = 0$.

Tout polynôme $P(X) = a_nX^n + \ldots + a_1X + a_0$ de $K[X]$ définit une application $f(P) : K \to K$ donnée par $x \mapsto P(x) = \sum_{0\leq k\leq n} a_kx^k$. On obtient ainsi une application f de $K[X]$ dans l'ensemble $\mathcal{A}(K, K)$ des applications de K dans K :

$$f : K[X] \longrightarrow \mathcal{A}(K, K)$$
$$P(X) \longmapsto f(P) : \begin{cases} K \to K \\ x \mapsto P(x) \end{cases}$$

Noter que par construction $K[X]$ est infini même si K est fini. En particulier, ceci montre que l'application f n'est pas injective lorsque K est fini, puisque dans ce cas l'ensemble $\mathcal{A}(K, K)$ des applications de K dans K est également fini. Par exemple, dans le corps fini $F_2 = \{0, 1\}$, on a $x^2 = x$ pour tout $x \in F_2$, donc les applications $F_2 \to F_2$, $x \mapsto x^2$ et $F_2 \to F_2$, $x \mapsto x$ sont égales, alors que les polynômes X^2 et $X \in F_2[X]$ ne sont pas égaux.

4. Anneau de matrices à coefficients dans un corps

Soient K un corps (par exemple $\mathbb{Q}$, $\mathbb{R}$, ou $\mathbb{C}$) et $n \geq 1$ un entier. Une matrice carrée de taille n à coefficients dans K est un tableau

$$\big(a_{i,j}\big)_{1\leq i,j\leq n} = \begin{pmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n-1} & a_{1,n} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n-1} & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1,1} & a_{n-1,2} & \ldots & a_{n-1,n-1} & a_{n-1,n} \\ a_{n,1} & a_{n,2} & \ldots & a_{n,n-1} & a_{n,n} \end{pmatrix}$$

avec $a_{i,j} \in K$ pour tous $1 \leq i, j \leq n$. Dans cette écriture l'indice i compte les lignes et l'indice j compte les colonnes de la matrice. On note $M_n(K)$ l'ensemble des matrices carrées de taille n à coefficients dans K. On utilise l'addition et la multiplication de K pour définir celles de $M_n(K)$ de la façon suivante. Pour $A = (a_{i,j})_{1\leq i,j\leq n}$ et $B = (b_{i,j})_{1\leq i,j\leq n}$ dans $M_n(K)$ on pose

$$A + B \underset{\text{def}}{=} \big(a_{i,j} + b_{i,j}\big)_{1\leq i,j\leq n} \quad \text{et} \quad AB \underset{\text{def}}{=} \big(c_{i,j}\big)_{1\leq i,j\leq n} \text{ avec } c_{i,j} = \sum_{1\leq k\leq n} a_{i,k}b_{k,j}\,.$$

Cela signifie que l'on effectue l'addition coefficient par coefficient, alors que le coefficient de la i-ième ligne et j-ième colonne de la matrice produit AB est obtenu en multipliant la

k-ième composante de la i-ième ligne de A avec celle de la j-ième colonne de B, puis en sommant ces produits sur $1 \leq k \leq n$.

L'ensemble $M_n(K)$ muni de cette addition et multiplication est un anneau. Encore une fois cela découle du fait que K lui-même en est un. Les deux éléments neutres de $M_n(K)$ sont respectivement

$$0_{M_n(K)} = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} \quad \text{et} \quad 1_{M_n(K)} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

et l'on a $-(a_{i,j})_{1\leq i,j\leq n} = (-a_{i,j})_{1\leq i,j\leq n}$.

Lorsque $n = 1$ on a $M_1(K) = K$. Cependant dès que $n \geq 2$ l'anneau $M_n(K)$ n'est pas commutatif. Par exemple, si $n = 2$, dans $M_2(K)$ on a

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Dans les deux sections suivantes on munit certains ensembles d'applications d'une structure d'anneau. Ces applications sont obtenues à partir d'un corps dans le premier et à partir d'un groupe abélien dans le deuxième. L'addition y est définie de manière similaire, mais la multiplication est de nature très différente, en particulier l'une est commutative et l'autre ne l'est pas.

5. Anneau des applications dans un corps

Soient K un corps (par exemple $\mathbb{Q}$, $\mathbb{R}$, ou $\mathbb{C}$) et $n \geq 1$ un entier. Les éléments $(a_1, \dots, a_n) = (a_k)_{1\leq k\leq n}$ de K^n (cf. section 2) peuvent être vus comme des suites d'éléments de K indexées par l'ensemble $\{1, \dots, n\}$, ou bien encore comme des applications $a : \{1, \dots, n\} \to K$, $k \mapsto a_k = a(k)$. Soit $\mathcal{A}(\{1, \dots, n\}, K)$ l'ensemble des applications de $\{1, \dots, n\}$ dans K. On obtient ainsi une application bijective

$$\begin{aligned} \mathcal{A}(\{1, \dots, n\}, K) &\longrightarrow K^n \\ a &\longmapsto \big(a(k)\big)_{1\leq k\leq n} \end{aligned}$$

qui transporte la structure d'anneau de K^n sur l'ensemble des applications de $\{1, \dots, n\}$ dans K de la façon suivante. Pour des applications a et $b : \{1, \dots, n\} \to K$ on définit les applications $a + b$ et $ab : \{1, \dots, n\} \to K$ par

$$(a + b)(k) \underset{\text{def}}{=} a(k) + b(k) \quad \text{et} \quad (ab)(k) \underset{\text{def}}{=} a(k)b(k) \quad \text{pour tout } 1 \leq k \leq n.$$

L'ensemble $\mathcal{A}(\{1, \dots, n\}, K)$ muni de cette addition et multiplication est un anneau commutatif, puisque K^n muni de son addition et multiplication en est un. Les deux éléments neutres de $\mathcal{A}(\{1, \dots, n\}, K)$ sont les applications constantes $\{1, \dots, n\} \to K$ données par $k \mapsto 0$ et $k \mapsto 1$ respectivement.

Soit maintenant $\mathcal{S}(K) = K^{\mathbb{N}}$ l'ensemble des suites $(a_k)_{k\in\mathbb{N}}$ d'éléments de K indexées par l'ensemble $\mathbb{N}$. Comme pour K^n, on définit l'addition et la multiplication des suites composante par composante

$$(a_k)_{k\in\mathbb{N}} + (b_k)_{k\in\mathbb{N}} \underset{\text{def}}{=} (a_k + b_k)_{k\in\mathbb{N}} \quad \text{et} \quad (a_k)_{k\in\mathbb{N}} \cdot (b_k)_{k\in\mathbb{N}} \underset{\text{def}}{=} (a_k b_k)_{k\in\mathbb{N}}.$$

Comme K^n, l'ensemble $\mathcal{S}(K)$ muni de cette addition et multiplication est un anneau commutatif ; les deux éléments neutres sont les suites constantes $(0, 0, \dots)$ et $(1, 1, \dots)$, et l'on a $-(a_k)_{k\in\mathbb{N}} = (-a_k)_{k\in\mathbb{N}}$. Comme K^n avec $n \geq 2$, cet anneau n'est pas un corps. Aussi, les suites $(a_k)_{k\in\mathbb{N}}$ d'éléments de K peuvent être vues comme des applications $a : \mathbb{N} \to K$, $k \mapsto a_k = a(k)$. Soit $\mathcal{A}(\mathbb{N}, K)$ l'ensemble des applications de $\mathbb{N}$ dans K. On a une bijection de l'ensemble $\mathcal{A}(\mathbb{N}, K)$ dans $\mathcal{S}(K)$

$$\begin{aligned} \mathcal{A}(\mathbb{N}, K) &\longrightarrow \mathcal{S}(K) \\ a &\longmapsto \big(a(k)\big)_{k\in\mathbb{N}} \end{aligned}$$

qui transporte la structure d'anneau de $\mathcal{S}(K)$ sur l'ensemble $\mathcal{A}(\mathbb{N}, K)$ par

$$(a+b)(k) \underset{\text{def}}{=} a(k) + b(k) \quad \text{et} \quad (ab)(k) \underset{\text{def}}{=} a(k)b(k) \quad \text{pour tout } k \in \mathbb{N}.$$

Alors, de même que $\mathcal{S}(K)$, l'ensemble $\mathcal{A}(\mathbb{N}, K)$ muni de cette addition et multiplication est un anneau commutatif qui n'est pas un corps.

Plus généralement, soient S un ensemble non vide et $\mathcal{A}(S, K)$ l'ensemble des applications de S dans K. On construit une addition et une multiplication dans $\mathcal{A}(S, K)$ à partir de celles de K de la façon suivante. Pour des applications f et $g : S \to K$ on définit les applications $f + g$ et fg par

$$(f+g)(x) \underset{\text{def}}{=} f(x) + g(x) \quad \text{et} \quad (fg)(x) \underset{\text{def}}{=} f(x)g(x) \quad \text{pour tout } x \in S.$$

Alors, de même que $\mathcal{A}(\mathbb{N}, K)$, l'ensemble $\mathcal{A}(S, K)$ muni de cette addition et multiplication est un anneau commutatif, qui n'est pas un corps dès que $\mathrm{Card}(S) \geq 2$. Les deux éléments neutres sont les applications constantes $S \to K$ données par $x \mapsto 0$ et $x \mapsto 1$ respectivement, et l'on a $(-f)(x) = -f(x)$ pour tout $x \in S$.

6. Anneau des endomorphismes d'un groupe abélien

Soit E un groupe abélien, c'est-à-dire un ensemble muni d'une addition $E \times E \to E$, $(a, b) \mapsto a + b$, satisfaisant les propriétés (A1)–(A4) de la définition 1.1. Noter que pour chaque anneau $(R, +, \cdot)$ décrit précédemment, on obtient un groupe abélien $(R, +)$ en ne considérant que l'addition (c'est-à-dire en "oubliant" la multiplication). Par exemple, on dispose des groupes abéliens $(\mathbb{Z}, +)$, $(\mathbb{C}, +)$, et $(K^n, +)$, $(K[X], +)$, $(\mathcal{S}(K), +)$. Comme dans la section 5, pour tout ensemble S non vide on en déduit une structure de groupe abélien sur l'ensemble des applications $S \to E$ en posant $(f + g)(x) = f(x) + g(x)$ pour tout $x \in S$. En particulier cela s'applique lorsque l'on choisit $S = E$, d'où une structure de groupe abélien sur l'ensemble $\mathcal{A}(E, E)$ des applications de E dans E.

On souhaite maintenant définir une multiplication dans $\mathcal{A}(E, E)$ telle que, muni de l'addition ci-dessus et de cette multiplication, l'ensemble $\mathcal{A}(E, E)$ est un anneau. Puisqu'on a convenu de ne pas se donner de multiplication dans E lui-même, on doit utiliser un autre procédé que celui de la section 5. Pour cette raison on considère l'ensemble des applications de E dans E. En effet, dans ce cas (et seulement dans ce cas) on peut définir une "multiplication" des applications par

$$\begin{aligned} \mathcal{A}(E, E) \times \mathcal{A}(E, E) &\longrightarrow \mathcal{A}(E, E) \\ (f, g) &\longmapsto f \circ g \end{aligned}$$

où $f \circ g : E \to E$ est l'application composée donnée par $a \mapsto f(g(a))$. Cette multiplication vérifie les propriétés (M1) et (M2) de la définition 1.1. En effet, pour $f, g, h : E \to E$, on a $(f \circ (g \circ h))(a) = f(g(h(a))) = ((f \circ g) \circ h)(a)$ pour tout $a \in E$, donc $f \circ (g \circ h) = (f \circ g) \circ h$. L'élément neutre est l'identité $\mathrm{Id}_E : E \to E$, $a \mapsto a$, puisque $\mathrm{Id}_E \circ f = f \circ \mathrm{Id}_E = f$ pour tout $f : E \to E$. Rappelons qu'une application $\varphi : E \to F$ est bijective si et seulement s'il existe une application $\psi : F \to E$ telle que $\varphi \circ \psi = \mathrm{Id}_F$ et $\psi \circ \varphi = \mathrm{Id}_E$. Donc $f : E \to E$ vérifie la condition (M3) si et seulement si elle est bijective, auquel cas son inverse pour la multiplication $\circ$ est son application réciproque f^{-1}. De plus, la plupart des applications ne commutent pas entre elles, c'est-à-dire ne vérifient pas la condition (M4).

Pour que $\mathcal{A}(E, E)$ muni de cette addition et multiplication soit un anneau, il reste à vérifier la condition (D) de compatibilité de la multiplication par rapport à l'addition. Pour tous $f, g, h : E \to E$ et tout $a \in E$ on a $(f \circ (g+h))(a) = f((g+h)(a)) = f(g(a)+h(a))$ et $(f \circ g + f \circ h)(a) = (f \circ g)(a) + (f \circ h)(a) = f(g(a)) + f(h(a))$. Donc pour obtenir l'égalité des applications $f \circ (g + h)$ et $f \circ g + f \circ h$ on doit considérer des applications $f : E \to E$ satisfaisant la condition

$$f(a + b) = f(a) + f(b) \quad \text{pour tous } a, b \in E.$$

Definition 6.1. Soit $(E, +)$ un groupe abélien. Une application $f : E \to E$ est un endomorphisme du groupe abélien E (ou plus simplement un morphisme de E) si pour tous $a, b \in E$ on a $f(a + b) = f(a) + f(b)$.

La condition ci-dessus signifie que les morphismes sont les applications compatibles avec l'addition de E.

Example 6.2. Les deux éléments neutres de $\mathcal{A}(E, E)$, l'application $\mathbf{0}_E : E \to E$, $a \mapsto 0_E$ et l'identité Id_E, sont des morphismes.

Lemma 6.3. *Soit $f : E \to E$ un morphisme. On a*

$$f(0_E) = 0_E \quad \text{et} \quad f(-a) = -f(a) \text{ pour tout } a \in E.$$

Proof. Comme $0_E = 0_E + 0_E$, on a $f(0_E) = f(0_E + 0_E) = f(0_E) + f(0_E)$ puisque f est un morphisme, d'où $f(0_E) - f(0_E) = f(0_E) + f(0_E) - f(0_E)$, c'est-à-dire $0_E = f(0_E)$. Puis pour tout $a \in E$, comme $a + (-a) = 0_E$, on a $f(a + (-a)) = f(0_E)$, d'où $f(a) + f(-a) = 0_E$ puisque f est un morphisme, c'est-à-dire $f(-a) = -f(a)$. □

Lemma 6.4. *Soient f et $g : E \to E$ des morphismes. Les applications $f + g$, $-f$, et $f \circ g : E \to E$ sont des morphismes.*

Proof. Soient f et $g : E \to E$ des morphismes. On a $(f+g)(a+b) = f(a+b) + g(a+b) = f(a)+f(b)+g(a)+g(b) = (f+g)(a)+(f+g)(b)$, $(-f)(a+b) = -f(a+b) = -(f(a)+f(b)) = -f(a) - f(b) = (-f)(a) + (-f)(b)$, et $(f \circ g)(a + b) = f(g(a + b)) = f(g(a) + g(b)) = f(g(a)) + f(g(b)) = (f \circ g)(a) + (f \circ g)(b)$ pour tous $a, b \in E$. □

On note $\mathrm{End}_{\mathrm{grp}}(E)$ l'ensemble des endomorphismes du groupe abélien E. Les arguments ci-dessus montrent la proposition suivante.

Proposition 6.5. *Soit E un groupe abélien. L'ensemble $\mathrm{End}_{\mathrm{grp}}(E)$ muni de l'addition et de la composition est un anneau.*

Noter qu'en général cet anneau pas commutatif.

7. Matrices et endomorphismes

Soient K un corps et $n \geq 1$ un entier. Un cas particulier de la construction 6 précédente est celui où l'on prend pour E le groupe abélien K^n muni de l'addition de la section 2. On obtient alors l'anneau $(\mathrm{End}_{\mathrm{grp}}(K^n), +, \circ)$.

Soit $(M_n(K), +, \cdot)$ l'anneau des matrices carrées de taille n à coefficients dans K de la section 4. Une matrice $A = (a_{i,j})_{1\leq i,j\leq n}$ de $M_n(K)$ définit une application $f(A) : K^n \to K^n$ de la façon suivante. Pour tout élément $(x_k)_{1\leq k\leq n} \in K^n$ on pose

$$f(A)\Big((x_k)_{1\leq k\leq n}\Big) \underset{\text{def}}{=} \Big(\sum_{1\leq k\leq n} a_{i,k}x_k\Big)_{1\leq i\leq n}.$$

Cela signifie que l'on obtient la i-ième composante de $f(A)((x_k)_{1\leq k\leq n})$ en multipliant la k-ième composante de la i-ième ligne de A avec celle de $(x_k)_{1\leq k\leq n}$, puis en sommant ces produits sur $1 \leq k \leq n$. Noter l'analogie avec la multiplication dans $M_n(K)$: si $(x_k)_{1\leq k\leq n} = (x_{k,j})_{1\leq k\leq n}$ est la j-ième colonne d'une matrice $X = (x_{k,j})_{1\leq k,j\leq n}$ de $M_n(K)$, alors $\sum_{1\leq k\leq n} a_{i,k}x_{k,j}$ est le coefficient de la i-ième ligne et j-ième colonne de la matrice produit AX. Pour cette raison on écrit les éléments de K^n sous forme de colonne plutôt que de ligne, et l'on pose

$$\begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \underset{\text{def}}{=} \begin{pmatrix} a_{1,1}x_1 + \ldots + a_{1,n}x_n \\ \vdots \\ a_{n,1}x_1 + \ldots + a_{n,n}x_n \end{pmatrix}.$$

Lemma 7.1. *Pour tout $A \in M_n(K)$ l'application $f(A) : K^n \to K^n$ est un morphisme.*

Proof. Soit $A \in M_n(K)$. Soient $x = (x_k)_{1\leq k\leq n}$ et $y = (y_k)_{1\leq k\leq n}$ dans K^n. Alors $x + y = (x_k + y_k)_{1\leq k\leq n}$ et la i-ième composante de $f(A)(x + y)$ est

$$\sum_{1\leq k\leq n} a_{i,k}(x_k + y_k) = \sum_{1\leq k\leq n} (a_{i,k}x_k + a_{i,k}y_k) = \sum_{1\leq k\leq n} a_{i,k}x_k + \sum_{1\leq k\leq n} a_{i,k}y_k \ ,$$

c'est-à-dire la somme de la i-ième composante de $f(A)(x)$ et de celle de $f(A)(y)$. Donc $f(A)(x + y) = f(A)(x) + f(A)(y)$ pour tous $x, y \in K^n$, autrement dit $f(A) : K^n \to K^n$ est un endomorphisme du groupe abélien K^n. □

On obtient ainsi une application

$$\begin{aligned} f : M_n(K) &\longrightarrow \mathrm{End}_{\mathrm{grp}}(K^n) \\ A &\longmapsto f(A). \end{aligned}$$

Noter que $f(0_{M_n(K)}) = \mathbf{0}_{K^n}$ et $f(1_{M_n(K)}) = \mathrm{Id}_{K^n}$, autrement dit l'application f envoie les deux éléments neutres de l'anneau $M_n(K)$ dans ceux de l'anneau $\mathrm{End}_{\mathrm{grp}}(K^n)$. De plus, l'application f possède la propriété importante suivante : elle est compatible avec les deux additions et multiplications sur ces anneaux.

Proposition 7.2. *Pour tous $A, B \in M_n(K)$ on a*

$$f(A + B) = f(A) + f(B) \quad \text{et} \quad f(AB) = f(A) \circ f(B).$$

Proof. Soient $A = (a_{i,j})_{1\leq i,j\leq n}$ et $B = (b_{i,j})_{1\leq i,j\leq n}$ des matrices de $M_n(K)$. Par définition de l'addition et de la multiplication des matrices, on a

$$A + B = \big(a_{i,j} + b_{i,j}\big)_{1\leq i,j\leq n} \quad \text{et} \quad AB = \Big(\sum_{1\leq \ell\leq n} a_{i,\ell}b_{\ell,j}\Big)_{1\leq i,j\leq n}.$$

Soit $x = (x_k)_{1\leq k\leq n} \in K^n$. Par définition de f on a

$$f(A)(x) = (a_{i,j})_{1\leq i,j\leq n}\,(x_k)_{1\leq k\leq n} = \Big(\sum_{1\leq k\leq n} a_{i,k}x_k\Big)_{1\leq i\leq n}.$$

On obtient alors

$$\begin{aligned}
f(A+B)(x) &= \big(a_{i,j} + b_{i,j}\big)_{1\leq i,j\leq n}\,(x_k)_{1\leq k\leq n} \\
&= \Big(\sum_{1\leq k\leq n} (a_{i,k} + b_{i,k})x_k\Big)_{1\leq i\leq n} \\
&= \Big(\sum_{1\leq k\leq n} (a_{i,k}x_k + b_{i,k}x_k)\Big)_{1\leq i\leq n} \\
&= \Big(\sum_{1\leq k\leq n} a_{i,k}x_k + \sum_{1\leq k\leq n} b_{i,k}x_k\Big)_{1\leq i\leq n} \\
&= \Big(\sum_{1\leq k\leq n} a_{i,k}x_k\Big)_{1\leq i\leq n} + \Big(\sum_{1\leq k\leq n} b_{i,k}x_k\Big)_{1\leq i\leq n} \\
&= f(A)(x) + f(B)(x).
\end{aligned}$$

Donc $f(A + B) = f(A) + f(B)$. Puis on a

$$\begin{aligned}
f(AB)(x) &= \Big(\sum_{1\leq \ell\leq n} a_{i,\ell}b_{\ell,j}\Big)_{1\leq i,j\leq n}\,(x_k)_{1\leq k\leq n} \\
&= \Big(\sum_{1\leq k\leq n}\,\big(\sum_{1\leq \ell\leq n} a_{i,\ell}b_{\ell,k}\big)x_k\Big)_{1\leq i\leq n} \\
&= \Big(\sum_{1\leq k\leq n}\sum_{1\leq \ell\leq n} a_{i,\ell}b_{\ell,k}x_k\Big)_{1\leq i\leq n} \\
&= \Big(\sum_{1\leq k,\ell\leq n} a_{i,\ell}b_{\ell,k}x_k\Big)_{1\leq i\leq n}.
\end{aligned}$$

D'autre part on a

$$\begin{aligned}
f(B)(x) &= (b_{\ell,j})_{1\leq \ell,j\leq n}\,(x_k)_{1\leq k\leq n} \\
&= \Big(\sum_{1\leq k\leq n} b_{\ell,k}x_k\Big)_{1\leq \ell\leq n},
\end{aligned}$$

d'où

$$\begin{aligned}\big(f(A)\circ f(B)\big)(x) &= f(A)\big(f(B)(x)\big)\\ &= (a_{i,j})_{1\le i,j\le n}\Big(\sum_{1\le k\le n} b_{\ell,k}x_k\Big)_{1\le \ell\le n}\\ &= \Big(\sum_{1\le \ell\le n} a_{i,\ell}\big(\sum_{1\le k\le n} b_{\ell,k}x_k\big)\Big)_{1\le i\le n}\\ &= \Big(\sum_{1\le \ell\le n}\sum_{1\le k\le n} a_{i,\ell}b_{\ell,k}x_k\Big)_{1\le i\le n}\\ &= \Big(\sum_{1\le k,\ell\le n} a_{i,\ell}b_{\ell,k}x_k\Big)_{1\le i\le n}\\ &= f(AB)(x)\,.\end{aligned}$$

Donc $f(AB) = f(A)\circ f(B)$. □

On en déduit les propriétés suivantes de l'application $f : M_n(K) \to \mathrm{End}_{\mathrm{grp}}(K^n)$.

Corollary 7.3. *Soit $A \in M_n(K)$.*

(i) *On a $f(-A) = -f(A)$.*
(ii) *S'il existe $A^{-1} \in M_n(K)$ telle que $AA^{-1} = A^{-1}A = 1_{M_n(K)}$, alors $f(A)$ est bijective et $f(A)^{-1} = f(A^{-1})$.*

Proof. (i) On a $f(0_{M_n(K)}) = \mathbf{0}_{K^n}$ et $A + (-A) = 0_{M_n(K)}$, d'où $f(A + (-A)) = \mathbf{0}_{K^n}$. Par la proposition 7.2 on a $f(A + (-A)) = f(A) + f(-A)$, donc $f(A) + f(-A) = \mathbf{0}_{K^n}$, ce qui équivaut à $f(-A) = -f(A)$.
(ii) Soit $A^{-1} \in M_n(K)$ telle que $AA^{-1} = A^{-1}A = 1_{M_n(K)}$. On a $f(1_{M_n(K)}) = \mathrm{Id}_{K^n}$, d'où $f(AA^{-1}) = f(A^{-1}A) = \mathrm{Id}_{K^n}$. Par la proposition 7.2 on a $f(AA^{-1}) = f(A)\circ f(A^{-1})$ et $f(A^{-1}A) = f(A^{-1})\circ f(A)$, d'où $f(A)\circ f(A^{-1}) = f(A^{-1})\circ f(A) = \mathrm{Id}_{K^n}$. Donc $f(A)$ est bijective et $f(A)^{-1} = f(A^{-1})$. □

En particulier la proposition 7.2 implique que $f(A - B) = f(A) - f(B)$ pour tous $A, B \in M_n(K)$. En effet, on a $f(A - B) = f(A + (-B)) = f(A) + f(-B) = f(A) - f(B)$.

Proposition 7.4. *L'application $f : M_n(K) \to \mathrm{End}_{\mathrm{grp}}(K^n)$ est injective.*

Proof. Rappelons que f est injective si $f(B) = f(C)$ implique $B = C$. L'égalité $B = C$ dans $M_n(K)$ équivaut à $B - C = 0_{M_n(K)}$. L'égalité $f(B) = f(C)$ dans $\mathrm{End}_{\mathrm{grp}}(K^n)$ équivaut à $f(B) - f(C) = \mathbf{0}_{K^n}$, et par la proposition 7.2 on a $f(B) - f(C) = f(B - C)$. Par conséquent f est injective si $f(A) = \mathbf{0}_{K^n}$ implique $A = 0_{M_n(K)}$.

Soit $A = (a_{i,j})_{1\le i,j\le n} \in M_n(K)$ telle que $f(A) = \mathbf{0}_{K^n}$. L'égalité $f(A) = \mathbf{0}_{K^n}$ dans $\mathrm{End}_{\mathrm{grp}}(K^n)$ équivaut à

$$\Big(\sum_{1\le k\le n} a_{i,k}x_k\Big)_{1\le i\le n} = 0_{K^n} \quad \text{pour tout } (x_k)_{1\le k\le n} \in K^n,$$

ou bien encore $\sum_{1\le k\le n} a_{i,k}x_k = 0$ pour tous $1 \le i \le n$ et $(x_k)_{1\le k\le n} \in K^n$. Pour $1 \le j \le n$ soit $e_j \in K^n$ l'élément dont toutes les composantes sont 0 sauf la j-ième qui est 1. On a donc

$$e_j \underset{\text{def}}{=} \big(\delta_{k,j}\big)_{1\le k\le n} \in K^n \quad \text{avec } \delta_{k,j} = 0 \text{ si } k \ne j \text{ et } \delta_{j,j} = 1.$$

Alors, pour tous $1 \leq j \leq n$ et $1 \leq i \leq n$ on a

$$a_{i,j} = \sum_{1 \leq k \leq n} a_{i,k}\delta_{k,j} = 0\,,$$

c'est-à-dire $A = 0_{M_n(K)}$. Donc f est injective. □

La proposition 7.4 permet d'identifier $M_n(K)$ avec son image dans $\mathrm{End}_{\mathrm{grp}}(K^n)$, et la proposition 7.2 montre que les propriétés de l'anneau $(\mathrm{End}_{\mathrm{grp}}(K^n), +, \circ)$ impliquent celles de $(M_n(K), +, \cdot)$. Le résultat suivant en est un exemple.

Corollary 7.5. *Pour tous $A, B, C \in M_n(K)$ on a $A(BC) = (AB)C$.*

Proof. Soient $A, B, C \in M_n(K)$. On a $f(A(BC)) = f(A) \circ f(BC) = f(A) \circ (f(B) \circ f(C))$ et $f((AB)C) = f(AB) \circ f(C) = (f(A) \circ f(B)) \circ f(C)$ par la proposition 7.2. L'associativité de la composition dans $\mathrm{End}_{\mathrm{grp}}(K^n)$ donne alors l'égalité $f(A(BC)) = f((AB)C)$, et la proposition 7.4 implique $A(BC) = (AB)C$. □