9

Lois de composition

Dans tout le chapitre, $\mathbb{K}$ désigne indifféremment $\mathbb{R}$ ou $\mathbb{C}$.

1. Lois de composition interne (Mpsi)

Définition.– Une loi de composition interne sur un ensemble E est une application $\otimes$ de $E \times E$ dans E. Un magma est un couple $(E,\otimes)$ où E est un ensemble et où $\otimes$ est une loi de composition interne sur E.

<u>Remarque</u> : L'image du couple (x,y) par l'application $\otimes$ est notée $x \otimes y$ au lieu de $\otimes((x,y))$.

Définition.– Soit $(E,\otimes)$ un magma.

1) La loi $\otimes$ est dite associative si et seulement si : $\forall (x,y,z) \in E^3,\ (x\otimes y)\otimes z = x \otimes (y \otimes z)$.
   Lorsque la loi $\otimes$ est associative on dit que le magma $(E,\otimes)$ est associatif.
2) La loi $\otimes$ est dite commutative si et seulement si : $\forall (x,y) \in E^2,\ x\otimes y = y \otimes x$.
   Lorsque $\otimes$ est commutative on dit que le magma $(E,\otimes)$ est commutatif.
3) Un élément neutre du magma $(E,\otimes)$ est un élément e de E vérifiant :
   $\forall x \in E,\ x \otimes e = e \otimes x = x$.
   Lorsque le magma $(E,\otimes)$ admet un élément neutre e on dit qu'il est unifère.

Théorème.– Si le magma $(E,\otimes)$ admet un élément neutre alors il est unique.

Définition.– Soient $(E,\otimes)$ un magma unifère d'élément neutre e et a un élément de E.
Tout élément b de E vérifiant $a\otimes b = b \otimes a = e$ est appelé un symétrique de a dans $(E,\otimes)$.
L'élément a est dit symétrisable dans $(E,\otimes)$ si et seulement si il admet au moins un symétrique dans $(E,\otimes)$.

Définition.– Soient $\oplus$ et $\otimes$ deux lois de composition internes sur un ensemble E.

1) Une partie A de E est dite stable pour la loi $\otimes$ si et seulement si : $\forall (a,b) \in E^2, a\otimes b \in A$.
2) La loi $\otimes$ est dite distributive par rapport à la loi $\oplus$ si et seulement si :
   $\forall (x,y,z) \in E^3,\ x \otimes (y \oplus z) = (x\otimes y)\oplus(x\otimes z)$ et $(x\oplus y)\otimes z = (x \otimes z)\oplus(y\otimes z)$.

1.1 Notions de monoïde et de groupe

Définition.– Un monoïde est un magma associatif et unifère.
Un groupe est un monoïde dans lequel tout élément est symétrisable.

Théorème.– Soit $(M,\otimes)$ un monoïde et $(x,y) \in M^2$.

1) Si l'élément x est symétrisable dans $(M,\otimes)$ alors x admet un unique symétrique dans $(M,\otimes)$ et cet unique symétrique est noté x^{-1}.
2) Si les éléments x et y sont symétrisables dans $(M,\otimes)$ alors l'élément $x\otimes y$ est symétrisable dans $(M,\otimes)$ et $(x\otimes y)^{-1} = y^{-1}\otimes x^{-1}$.

1.2 Notions d'anneaux et de corps

Définition.– On appelle anneau tout triplet $(A,+,\times)$ où A est un ensemble, + et $\times$ sont deux lois de composition interne sur A tels que :

(A_1) $(A,+)$ est un groupe abélien.
(A_2) $(A,\times)$ est un monoïde.
(A_3) $\times$ est distributive par rapport à +.

<u>Notations adoptées dans un anneau</u>
Soit $(A,+,\times)$ un anneau. L'élément neutre du groupe $(A,+)$ est noté 0_A. L'élément neutre du monoïde $(A,\times)$ est noté 1_A. On a donc : $\forall a \in A,\ a + 0_A = a$ et $a \times 1_A = a \times 1_A = a$.
L'anneau $(A,+,\times)$ est dit non nul si et seulement si $1_A \neq 0_A$. On dit que l'anneau $(A,+,\times)$ est commutatif si et seulement si la loi $\times$ est commutative.
$(A,+)$ étant un groupe tout élément a de A est symétrisable dans $(A,+)$. Le symétrique de a dans $(A,+)$ est noté $-a$ et est appelé opposé de a dans A. On a donc : $\forall a \in A,\ a + (-a) = 0_A$.
Par contre un élément de A n'est pas nécessairement symétrisable dans $(A,\times)$. C'est d'ailleurs la seule chose qui empêche $(A,\times)$ d'être un groupe. On dit qu'un élément a de A est inversible dans l'anneau $(A,+,\times)$ si et seulement si il est symétrisable dans le monoïde $(A,\times)$ c'est-à-dire si et seulement si il existe $b \in A$ tel que $ab = ba = 1_A$. Dans ces conditions la symétrique b de a dans $(A,\times)$ est noté a^{-1} et est appelé inverse de a dans l'anneau $(A,+,\times)$.
On note $A^\times$ ou encore $U(A)$ l'ensemble des éléments inversibles de l'anneau $(A,+,\times)$.
Par définition même on a donc : $A^\times = \{a \in A, \exists b \in A \mid ab = ba = 1_A\}$.

Théorème.– Soit $(A,+,\times)$ un anneau.
$(A^\times,\times)$ est un groupe. Il est appelé groupe des éléments inversibles de l'anneau $(A,+,\times)$.

Définition.– Un anneau $(A,+,\times)$ est dit sans diviseurs de zéro si et seulement si il vérifie la propriété : $\forall (a,b) \in A^2,\ ab = 0_A \Rightarrow a = 0_A$ ou $b = 0_A$.
Un anneau intègre est un anneau commutatif non nul et sans diviseurs de zéro.

Définition.– Un corps est un anneau commutatif non nul dans lequel tout élément non nul est inversible.

Proposition.– Si $(K,+,\times)$ est un corps alors $(K,+)$ est un groupe abélien, $(K \setminus \{0_K\},\times)$ est un groupe, $(K,+,\times)$ est un anneau intègre, $K^\times = K \setminus \{0_K\}$ et $1_K \neq 0_K$.

2. Exemples fondamentaux de lois de composition interne (Mpsi)

2.1 Du côté des nombres

- ✓ $(\mathbb{N},+)$ est un monoïde commutatif d'élément neutre 0. Ce neutre 0 est le seul entier naturel à être inversible dans $(\mathbb{N},+)$ et il est son propre inverse.
- ✓ $(\mathbb{N},\times)$ est un monoïde commutatif d'élément neutre 1. Ce neutre 1 est l'unique entier naturel à être inversible dans $(\mathbb{N},\times)$ et il est son propre inverse.
- ✓ $(\mathbb{N},+,\times)$ n'est pas un anneau.
- ✓ $(\mathbb{Z},+)$ est un groupe commutatif d'élément neutre 0. L'inverse de $n \in \mathbb{Z}$ dans $(\mathbb{Z},+)$ est $-n$.
- ✓ $(\mathbb{Z},\times)$ est un monoïde commutatif d'élément neutre 1. Les éléments 1 et -1 sont les seuls entiers relatifs à être inversibles dans $(\mathbb{Z},\times)$ et ils sont leurs propres inverses.
- ✓ $(\mathbb{Z},+,\times)$ est un anneau intègre, $0_\mathbb{Z} = 0$, $1_\mathbb{Z} = 1$ et $\mathbb{Z}^\times = \{-1,1\}$.
- ✓ $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des corps.

2.2 Du côté du produit cartésien

$\mathbb{K}^n$ est l'ensemble des n-uplets de la forme $(x_1,\cdots,x_n)$ où $x_1,\cdots,x_n$ sont des éléments de $\mathbb{K}$.
Etant donnés deux éléments $x = (x_1,\cdots,x_n)$ et $y = (y_1,\cdots,y_n)$ de $\mathbb{K}^n$ on pose par définition :
$x + y = (x_1 + y_1,\cdots,x_n + y_n)$ et $x \times y = (x_1y_1,\cdots,x_ny_n)$.

- ✓ $(\mathbb{K}^n,+)$ est un groupe commutatif d'élément neutre $(0,\cdots,0)$.
  L'inverse de $x = (x_1,\cdots,x_n) \in \mathbb{K}^n$ dans $(\mathbb{K}^n,+)$ est égal à $(-x_1,\cdots,-x_n)$.
- ✓ $(\mathbb{K}^n,\times)$ est un monoïde d'élément neutre $(1,\cdots,1)$. Un élément $x = (x_1,\cdots,x_n) \in \mathbb{K}^n$ est inversible dans $(\mathbb{K}^n,\times)$ si et seulement si $x_1 \cdots x_n \neq 0$. L'inverse de x dans $(\mathbb{K}^n,\times)$ est alors égal à $\left(\frac{1}{x_1},\cdots,\frac{1}{x_n}\right)$.

Proposition.– $(\mathbb{K}^n,+,\times)$ est un anneau commutatif, $0_{\mathbb{K}^n} = (0,\cdots,0)$ et $1_{\mathbb{K}^n} = (1,\cdots,1)$.
$(\mathbb{K}^n)^\times$ est égal à l'ensemble des éléments $x = (x_1,\cdots,x_n)$ de $\mathbb{K}^n$ vérifiant $x_1 \cdots x_n \neq 0$.

2.3 Du côté des applications

Soit E un ensemble. On rappelle que E^E désigne l'ensemble des applications de E dans E.
L'ensemble des bijections de E sur E est noté S_E.
Un élément de S_E est appelé une permutation de E.

- ✓ $(E^E,\circ)$ est un monoïde d'élément neutre Id_E. Il n'est pas nécessairement commutatif.
  Les éléments inversibles de $(E^E,\circ)$ sont les bijections.
- ✓ $(S_E,\circ)$ est un groupe d'élément neutre Id_E. E. Si $f \in S_E$ alors l'inverse de f dans $(S_E,\circ)$ est la bijection réciproque f^{-1} de f. Le groupe $(S_E,\circ)$ est appelé groupe symétrique, ou encore groupe des permutations, de l'ensemble E. Il n'est pas nécessairement commutatif.
- ✓ Soit $n \in \mathbb{N}^*$. L'ensemble $S_{[1,n]}$ des permutations de l'ensemble $[\![1,n]\!]$ est noté S_n.
  $(S_n,\circ)$ est un groupe fini de cardinal $n!$.

D est un ensemble quelconque. $\mathbb{K}^D$ désigne l'ensemble des applications de D dans $\mathbb{K}$.
Etant données f et g dans $\mathbb{K}^D$ on définit les applications $f+g : D \to \mathbb{K}$ et $f \times g : D \to \mathbb{K}$ par :
$\forall t \in D$, $(f+g)(t) = f(t) + g(t)$ et $(f \times g)(t) = f(t)g(t)$.

- ✓ $(\mathbb{K}^D,+)$ est un groupe commutatif de neutre l'application constante égale à 0.
  L'inverse de f dans le groupe $(\mathbb{K}^D,+)$ est l'application $(x \to -f(x))$. On la note $-f$.
- ✓ $(\mathbb{K}^D,\times)$ est un monoïde de neutre l'application constante égale à 1. Les éléments de $\mathbb{K}^D$ qui sont inversibles dans $(\mathbb{K}^D,\times)$ sont les applications $f : D \to \mathbb{K}$ qui ne s'annulent pas sur D.

Proposition.– $(\mathbb{K}^D,+,\times)$ est un anneau commutatif non intègre.
$0_{\mathbb{K}^D}$ est l'application constante égale à 0 et $1_{\mathbb{K}^D}$ est l'application constante égale à 1
$(\mathbb{K}^D)^\times$ est l'ensemble des applications $f : D \to \mathbb{K}$ qui ne s'annule pas sur D.

<u>Remarque</u> : La plupart du temps le symbole $\times$ est omis dans l'écriture des calculs. L'application $0_{\mathbb{K}^D}$ (resp $1_{\mathbb{K}^D}$) est simplement notée 0 (resp 1). C'est abusif mais pratique. On prendra garde à ce que dans cet anneau la propriété $fg = 0$ n'implique pas nécessairement ($f = 0$ ou $g = 0$).

3. Lois de composition externe

3.1 Définition et notation (Mpsi)

Définition.– Soient Λ et E deux ensembles. On appelle loi de composition externe sur E à domaine d'opérateurs dans Λ toute application $\odot$ de $\Lambda \times E$ dans E.

<u>Notations</u> Soient $\odot : \Lambda \times E \to E$ une loi de composition externe sur E à domaine d'opérateurs dans Λ et $(\lambda, x) \in \Lambda \times E$. L'image de (λ, x) par $\odot$ est notée $\lambda \odot x$ au lieu de $\odot((\lambda, x))$.
La plupart du temps une loi de composition externe $\odot$ est notée $\bullet$.

3.2 Structure de $\mathbb{K}$-espace vectoriel (Mpsi)

Définition.– Un $\mathbb{K}$-espace vectoriel est un triplet $(E,+,\bullet)$ où E est un ensemble, $+$ une loi de composition interne sur E, $\bullet$ une loi de composition externe sur E à domaine d'opérateurs dans $\mathbb{K}$ tels que :

(E_1) $(E,+)$ est un groupe abélien.

(E_2) $\forall \alpha \in \mathbb{K}, \forall (x,y) \in E^2, \alpha\bullet(x+y) = \alpha\bullet x + \beta\bullet y.$

(E_3) $\forall (\alpha,\beta) \in \mathbb{K}^2, \forall x \in E, (\alpha+\beta)\bullet x = \alpha\bullet x + \beta\bullet x.$

(E_4) $\forall (\alpha,\beta) \in \mathbb{K}^2, \forall x \in E, (\alpha\beta)\bullet x = \alpha\bullet(\beta\bullet x).$

(E_5) $\forall x \in E, 1\bullet x = x.$

<u>Notations adoptées dans un espace vectoriel</u>

Soit $(E,+,\bullet)$ un $\mathbb{K}$-espace vectoriel. L'élément neutre du groupe $(E,+)$ est noté 0_E. On a donc : $\forall x \in E, \ x + 0_E = 0_E + x = x$. L'inverse de $x \in E$ dans $(E,+)$ est noté $-x$ et est appelé opposé de x. On a donc : $\forall x \in E, \ x + (-x) = (-x) + x = 0_E$. Les éléments de l'ensemble E sont appelés des vecteurs et ceux de l'ensemble $\mathbb{K}$ sont appelés des scalaires. La plupart du temps, le symbole $\bullet$ est omis dans les calculs. Pour $(\alpha,\beta) \in \mathbb{K}^2$ et $(x,y) \in E^2$ on note $\alpha x + \beta y$.

<u>Des exemples fondamentaux</u>

$\mathbb{K}^n$ est l'ensemble des n-uplets de la forme $(x_1,\cdots,x_n)$ où $x_1,\cdots,x_n$ sont des éléments de $\mathbb{K}$.
On sait que $(\mathbb{K}^n,+)$ est un groupe commutatif.
Etant donnés λ dans $\mathbb{K}$ et $x = (x_1,\cdots,x_n)$ dans $\mathbb{K}^n$ on pose par définition : $\lambda\bullet x = (\lambda x_1,\cdots,\lambda x_n)$.

Proposition.– $(\mathbb{K}^n,+,\bullet)$ est un $\mathbb{K}$-espace vectoriel.

Soit D un ensemble quelconque. On sait que $(\mathbb{K}^D,+)$ est un groupe commutatif.

Etant donnés $\alpha \in \mathbb{K}$ et $f \in \mathbb{K}^D$ on note $\alpha\bullet f$ l'application de D dans $\mathbb{K}$ définie par : $(\alpha\bullet f)(t) = \alpha f(t)$. On définit ainsi une loi de composition externe $\bullet$ sur $\mathbb{K}^D$ à domaine d'opérateurs dans $\mathbb{K}$.

Proposition.– $(\mathbb{K}^D,+,\bullet)$ est un $\mathbb{K}$-espace vectoriel.

3.3 Familles presque nulles d'éléments d'un $\mathbb{K}$-espace vectoriel (Mpsi)

Soient $(E^I,+,\bullet)$ un $\mathbb{K}$-espace vectoriel et I un ensemble quelconque.
L'ensemble des familles de vecteurs de E indexée par I, qui n'est autre que l'ensemble des applications de I dans E, est noté E^I.

Définition.– Soit $x = (x_i)_{i\in I} \in E^I$.
L'ensemble $S_x = \{i \in I \mid x_i \neq 0_E\}$ est appelé support de la famille $x = (x_i)_{i\in I}$.
La famille $x = (x_i)_{i\in I}$ est dite presque nulle si et seulement si son support S_x est un ensemble fini.
L'ensemble des familles presque nulle de vecteurs de E indexée par I est notée $E^{(I)}$.

<u>Exemples</u> :
- ➤ Toute famille finie de vecteurs de E est une famille presque nulle de vecteurs de E.
- ➤ Un polynôme à coefficients dans $\mathbb{K}$ est une suite presque nulle d'éléments de $\mathbb{K}$.

Proposition.– Si $(\alpha_i)_{i\in I}$ est une famille presque nulle de scalaires et si $(x_i)_{i\in I}$ est une famille de vecteurs de E alors $(\alpha_i x_i)_{i\in I}$ est une famille presque nulle de vecteurs de E.

Proposition.– $(E^I,+,\bullet)$ est un $\mathbb{K}$-espace vectoriel et $E^{(I)}$ est un sous espace vectoriel de $(E^I,+,\bullet)$.

3.4 La $\mathbb{K}$-algèbre $\mathbb{K}^D$ des applications de D dans $\mathbb{K}$

Soit D un ensemble quelconque. On rappelle que $\mathbb{K}^D$ désigne l'ensemble des applications de D dans $\mathbb{K}$. Soient $+$ et $\times$ les lois de composition interne sur $\mathbb{K}^D$ définies au paragraphe 2.4.
On sait que $(\mathbb{K}^D,+,\times)$ est un anneau commutatif.
Soit $\bullet$ la loi de composition externe sur $\mathbb{K}^D$ définie au paragraphe 3.2.
On sait que $(\mathbb{K}^D,+,\bullet)$ est un $\mathbb{K}$-espace vectoriel.

On constate d'autre part que : $\forall (f,g) \in (\mathbb{K}^D)^2, \forall \alpha \in \mathbb{K},\ \alpha\bullet(f \times g) = (\alpha\bullet f) \times g = f \times (\alpha\bullet g)$.

Le quadruplet $(\mathbb{K}^D,+,\times,\bullet)$ vérifie donc les trois propriétés suivantes :

1) $(\mathbb{K}^D,+,\times)$ est un anneau.

2) $(\mathbb{K}^D,+,\bullet)$ est un $\mathbb{K}$-espace vectoriel.

3) $\forall (f,g) \in (\mathbb{K}^D)^2, \forall \alpha \in \mathbb{K},\ \alpha\bullet(f \times g) = (\alpha\bullet f) \times g = f \times (\alpha\bullet g)$.

Pour résumer cela on dit que $(\mathbb{K}^D,+,\times,\bullet)$ est une $\mathbb{K}$-algèbre.

Comme $\times$ est commutative, on dit que la $\mathbb{K}$-algèbre $(\mathbb{K}^D,+,\times,\bullet)$ est commutative.

Pour simplifier les notations, les lois $\times$ et $\bullet$ sont la plupart du temps omises dans l'écriture des calculs. Pour λ,μ dans $\mathbb{K}$ et pour f,g dans $\mathbb{K}^D$ on adoptera donc les écritures : $\lambda f + \mu g$ et fg.

On prendra garde à ce que dans cette algèbre la propriété $fg = 0$ n'implique pas nécessairement $(f = 0$ ou $g = 0)$. L'anneau $(\mathbb{K}^D,+,\times)$ n'est donc pas intègre.

Définition.– On appelle $\mathbb{K}$-algèbre tout quadruplet $(\mathcal{A},+,\times,\bullet)$ où $\mathcal{A}$ est un ensemble, où $+$ et $\times$ sont des lois de composition internes sur $\mathcal{A}$, et où $\bullet$ est une loi de composition externe sur $\mathcal{A}$ à domaine d'opérateurs dans $\mathbb{K}$ tels que :

(AL_1) $(\mathcal{A},+,\times)$ est un anneau.

(AL_2) $(\mathcal{A},+,\bullet)$ est un $\mathbb{K}$-espace vectoriel.

(AL_3) $\forall \alpha \in \mathbb{K},\ \forall (a,b) \in \mathcal{A}^2,\ \alpha\bullet(a \times b) = (\alpha\bullet a) \times b = a \times (\alpha\bullet b)$.

Une $\mathbb{K}$-algèbre $(\mathcal{A},+,\times,\bullet)$ est dite commutative (resp intègre) si et seulement si l'anneau sous-jacent $(\mathcal{A},+,\times)$ est commutatif (resp intègre).

Théorème.– $(\mathbb{K}^D,+,\times,\bullet)$ est une $\mathbb{K}$-algèbre commutative non intègre.

3.5 La $\mathbb{K}$-algèbre des suites d'éléments de $\mathbb{K}$

On appelle suite d'éléments de $\mathbb{K}$ toute application de $\mathbb{N}$ dans $\mathbb{K}$.

Si $u : \mathbb{N} \to \mathbb{K}$ est une suite d'éléments de $\mathbb{K}$ alors pour tout $n \in \mathbb{N}$, le scalaire $u(n)$ est noté u_n et la suite u est notée $(u_n)_{n\in\mathbb{N}}$ ou encore plus simplement (u_n).

Les résultats du paragraphe précédent sont valables dans le cas particulier où $D = \mathbb{N}$ et on dispose donc de la $\mathbb{K}$-algèbre $(\mathbb{K}^{\mathbb{N}},+,\times,\bullet)$ où les lois $+,\times$ et $\bullet$ sont définies par :

$(u_n)+(v_n) = (u_n + v_n),\ \ (u_n)\times(v_n) = (u_n v_n)$ et $\alpha(u_n) = (\alpha u_n)$.

Proposition.– $(\mathbb{K}^{\mathbb{N}},+,\times,\bullet)$ est une $\mathbb{K}$-algèbre intègre.

3.6 La $\mathbb{K}$-algèbre des endomorphismes d'un $\mathbb{K}$-espace vectoriel

Soit E un $\mathbb{K}$-espace vectoriel. Sur l'ensemble des applications de E dans E, alias E^E, on dispose des lois de composition internes $+$ et $\circ$. Si f et g sont des applications de E dans E alors $f+g$ et $f \circ g$ sont les applications de E dans E définies par : $(f+g)(x) = f(x)+g(x)$ et $(f \circ g)(x) = f(g(x))$.

$(E^E,+)$ est un groupe abélien d'élément neutre l'application nulle.

$(E^E,\circ)$ est un monoïde d'élément neutre Id_E.

Dans E^E, la loi $\circ$ n'est pas distributive par rapport à la loi $+$.

Sur E^E on dispose aussi d'une loi de composition externe $\bullet$ à domaine d'opérateurs dans $\mathbb{K}$.

Si f est une application de E dans E et si λ est un scalaire alors $\lambda\bullet f$ est l'application de E dans E définie par : $\forall x \in E,\ (\lambda\bullet f)(x) = \lambda f(x)$.

Proposition.– $(E^E,+,\bullet)$ est un $\mathbb{K}$-espace vectoriel.

Un endomorphisme de E est par définition une application linéaire de E dans E.

On note $L(E)$ l'ensemble des endomorphismes de E. On vérifie que si u et v sont des applications linéaires et λ est un scalaire alors $u+v$, $u \circ v$ et $\lambda\bullet u$ sont encore des applications linéaires.

$(L(E),+)$ est un groupe abélien d'élément neutre l'application nulle.

$(L(E),\circ)$ est un monoïde d'élément neutre Id_E.

Dans $L(E)$, la loi $\circ$ est distributive par rapport à $+$.

$(L(E),+,\circ)$ est donc un anneau, contrairement à $(E^E,+,\circ)$.

$(L(E),+,\bullet)$ est un $\mathbb{K}$-espace vectoriel.

$\forall \lambda \in \mathbb{K}, \forall (u,v) \in L(E)^2,\ \lambda(u \circ v) = (\lambda u) \circ v = u \circ (\lambda v)$.

Théorème.– $(L(E),+,\circ,\bullet)$ est une $\mathbb{K}$-algèbre, non commutative et non intègre lorsque $\dim E \geq 2$.

<u>Remarque</u> : Etant donné $(u,v) \in L(E)^2$, la composée $u \circ v$ est souvent notée uv. Il faut prendre garde à ce qu'à priori ce « produit » n'est pas commutatif. On peut en effet avoir $uv \neq vu$.

Il faut aussi noter que la condition $uv = 0_{L(E)}$ n'entraîne nullement $u = 0_{L(E)}$ ou $v = 0_{L(E)}$.

Un automorphisme de E est un endomorphisme bijectif de E. L'ensemble des automorphismes de E est noté $GL(E)$. $GL(E)$ n'est rien d'autre que l'ensemble des éléments inversibles de l'anneau $(L(E),+,\circ)$ c'est-à-dire l'ensemble des éléments inversibles du monoïde $(L(E),\circ)$.

Théorème.– $(GL(E),\circ)$ est un groupe. Il est appelé groupe linéaire de E.

4. La $\mathbb{K}$-algèbre des polynômes à une indéterminée

On appelle polynôme à une indéterminée à coefficients dans $\mathbb{K}$ toute suite $P=(a_n)$ d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang c'est à dire telle que : $\exists N \in \mathbb{N}, \forall n \geq N,\ a_n = 0_{\mathbb{K}}$.

Si $P=(a_n)$ est un polynôme alors les scalaires a_k, $k \in \mathbb{N}$ sont appelés les coefficients du polynôme P. On note aussi : $P=(a_0,a_1,\cdots,a_n,\cdots)$.

Deux polynômes $P=(a_n)$ et $Q=(b_n)$ sont égaux si et seulement si ils ont mêmes coefficients c'est-à-dire si et seulement si $\forall n \in \mathbb{N},\ a_n = b_n$.

L'ensemble des polynômes à une indéterminée à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$.

Etant donnés deux polynômes $P=(a_n)$, $Q=(b_n)$ à coefficients dans $\mathbb{K}$ et un scalaire $\lambda \in \mathbb{K}$ on définit les polynômes $P+Q$, $\lambda\bullet P$ et $P\times Q$ par :

$$P+Q=(a_n+b_n),\ \lambda\bullet P=(\lambda a_n) \text{ et } P\times Q=(c_n) \text{ avec } c_n=\sum_{k=0}^{n} a_k b_{n-k}.$$

Il est important de remarquer que si l'addition des polynômes « coïncide » avec l'addition des suites définie au paragraphe précédent il n'en est pas de même de la multiplication des polynômes. C'est d'ailleurs cette nouvelle multiplication qui fait tout l'intérêt de la notion de polynôme.

$(\mathbb{K}[X],+)$ est un groupe abélien d'élément neutre $0_{\mathbb{K}[X]}=(0,0,\cdots,0,\cdots)$.

$(\mathbb{K}[X],\times)$ est un monoïde commutatif d'élément neutre $1_{\mathbb{K}[X]}=(1,0,\cdots,0,\cdots)$.

La loi $\times$ est distributive par rapport à la loi $+$.

$(\mathbb{K}[X],+,\times)$ est donc un anneau commutatif.

$(\mathbb{K}[X],+,\bullet)$ est un $\mathbb{K}$-espace vectoriel.

$\forall \lambda \in \mathbb{K}, \forall (P,Q) \in \mathbb{K}[X]^2,\ \lambda(PQ)=(\lambda P)Q=P(\lambda Q)$.

Théorème.– $(\mathbb{K}[X],+,\times,\bullet)$ est une $\mathbb{K}$-algèbre intègre.

Par définition on pose : $X=(0,1,0,\cdots,0,\cdots)$. On constate, en utilisant la définition de la multiplication des polynômes, que pour tout $n \in \mathbb{N}$ $X^n=(0,\cdots,0,1,0,\cdots)$, le un se situant en $n^{\text{ème}}$ position, étant entendu que l'on numérote les positions en commençant par 0.

Pour tout polynôme P de $\mathbb{K}[X]$ il existe une unique suite (a_n) d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang telle que $P=\sum_{n\in\mathbb{N}} a_n X^n$. Les a_n, $n \in \mathbb{N}$ ne sont autre que les coefficients du polynôme P et il faut bien comprendre que le symbole $\sum_{n\in\mathbb{N}} a_n X^n$ désigne une somme <u>finie</u> de polynômes qui vaut par définition $\sum_{n\in S_P} a_n X^n$ où S_P est l'ensemble fini défini par $S_P=\{n \in \mathbb{N} \mid a_n \neq 0_{\mathbb{K}}\}$.

Via cette nouvelle notation on a les propriétés suivantes :

$$\sum_{n\in\mathbb{N}} a_n X^n = \sum_{n\in\mathbb{N}} b_n X^n \Leftrightarrow \forall n \in \mathbb{N},\ a_n = b_n.$$

$$\sum_{n\in\mathbb{N}} a_n X^n = 0_{\mathbb{K}[X]} \Leftrightarrow \forall n \in \mathbb{N},\ a_n = 0.$$

$$\sum_{n\in\mathbb{N}} a_n X^n + \sum_{n\in\mathbb{N}} b_n X^n = \sum_{n\in\mathbb{N}} (a_n+b_n) X^n \text{ et } \lambda\sum_{n\in\mathbb{N}} a_n X^n = \sum_{n\in\mathbb{N}} \lambda a_n X^n.$$

$$\left(\sum_{n\in\mathbb{N}} a_n X^n\right)\left(\sum_{n\in\mathbb{N}} b_n X^n\right) = \sum_{n\in\mathbb{N}} (a_0 b_n + \cdots + a_n b_0) X^n.$$

5. La $\mathbb{K}$-algèbre des matrices carrées d'ordre n

Soit $n \in \mathbb{N}^*$. On note $M_n(\mathbb{K})$ l'ensemble des matrices carrées d'ordre n à coefficients dans $\mathbb{K}$.

Etant données $A=(a_{ij})$, $B=(b_{ij})$ dans $M_n(\mathbb{K})$ et λ dans $\mathbb{K}$ on définit les matrices $A+B$, λA et $A\times B$ de $M_n(\mathbb{K})$ par :

$$A+B=(a_{ij}+b_{ij}),\ \lambda\bullet A=(\lambda a_{ij}) \text{ et } A\times B=(c_{ij}) \text{ avec } c_{ij}=\sum_{k=1}^{m} a_{ik} b_{kj}.$$

La matrice identité d'ordre n est la matrice I_n définie par : $I_n=(\delta_{ij})$ avec $\delta_{ii}=1$ et $\delta_{ij}=0$ pour $i \neq j$.

$(M_n(\mathbb{K}),+)$ est un groupe abélien de neutre la matrice nulle.

$(M_n(\mathbb{K}),\times)$ est un monoïde d'élément neutre I_n.

La loi $\times$ est distributive par rapport à la loi $+$.

$(M_n(\mathbb{K}),+,\times)$ est donc un anneau.

D'autre part, $(M_n(\mathbb{K}),+,\bullet)$ est un $\mathbb{K}$-espace vectoriel.

$\forall \lambda \in \mathbb{K}, \forall (A,B) \in M_n(\mathbb{K})^2, \ \lambda(AB) = (\lambda A)B = A(\lambda B).$

Théorème.– $(M_n(\mathbb{K}),+,\times,\cdot)$ est une $\mathbb{K}$-algèbre, non commutative et non intègre pour $n \geq 2$.

<u>Remarque</u> : Il est à noter que pour $n \geq 2$, la multiplication matricielle n'est pas commutative et que dans $M_n(\mathbb{K})$ on peut avoir $AB = 0$ avec $A \neq 0$ et $B \neq 0$.

$(M_n(\mathbb{K}),\times)$ est un monoïde d'élément neutre I_n où $I_n = \mathrm{Diag}(1,\cdots,1)$.
On notera que $(M_n(\mathbb{K}),\times)$ n'est pas un groupe.
Soit $A \in M_n(\mathbb{K})$. Dire que la matrice A est inversible signifie qu'elle est inversible dans l'anneau $(M_n(\mathbb{K}),+,\times)$ c'est-à-dire inversible dans le monoïde $(M_n(\mathbb{K}),\times)$. Cela signifie qu'il existe $B \in M_n(\mathbb{K})$ telle que $AB = BA = I_n$. En cas d'existence l'inverse de A est noté A^{-1}.
L'ensemble des matrices inversibles de $M_n(\mathbb{K})$ est noté $GL_n(\mathbb{K})$.

Théorème.– $(GL_n(\mathbb{K}),\times)$ est un groupe. Il est appelé groupe linéaire d'ordre n.

Pour $(i,j) \in [\![1,n]\!]^2$ on note $E_{ij}^{(n)}$ la matrice de $M_n(\mathbb{K})$ dont tous les éléments sont nuls sauf celui se situant à l'intersection de la $i^{\text{ème}}$ ligne et de la $j^{\text{ème}}$ colonne qui lui vaut 1. Pour des raisons de commodité la matrice $E_{ij}^{(n)}$ est la plupart du temps simplement notée E_{ij}.

Proposition.– Etant donné $(i,j,k,l) \in [\![1,n]\!]^4$ on a : $E_{ij}^{(n)}E_{kl}^{(n)} = \delta_{jk}E_{il}^{(n)}$.

Proposition.– Soit $(A,B) \in M_n(\mathbb{K})^2$.
1) Si A et B sont triangulaires supérieures (resp triangulaires inférieures, resp diagonales) alors AB est une matrice triangulaire supérieure (resp triangulaire inférieure, resp diagonale) dont chaque élément diagonal est le produit des éléments diagonaux correspondants des matrices A et B. (Mpsi)
2) Si A est triangulaire supérieure (resp triangulaire inférieure) alors A est inversible si et seulement si les éléments diagonaux de A sont tous non nuls et dans ces conditions A^{-1} est une matrice triangulaire supérieure (resp triangulaire inférieure) dont les éléments diagonaux sont les inverses des éléments diagonaux de A. (Mpsi)
3) Si A est triangulaire supérieure (resp triangulaire inférieure) et à diagonale nulle alors $A^n = 0$. (HP)

6. Opérations élémentaires sur les matrices

Soit $n \in \mathbb{N}^*$. $M_n(\mathbb{K})$ désigne l'ensemble des matrices carrées d'ordre n à coefficients dans $\mathbb{K}$.

6.1 Matrices de permutation, matrices élémentaires de dilatation et de transvection

Définition.– A toute permutation $\sigma \in S_n$ on associe la matrice $P_\sigma = (p_{ij})$ de $M_n(\mathbb{K})$ définie par $\forall (i,j) \in [\![1,n]\!]^2$, $p_{ij} = \delta_{i\sigma(j)}$. On dit que $A \in M_n(\mathbb{K})$ est une matrice de permutation si et seulement si il existe $\sigma \in S_n$ telle que $A = P_\sigma$.

Proposition.– Soit $(\sigma,\sigma')^2 \in S_n^2$.
1) $P_\sigma P_{\sigma'} = P_{\sigma\circ\sigma'}$.
2) $P_\sigma \in GL_n(\mathbb{K})$, $P_\sigma^{-1} = P_{\sigma^{-1}}$ et $\det P_\sigma = \varepsilon(\sigma)$.

Définition.– A tout $\alpha \in \mathbb{K}^*$ et à tout $i \in [\![1,n]\!]$ on associe la matrice $D_i(\alpha)$ de $M_n(\mathbb{K})$ définie par $D_i(\alpha) = I_n + (\alpha-1)E_{ii} = \mathrm{diag}(1,\cdots,1,\alpha,1,\cdots,1)$. On dit que $A \in M_n(\mathbb{K})$ est une matrice élémentaire de dilatation si et seulement si il existe $\alpha \in \mathbb{K}^*$ et $i \in [\![1,n]\!]$ tels que $A = D_i(\alpha)$.

Proposition.– Soient $i \in [\![1,n]\!]$ et $(\alpha,\alpha') \in (\mathbb{K}^*)^2$.
1) $D_i(\alpha)D_i(\alpha') = D_i(\alpha\alpha')$.
2) $D_i(\alpha) \in GL_n(\mathbb{K})$, $D_i(\alpha)^{-1} = D_i(\alpha^{-1})$ et $\det D_i(\alpha) = \alpha$.

Définition.– A tout $\lambda \in \mathbb{K}$ et à tout couple $(i,j) \in [\![1,n]\!]^2$ vérifiant $i \neq j$ on associe la matrice $T_{i,j}(\lambda)$ de $M_n(\mathbb{K})$ définie par $T_{i,j}(\lambda) = I_n + \lambda E_{ij}$. On dit que $A \in M_n(\mathbb{K})$ est une matrice élémentaire de transvection si et seulement si il existe $\lambda \in \mathbb{K}$ et $(i,j) \in [\![1,n]\!]^2$ vérifiant $i \neq j$ tels que $A = T_{i,j}(\lambda)$.

Proposition.– Soient $(\lambda,\lambda') \in \mathbb{K}^2$ et $(i,j) \in [\![1,n]\!]^2$ vérifiant $i \neq j$.
1) $T_{i,j}(\lambda)T_{i,j}(\lambda') = T_{i,j}(\lambda+\lambda')$.
2) $T_{i,j}(\lambda) \in GL_n(\mathbb{K})$, $T_{i,j}(\lambda)^{-1} = T_{i,j}(-\lambda)$ et $\det T_{i,j}(\lambda) = 1$.

6.2 Interprétation matricielle des opérations élémentaires sur les matrices

Proposition.– (opérations élémentaires sur les lignes d'une matrice)
Soient $A \in M_n(\mathbb{K})$, $\alpha \in \mathbb{K}^*$, $\lambda \in \mathbb{K}$ et $(i,j) \in [\![1,n]\!]^2$ tel que $i \neq j$.

1) $P_{(i,j)}A$ se déduit de A en permutant les $i^{\text{ème}}$ et $j^{\text{ème}}$ lignes de A $\left(L_i \leftrightarrow L_j\right)$.

2) $D_i(\alpha)A$ se déduit de A en multipliant la $i^{\text{ème}}$ ligne de A par α $\left(L_i \leftarrow \alpha L_i\right)$.

3) $T_{i,j}(\lambda)A$ se déduit de A en additionnant à la $i^{\text{ème}}$ ligne de A, λ fois la $j^{\text{ème}}$ ligne de A $\left(L_i \leftarrow L_i + \lambda L_j\right)$.

Proposition.– (opérations élémentaires sur les colonnes d'une matrice)

Soient $A \in M_n(\mathbb{K})$, $\alpha \in \mathbb{K}^*$, $\lambda \in \mathbb{K}$ et $(i,j) \in [\![1,n]\!]^2$ tel que $i \neq j$.

1) $AP_{(i,j)}$ se déduit de A en permutant les $i^{\text{ème}}$ et $j^{\text{ème}}$ colonnes de A $\left(C_i \leftrightarrow C_j\right)$.

2) $AD_i(\alpha)$ se déduit de A en multipliant la $i^{\text{ème}}$ colonne de A par α $\left(C_i \leftarrow \alpha C_i\right)$.

3) $AT_{j,i}(\lambda)$ se déduit de A en additionnant à la $i^{\text{ème}}$ colonne de A λ fois la $j^{\text{ème}}$ colonne de A $\left(C_i \leftarrow C_i + \lambda C_j\right)$.

Théorème.– Soit $A \in M_{n,p}(\mathbb{K})$.

1) Une matrice A' déduite de A par une succession d'opérations élémentaires sur les lignes s'écrit $A' = UA$ avec $U \in GL_n(\mathbb{K})$. Une telle matrice A' est équivalente à A. Elle a le même noyau, la même image et le même rang que A.

2) Une matrice A' déduite de A par une succession d'opérations élémentaires sur les colonnes s'écrit $A' = AV$ avec $V \in GL_p(\mathbb{K})$. Une telle matrice A' est équivalente à A. Elle a le même noyau, la même image et le même rang que A.

3) Une matrice A' déduite de A par une succession d'opérations élémentaires sur les lignes et les colonnes s'écrit $A' = UAV$ avec $U \in GL_n(\mathbb{K})$ et $V \in GL_p(\mathbb{K})$. Une telle matrice A' est équivalente à A. Elle a le même noyau, la même image et le même rang que A.