ALGÈBRE

Omar Boukhadra

Dép. Mathématiques
Faculté des Sciences Exactes
Université de Constantine 1
boukhadra@umc.edu.dz

4 mai 2021

Ce document se veut une présentation relativement sommaire du cours d'algèbre à l'intention des étudiants de L1-SM*, lequel est dérivé de* [2]*. Il s'agit essentiellement de connaître les structures algébriques, les espaces vectoriels et les applications linéaires qui sont naturellement suivies des matrices. À la fin, nous parlerons de déterminants et des systèmes d'équations linéaires simples.*

Contenu

1 Ensembles, Relations et applications

Ce premier chapitre introduit les notions de base en mathématique, à commencer par le concept d'ensemble. Ensuite, viennent les relations dans un ensemble, notamment l'équivalence et l'ordre. Enfin, il s'agit d'aborder les applications entre ensembles. Cela permettra de se lancer dans toutes les mathématiques.

1.1 Ensembles

Un **ensemble mathématique** E est une représentation abstraite d'une collection d'objets, *finie* ou *infinie*, appelés **éléments** de E, lesquels peuvent représenter aussi bien des êtres physiques (caillou, élève, table ...) que des objets de notre pensée (nombre, fonction ...), lesdits éléments satisfaisant alors une propriété commune en ce sens qu'il existe un critère permettant d'affirmer pour tout objet, s'il appartient à l'ensemble E ou non. Un même être mathématique ne peut pas être à la fois un ensemble et un élément de cet ensemble, autrement on arrive à une contradiction dans notre théorie !

EXEMPLES **1.1** Nous avons l'ensemble des nombres naturels $\mathbb{N}$, des entiers relatifs $\mathbb{Z}$, des nombres rationnels $\mathbb{Q}$. Mais aussi, il y l'ensemble des points d'un plan, l'ensemble des étudiants de l'Université de Constantine. ○

Quand un élément x *appartient à* un ensemble E, ou de manière équivalente, quand E *contient* x, on écrit $x \in E$, et le contraire est noté par $x \notin E$; on lit alors que x *n'appartient pas à* E ou que E *ne contient pas* x. Si deux éléments a et b de E sont *identiques* suivant le critère de définition de E, on écrit $a = b$; cette proposition est dite **égalité**, sinon, ils sont *distincts* et on écrit $a \neq b$, ce que l'on appelle **inégalité**.

Deux ensembles sont identiques (ou égaux) s'ils sont constitués des mêmes éléments, sinon ils sont dits distincts (ou inégaux), on écrit respectivement $E = F$ et $E \neq F$.

Une partie A d'un ensemble E ou un sous-ensemble de E est un ensemble dont tous les éléments appartiennent à E. On dit alors que A est incluse dans E ou que E contient A et on écrit

$$A \subset E \Longleftrightarrow E \supset A \Longleftrightarrow \forall x \in A : \ x \in E$$

Par définition, un ensemble E est une partie de lui-même, i.e. $E \subset E$, et par convention, le vide, noté $\emptyset$, est considéré comme une partie de tout ensemble, $\emptyset \subset E$.

L'ensemble de toutes les parties de E, y compris le vide, est noté $\mathscr{P}(E)$; on a donc

$$A \subset E \Longleftrightarrow A \in \mathscr{P}(E),$$

en particulier

$$\emptyset \in \mathscr{P}(E), \qquad E \in \mathscr{P}(E)$$

Le **complémentaire** d'une partie A dans un ensemble (total) E est l'ensemble de tous les éléments de E qui n'appartiennent pas à A. On le note $\overline{A}$ ou A^c ou $\complement A$, i.e.

$$\overline{A} = \{x \in E : \ x \notin A\}$$

On remarque alors que

$$\overline{\overline{A}} = A$$

Et on convient que

$$\overline{E} = \emptyset, \quad \overline{\emptyset} = E$$

Étant donné deux parties A, B de E, la partie désignée par $A \setminus B$ est l'ensemble des éléments qui appartiennent à A sans appartenir à B, i.e.

$$A \setminus B = \{x \in A : x \notin B\}$$

Par conséquent, il vient que

$$\overline{A} = E \setminus A$$

Union, intersection, ensemble produit

L'**union** des parties A et B, noté $A \cup B$, est l'ensemble des éléments appartenant ou bien à A ou bien à B ou bien aux deux parties en même temps :

$$x \in A \cup B \Longleftrightarrow x \in A \vee x \in B.$$

L'ensemble noté, $A \cap B$, est appelé l'**intersection** de A et B, lequel ensemble contient les éléments appartenant à la fois à A et à B :

$$x \in A \cap B \Longleftrightarrow x \in A \wedge x \in B.$$

Deux parties A et B sont dites **disjointes** si leur intersection est vide, i.e. $A \cap B = \emptyset$.

Il découle immédiatement de la définition même de l'union et de l'intersection que

$$\emptyset \cap A = \emptyset, \quad \emptyset \cup A = A \tag{1.1}$$

de plus, on a

$$E \cap A = A, \quad E \cup A = E \tag{1.2}$$

En outre, l'intersection et de l'union des ensembles possèdent les propriétés suivantes.

Proposition 1.2 *Soit A, B et C des parties d'un ensemble E. Alors, on a que*

(i) l'intersection et l'union sont ***commutatives****, i.e.*

$$A \cup B = B \cup A, \quad A \cap B = B \cap A \tag{1.3}$$

(ii) l'intersection et l'union sont ***associatives****, i.e.*

$$\begin{aligned} A \cap (B \cap C) &= (A \cap B) \cap C = A \cap B \cap C \\ A \cup (B \cup C) &= (A \cup B) \cup C = A \cup B \cup C \end{aligned} \tag{1.4}$$

(iii) l'intersection est ***distributive*** *par rapport à l'union et la réunion est distributive par rapport à la l'intersection, i.e.*

$$\begin{aligned} A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \\ A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \end{aligned} \tag{1.5}$$

En outre, on a des propriétés fondamentales liées au complémentaire d'ensemble.

Proposition 1.3 *Soit A, B deux parties d'un ensemble E. Alors, on a*

$$\begin{array}{lllll} (i) & A \cup \overline{A} & = & E \\ (ii) & \overline{A \cup B} & = & \overline{A} \cap \overline{B} \\ (iii) & \overline{A \cap B} & = & \overline{A} \cup \overline{B} \\ (iv) & A \subset B & \Leftrightarrow & \overline{A} \supset \overline{B} \end{array}$$

Nous terminons cette section générale sur les ensembles par une autre notion fondamentale qui généralise la première notion d'ensemble et qui va nous servir juste après à établir la notion de *relation* dans un ensemble. On appelle **produit de deux ensembles** E et F l'ensemble, noté $E \times F$, constitué de tous les couples ordonnés (x, y) où $x \in E$ et $y \in F$, appelés **coordonnées**, i.e.

$$E \times F = \{(x, y) : x \in E, y \in F\}.$$

$E \times F$ est alors appelé **ensemble produit**. Par définition, deux couples du produit $E \times F$ sont égaux si l'on a

$$(x, y) = (u, v) \Longleftrightarrow x = u \text{ et } y = v.$$

Si $E = F$, on écrit E^2 et on appelle l'ensemble $\Delta = \{(x, x) : x \in E\}$ la diagonale de E^2. Par exemple, on a $\mathbb{R}^2$ qui représente le plan géométrique coupé en deux par la diagonale.

On vérifie facilement que le produit des ensembles est une opération distributives sur l'union et l'intersection, i.e.

$$(E \cup F) \times G = (E \times G) \cup (F \times G),$$
$$(E \cap F) \times G = (E \times G) \cap (F \times G).$$

On peut généraliser cette notion à plusieurs ensembles $E_i, i = 1, \ldots, d, d \in \mathbb{N}$, de la manière suivante :

$$E_1 \times \cdots \times E_d = \prod_{i=1}^{d} E_i = \{(x_1, \ldots, x_d) : x_i \in E_i, \forall i = 1, \ldots, d\}.$$

Deux éléments d'un tel ensemble sont égaux ssi leur coordonnées sont égales. Si les ensembles E_i sont identiques à un même ensemble E, on notera le produit par E^d.

1.2 Relations

La notion de produit d'ensembles mène à la notion de relation dans un ensemble. On appelle **relation** * entre deux variables décrivant respectivement deux ensembles E et F, toute propriété définie sur $E \times F$ en ce sens que c'est une propriété caractéristique des éléments d'une partie de $E \times F$, laquelle partie s'appelle **graphe** de la relation. On note généralement une relation par $\mathcal{R}$ et son graphe par

∗. *Introduction à l'Algèbre*, O. Boukhadra. 20/21.

G. Par abus de langage, $\mathcal{R}$ peut être considérée la partie G elle-même. Ainsi, dire que (x, y) appartient à G revient à dire que x *est en relation* $\mathcal{R}$ *avec* y ou que x *et* y *vérifient* $\mathcal{R}$, ce que l'on écrit en abrégé

$$x\mathcal{R}y = \mathcal{R}(x, y)$$

d'où

$$G = \{(x, y) \in E \times F : x\mathcal{R}y\}$$

Dans le cas particulier où $E = F$, une relation entre x et y de E est dite **relation binaire** sur E, ou tout simplement une relation en tant que partie de $E \times E$. Remarquons que si une relation est vraie pour tout couple (x, y), on dit que c'est une identité, son graphe étant $E \times E$.

EXEMPLES **1.4** L'égalité $x = y$ est une relation binaire définie sur un ensemble E quelconque, son graphe Δ, décrit par les couple (x, x), est appelé la **diagonale** de $E \times E$. Le meilleur exemple visuel de cette relation est la droite bissectrice dans le plan $\mathbb{R}^2$ d'équation $y = x$. Et plus généralement, la droite dans un plan est une relation binaire sur $\mathbb{R}^2$. ○

Une relation binaire définie sur E est dite **réflexive, symétrique, antisymétrique** ou **transitive** si elle vérifie respectivement les propositions suivantes :

$$\forall x \in E : \quad x \,\mathcal{R}\, x \qquad \text{(réflexive)}$$
$$\forall x, y \in E : \quad x \,\mathcal{R}\, y \Longrightarrow y \,\mathcal{R}\, x \qquad \text{(symétrique)}$$
$$\forall x, y \in E : \quad x \,\mathcal{R}\, y \wedge y \,\mathcal{R}\, x \Longrightarrow x = y \qquad \text{(antisymétrique)}$$
$$\forall x, y, z \in E : \quad x \,\mathcal{R}\, y \wedge y \,\mathcal{R}\, z \Longrightarrow x \,\mathcal{R}\, z \qquad \text{(transitive)}$$

EXEMPLES **1.5** La relation d'égalité $x = y$ sur un ensemble E est clairement réflexive, symétrique et transitive. D'autre part, l'ordre *naturel* "$\leq$" des nombres ($\mathbb{N}$ ou $\mathbb{R}$) définit une relation binaire antisymétrique. En effet, deux nombres naturels (ou réels) tels que $x \leq y$ et $y \leq x$ donnent nécessairement que $x = y$. □

Relations d'équivalence

Une relation binaire $\mathcal{R}$ sur un ensemble E est dite **relation d'équivalence** si elle est (réflexive), (symétrique) et (transitive). Dans ce cas, si $x \,\mathcal{R}\, y$, on écrit

$$x = y \ (\mathrm{mod}\, \mathcal{R})$$

que l'on énonce en disant que x et y sont **équivalents** ou **congrus** modulo $\mathcal{R}$, ou encore x est équivalent ou congru à y, modulo $\mathcal{R}$.

EXEMPLE **1.6** (**Identité**) L'exemple basique d'une relation d'équivalence est donné par l'égalité ou l'identité dans un ensemble quelconque E :

$$x\mathcal{R}y \iff x = y$$

○

EXEMPLE **1.7** (**Congruence modulo** n) Soit $n \in \mathbb{N}$. Dans $\mathbb{Z}$, définissons la relation $\mathcal{R}$

$$p\,\mathcal{R}\,q \iff p - q \in n\mathbb{Z}$$

Cette relation équivaut à dire que $p - q$ *est multiple de* n ou que $p - q$ *est divisible par* n. En même temps, notons que si l'on prenait $(-n)$, ladite relation reste la même chose. Si $n = 0$, cette relation est tout simplement l'égalité dans $\mathbb{Z}$.

Il est facile de vérifier que nous avons là une relation d'équivalence appelée *congruence modulo* n, n étant le **module**. On écrit alors

$$p = q \,(\mathrm{mod}\, n) = q\,[n]$$

et on lit que p et q sont **congrus modulo** n. Cette relation met en lien les éléments de $\mathbb{Z}$ qui possèdent le même reste de la *division* euclidienne par n, ce que nous allons revoir plus bas. ○

Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$. On appelle **classe d'équivalence** une partie de E formée de tous les éléments équivalents entre eux. Pour un élément x de E, on note sa classe d'équivalence par $\dot{x}$ ou par $c_{\mathcal{R}}(x)$ ou simplement $c(x)$ s'il n'y a pas de risque de confusion, i.e.

$$\dot{x} = c_{\mathcal{R}}(x) = \{y \in E :\ x\,\mathcal{R}\,y\}$$

Clairement, on voit que

$$\forall y \in \dot{x} :\ \dot{y} = \dot{x}$$

De plus, nous avons la propriété des classes suivante qui est leur principale caractéristique.

Théorème 1.8 *Deux classes d'équivalence sont disjointes ou confondues.*

On appelle **ensemble quotient** de E par la relation d'équivalence $\mathcal{R}$, l'ensemble, noté généralement $E/\mathcal{R}$, des classes d'équivalence selon $\mathcal{R}$.

Théorème 1.9 *Étant donné une relation d'équivalence $\mathcal{R}$ sur un ensemble E, l'ensemble des classes d'équivalence modulo $\mathcal{R}$, soit $E/\mathcal{R}$, est une partition de E, i.e.*

$$\begin{aligned} &(i)\, \forall X \in E/\mathcal{R} :\ X \neq \emptyset \\ &(ii)\, \forall X, Y \in E/\mathcal{R} :\ X \cap Y = \emptyset \\ &(iii)\ \cup_{X \in E/\mathcal{R}}\, X = E \end{aligned} \tag{1.6}$$

Réciproquement, toute partition de E définit une relation d'équivalence sur E.

Remarque 1.10 *Les classes d'équivalence sont par définition des parties de E, donc des éléments de $\mathscr{P}(E)$. D'où, $E/\mathcal{R}$ est une partie de $\mathscr{P}(E)$. On a*

$$x \in \dot{x}, \quad \dot{x} \subset E, \quad \dot{x} \in E/\mathcal{R} \subset \mathscr{P}(E)$$

EXEMPLE **1.11** Les classes d'équivalence de la relation d'égalité $x = y$ sur un ensemble E sont les singletons $\{x\}$. Donc, $E/\mathcal{R} = \{\{x\} : x \in E\}$. ○

EXEMPLE **1.12** (**Division euclidienne**) L'ensemble quotient de la relation de congruence modulo n vu dans l'Exemple (1.7) est donnée par

$$\mathbb{Z}/n\mathbb{Z} = \{\dot{k} :\ k = 0, \ldots, n-1\}$$

○

Relations d'ordre

Une relation binaire $\mathcal{R}$ entre éléments d'un ensemble E est une **relation d'ordre**, si elle est (réflexive), (transitive) et (antisymétrique).

La notation standard pour une relation d'ordre est $x \leq y$, et on lit x *inférieur ou égal à* y ou x *est plus petite ou égal à* y. On peut de manière équivalente écrire $y \geq x$ et dire que y est *supérieur ou égale à* x ou y *est plus grand ou égale à* x. Si $x \leq y$ et $x \neq y$, on écrit $x < y$ qui se lit x *strictement inférieur à* y ou x *plus petit que* y. Aussi, on peut écrire $y > x$ et lire y *plus grand que* x.

EXEMPLE **1.13** (**Ordre naturel des nombres**) La relation définie dans l'ensemble des nombres naturels $\mathbb{N}$, des entiers relatifs $\mathbb{Z}$, des rationnels $\mathbb{Q}$, et par extension dans l'ensemble des nombres réels $\mathbb{R}$, par $x\mathcal{R}y$ si $x \leq y$, est une relation d'ordre dit *naturel*. ○

EXEMPLE **1.14** (**Inclusion**) Soit E un ensemble. Soit dans $\mathscr{P}(E)$, l'ensemble de toutes la parties de E, la relation $\mathcal{R}$ définie par

$$A\mathcal{R}B \Longleftrightarrow A \subset B$$

Il est facile de voir que celle-ci est une relation d'ordre. En effet, il est clair que pour toute partie A de E, qui est en même temps un élément de $\mathscr{P}(E)$, nous avons $A \subset A$, d'où la réflexivité. De plus, si $A \subset B$ et $B \subset A$, alors $A = B$, par conséquent notre relation est antisymétrique. Et si $A \subset B$ et $B \subset C$, nécessairement les éléments de A sont dans C, i.e. $A \subset C$, d'où la transitivité. ○

Soit l'ensemble E sur lequel est définie une relation d'ordre. Si quels que soient les éléments $x, y \in E$, ils sont toujours comparables en ce sens que $x \leq y \quad$ ou $\quad y \leq x$ on parle alors d'**ordre total** ou que E est **totalement ordonné**. Lorsqu'il existe au moins deux éléments de E non comparables pour l'ordre défini par $\mathcal{R}$, on dit que E est **partiellement ordonnée**.

Dans un ensemble totalement ordonné E, on appelle **segment** ou **intervalle fermé** $[a, b]$ et **intervalle ouvert** (a, b) les deux parties de E définies respectivement par :

$$[a, b] = \{x \in E : \ a \leq x \leq b\}$$
$$(a, b) = \{x \in E : \ a < x < b\}$$

De manière similaire, nous appelons intervalles **semi-ouverts** à droite ou à gauche les parties suivantes :

$$[a, b) = \{x \in E : \ a \leq x < b\}$$
$$(a, b] = \{x \in E : \ a < x \leq b\}$$

Nous avons aussi les les ensembles dits respectivement **sections commençante fermé ou ouverte, finissante fermée ou ouverte** :

$$[a, \rightarrow) = \{x \in E : \ x \geq a\}$$
$$(a, \rightarrow) = \{x \in E : \ x > a\}$$
$$(\leftarrow, a] = \{x \in E : \ x \leq a\}$$
$$(\leftarrow, a) = \{x \in E : \ x < a\}$$

Cependant, dans le cas des ensembles *infinis* comme les nombres réels, nous adopterons plutôt une notation à l'aide de ∞ plutôt qu'une flèche, par exemple $[a, \infty)$ ou $(-\infty, a]$.

Toujours dans un ensemble totalement ordonné, on appelle **successeur** a_+ de a tout élément tel que (a, a') soit vide. Il est facile de voir que si un tel élément existe, il est unique. À l'opposé, on dit que a_- est **prédécesseur** de a, unique s'il existe, ssi $(a_-, a) = \emptyset$.

EXEMPLE **1.15** Dans $\mathbb{Z}$, le successeur de tout a est $a + 1$ et son prédécesseur est $a - 1$. Par contre, il n'existe ni le premier le le second dans $\mathbb{Q}$ ou $\mathbb{R}$. ○

Soit A une partie d'un ensemble E ordonné. On appelle un **majorant** de A tout élément de E tel que tout élément de A lui est inférieur ou égal, autrement dit, $M \in E$ est un majorant de A si

$$\forall x \in A : \qquad x \leq M$$

S'il existe un majorant de A, on dit alors que A est *majorée*.

Inversement, un élément m de E ordonné est dit **minorant** de A si

$$\forall x \in A : \qquad m \leq x$$

A est dite *minorée* si elle admet un minorant. A est **bornée** si elle est à la fois majorée et minorée.

EXEMPLE **1.16** Dans un ensemble totalement ordonné (par exemple $\mathbb{R}$), un intervalle $[a, \infty)$ est minoré sans être majoré, par contre un intervalle du type $[a, b)$ est borné. ○

Maintenant, supposons qu'il existe dans un ensemble ordonné un élément M tel que

$$\forall x \in E : x \leq M$$

Alors, M est unique. En effet, soit N un autre élément satisfaisant le même condition précédente. Alors, Il en résulte que

$$M \leq N \quad \text{et} \quad N \leq M$$

D'où $M = N$. Ainsi, s'il existe dans E un élément supérieur à tous les autres, il est unique et on l'appelle le **plus grand élément de** E. De même, on définit le **plus petit élément de** E qui est aussi unique s'il existe.

On peut aussi adapter la dernière définition à une partie A de E ordonné et dire qu'un élément donné de A est le plus grand, le plus petit, de A s'ils existent et sont uniques.

EXEMPLE **1.17** $\mathbb{Z}, \mathbb{Q}$ et $\mathbb{R}$ muni de la structure d'ordre naturel $\leq$ n'ont pas de plus grand élément ni de plus petit. Par contre, le plus petit élément de $\mathbb{N}$ est 0. ○

EXEMPLE **1.18** Dans $\mathscr{P}(E)$ ordonné par $\subset$, il existe un plus petit élément $\emptyset$ et un plus grand élément E. ○

On appelle **borne supérieure** dans E, d'une partie majorée A de E ordonné le plus petit des majorants (s'il existe) et **borne inférieure** dans E d'une partie de A de E le plus petit des minorants (s'il existe).

Ces bornes, supérieure et inférieure, si elles existent, sont uniques. On les notes : $\sup_E A, \inf_E A$, ou tout simplement $\sup A$ et $\inf A$ s'il n'y a pas de risque de confusion sur l'ensemble d'origine. On dit alors "inf de A dans E" et "sup de A dans E". Remarquons que ces deux notions sont relatives à A et à E ; si $A \subset F \subset E$, alors A peut très bien avoir une borne supérieure (ou inférieure) dans E et ne pas en avoir dans F.

EXEMPLE **1.19** Dans $\mathbb{Q}$ ou $\mathbb{R}$, on a

$$\inf[a,b] = \inf(a,b) = \inf(a,b] = \inf[a,b) = a$$

De même, on a

$$\sup[a,b] = \sup(a,b) = \sup(a,b] = \sup[a,b) = b$$

Par exemple, nous avons

$$\sup_{\mathbb{Q}}[1/2,3/2] = \frac{3}{2}, \qquad \inf[1/2,3/2] = \frac{1}{2}$$

et d'autre part,

$$\inf[1/3,\infty) = \frac{1}{3}$$

Toutefois, ce dernier ensemble ne possède pas de majorant. ○

EXEMPLE **1.20** Considérons dans $\mathbb{Q}$ la partie $(-\infty, \sqrt{2})$. Cet intervalle est visiblement majoré par $\sqrt{2}$ mais il n'admet pas de maximum ni de borne supérieure dans $\mathbb{Q}$ étant donné que $\sqrt{2} \notin \mathbb{Q}$ (voir [2, Annexe B]).

○

EXEMPLE **1.21** Soit $\mathscr{P}(E)$ l'ensemble des parties d'un ensemble E, muni de la relation d'ordre $\subset$. Les singletons dans $\mathscr{P}(E)$, i.e. les parties constituées d'un seul élément, sont majorées. Par exemple, considérons

$$E = \{a,b,c\}, \qquad \mathscr{P}(E) = \big\{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\big\}$$

Nous avons

$$\{a\} \subset \{a, b\}.$$

Autrement dit la partie $\{\{a\}\}$ est majorée par $\{a, b\}$. Nous avons aussi que la partie $\{\{a\}, \{b\}\}$ est majorée par $\{a, b\}$. ○

Dans les derniers exemples, on voit qu'une borne, supérieure ou inférieure, peut ou non appartenir à l'ensemble qu'elle borne. À ce propos, on a

Théorème 1.22 *Soit A une partie d'un ensemble ordonné. Alors, les deux propositions suivantes sont équivalentes :*

(i) M est la borne supérieure (resp. inférieure) de A et appartient à A

(ii) M est le plus grand (resp. le plus petit) élément de A.

Enfin, soit E un ensemble ordonné. S'il existe un élément a de E tel que

$$\forall x \in E : \ a \leq x \Longrightarrow x = a \tag{1.7}$$

on dit que a est un élément **maximal** de E. Et s'il existe un élément a de E tel que

$$\forall x \in E : \ x \leq a \Longrightarrow x = a \tag{1.8}$$

alors a est dit un élément **minimal** de E.

Autrement dit, un élément de E ordonné est maximal s'il n'existe pas dans E d'éléments qui lui soient strictement supérieures, et il est minimal si aucun des éléments de E ne lui soit strictement inférieure.

Remarquons que le plus grand élément de E, s'il existe, est évidemment maximal, et c'est d'ailleurs le seul ; de même, le plus grand élément de E, s'il existe, est clairement minimal et unique.

Cependant, les réciproques des dernière remarques sont fausses comme nous allons le voir dans l'exemple suivant. Toutefois, si E est totalement ordonné, les notions se confondent : si a est maximal, tout élément x de E lui est comparable et il est impossible que a admette des éléments qui lui soient strictement supérieures, il est donc supérieur à tout x de E, c'est le plus grand élément de E et il est unique. Idem, un élément minimal dans E totalement ordonné est le plus petit élément et il est unique. En conclusion, les notions d'éléments maximal ou minimal d'un ensemble ordonné n'ont vraiment d'intérêt que dans un ensemble partiellement ordonné.

Exemple **1.23** Comme nous l'avons déjà vu, $\mathscr{P}(E)$ ordonné par l'inclusion possède un plus petit élément $\emptyset$ et un plus grand élément E. Mais, dans $\mathscr{P}(E) \setminus \emptyset$, il n'y a

pas de plus petit élément ; les parties à un seul élément dites **singletons** sont les éléments minimaux. Et dans $\mathscr{P}(E) \setminus \{\emptyset, E\}$, l'ensemble des parties propres de E, il y a des éléments minimaux $\{x\}$ et des parties maximales $E \setminus \{x\}$. ○

1.3 Applications

Soit deux ensembles E et F. On définit une **application**[†] de l'ensemble E, dit **ensemble de départ**, dans l'ensemble F, , dit **ensemble d'arrivé**, ou **fonction** définie sur E et à valeurs dans F, toute correspondance, disons f, qui associe à tout élément x de E, un élément de F unique en ce sens que x ne doit pas être lié à plus d'un seul élément de F, noté $f(x)$ et appelé **image** de x. L'élément x est appelé la **variable** ou *argument* de la fonction et constitue alors l'élément **réciproque** ou *antécédent* de $f(x)$. Cette correspondance est représentée sous la forme

$$\begin{array}{rccc} f: & E & \longrightarrow & F \\ & x & \longmapsto & f(x) \end{array}$$

On écrit aussi

$$f : E \longrightarrow F \quad \text{ou} \quad E \xrightarrow{f} F$$

On appelle **graphe** de l'application $f : E \to F$ la partie G de $E \times F$ définie par :

$$G = \{(x, y) \in E \times F : \ y = f(x)\}$$

Une application $f : E \to F$ est donc définie par le **triplet** $f = (E, F, G)$. Et l'ensemble de toutes les applications de E dans F est noté

$$\mathcal{A}(E, F) = F^E$$

Quand $E = F$, on appelle $f : E \to F$ une application ou **fonction réelle** ou **numérique**. C'est là l'objet essentiel de l'analyse mathématique (voir Partie **??**).

EXEMPLES **1.24** Nous avons les applications suivantes

$$\begin{array}{rccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array} \qquad \begin{array}{rccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \sin x \end{array}$$

et aussi

$$\begin{array}{rccc} \mathbb{N} & \longrightarrow & \mathbb{N} \\ n & \longmapsto & 2n \end{array} \qquad \begin{array}{rccc} [-1,1] & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \sqrt{1-x^2} \end{array}$$

○

†. *Introduction à l'Algèbre*, O. Boukhadra. 20/21.

EXEMPLE **1.25** (**Application identique**) L'application identique ou **identité** de E dans lui-même, notée $\mathrm{Id}_E = \mathrm{I_E}$, est telle que

$$\forall x \in E : \quad \mathrm{Id}_E(x) = x$$

Si $E \subset F$, alors Id_E est dite l'**application canonique** de E dans F. ○

EXEMPLE **1.26** (**Application caractéristique**) Soit E un ensemble et A une de ses parties. L'application caractéristique ou **fonction indicatrice** de A est l'application définie par

$$\mathbb{1}_A(x) = \begin{cases} 1 & \text{si } x \in A; \\ 0 & \text{sinon} \end{cases}$$

Nous avons par exemple de $\mathbb{R}$ dans $\mathbb{R}$,

$$\mathbb{1}_{\mathbb{Q}}(x) = \begin{cases} 1 & \text{si } x \in \mathbb{Q}; \\ 0 & \text{sinon} \end{cases}$$

○

EXEMPLE **1.27** (**Projections**) Les applications $\mathrm{Pr}_1 : E \times F \longrightarrow E$ et $\mathrm{Pr}_2 : E \times F \longrightarrow F$ définies respectivement comme suit

$$\mathrm{Pr}_1(x, y) = x, \qquad \mathrm{Pr}_2(x, y) = y$$

sont des surjections. En effet, prenons par exemple Pr_1. Pour tout choix de $x \in E$, le couple (x, y) pour un choix arbitraire de $y \in F$, est un élément réciproque. Pr_1 et Pr_2 sont appelées **projections** sur E, respectivement sur F. ○

La **restriction d'une application** $f : E \longrightarrow F$ est une application définie sur une partie A de E, ce qui est noté par $f_{|A}$. Par exemple, la restriction de l'application Id_E à une partie $A \subset E$, notée Id_A.

Si une fonction $g : E \to F$ définie sur E coïncide avec une fonction f définie sur une partie $A \subset E$, on dit alors que g est un **prolongement** de f. Une fonction est toujours le prolongement de ses restrictions.

Soit une application $f : E \longrightarrow F$ et $A \subset E$. On définit l'**image directe** de A par f comme suit

$$f(A) = \{y \in F, \exists x \in A : \ y = f(x)\} = \{f(x), x \in A\},$$

ce qui est égal à l'ensemble des images des éléments de A par f, autrement dit, $f(A)$ est décrit par $f(x)$ lorsque x décrit A. En particulier, nous avons $f(E)$, l'image de tout l'ensemble de départ, que l'on appelle **Image de** f que l'on note $\mathrm{Im}\,(f)$.

D'un autre côté, pour une partie B de F, l'**image réciproque** de B par $f : E \longrightarrow F$ est la partie de E définie par

$$f^{-1}(B) = \{x \in E : f(x) \in B\}$$

Remarquons que $f(A)$ est vide ssi A est vide mais $f^{-1}(B)$ peut être vide sans que B le soit, ceci arrive quand $f(E) \subset F \setminus B$. En même temps, notons que $f(\{x\})$ est l'ensemble $\{f(x)\}$. Par contre, $f^{-1}(\{y\})$ peut être vide ou contenir plus d'une réciproque et avec un abus de notation, on écrit aussi $f^{-1}(y)$.

EXEMPLE **1.28** Considérons $f(x) = \sin x$ sur $\mathbb{R}$. Nous avons

$$f^{-1}(2) = \emptyset, \qquad f^{-1}(1/2) = \{\pi/6 + 2n\pi, 5\pi/6 + 2n\pi\}$$

○

Propriétés générales

En premier, on a les propriétés suivantes

Proposition 1.29 *Soit $f : E \to F$ et considérons des parties A, B de E. Alors, on a*

$$\begin{aligned} A \subset B &\implies f(A) \subset f(B) && (1.9)\\ f(A \cup B) &= f(A) \cup f(B) && (1.10)\\ f(A \cap B) &\subset f(A) \cap f(B) && (1.11) \end{aligned}$$

Remarque 1.30 *L'égalité dans (1.11) n'est pas toujours vraie !*

Comme pour l'image directe des ensembles, nous avons des résultat similaires, à une égalité près, pour l'image réciproque.

Proposition 1.31 *Soit $f : E \to F$ et A et B des parties de F. Alors, on a*

$$\begin{aligned} A \subset B &\implies f^{-1}(A) \subset f^{-1}(B)\\ f^{-1}(A \cup B) &= f^{-1}(A) \cup f^{-1}(B)\\ f^{-1}(A \cap B) &= f^{-1}(A) \cap f^{-1}(B) && (1.12)\\ f^{-1}(\overline{A}) &= \overline{f^{-1}(A)} \end{aligned}$$

Une application $f : E \longrightarrow F$ est dite **injective** ou une *injection* si les images de deux éléments différents sont différentes, autrement dit

$$\forall x, y \in E : \quad x \neq y \Longrightarrow f(x) \neq f(y),$$

ce qui est équivalent à

$$\forall x, y \in E : f(x) = f(y) \Longrightarrow x = y \tag{1.13}$$

Une **application surjective** ou une *surjection* $f : E \longrightarrow F$ est une application telle que tout élément de F est l'image d'au moins un élément de E, i.e.

$$\forall y \in F, \exists x \in E : \quad f(x) = y \tag{1.14}$$

Enfin, on dit qu'une application est **bijective** ou une *bijection* si elle est simultanément injective et surjective.

EXEMPLE **1.32** L'application f définie de $\mathbb{N}$ dans $\mathbb{N}$ telle que

$$\forall n \in \mathbb{N} : \quad f(n) = 2n,$$

est une injection. En effet, on a pour tous entiers n, k,

$$2n = 2k \Longrightarrow n = k$$

Cependant, f n'est pas surjective car les nombre impairs n'ont pas d'image réciproque. ○

EXEMPLE **1.33** Soit $f : \mathbb{Z} \longrightarrow \mathbb{N}$ telle que $f(-n) = f(n) = n \in \mathbb{N}$. Alors, f est surjective. En, effet, pour tout $n \in \mathbb{N}$, il existe deux images réciproques $-n$ et n. ○

EXEMPLE **1.34** (**Injection canonique**) L'application identité Id_E est bijective. Sa restriction à une partie A de E est une injection dite *canonique*. ○

Rappelons-nous la définition de $\mathrm{Im}\,(f)$. Nous avons alors

Proposition 1.35 *Soit $f : E \to F$. Alors, on a que*

(i) f est surjective ssi $\mathrm{Im}\,(f) = F$,

(ii) si f est injective, elle est bijective entre E et $\mathrm{Im}\,(f)$.

La bijectivité d'une application conduit à une autre notion importante que nous donnons ci-après. Soit $f : E \to F$ une application bijective. Il existe alors pour tout $y \in F$, un unique élément $x \in E$ telle que $y = f(x)$. On peut alors associer à tout

élément y de F un seul élément x de E de sorte que $y = f(x)$. Cette application est appelée l'**application réciproque** de f et elle est notée f^{-1}.

Par définition, f^{-1} est aussi bijective. En effet, il suffit d'observer que l'implication dans (1.13) équivaut par application de f^{-1} à

$$x = y \Longrightarrow f^{-1}(x) = f^{-1}(y)$$

D'un autre côté, f^{-1} est bien surjective car pour tous $x \in E$ et $y \in F$, on a

$$y = f(x) \Longleftrightarrow x = f^{-1}(y)$$

Pour éviter toute confusion avec la notion d'image réciproque d'ensemble, observons que $f^{-1}(\{y\})$ est toujours défini alors que $f^{-1}(y)$ n'existe que si f est bijective.

EXEMPLE **1.36** Soit

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto x + 1 \end{aligned}$$

Clairement, elle est bijective. En effet, on a en premier

$$x \neq y \Longrightarrow x + 1 \neq y + 1 \Longrightarrow f(x) \neq f(y).$$

Et pour tout $y \in \mathbb{R}$, il existe dans $\mathbb{R}$ une image réciproque égale à $y - 1$. Ainsi, f^{-1} est donnée par

$$\begin{aligned} f^{-1} : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto x - 1 \end{aligned}$$

○

EXEMPLES **1.37** (**fonctions trigonométriques**) Il y a aussi les exemples importants des fonctions dites *trigonométriques* comme les célèbres *cosinus*, noté cos et *sinus*, noté sin. Ces dernières fonctions sont bijectives de $[0, \pi]$ sur $[-1, 1]$ ou sur tout intervalle de longueur π. Par conséquent, elles admettent des fonctions réciproques que l'on appelle respectivement *arc cosinus* et *arc sinus* et notées par arccos et arcsin.

Ces deux fonctions servent à définir une troisième fonction aussi importante, à savoir la tangente :

$$\tan = \frac{\sin}{\cos}$$

Elle est bijective de $(-\pi/2, \pi/2)$ sur $\mathbb{R}$. Sa réciproque est la fonction dite *cotangente*, notée par cot.

Nous reverrons les présentes fonctions plus formellement à l'aide de la notion d'*intégration*. ○

Compositions des applications

Soit deux applications $f : E \longrightarrow F$ et $g : F \longrightarrow G$. On appelle **application composée** de f et g, notée $g \circ f$, l'application qui associe à tout élément x de E l'élément de G donné par

$$(g \circ f)(x) = g(f(x))$$

Notons que dans cette composition, l'application f vient en premier, ensuite, on applique g. De plus, la composition des applications n'a de sens que si la deuxième application composée soit définie sur l'image de la première.

EXEMPLES **1.38** Soit f, g deux applications de $\mathbb{N}$ dans lui-même telles que

$$f(n) = n + 1 \qquad \text{et} \qquad g(n) = n^2$$

Alors,

$$(g \circ f)(n) = g(f(n)) = (n + 1)^2$$

Nous avons aussi les fonctions réelles $f : x \mapsto x^2$ et $g : x \mapsto \sin x$, lesquelles donnent

$$g \circ f(x) = \sin(f(x)^2) = \sin x^2$$

Cependant, ces deux exemples donnent

$$\begin{aligned} f \circ g(n) = n^2 + 1 &\neq (n + 1)^2 = g \circ f(n) \\ f \circ g(x) = (\sin x)^2 &\neq \sin x^2 = g \circ f(x) \end{aligned}$$

Ce qui montre que généralement, la composition des applications est **non commutative**, i.e.

$$g \circ f \neq f \circ g \tag{1.15}$$

○

EXEMPLE **1.39** (**factorisation**) Soit $f : E \to F$. il est clair que $g : E \to f(E)$ tel que $g(x) = f(x)$ est surjective. Posons $\mathrm{Id}_f = \mathrm{Id}_{f(E)}$, l'injection canonique. Ainsi, toute application $f : E \to F$ admet la factorisation suivante

$$f = \mathrm{Id}_f \circ g$$

○

L'opération de composition des fonctions peut être généralisée par récurrence à plus de deux fonctions. Par définition, cette opération est **associative** : si $f : E \to F$, $g : F \to G$ et $h : G \to H$, alors on écrit

$$h \circ (g \circ f) = (h \circ g) \circ f = h \circ g \circ f$$

et pour un élément $x \in E$, on a

$$(h \circ g \circ f)(x) = h((g \circ f)(x)) = h(g(f(x)))$$

EXEMPLE **1.40** Considérons les deux applications f, g du dernier exemple et soit $h : \mathbb{N} \longrightarrow \mathbb{N}$ telle que $h(n) = 2n$. Alors,

$$(h \circ g \circ f)(n) = h(g(f(n))) = 2(n+1)^2$$

○

Soit $f : E \longrightarrow F$ une application bijective. Il est alors facile de voir que

$$f^{-1} \circ f = \mathrm{Id}_E, \tag{1.16}$$
$$f \circ f^{-1} = \mathrm{Id}_F \tag{1.17}$$

En outre, nous avons

Théorème 1.41 *Si f et g sont surjectives (resp. injectives), alors $g \circ f$ est surjective (resp. injective). De plus, si f et g sont bijective, $g \circ f$ est bijective et on a*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1} \tag{1.18}$$

Décomposition canonique d'une application

Reprenons le concept de relation d'équivalence. Soit E un ensemble non vide muni d'une relation d'équivalence $\mathcal{R}$. On appelle **projection canonique** l'application

$$\begin{array}{rccc} \pi : & E & \longrightarrow & E/\mathcal{R} \\ & x & \longmapsto & \dot{x} \end{array}$$

Ladite projection canonique est clairement surjective et caractérise $\mathcal{R}$ de la manière suivante :

$$x\mathcal{R} \Longleftrightarrow \pi(x) = \pi(y)$$

On a alors

$$E/\mathcal{R} = \{\pi^{-1}(X) : X \in E/\mathcal{R}\}$$

Le résultat important donne une décomposition de toute application en une composition d'applications dite canonique.

Théorème 1.42 (factorisation canonique d'une application) *Soit $f : E \to F$ et appelons $\mathcal{R}$ la relation sur E définie par*

$$x\mathcal{R}y \Longleftrightarrow f(x) = f(y)$$

*Alors, $\mathcal{R}$ est une relation d'équivalence dite **associée à** f. De plus, il existe une application bijective unique $\widehat{f} : E/\mathcal{R} \to f(E)$ telle que*

$$f = \mathrm{Id}_f \circ \widehat{f} \circ \pi \tag{1.19}$$

où $\mathrm{Id}_f : f(E) \to F$ est l'injection canonique et $\pi : E \to E/\mathcal{R}$ est la projection canonique.

Remarque 1.43 *La factorisation (1.19) est schématisée comme suit*

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle \mathrm{Id}_f} \\ E/\mathcal{R} & \xrightarrow{\widehat{f}} & \mathrm{Im}(f) \end{array}$$

*Ce type de schéma est dit **diagramme commutative** en ce sens que deux points sont connectés (quand c'est possible) indépendamment du chemin suivi, par exemple, en partant de E, on joint F par deux chemins possibles.*

2 Structures algébriques

*Un ensemble mathématique n'acquiert de sens pratique que s'il est structuré par des **opérations** entre ses éléments. Ce chapitre présente les structures algébriques fondamentales, à savoir groupe, anneau et corps, lesquelles sont définies par des opérations qui, elles-mêmes, sont des abstractions généralisées des opérations naturelles d'addition et de multiplication.*

2.1 Lois de composition internes

Soit E un ensemble non vide. On appelle **loi de composition interne** entre éléments de E, toute application d'une partie A de E^2 dans E. On dit alors que E est **munie de la loi** interne considérée. Lorsque $A = E^2$, on dit que la loi est partout définie sur E, et que c'est une **opération algébrique interne** sur E, ou plus simplement une opération interne sur E ou une **loi interne** sur E. L'image d'un couple $(x, y) \in E^2$ par l'opération interne est le **composé** de x et de y qui en sont les **termes**. On note le composé avec des symboles divers, notamment :

$$x + y;\ x \cdot y;\ x * y;\ x \top y;\ x \perp y$$

Pour un ensemble E muni d'une opération interne $*$, on écrit $(E, *)$.

Notons en particulier que l'opération $(x, y) \longmapsto x + y$ est appelée **addition** et se lit x *plus* y ou *somme des termes* x *et* y. D'autre part, l'opération $(x, y) \longmapsto x \times y$ est dite **multiplication** et s'énonce x *multiplié par* y, ou x $fois$ y, ou *produit des facteurs* x et y. Pour simplifier, on l'écrit sous la forme $x \cdot y$ ou tout simplement sans symbole xy.

Exemple **2.1** ($+, \times$ naturelles) Sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ et aussi $\mathbb{R}$, les deux opérations standard $x + y$ et xy sont des lois partout définies. ○

EXEMPLE **2.2** $((\mathcal{A}(E,E),\circ))$ L'opération de composition des applications $f \circ g$ définies sur un ensemble E dans lui-même est une loi interne dans l'ensemble de ces applications. ○

EXEMPLE **2.3** $((\mathscr{P}(E),\cup,\cap))$ L'intersection et l'union des parties d'un ensemble donné E sont des lois internes dans l'ensemble $\mathscr{P}(E)$. ○

Les principales **propriétés** d'une opération interne sont les suivantes. Soit $(E,*)$. Alors,

(i) on dit que l'opération est **commutative** si

$$\forall x,y \in E : \quad x*y = y*x; \tag{2.1}$$

(ii) l'opération est dite **associative** si :

$$\forall x,y,z \in E : \quad (x*y)*z = x*(y*z) \tag{2.2}$$

(iii) on appelle e un **élément neutre** de l'opération si

$$\forall x \in E : \quad x*e = e*x = x \tag{2.3}$$

Remarquons que l'élément neutre est unique. En effet, si e et e' étaient deux éléments neutres pour la même opération, nous aurions alors

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

(iv) si la loi admet un élément neutre e, on appelle **élément symétrique à gauche** (resp. **à droite**) d'un élément x, ou que x est *symétrisable à gauche*) (resp. *droite*), tout élément y tel que

$$y*x = e \quad (\text{resp. } x*y = e)$$

On dit que x est **symétrisable** ssi il l'est à gauche et à droite.

Notons que si l'opération est associative, l'élément symétrique est unique, sinon on aurait deux éléments x', x'' tels que

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

Dans ce cas, on a un seul élément symétrique à gauche et à droite de x, dit **élément symétrique** et noté x', tel que

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

(*v*) Un élément $a \in E$ est dit **régulier à gauche** (resp. **à droite**) ssi l'application $x \mapsto a * x$ est injective (resp. $x \mapsto x * a$ est injective). On dit que a est **régulier** ssi il est régulier à gauche et à droite.

(*vi*) si $\top$ est une deuxième loi interne dans l'ensemble E, on dit qu'elle est **distributive à gauche** (resp. **à droite**) par rapport à la loi $*$ si pour tous x, y, z de E :

$$\begin{aligned} x\top(y * z) &= (x\top y) * (x\top z) \\ (y * z)\top x &= (y\top x) * (z\top x) \end{aligned} \tag{2.4}$$

On dit que la loi $\top$ est **distributive** par rapport à la loi $*$ si elle est à la fois distributive à gauche et distributive à droite.

Remarque 2.4 *La propriété* (*v*) *de dire que a est régulier à gauche* (*resp. à droite*) *donne par injectivité que*

$$a * x = a * y \Longrightarrow x = y \quad (resp. x * a = y * a \Longrightarrow x = y)$$

On dit alors que a est ***simplifiable*** *à gauche* (*reps. à droite*). *Il est simplement simplifiable s'il l'est à gauche et à droite. Si un élément neutre e existe, il est clairement régulier. Par conséquent, il doit être* ***unique****. En effet, si e et e′ sont deux éléments neutre, on a* $e * e' = e$ *par neutralité de* e', *et aussi* $e * e' = e'$ *par neutralité de e, donc* $e = e'$ *par régularité.*

L'intérêt majeure de la propriété d'associativité est qu'elle permet l'écriture sans parenthèse du composé itéré d'éléments pris dans un ordre déterminé. Par exemple, on peut écrire

$$((x * y) * z) * t = (x * y) * (z * t) = x * y * z * t$$

Si de plus, la loi est commutative, on peut lever la contrainte sur l'ordre des éléments composés.

Pour l'opération d'addition, l'élément neutre est noté 0_E *ou simplement* 0 *s'il n'y a pas de confusion. L'élément symétrique est noté* $-x$, *et on écrit*

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

Si l'addition est associative, on écrit pour $n \in \mathbb{N}^*$

$$\underbrace{x + \cdots + x}_{n fois} = nx \tag{2.5}$$

Ce que l'on généralise encore à des multiples négatifs par

$$-nx = n(-x) \tag{2.6}$$

avec la convention que $0x = 0$*, laquelle sera justifiée avec la structure d'anneau. Ainsi, par associativité, nous avons pour* $n, m \in \mathbb{Z}$*,*

$$(m+n)x = mx + nx$$

Pour la multiplication, l'élément neutre, dit ***unité****, est noté* 1_E *ou simplement* 1 *s'il n'y a pas de confusion. Dans ce cas, l'élément symétrique est appelé* ***inverse*** *de* x *et noté*

$$x^{-1} = 1/x = \frac{1}{x}$$

Si x^{-1} *existe, on dit que* x *est* ***inversible****.*

Si la multiplication est associative, on écrit $x^0 = 1$ *et*

$$\overbrace{x \cdots x}^{n\,fois} = x^{n-1}x = x^n = \textit{puissance n-ème de } x \tag{2.7}$$

Ceci est aussi étendu à des puissances négatives de x *par*

$$x^{-n} = (x^{-1})^n$$

D'où, en vertu de l'associativité, on obtient que

$$x^{m+n} = x^m x^n$$

Cependant, $(xy)^n = x^n y^n$ *est vrai ssi* x *et* y *sont permutables, i.e.* $(xy = yx)$*.*

EXEMPLE **2.5** ($\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ et $\mathbb{R}$) L'addition et la multiplication (naturelles) dans $\mathbb{N}$ sont des opérations commutatives et associatives et qui admettent respectivement le zéro et l'unité 1 comme élément neutre. Cependant, tous les nombres naturels, excepté le zéro et le 1, n'ont pas de symétrique pour les deux opérations. Dans $\mathbb{Q}$ (et aussi dans $\mathbb{R}$), en plus de la commutativité et de l'associativité de l'addition et du produit, les éléments symétriques existent pour les deux opérations. Dans ces quatre ensembles, la multiplication est distributive par rapport à l'addition. ○

EXEMPLE **2.6** ($(\mathcal{A}(E,E), \circ)$) Dans l'ensemble des applications d'un ensemble E dans lui-même, i.e. $\mathcal{A}(E,E)$, l'opération de composition des applications est par définition associative mais elle n'est pas commutative. L'élément neutre est clairement l'identité Id_E. Les seules applications qui admettent des inverses sont les application bijectives, l'inverse d'une application f étant f^{-1}. ○

2.2 Groupes

Soit G un ensemble muni d'une loi interne $*$. On dit que le couple $(G, *)$ ou tout simplement G est un **groupe** si la loi interne considérée vérifie les propriétés suivantes :

(i) la loi $*$ est associative ;

(ii) il existe un élément neutre pour l'opération considérée ;

(iii) il existe un élément symétrique pour tout élément de E.

Si l'opération interne considérée est commutative, on dit alors que G est un **groupe commutative** ou **abélien**.

EXEMPLE **2.7** ($(\mathbb{Z}, +)$) L'ensemble des entiers relatifs $\mathbb{Z}$ muni de l'opération d'addition est un groupe abélien. Cependant, $\mathbb{N}$ n'est pas un groupe ! ○

EXEMPLE **2.8** ($\mathcal{A}(E, G)$) Soit $(G, +)$ un groupe. Considérons dans $\mathcal{A}(E, G)$, l'ensemble des applications de E dans un groupe G, l'opération

$$(f + g)(x) = f(x) + g(x)$$

C'est là l'*addition naturellement induite* sur l'ensemble des applications. Alors, on obtient une structure de groupe sur $\mathcal{A}(E, G)$, qui plus est, commutatif si G l'est, l'élément neutre étant l'application nulle et l'opposé d'une application f étant $-f$. ○

EXEMPLE **2.9** (**Permutations**) Soit E un ensemble non vide. L'ensemble des application bijectives de E dans E muni de la loi de composition des applications $(f, g) \longmapsto f \circ g$ est un groupe appelé **groupe des permutations** de E ; l'élément neutre est l'identité et l'élément inverse de f est l'application réciproque f^{-1}. Lorsque $E = \{1, 2, \ldots, n\}$, l'ensemble des permutations s'appelle **groupe symétrique** et on le note $\mathcal{S}_n$. ○

Sous-groupe

Une partie H d'un groupe $(G, *)$, elle-même un groupe par rapport à la même opération interne considérée, s'appelle **sous-groupe**. Par définition, pour tout couple $(x, y) \in H^2$, H étant un sous-groupe, nous avons $x * y \in H$; on dit que l'opération est **stable** dans H. Remarquons que H contient toujours l'élément neutre qui est également l'élément neutre du sous-groupe.

Théorème 2.10 *Soit $(G, *)$ un groupe. Une partie non vide H de G est un sous-groupe ssi*

$$\forall x, y \in H : x * y' \in H \tag{2.8}$$

Exemple **2.11** (**Sous-groupe trivial**) Si G est un groupe quelconque, alors $\{e\}$ est un sous-groupe de G, dit *groupe trivial*. ○

Exemple **2.12** (**Pairs et impairs**) Considérons dans $(\mathbb{Z}, +)$ le sous-ensemble des entiers pairs :

$$2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$$

À l'aide de (2.8), il est facile de voir que $2\mathbb{Z}$ est un sous-groupe. Mais l'ensemble des entiers relatifs impairs ne l'est pas car la somme de deux impairs est pair. Plus généralement, à cause de la stabilité de l'opération dans un groupe, les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$ (cf. [2]). ○

Est-ce que l'intersection de sous-groupes est un sous-groupe ?

Théorème 2.13 *Toute intersection de sous-groupes d'un groupe G est un sous-groupe de G.*

En particulier, considérons une partie non vide A d'un groupe G et appelons $\mathscr{A}$ l'ensemble des sous-groupes de G contenant A ; cette famille compte au moins G. Alors, l'intersection des éléments de $\mathscr{A}$ est un sous-groupe et c'est manifestement le plus petit (la relation d'ordre étant l'inclusion des ensembles). Ce sous-groupe, intersection de la famille de la famille de sous-groupes de G contenant A, est appelé le **sous-groupe engendré** par A que l'on peut noté par $\langle A \rangle$.

Exemple **2.14**

$$2\mathbb{Z} \cap 3\mathbb{Z} = \text{ppcm}(2, 3)\,\mathbb{Z} = 6\mathbb{Z}$$

○

Homomoprphisme, noyau et image

Soit $(E, *), (G, \top)$ deux groupes. On appelle **homomorphisme** de E dans G toute application f telle que

$$\forall (x, y) \in E^2 : f(x * y) = f(x) \top f(y) \tag{2.9}$$

L'ensemble de telles applications est noté $\mathrm{Hom}\,(E,G)$. Si $G = E$, on dit alors **endomorphisme** ; leur ensemble est alors noté $\mathrm{Hom}\,(E)$. Un **isomorphisme** est une bijection f entre E et G telle que f est un homomorphisme de E dans G et f^{-1} est un homomorphisme de G dans E. Et si $E = G$, une telle application est dite **automorphisme**. Par exemple, l'application identique d'un groupe E sur lui-même est un automorphisme.

De la définition même de l'homomorphisme, il découle des résultats basiques :

Proposition 2.15 *(i) Le composé de deux homomorphismes en est un. Idem pour les isomorphismes.*
(ii) Si f est un isomorphisme, alors f^{-1} l'est aussi. Un homomorphisme bijectif est un isomorphisme.
(iii) Si $f : E \mapsto G$ est un homomorphisme alors, $f(e_E) = e_G$.

EXEMPLE **2.16** (**Homomorphisme de $\mathbb{Z}$ dans un groupe**) Soit G un groupe dont la loi est notée multiplicativement. Rappelons-nous la Remarque 2.4 sur la multiplication et considérons pour un $x \in G$ l'application

$$\varphi_x : n \mapsto x^n = \begin{cases} x^n & \text{si } n \geq 1 \\ 1_G & \text{si } n = 0 \\ (x^{-1})^{-n} & \text{si } n < 0 \end{cases} \tag{2.10}$$

En vertu de l'associativité, pour $x \in G$ fixé, φ_x est un homomorphisme. Ceci est cohérent avec la notation de l'inverse de x par x^{-1} et de x^n par x^{-n}.

Réciproquement, soit $f : \mathbb{Z} \to G$ un homomorphisme de groupes. Posons $x = f(1)$. Ce qui donne par récurrence que $f(n) = x^n$ pour $n \in \mathbb{N}$. Par conséquent, nous obtenons

$$1_G = f(0) = f(-n+n) = f(-n)f(n) = f(-n)x^n$$

D'où, $f(-n) = x^{-n}$.

Ainsi, les seuls homomorphismes de $(\mathbb{Z}, +)$ dans un groupe multiplicatif G sont toujours de la forme $n \mapsto x^n$.

Notons que l'on peut choisir un groupe additif G, et dans ce cas, les homomorphismes possibles s'écrivent sous la forme $n \mapsto nx$. ○

EXEMPLE **2.17** Soit $(G, *)$ un groupe et E un ensemble non vide. Sur $\mathcal{A}(E,G) = G^E$, définissons l'opération

$$f * g : x \longmapsto f(x) * g(x)$$

Grâce à cette dernière, nous obtenons une structure de groupe sur G^E, dite *naturelle*. L'élément neutre est clairement l'application $\eta : x \mapsto e_G$. Si G est abélien, G^E l'est aussi. En notation additive, l'élément neutre est l'application nulle. Et pour $E = \{1, \ldots, n\}$ avec $n \in \mathbb{N}^*$, on écrit G^n au lieu de $G^{\{1,\ldots,n\}}$, ce qui correspond en même temps au produit des ensembles. En effet, dans ce cas, une application est définie par des $n-$uplet dans le produit G^n.

Maintenant, observons que pour une valeur fixée $a \in E$, l'application de G^E dans G telle que $f \mapsto f(a)$ est un homomorphisme de groupes. ○

Une des particularité d'un homomorphisme est qu'il crée des sous-groupes dans l'ensemble d'arrivé et dans celui de départ.

Théorème 2.18 *Soit E et G deux groupes et $f : E \to G$ un homomorphisme. Alors, pour tout sous-groupe H de E, on a que $f(H)$ est un sous-groupe de G, et inversement, pour tout sous-groupe H' de G, on a que $f^{-1}(H')$ est un sous-groupe de E.*

Le Théorème 2.19 donne en particulier que $f(F)$ est un sous-groupe de G, appelé l'**image** de F par f ou *image de f* ; ce qui est noté $\mathrm{Im}\,(f)$. De l'autre côté, $f^{-1}(G)$ et $f^{-1}(e_G)$ sont des sous-groupes de F. Le dernier est est appelé le **noyau** de f que l'on note par $\mathrm{Ker}\,(f)$.

Théorème 2.19 *Soit E et G deux groupes et $f : E \to G$ un homomorphisme. Alors, f est injectif ssi* $\mathrm{Ker}\,(f) = \{e_E\}$.

2.3 Anneaux

On appelle **anneau** un ensemble A muni d'une première loi interne notée additivement "+", et d'une autre que l'on note multiplicativement "×" (ou sans symbole), pour des raisons de facilité de notation, lesquelles satisfont aux axiomes suivants :

(*i*) $(A, +)$ est un groupe abélien ; son **élément nul** est $0_A (= 0)$.

(*ii*) la multiplication est associative et distributive par rapport à l'addition, à gauche et à droite : pour tous $x, y, z \in A$,

$$(xy)z = x(yz), \quad x(y+z) = xy + xz, \quad (y+z)x = yx + zx$$

(*iii*) si, de plus, la multiplication admet une **unité** $1_A (= 1)$, on dit que A est un anneau **unitaire**.

On écrit aussi $(A, +, \cdot)$ pour exprimer que A est un anneau. Et si la multiplication est commutative, l'anneau est dit **commutatif**.

Si A est réduit au seul élément nul 0, A est alors un anneau *trivial* dans lequel $1 = 0$. Par contre, si $1 \neq 0$, alors A est dit **non nul**.

EXEMPLE **2.20** ($\mathbb{Z}, \mathbb{Q}$ et $\mathbb{R}$) Les ensembles $\mathbb{Z}, \mathbb{Q}$ et $\mathbb{R}$ sont des anneaux commutatifs pour l'addition et la multiplication standards. ○

EXEMPLE **2.21** ($\mathcal{A}(E, A)$) Soit A un anneau commutatif et E un ensemble non vide. Définissons dans $\mathcal{A}(E, A)$, l'ensemble des applications de E dans A, deux lois internes comme suit

$$(f + g)(x) = f(x) + g(x) \qquad \text{et} \qquad (fg)(x) = f(x)g(x) \tag{2.11}$$

Alors $(\mathcal{A}(E, A), +, \cdot)$ est un anneau commutatif unitaire, l'élément unité étant l'application constante égale à 1. ○

EXEMPLE **2.22** ($\mathbb{Z}/n\mathbb{Z}$) Dans l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$, on vérifier facilement à l'aide des propriétés de l'addition et de la multiplication dans $\mathbb{Z}$ que l'on a

$$\begin{aligned} c_n(x) + c_n(y) &= c_n(x + y) \\ c_n(x)c_n(y) &= c_n(xy) \end{aligned}$$

Ces deux opérations confèrent à $\mathbb{Z}/n\mathbb{Z}$ une structure d'un anneau commutatif unitaire (cf. [2]). ○

Dans un anneau quelconque A, on a les règles de calcul suivantes :

Proposition 2.23 *Soit A un anneau. Alors, pour tous $x, y \in A$, on a*

$$x\,0 = 0\,x = 0 \tag{2.12}$$

et aussi

$$-(xy) = (-x)y = x(-y) \tag{2.13}$$

Si, en plus, A est commutatif, alors on a les formules suivantes, dites ***développements usuelles****,*

$$\begin{aligned} (x + y)^2 &= x^2 + 2xy + y^2; \\ (x - y)^2 &= x^2 - 2xy + y^2 \end{aligned} \tag{2.14}$$

Remarque 2.24 *Pour les opérations d'addition et de multiplication, rappelons-nous les notations* (2.5) *et* (2.7). *Grâce à* (2.12), *nous avons alors que pour* $n \in \mathbb{N}$,

$$nx = (n1_A)x = x(n1_A)$$

D'autre part, la propriété (2.13) *donne*

$$(-x)^n = \begin{cases} x^n & n \in 2\mathbb{N}; \\ -x^n & n \notin 2\mathbb{N} \end{cases}$$

et aussi que

$$(-x)(-y) = -((-x)y) = -(x(-y)) = -(-(xy)) = xy$$

On reconnaît alors les ***règles des signes***.

Les deux expressions dans (2.14) peuvent être généralisées de la manière suivante :

Théorème 2.25 (Formule du binôme) *Soit* A *un anneau commutatif. Quelque soient les éléments* a, b *de* A *et pour tout entier* $n \geq 1$, *on a*

$$(a+b)^n = a^n + C_n^1 a^{n-1}b + C_n^2 a^2 b^{n-2} + \cdots + C_n^{n-1} a^1 b^{n-1} + b^n \tag{2.15}$$

où les $C_n^p, 0 = 1, 2, \ldots, n$, *sont donnés par*

$$C_n^p = \frac{n!}{p!(n-p)!}$$

Remarque 2.26 *En analyse combinatoire,* C_n^p *est le nombre de parties de* p *éléments choisis dans un ensemble de* n *éléments, appelées* ***combinaisons*** *de* p *éléments choisis parmi* n *éléments. Nous rappelons aussi que le factoriel d'un nombre premier* n *est, par définition,* $n = 1 \times 2 \times \cdots n$, *et par convention, on pose*

$$0! = 1$$

Éléments réguliers, inversibles et diviseurs de zéro

Supposons que A soit non nul. On dit que $a \in A$ est **régulier à gauche** (resp. **à droite**) ssi $x \mapsto ax$ (resp. $x \mapsto xa$) est une application injective, i.e.

$$ax = ay \Longrightarrow x = y$$

Ce qui, par soustraction, équivaut à

$$ax = 0 \Longrightarrow x = 0$$

Un élément régulier à gauche (resp. à droite) est nécessairement non nul mais un élément peut être régulier à gauche sans l'être à droite et vice versa. Un élément est **régulier** ssi il l'est à gauche et à droite.

Il est possible dans un anneau que le produit de deux éléments non nuls x et y donne zéro, i.e.

$$xy = 0 \qquad \text{mais} \qquad x \neq 0 \neq y$$

On appelle un élément $a \in A$ **diviseur de zéro à gauche** (resp. à droite) ssi $a \neq 0$ et a n'est pas régulier à gauche (resp. à droite), i.e.

$$\exists x \in A \setminus \{0\} : \; ax = 0 \quad (\text{resp. } xa = 0)$$

Un élément donné est alors dit **diviseurs de zéro** s'il l'est à gauche et à droite.

Notons que lorsque A est commutatif, un élément quelconque est soit nul, soit régulier, soit un diviseur de 0.

EXEMPLES **2.27** Dans $\mathcal{A}(\mathbb{N}, \{0, 1\})$. Considérons les deux fonctions

$$f(n) = \begin{cases} 1 & \text{si } n \text{ est pair;} \\ 0 & \text{sinon} \end{cases} \qquad g(n) = \begin{cases} 0 & \text{si } n \text{ est pair;} \\ 1 & \text{sinon} \end{cases}$$

Clairement, pour tout n de $\mathbb{N}$, on a $f(n)g(n) = 0$ mais les deux fonctions ne sont pas nulles.

Nous avons aussi l'exemple de l'ensemble quotient $\mathbb{Z}/6\mathbb{Z}$ (voir Exemple. 2.20). Nous voyons que

$$\dot{2} \cdot \dot{3} = \dot{6} = \dot{0}$$

○

Un anneau non nul, commutatif et sans diviseur de zéro est appelé **anneau intègre**. Un tel anneau doit donc vérifier :

$$\forall (x, y) \in A^2 : \; xy = 0 \Longrightarrow x = 0 \vee y = 0 \tag{2.16}$$

EXEMPLE **2.28** $(\mathbb{Z}, +, \times)$ est un anneau intègre. ○

Comme deuxième exemple d'anneau intègre, nous avons

Théorème 2.29 *Soit $n \geq 2$. Alors, on a*

$$n \text{ est premier} \iff \mathbb{Z}/n\mathbb{Z} \text{ est un anneau intègre} \tag{2.17}$$

Dans un un anneau non nul A, un élément a est dit **inversible à droite** (resp. **à gauche**) ssi il est symétrisable à droite (resp. à gauche) pour la multiplication, i.e.

$$\exists b \in A : ab = 1 \quad (\text{resp. } \exists c \in A : ca = 1)$$

Si a est inversible sur les deux côtés, on dit que a est **inversible** ; l'inverse alors est noté $1/a = a^{-1}$.

EXEMPLE **2.30** Dans $\mathbb{Z}$, les seuls éléments inversibles sont -1 et 1. ○

Dans un anneau intègre A, on dit que a **divise** b ssi

$$\exists c \in A : b = ca \tag{2.18}$$

En l'occurrence, on dit aussi que a est un **diviseur** de b ou que b est **divisible** par a. Et on écrit $a|b$. Notons que si (2.18) est vraie, cela signifie clairement que $b \in aA$. Ce qui équivaut en même temps à ce que $bA \subset aA$.

La relation $a|b$ est clairement réflexive et transitive. Ceci définit alors ce que l'on appelle un **préordre** dans A. Cependant, il est possible que $a|b$ et $b|a$ soient simultanément vraies sans que $a \neq b$, autrement dit $aA = bA$; quand cette propriété est satisfaite, on dit que a et b sont **associés**. Mais dans $\mathbb{Z}$, l'actuelle relation de division induit sur $\mathbb{N}$ une relation d'ordre.

Remarquons aussi que c est *unique* dans (2.18) si $a \neq 0$. En effet, si $d \neq 0$ est un autre diviseur de b, alors, comme A est supposé intègre et que $a \neq 0$, nous avons

$$ca = da \Longrightarrow a(c-d) = 0 \Longrightarrow c - d = 0 \Longrightarrow c = d$$

EXEMPLE **2.31** Dans l'anneau intègre $\mathbb{Z}$, il existe des nombres divisibles par d'autres comme 10 par 2 ; cette notion de divisibilité se confond en fait avec la multiplicité : 10 est un multiple de 2. Toutefois, tous les entiers ne sont pas divisibles comme les célèbres *nombres premiers*, ou plus généralement, les entiers qui sont des multiples de nombres premiers différents comme $2 \cdot 5$ et $5 \cdot 7$. On voit donc que $\mathbb{Z}$ a besoin d'être étendu à une structure plus large, à savoir les *nombres rationnels* ○

Quant aux éléments inversibles d'un anneau, nous avons

Proposition 2.32 *Soit A un anneau non nul. L'ensemble des éléments inversibles de A est stable pour la multiplication et forme un groupe multiplicatif dans $A \setminus \{0\}$, dit* ***groupe des éléments inversibles*** *de A.*

Une partie d'un anneau est dite un **sous-anneau** si elle est elle-même un anneau relativement aux mêmes opérations internes. Grâce au Théorème 2.10, on montre facilement la caractérisation suivante d'un sous-anneau.

Proposition 2.33 *Pour qu'une partie non vide H d'un anneau A soit un sous-anneau de A il faut et il suffit que*

$$\forall x, y \in H : \qquad x - y \in H \quad et \quad xy \in H \tag{2.19}$$

En outre, si A est commutatif ou intègre, il en est de même de H.

De plus, un anneau A peut être unitaire sans qu'un sous-anneau B le soit comme le montre l'exemple suivant :

Théorème 2.34 *Les sous-anneaux de $\mathbb{Z}$ sont les ensembles $n\mathbb{Z}$ avec $n \in \mathbb{N}$.*

En outre, remarquons le fait facile à établir que toute intersection de sous-anneaux d'un anneau A est un sous-anneau de A comme pour les sous-groupes. On pourra donc définir le plus petit sous-anneau contenant une partie non vide B : c'est l'intersection de tous les sous-anneaux de A contenant B, on l'appelle le **sous-anneau engendré** par B.

Homomorphismes d'anneaux

Soit A et B deux anneaux. On appelle **homomorphisme** de A dans B toute application $f : A \to B$ telle que

(i) $f(1_A) = 1_B$

(ii) f est un morphisme pour l'addition et la multiplication, i.e.

$$\forall x, y \in A : \ f(x + y) = f(x) + f(y), \quad f(xy) = f(x)f(y)$$

Un **endomorphisme** est un homomorphisme de A dans A. Un **isomorphisme** est une bijection $f : A \to B$ telle que f et f^{-1} soient des homomorphismes. Et on appelle un **automorphisme** tout isomorphisme de A dans A.

EXEMPLE **2.35** Soit A un anneau et E un ensemble. Sur $\mathcal{A}(E, A) = A^E$, définissons les opérations

$$f + g : \ x \mapsto f(x) + g(x), \quad fg : \ x \mapsto f(x)g(x)$$

Ces deux dernières définissent une structure d'anneau sur A^E, dite *naturelle*. L'élément unité est l'application constante $u : x \mapsto 1$.

Il est facile de voir que A^E est commutatif si A l'est. Par ailleurs, si $E = \{1, \ldots, n\}$, on écrit A^n au lieu de A^E, ce qui est conforme à la notation d'ensemble produit.

Observons alors que pour $x \in E$, l'application $p_x : A^E \to A$ telle que $f \mapsto f(x)$, est un homomorphisme que l'on appelle **projection** de la x-ème coordonnée. ○

En même temps, nous avons quelques propriétés immédiates des homomorphismes d'anneaux.

Proposition 2.36 *Le composé de deux homomorphismes (resp. isomorphismes) en est un aussi. La réciproque d'un isomorphisme d'anneaux en est un. Et un homomorphisme d'anneaux bijective est un isomorphisme.*

2.4 Corps

Un ensemble non vide K est dit **corps** s'il possède une structure d'anneau *non nul* et que l'ensemble K sans l'élément neutre de la première loi est un groupe par rapport à la deuxième loi. Si, en plus, cette dernière est commutative, on dit alors que le corps est commutatif.

Pour simplifier, nous notons la première loi d'un corps additivement et la seconde multiplicativement. Ainsi, un ensemble K est un corps ssi $(K, +, \times)$ est anneau non nul et $(K \setminus \{0\}, \times)$ est un groupe. Dans ce cas, K contient au moins les deux éléments neutres 0 et 1. Ainsi, un anneau K est un corps ssi le groupe de ses éléments inversibles est $K \setminus \{0\}$ que l'on note alors K^*.

EXEMPLES **2.37** L'ensemble des rationnels $\mathbb{Q}$ constitue un corps commutatif pour les opérations d'addition et de multiplication naturelles. C'est là l'exemple basique dont une construction est donnée dans [2]. En même temps, l'exemple important et le plus connu d'un corps est le corps des nombres réels $\mathbb{R}$ auquel nous consacrons le Chapitre **??**. ○

Dans un corps commutatif, nous adoptons souvent la notation fractionnelle suivante :

$$x^{-1} = \frac{1}{x} \qquad \text{et} \qquad xy^{-1} = y^{-1}x = \frac{x}{y} = x/y \quad (y \neq 0)$$

En plus des propriétés de calcul générales des groupes et des anneaux, nous avons les propriétés suivantes dans un corps :

Proposition 2.38 *Un corps est un anneau intègre : pour qu'un produit de deux éléments d'un corps donné soit nul, il faut et il suffit que l'un des deux termes soit nul, i.e.*

$$xy = 0 \Longleftrightarrow x = 0 \quad ou \quad y = 0$$

De plus, on a

$$\frac{x}{z} + \frac{y}{z} = \frac{x+y}{z} \tag{2.20}$$

Remarque 2.39 *La propriété (2.20) donne aussi*

$$\frac{x}{y} + \frac{z}{w} = \frac{xw}{yw} + \frac{yz}{yw} = \frac{xw+zy}{yw}; \tag{2.21}$$

$$\frac{x}{y} = \frac{z}{w} \Leftrightarrow xw = yz; \tag{2.22}$$

$$\frac{x/y}{z/w} = \frac{xw}{yz} \tag{2.23}$$

Nous avons comme exemple de corps le résultat suivant qui fait suite au Théorème 2.29.

Théorème 2.40 *Pour tout $n \geq 2$, on a*

$$\mathbb{Z}/n\mathbb{Z} \text{ est un anneau intègre} \Longleftrightarrow \mathbb{Z}/n\mathbb{Z} \text{ est un corps} \tag{2.24}$$

Toute partie d'un corps donné qui est elle-même un corps par rapport aux mêmes opérations s'appelle **sous-corps** comme le sous-corps $\mathbb{Q}$ des rationnels dans le corps des nombres réels $\mathbb{R}$.

Pour reconnaître un sous-corps, nous avons

Proposition 2.41 *une partie H d'un corps K est un sous-corps ssi*

$$\forall x, y \in H : \qquad x - y \in H \quad et \quad xy^{-1} \in H \tag{2.25}$$

Remarque 2.42 *Ce résultat équivaut à ce que H soit un sous-anneau et que pour tout $x \in H \setminus \{0\}$, on a $x^{-1} \in H$. Ceci est équivalent aussi à ce que H soit un sous-anneau et que le groupe des éléments inversibles de H est $H \cap K^*$.*

Intéressons-nous maintenant aux homomorphismes d'anneaux entre corps. Un isomorphisme d'anneaux entre corps s'appelle **isomorphisme de corps**. Un isomorphisme d'un corps sur lui-même est dit **automorphisme de corps**.

Proposition 2.43 *Soit K un corps et A un anneau. Si $\phi : K \to A$ est un homomorphisme d'anneaux, alors ϕ est injectif, le sous-anneau $\phi(K)$ est un corps dans A, et $\widetilde{\phi} : K \to \phi(K)$ est un isomorphisme de corps.*

Remarque 2.44 *Si K et A sont commutatifs, alors la présente proposition justifie le langage suivant : un isomorphisme de K dans A est un homomorphisme d'anneaux de K dans A ; un isomorphisme de K* ***sur*** *A suppose que A soit un corps en bijection avec K. Ainsi, nous n'emploierons pas l'expression homomorphisme de corps.*

3 Espaces vectoriels

En mathématiques comme en sciences appliquées telles la physique, la chimie ou la biologie, il est fréquent que les solutions (mathématiques) aux problèmes étudiés se superposent en ce sens que si u et v sont deux solutions distinctes, alors leur somme $u+v$ est aussi une solution, mais aussi la multiplication des solutions par une quantité réelle ou complexe, c'est-à-dire λu reste aussi une solution avec $\lambda \in \mathbb{R}$ ou $\mathbb{C}$. Ce genre de problèmes sont dits linéaires comme pour les équations des cordes vibrantes ou de l'électricité. Nous sommes alors conduits à construire une structure abstraite qui exprime explicitement ces solutions, ce que l'on appelle "espaces vectoriel".

3.1 Définition

Soit K un corps commutatif qui sera le plus souvent $\mathbb{R}$ ou $\mathbb{C}$. Soit $(E,+)$ un groupe abélien (cf. Sous-section 2.2). On appelle E un **espace vectoriel** sur le corps K (en abrégé **e.v.** ou K-**e.v.**) s'il existe une loi de composition dite **externe** de domaine K en ce sens que c'est une application $K \times E \longrightarrow E$, qui associe au couple (λ, x) l'image, notée multiplicativement, $\lambda \times x = \lambda \cdot x = \lambda x$, telle que les propriétés suivantes soient vérifiées :

(i) $(\lambda\mu)x = \lambda(\mu x), \quad \forall \lambda, \mu \in K, \forall x \in E\,;$

(ii) $(\lambda+\mu)x = \lambda x + \mu x, \quad \forall \lambda, \mu \in K, \forall x \in E\,;$

(iii) $\lambda(x+y) = \lambda x + \lambda y, \quad \forall \lambda, \mu \in K, \forall x \in E\,;$

(iv) $1_K\, x = x, \quad \forall x \in E.$

Les éléments de K sont dits des **scalaires** dont les éléments neutres, additif et multiplicatif, sont notés respectivement 0 et 1, et ceux de E sont appelés des **vecteurs**. Si E se réduit à un seul point qui doit clairement être 0_E, on dit que E est **trivial**.

Notons que l'appellation de vecteur vient de la géométrie. En effet, l'on remarque facilement que le plan géométrique muni d'un repère vérifie bien les conditions de la définition de l'espace vectoriel. Les éléments d'un tel ensemble géométrique sont alors désignés par $k\vec{v}$. Cette représentation est utile par exemple en physique où certaines grandeurs sont représentées par des segments orientés que l'on appelle *vecteurs*. Une force par exemple est déterminée par son intensité mais aussi par son point d'application et par le direction et le sens suivant lequel elle s'exerce.

EXEMPLES **3.1** ($\mathbb{R}$) Nous avons en premier l'espace incontournables $\mathbb{R}$ qui est clairement un e.v. sur $\mathbb{R}$ pour les opérations usuelles.

EXEMPLE **3.2** ($\mathbb{R}^n$ et $\prod_{i=1}^n E_i$) Dans l'ensemble produit $\mathbb{R}^n$ avec $n \in \mathbb{N}^*$, il est possible de définir un e.v. sur $\mathbb{R}$ à partir des lois déjà définies dans $\mathbb{R}$. En effet, les deux opérations interne et externe sont respectivement données par

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$
$$\lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$$

De manière générale, K^n possède de la même façon une structure d'espace vectoriel sur K. Et plus généralement, si $E_1, \cdots, E_n$ sont des e.v. sur K, alors $\prod_{i=1}^n E_i$ possède de la même façon une structure d'e.v. ○

EXEMPLE **3.3** (**L'e.v. des polynômes** $\mathbb{R}_n[x], \mathbb{R}[x]$) L'ensemble $\mathbb{R}_n[x]$ des fonctions polynômes à coefficient dans $\mathbb{R}$ de degré $k \leq n$ est un e.v. sur $\mathbb{R}$ pour les lois

$$(a_n x^n + \cdots + a_0) + (b_n x^n + \cdots + b_0) = (a_n + b_n)x^n + \cdots + a_0 + b_0$$
$$\lambda(a_n x^n + \cdots + a_0) = \lambda a_n x^n + \cdots + \lambda a_0$$

Plus généralement, l'ensemble $\mathbb{R}[x]$ de tous polynômes à coefficient dans $\mathbb{R}$ définit un e.v. sur $\mathbb{R}$ avec les lois

$$\sum a_k x^k + \sum b_k x^k = \sum (a_k + b_k)x^k$$
$$\lambda \sum a_k x^k = \sum (\lambda a_k)x^k$$

○

EXEMPLE **3.4** ($\mathcal{A}(D, E)$) Soit E un e.v. sur K et D un ensemble quelconque non vide. Soit $\mathcal{A}(D, E)$ l'ensemble des applications de D dans E. La structure d'e.v. de

E induit une autre sur $\mathcal{A}(D,E)$ définie par les opérations : $f,g \in \mathcal{A}(D,E), \lambda \in K$, alors

$$(f+g)(x) = f(x) + g(x)$$
$$(\lambda f)(x) = \lambda f(x)$$

L'élément neutre additif est alors l'application constante nulle et l'opposé à une application donnée f et $-f = -1\, f$. ○

L'opération externe dans un e.v. possède des propriétés essentielles que nous donnons dans la proposition suivante.

Proposition 3.5 *Pour tout $\lambda \in K$ et $x \in E$, on a :*
(i) $\lambda 0_E = 0_E, \quad 0\, x = 0_E$
(ii) $\lambda x = 0_E \Longrightarrow \lambda = 0 \vee x = 0_E$
(iii) $(-\lambda)x = \lambda(-x) = -(\lambda x) =: -\lambda x.$

3.2 Sous-espace vectoriel

Soit E un e.v. sur K et F une partie non vide de E. On dit que F est un sous-espace vectoriel de E sur K (en abrégé **s.e.v.**) si F est un e.v. pour les mêmes opérations internes et externe définies sur E.

Pour vérifier que F est un s.e.v., il faudrait donc que toutes les conditions de l'e.v. soit satisfaites. Cependant, on va voir qu'il suffit de vérifier la stabilité des deux lois en question.

Proposition 3.6 *F est un s.e.v. de E sur K ssi*

$$\forall \lambda, \mu \in K, \forall x, y \in F : \quad \lambda x + \mu y \in F$$

Pour la suite, l'élément neutre 0_E qui reste le même pour tout s.e.v. sera noté 0 s'il n'y a pas de risque de confusion. Et nous sous-entendons toujours que K est le corps associé à l'e.v. E sauf mention contraire.

EXEMPLE **3.7** (**Droite vectorielle**) Soit E un e.v. et $v \in E$. Soit

$$F = \{u \in E : \exists \lambda \in K :\ u = \lambda v\} =: \langle v \rangle$$

Alors F est un s.e.v. de E dit **s.e.v. engendré** par v. En effet, nous avons $0v = 0 \in F$ et de plus, nous avons

$$x + y = \lambda v + \mu v = (\lambda + \mu)v \in F, \quad \lambda x = \lambda\mu\, v \in F$$

Particulièrement, toute droite du plan géométrique qui passe par l'origine est un s.e.v. ○

De manière générale, soit $G = \{v_1, \ldots, v_n\}$ une famille de vecteurs d'un e.v. E. On appelle **combinaisons linéaires** de G toute expression de la forme

$$\lambda_1 v_1 + \cdots + \lambda_n v_n \tag{3.1}$$

On définit alors le **s.e.v. engendré** par les vecteurs de la famille G l'ensemble donné par

$$\langle G \rangle \coloneqq \{x \in E : \exists \lambda_1, \ldots, \lambda_n \in K : x = \lambda_1 v_1 + \cdots + \lambda_n v_n\} \tag{3.2}$$

Les vecteurs de $\langle G \rangle$ sont alors des combinaisons linéaires de G qui, en l'occurrence, est appelée **famille génératrice** de $\langle G \rangle$.

EXEMPLE **3.8** Soit dans $\mathbb{R}^3$, la partie

$$F = \{\lambda(1,1,0) + \mu(1,0,1)\}$$

Alors F est bien un s.e.v. engendré par la famille $\{(1,1,0),(1,0,1)\}$. Remarquons en même temps que

$$(x,y,z) = \lambda(1,1,0) + \mu(1,0,1) \iff x = y + z$$

Ainsi, on peut écrire que

$$F = \{(x,y,z) : x = y + z\}$$

○

Quand on manipule des parties, on s'intéresse forcément à leur union et leur intersection. La question alors, avons-nous toujours un s.e.v. si on prend l'union ou l'intersection de s.e.v. ?

Théorème 3.9 *L'intersection de deux s.e.v. est un s.e.v.*

Remarque 3.10 *L'union de deux s.e.v. n'est en général pas un s.e.v. Par exemple, il est facile de vérifier que* $2\mathbb{Z}$ *et aussi* $3\mathbb{Z}$ *sont deux s.e.v. de l'e.v.* $\mathbb{Z}$ *sur* $\mathbb{N}$ *sauf que* $2 + 3 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$. *En même temps, si* F *est un s.e.v. de* E, *alors* $E \setminus F$ *n'est pas un s.e.v. car* $0 \notin E \setminus F$.

3.3 Bases et dimension

Soit $G = \{v_1, \ldots, v_n\}$ une famille de vecteurs d'un K-e.v. E. On dit que G est une **famille génératrice** de E si tous les éléments de E se décomposent en combinaisons linéaires des vecteurs de ladite famille, i.e.

$$\forall v \in E, \exists \lambda_1, \ldots, \lambda_n \in K : \; v = \lambda_1 v_1 + \cdots + \lambda_n v_n$$

donc,

$$E = \{\lambda_1 v_1 + \cdots + \lambda_n v_n : \; \lambda_1, \ldots, \lambda_n \in K\}$$

On écrit alors

$$E = \langle G \rangle_K$$

mais, le plus souvent, on écrit tout simplement $\langle G \rangle$ s'il n'y a pas de risque de confusion.

Remarquons que tout e.v. ne peut être généré par une famille finie de vecteurs comme nous allons le voir dans l'exemple des polynômes ci-dessous.

EXEMPLE **3.11** $(\mathbb{R}^n, K^n)$ L'e.v. $\mathbb{R}^2$ qui est en même temps le plan géométrique est généré par $\{(1,0),(0,1)\} =: \{e_1, e_2\}$. En effet, nous avons

$$(x, y) = xe_1 + ye_2$$

Cependant, il est possible de trouver d'autres familles génératrices pour $\mathbb{R}^2$. Nous avons aussi $\{(1,1),(1,-1)\} = \{v_1, v_2\}$. En effet, soit $(x, y) \in \mathbb{R}^2$ et remarquons que

$$(x, y) = \lambda v_1 + \mu v_2 \iff x = \lambda + \mu, \; y = \lambda - \mu \iff \lambda = \frac{x+y}{2}, \; \mu = \frac{x-y}{2}$$

Ce fait peut être facilement généralisé à $\mathbb{R}^n$ avec la famille $\{e_1, \ldots, e_n\}$ où e_i est le vecteur avec des coordonnées nulles sauf la i-ème coordonnée qui est 1, les coordonnées étant les termes ordonnés d'un élément du produit $\mathbb{R}^n$. De manière générale, on peut définir une famille génératrice similaire pour K^n. Les vecteurs e_i sont dits les **vecteurs canoniques**. ○

Une famille de vecteurs non nuls $\{v_1, \ldots, v_n\}$ est dite **libre** ou **(linéairement) indépendante** si

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = 0 \Longrightarrow \lambda_1 = \cdots = \lambda_n = 0 \tag{3.3}$$

Si (3.3) n'est pas vérifiée, on dit alors que la famille est **liée** ou **(linéairement) dépendante**. Notons que si l'un des v_i est nul, disons v_1, alors la famille est liée. En effet, nous aurons dans ce cas pour un choix quelconque de $\lambda \neq 0$,

$$\lambda\, 0 + 0\, v_2 + \cdots + 0\, v_n = 0 \tag{3.4}$$

Et pour compléter cette définition, on convient que la **partie vide est libre**.

EXEMPLE **3.12** Dans $\mathbb{R}^3$, les vecteurs canoniques e_i sont libres. En effet, nous avons

$$\lambda_1 e_1 + \cdots + \lambda_n e_n = 0 \Longleftrightarrow (\lambda_1, \ldots, \lambda_n) = 0 \Longrightarrow \lambda_1 = \cdots = \lambda_n = 0$$

Mais ce ne sont pas les seuls. Prenons $v_1 = (1, 1, -1), v_2 = (0, 2, 1)$ et $v_3 = (0, 0, 5)$ et remarquons que

$$\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = 0 \Longleftrightarrow (\lambda_1, \lambda_1 + 2\lambda_2, -\lambda_1 + \lambda_2 + 5\lambda_3) = 0$$

ce qui implique que

$$\begin{cases} \lambda_1 = 0 \\ \lambda_1 + 2\lambda_2 = 0 \\ -\lambda_1 + \lambda_2 + 5\lambda_3 = 0 \end{cases} \Longrightarrow \lambda_1 = 0, \lambda_2 = 0, \lambda_3 = 0$$

Par contre, les vecteurs, $v_1 = (1, 2, 1), v_2 = (-1, 3, 1)$ et $v_3 = (-1, 13, 5)$ sont liés car

$$2v_1 + 3v_2 - v_3 = 0$$

○

Nous arrivons alors à la notion importante qui réunit celles de famille génératrice et de famille libre. Dans un e.v., on appelle **base** toute famille génératrice et libre. Une **base d'un e.v.** donné est alors une famille libre qui le génère.

Théorème 3.13 *Une famille de vecteurs donnée est une base pour un e.v. ssi tout vecteur se décompose linéairement de façon unique sur les éléments de la famille donnée.*

Remarque 3.14 *La présente assertion peut clairement s'énoncer de manière équivalente comme suit : $B = \{v_1, \ldots, v_n\}$ est une base de E ssi il y a une bijection entre E et K^n telle que*

$$x = x_1 v_1 + \cdots + x_n v_n \longmapsto (x_1, \ldots, x_n)$$

Les termes x_i sont alors les coordonnées de x dans la base B. À cause de l'unicité de la décomposition, un vecteur x est donc uniquement et totalement défini par ses coordonnées et de ce fait, pour base donnée, il est souvent noté par

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \tag{3.5}$$

EXEMPLE **3.15** (**Base canonique de** K^n) Précédemment, nous avons parlé des vecteurs canoniques dans $\mathbb{R}^n$, et plus généralement dans K^n, à savoir les vecteurs tels que $e_i = (\delta_{ij})_{j=1}^n, i = 1, \ldots, n$, où nous avons employé les symboles de Kronecker :

$$\delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon} \end{cases}$$

Ils constitue une famille génératrice pour K^n. En plus, ils sont libres, autrement dit une base, dite **base canonique**. En effet, nous avons

$$\lambda_1 e_1 + \cdots + \lambda_n e_n = 0 \Longleftrightarrow (\lambda_1, \ldots, \lambda_n) = 0 \Longrightarrow \lambda_1 = \cdots = \lambda_n = 0$$

○

EXEMPLE **3.16** Soit $F = \{x \in \mathbb{R}^3 : 2x + y + 3z = 0\}$. Il est facile de vérifier que c'est un s.e.v. de $\mathbb{R}^3$. Essayons de lui trouver une base. Remarquons que

$$(x, y, z) \in F \Longleftrightarrow (x, -2x - 3z, z) = x(1, 2, 0) + z(0, -3, 1) =: xv_1 + zv_2$$

En même temps, nous avons

$$\lambda_1 v_1 + \lambda_2 v_2 = 0 \Longleftrightarrow (\lambda_1, -2\lambda_1 - 3\lambda_2, \lambda_2) = 0 \Longrightarrow \lambda_1 = \lambda_2 = 0$$

Ainsi, $\{v_1, v_2\}$ constitue une base pour F. ○

Il est évident qu'une base est un objet important dans un e.v. La question est maintenant : une base existe-elle toujours dans un e.v. ?

Théorème 3.17 (Existence) *Soit E un espace vectoriel non trivial généré par une famille finie G. Si L une partie libre de G, alors il existe une base B telle que $L \subset B \subset G$.*

Remarque 3.18 *Notons que dans une famille quelconque de vecteurs non nuls, il existe toujours une partie libre. En effet, il suffit de prendre l'un d'entre eux qui est libre par lui-même. En même temps, l'assertion du théorème peut clairement être formulée de manière équivalente comme suit : de toute famille génératrice, on peut extraire une base. Ou nous avons aussi une autre proposition équivalente que l'on appelle* ***théorème de la base incomplète*** *: toute famille libre peut être complétée pour donner une base. Ceci est prouvé implicitement dans la preuve ci-après.*

La notion de base d'un e.v. conduit inévitablement à la notion de dimension qui est donnée dans le résultat fondamental suivant :

Théorème 3.19 (Dimension) *Soit E un K-e.v. généré par une famille finie de ses vecteurs. Alors, toutes les bases de E ont le même cardinal que l'on appelle* ***dimension*** *et que l'on note par* $\dim_K(E)$.

Remarque 3.20 *Le présent théorème permet donc d'appeler un* ***e.v. de dimension finie*** *tout e.v. généré par une famille finie de ses vecteurs, sinon il est dit de* ***dimension infinie****.*

Si $E = \{0\}$, on pose : $\dim_K(E) = 0$. *Il est clair alors que*

$$\dim_K(E) = 0 \Longleftrightarrow E = \{0\}$$

Notons que la dimension d'e.v. dépend du corps associé K. En effet, nous avons que les éléments de l'e.v. $\mathbb{C}$ sur $\mathbb{R}$. s'écrire de façon unique sous la forme

$$x + iy = x\,1 + y\,i$$

D'où, $\{1, i\}$ constitue une base pour $\mathbb{C}$ sur $\mathbb{R}$, donc $\dim_{\mathbb{R}}(\mathbb{C}) = 2$. *Mais d'après la deuxième remarque ci-dessus,* $\dim_{\mathbb{C}}(\mathbb{C}) = 1$. *Dorénavant, s'il n'y a pas de confusion sur le corps associé K, nous noterons la dimension par* $\dim(E)$.

Si $V = \{v_1, \ldots, v_n\}$ est une famille de vecteurs d'un e.v. E, on appelle ***rang*** *de V la dimension de $\langle G\rangle$, le s.e.v. généré par V, autrement dit le nombre de vecteurs libres dans V. Et on écrit*

$$\mathrm{rg}(V) = \dim(\langle V\rangle) \tag{3.6}$$

Par ailleurs, nous savons que K^n admet la base canonique $(e_1, \ldots, e_n)$. Ainsi, nous avons

$$\dim_K(K^n) = n \tag{3.7}$$

Par ailleurs, que peut-on dire sur la dimension d'un s.e.v. ?

Proposition 3.21 *Soit F un s.e.v. de E qui est de dimension finie, alors on a*

$$\dim(F) \leq \dim(E) \tag{3.8}$$

de plus,

$$\dim(F) = \dim(E) \Longrightarrow F = E \tag{3.9}$$

Remarque 3.22 *L'implication (3.9) permet de montrer qu'une partie est égale à l'ensemble total au lieu de montrer directement son inclusion.*

3.4 Somme directe

Soit A et B deux parties d'un groupe donné E. La somme de A et B est la partie définie par

$$A + B = \{x + y : x \in A, y \in B\} \tag{3.10}$$

Nous savons déjà que l'union de s.e.v. n'est généralement pas un s.e.v. Qu'en est-il de la somme ?

Théorème 3.23 *Soit E_1 et E_2 deux s.e.v. d'un e.v. E. Alors, on a que $E_1 + E_2$ est un s.e.v. En outre, la décomposition des éléments dudit s.e.v. en somme d'un élément du premier plus un autre du second est unique ssi $E_1 \cap E_2 = \{0\}$. Dans ce cas, cette somme est dite* ***somme directe*** *que l'on note par $E_1 \oplus E_2$.*

Notons qu'en général, $E_1 + E_2 \neq E$. Cependant, il est possible d'avoir une décomposition de E en une somme directe si sa base peut être aussi partagée :

Théorème 3.24 *Soit E_1 et E_2 deux s.e.v. de E. Alors, $E = E_1 \oplus E_2$ ssi pour toutes bases B_1 de E_1 et B_2 de E_2, $\{B_1, B_2\}$ est une base de E.*

Nous voyons maintenant que les s.e.v. formant une somme directe décompose uniquement l'espace total mais nous ne pouvons dire qu'ils se complètent étant donné qu'ils se partagent toujours 0. Toutefois, il est correct de dire qu'ils sont supplémentaires l'un de l'autre, et donc de les appeler des **s.e.v. supplémentaires**.

Nous avons la formule générale qui donne la dimension d'une somme de s.e.v., en particulier une somme directe.

Théorème 3.25 *Soit E_1 et E_2 deux s.e.v. d'un e.v. E. Alors, on a*

$$\dim(E_1 + E_2) = \dim(E_1) + \dim(E_2) - \dim(E_1 \cap E_2) \tag{3.11}$$

Remarque 3.26 *En vertu de la formule* (3.11)*, on obtient que*

$$\dim(E_1 \oplus E_2) = \dim(E_1) + \dim(E_2) \tag{3.12}$$

EXEMPLES **3.27** Soit dans $\mathbb{R}^2$ deux vecteurs indépendants v et w. Donc, $\{v, w\}$ est une base de $\mathbb{R}^2$. Alors, on a

$$\mathbb{R}^2 = \langle\{v\}\rangle + \langle\{w\}\rangle$$

Ce fait est facilement généralisable à $\mathbb{R}^n$ pour lequel on obtient que pour des vecteurs indépendants $v_1, \ldots, v_n$,

$$\mathbb{R}^n = \langle\{v_1\}\rangle + \cdots + \langle\{v_n\}\rangle$$

○

4 Applications linéaires

La notion d'espace vectoriel n'acquière tout son sens qu'après l'introduction des applications dites linéaires. Ces dernières qui, par définition, sont des homomorphismes entre e.v. ont la particularité de conserver la structure d'espace vectoriel.

4.1 Définition

Soit K un corps commutatif et E, F deux K-e.v. On appelle $f : E \to F$ une **application linéaire** (ou K-linéaire ou un homomorphisme de K-e.v. E dans F) si c'est un homomorphisme qui, de plus, vérifie la propriété suivante dite d'*homogénéité par rapport aux scalaires*,

$$\forall x \in E, \forall \lambda \in K : \ f(\lambda x) = \lambda f(x) \tag{AL}$$

L'ensemble de telles applications est noté $\mathrm{Hom_K}(E, F)$. En particulier, si $E = F$, on parle alors d'**endomorphismes** dont l'ensemble est noté $\mathrm{Hom_K}(E)$. Nous écrirons en abrégé **a.l.** pour signifier une application linéaire et nous considérerons toujours des e.v. par rapport à K sauf mention contraire.

Si $f : E \to F$ est une application bijective telle que $f \in \mathrm{Hom_K}(E, F), f^{-1} \in \mathrm{Hom_K}(F, E)$, alors f est dite **isomorphisme de K-e.v.** de E sur F. Un isomorphisme de K-e.v. : $E \to E$ est appelé **automorphisme** du K-e.v. E.

Si K est considéré comme K-e.v., les a.l. de $\mathrm{Hom_K}(E, K)$ sont appelées **formes linéaires** sur E et cet ensemble est dit **dual (algébrique)** de E, noté par E^*.

Exemples **4.1** (**a.l. nulle**) Soit

$$\begin{aligned} f : E &\longrightarrow F \\ x &\longmapsto 0 \end{aligned}$$

C'est là une application linéaire dite nulle que l'on note simplement par 0. ○

EXEMPLES **4.2** (**a.l. identique, injection canonique**) Si E est un s.e.v. de F. Alors l'injection canonique $j : E \to F$ est K-linéaire. En particulier, nous avons l'application identique ou identité Id_E qui est un automorphisme du K-e.v. E. ○

EXEMPLE **4.3** (**Projection**) Soit $E = E_1 \oplus E_2$ et $\mathrm{Pr}_1 : E \to E_1$ telle que

$$x_1 + x_2 \mapsto x_1$$

La présente application est clairement linéaire ; on l'appelle **projecteur** (ou projection) sur E_1 parallèle à E_2. De manière similaire, on définit Pr_2, la projection sur E_2 parallèle à E_1. ○

EXEMPLE **4.4** (**Homothétie**) Soit $\lambda \in K$ et définissons l'application

$$\begin{aligned} h_\lambda : E &\longrightarrow E \\ x &\longmapsto \lambda x \end{aligned}$$

On a alors un endomorphisme du K-e.v. E appelé *homothétie de rapport* λ, en particulier $\lambda 0_E = 0_E$. Remarquons que h_{0_K} est l'endomorphisme nul du groupe additif E.

Ladite homothétie h_λ est de plus K-linéaire et si $\lambda \neq 0_K$, alors elle est un automorphisme du K-e.v. E. ○

EXEMPLE **4.5** Soit $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^2$ telle que

$$(x_1, x_2, x_3) \longmapsto (2x_1 + x_2, x_2 - x_3)$$

Vérifions que c'est bien un application $\mathbb{R}$-linéaire. En premier, nous avons

$$\begin{aligned} f(x + x) &= f((x_1 + y_1, x_2 + y_2, x_3 + y_3) \\ &= (2(x_1 + y_1) + x_2 + y_2, x_2 + y_2 - (x_3 + y_3)) \\ &= (2x_1 + x_2, x_2 - x_3) + (2y_1 + y_2, y_2 - y_3) \\ &= f(x) + f(y) \end{aligned}$$

D'autre par, nous avons

$$f(\lambda x) = (2\lambda x_1 + \lambda x_2, \lambda x_2 - \lambda x_3) = \lambda(2x_1 + x_2, x_2 - x_3) = \lambda f(x)$$

○

4.2 Propriétés générales

Les applications linéaires possèdent des propriétés élémentaires réunies dans la proposition suivante.

Proposition 4.6 *Soit E, F et G des K-e.v. Alors, on a que*
(i) si $f \in \mathrm{Hom}_K(E,F), g \in \mathrm{Hom}_K(F,G)$, alors $g \circ f \in \mathrm{Hom}_K(E,G)$,
(ii) si f est une bijection K-linéaire de E sur F, alors f et f^{-1} sont des isomorphismes de E sur F et vice versa.
(iii) le composé d'isomorphismes de K-e.v. est un isomorphisme de K-e.v.

Remarque 4.7 *Notons que la relation entre K-e.v. définie par "E est isomorphe à F" est réflexive, symétrique et transitive. Mais, cela ne définit pas pour autant une relation d'équivalence car la relation "E est un K-e.v." n'est pas collectivisante en ce sens qu'il n'existe aucun ensemble dont tout K-e.v. est un élément.*

En outre, il est facile de munir $\mathrm{Hom}_K(E,F)$ de structures algébriques remarquables. Rappelons-nous de l'Exemple 3.4 l'opération interne d'addition et de la loi externe de multiplication.

Théorème 4.8 *$\mathrm{Hom}_K(E,F)$ est un K-e.v..*

Remarque 4.9 *L'ensemble $\mathrm{Hom}_K(E,F)$ sera systématiquement muni de cette structure d'e.v. dite **naturelle**. En même temps, notons ici la nécessité de la commutativité du corps K pour avoir la stabilité de la loi externe.*

Considérons maintenant la loi de composition des applications linéaires. Facilement, on vérifie que dans les e.v. adéquats, on a

$$\begin{aligned} g \circ (f+h) &= g \circ f + g \circ h \\ (g+k) \circ f &= g \circ f + k \circ f \\ g \circ (\lambda f) &= \lambda g \circ f \end{aligned} \tag{4.1}$$

De plus, nous avons

Proposition 4.10 *Ainsi, $(\mathrm{Hom}_K(E), +, \circ)$ est un anneau dont l'élément unité est Id_E. De plus, cet anneau est nul ssi $E = \{0_E\}$.*

Remarque 4.11 *Dorénavant, $\mathrm{Hom}_K(E)$ sera muni systématiquement de cette structure d'anneau. Observons de plus que $\mathrm{Hom}_K(E)$ ssi $E = \{0_E\}$. En effet, nous avons que $\mathrm{Id}_E \neq 0$ ssi $E \neq \{0_E\}$.*

EXEMPLE **4.12** Pour un corps commutatif K, considéré comme K-e.v., l'anneau $\mathrm{Hom}_K(K)$ s'identifie à K. En effet, pour tout f de $\mathrm{Hom}_K(K)$, nous avons $f(x) = xf(1)$, donc f n'est autre que l'homothétie $h_{f(1)}$ (cf. Exemple 4.4). Ce ce qui établit une correspondance bijective entre K et $\mathrm{Hom}_K(K)$. ○

Supposons que E soit non nul, alors, en vertu de la Proposition 4.10, l'anneau $\mathrm{Hom}_K(E)$ est non nul. En outre, nous savons (cf. Proposition 2.32) que l'ensemble des éléments inversibles d'un anneau forment un groupe pour la multiplication. Cela conduit alors à la définition suivante.

Pour un corps commutatif K et un K-e.v. E, le groupe des a.l. inversibles de l'anneau $\mathrm{Hom}_K(E)$ s'appelle **groupe linéaire** de E que l'on note par $\mathrm{GL}_K(E)$. Ce dernier est clairement l'ensemble des endomorphismes du K-e.v. E muni de la loi de composition des applications qui lui confère la structure de groupe en vertu de la Proposition 4.6.

EXEMPLE **4.13** (**Corps des homothéties**) Le groupe $\mathrm{GL}_K(K)$ s'identifie au groupe K^* : il suffit d'associer à tout $\lambda \in K^*$, l'homothétie h_λ de K (cf. Exemple 4.4) pour obtenir un isomorphisme de groupes de K^* sur $\mathrm{GL}_K(K)$.

Appelons

$$\begin{aligned} H : K &\longrightarrow \mathrm{Hom}_K(E) \\ \lambda &\longmapsto h_\lambda \end{aligned}$$

C'est là un homomorphisme d'anneaux, qui plus est, injectif puisque K est un corps et $\mathrm{Hom}_K(E) \neq \{0\}$ (cf. Remarque 4.11). Le sous-anneau $H(K)$ de $\mathrm{Hom}_K(E)$, isomorphe à K, s'appelle **corps des homothéties** de E. D'autre part, H restreinte à K^* prend ses valeurs dans $\mathrm{GL}_K(E)$ et définit donc un homomorphisme de groupes injectif. Par conséquent, le sous-groupe $H(K^*)$ de $\mathrm{GL}_K(E)$, formé des homothéties de rapport non nul, est isomorphe au groupe multiplicatif K^*, lequel est dit **groupe des homothéties** de E. ○

4.3 Dimension de $\mathrm{Hom}_K(E,F)$

Cette partie porte sur la dimension de l'e.v. $\mathrm{Hom}_K(E,F)$ pour des K-e.v. de dimensions finies. En premier, nous avons

À l'aide de la Proposition **??**, nous obtenons le résultat suivant qui permet de transporter la structure d'un K-e.v. à un autre.

Théorème 4.14 *Soit $\{e_1,\dots,e_n\}$ une base du K-e.v. E. Soit F un autre K-e.v. et $V=\{v_1,\dots,v_n\}$ une famille de F arbitraire. Alors, il existe une seule et une seule application K-linéaire $f:E\to F$ telle que*

$$\forall i:\ f(e_i)=v_i \tag{4.2}$$

De plus, on a
(i) f est injective ssi V est libre,
(ii) f est surjective ssi $F=\langle V\rangle$,
(iii) f est bijective ssi V est une base de F.

Remarque 4.15 *On dit que l'application linéaire unique f du présent théorème s'obtient par* ***prolongement par K-linéarité*** *des relations (4.2).*

Le résultat principal à connaître est le suivant.

Théorème 4.16 *Soit E et F des K-e.v. de dimensions finies. Alors, le K-e.v. $\mathrm{Hom}_K(E,F)$ possède une dimension finie donnée par*

$$\dim\left(\mathrm{Hom}_K(E,F)\right)=\dim(E)\dim(F) \tag{4.3}$$

En particulier, nous avons la dimension de l'espace dual E^*.

Théorème 4.17 *Soit E un K-e.v. de dimension finie. Alors, on a*

$$\dim(E^*)=\dim(E)$$

Remarque 4.18 *Si $B=(e_1,\dots,e_n)$ est une base de E, il existe en vertu de la preuve du Théorème 4.16 une base $\{f_{11},\dots,f_{1n}\}$ de E^* telle que $f_{1i}(e_j)=\delta_{ij}$. Celle-ci est appelé* ***base duale*** *de B et se note par $B^*=\{e_1^*,\dots,e_n^*\}$. Notons que B^* dépend par construction de toute B. Si $x=\sum_{k=1}^n x_k e_k$, alors, pour tout i,*

$$e_i^*(x)=\sum_{k=1}^n x_k\, e_i^*(e_k)=x_i \tag{4.4}$$

Donc, e_i^* fait correspondre, à chaque $x\in E$, sa i-ème coordonnée dans la base B. Ce qui donne la relation fondamentale

$$\forall x\in E:\ x=\sum_{i=1}^n e_i^*(x)\,e_i \tag{4.5}$$

4.4 Noyau, image et rang

Nous avons vu (cf. Théorème 2.18) qu'un homomorphisme conserve la structure de groupe. En fait, si, de plus, une telle application possède la propriété d'homogénéité par rapport aux scalaires, alors la structure d'e.v. est aussi conservée.

Si $f : E \to F$ est une application linéaire, rappelons (cf. Section 2.2) que l'image de f et son noyau sont définis par

$$\mathrm{Im}\,(f) = f(E), \quad \mathrm{Ker}\,(f) = f^{-1}(\{0_F\})$$

Proposition 4.19 *Les images direct ou réciproque de s.e.v. par une application linéaire sont aussi des s.e.v., en particulier, son image et son noyau.*

EXEMPLE **4.20** Soit $E = E_1 \oplus E_2$. Il est immédiat que

$$\mathrm{Im}(\mathrm{Pr}_1) = E_1, \quad \mathrm{Ker}\,(\mathrm{Pr}_1) = E_2$$

○

Nous arrivons alors à un des résultats les plus importants de l'algèbre linéaire, lequel donne, pour les e.v. de dimensions finies, une équation reliant les dimensions du noyau et de l'image d'une a.l. Auparavant, appelons le **rang** d'une a.l. f, la dimension de son image, i.e.

$$\mathrm{rg}\,(f) = \dim\,(\mathrm{Im}\,(f)) \tag{4.6}$$

Notons en même temps que cette notion de rang d'une a.l. est liée à celle de rang d'une famille de vecteurs (cf. Remarque 3.20). En effet, si $E = \langle (v_i)_{i\in I}\rangle$ et que $f \in \mathrm{Hom}_K(E, F)$, alors

$$\mathrm{rg}\,(f) = \mathrm{rg}\,((f(v_i))_{i\in I})$$

Autrement dit, le rand de f et le rang de la famille $(f(v_i))$ qui engendre $\mathrm{Im}\,(f)$.

Théorème 4.21 (du rang) *Soit E et F deux e.v. de dimensions finies et $f \in \mathrm{Hom}_K(E, F)$. Alors, on a*

$$\dim\,(E) = \mathrm{rg}\,(f) + \dim\,(\mathrm{Ker}\,(f)) \tag{4.7}$$

EXEMPLE **4.22** Soit $f : \mathbb{R}^3 \to \mathbb{R}^3$ telle que $(x, y, z) \mapsto (u, v, w)$ avec

$$\begin{cases} u = x + y - z \\ v = 2x + y - 3z \\ w = 3x + 2y - 4z \end{cases} \tag{4.8}$$

Alors, $\mathrm{Ker}\,(f)$ sont les vecteurs de $\mathbb{R}^3$ tels que

$$\begin{cases} x+y-z=0 \\ 2x+y-3z=0 \\ 3x+2y-4z=0 \end{cases}$$

Cela implique facilement que pour tout z,

$$\begin{cases} x=2z \\ y=-z \end{cases}$$

D'où, les vecteurs de $\mathrm{Ker}\,(f)$ s'écrivent sous la forme

$$\mathrm{Ker}\,(f)=\{(2z,-z,z)=z(2,-1,1), z\in\mathbb{R}\}=\langle\{(2,-1,1)\}\rangle$$

Donc, $\mathrm{Ker}\,(f)$ est la droite générée par le vecteur $(2,-1,1)$.

D'autre part, $\mathrm{Im}\,(f)$ sont les vecteurs de (u,v,w) de $\mathbb{R}^3$ tels qu'il existe $(x,y,z)\in\mathbb{R}^3$ satisfaisant le système (4.8). D'où,

$$\begin{cases} x+y-z &= u \\ -y-z &= v-2u \\ -y-z &= w-3u \end{cases}$$

donc

$$\begin{cases} x+y-z &= u \\ y+z &= -v+2u \\ 0 &= 2u-v+w-3u \end{cases}$$

Il en résulte que la condition sur (u,v,w) pour être dans $\mathrm{Im}\,(f)$ est $u+v-w=0$. Et à cause de (4.7), $\mathrm{Im}\,(f)$ est de dimension 2, donc c'est le plan satisfaisant cette dernière condition, i.e.

$$\mathrm{Im}\,(f)=\{u+v-w=0\}$$

○

Le Théorème 4.21 implique des conséquences importantes qui lient la notion de rang à celle de bijection.

Théorème 4.23 *Soit E et F deux e.v. de même dimension finie n et $f\in\mathrm{Hom}_K(E,F)$. Alors, les propositions suivantes sont équivalentes :*

(*i*) *f est injective.*
(*ii*) *f est surjective.*
(*iii*) *f est bijective.*
(*iv*) $\mathrm{rg}\,(f)=n$
(*v*) *f est inversible à gauche.*
(*vi*) *f est inversible à droite.*

5 Matrices

Ce chapitre traite d'un espace vectoriel particulier d'objets mathématiques fréquemment utilisés, à savoir les matrices, qui, à la base servent à donner une expression visuelle des applications linéaires. Cependant, lesdites matrices sont par définition des applications qui, en même temps, généralisent la notion de nombre.

5.1 Définitions et généralités

Soit A un anneau non trivial que nous manipulerons tout au long du chapitre, lequel sera généralement $\mathbb{R}$ ou $\mathbb{C}$.

Soit $p, n \geq 1$ deux entiers. L'ensemble des applications de $[\![1, p]\!] \times [\![1, n]\!]$ dans A est appelé l'ensemble des (p, n)**-matrices** ou matrices d'ordre (p, n) dans A. Ledit ensemble, pour p et n fixés, est généralement noté par $M_{p,n}(A)$, sinon $M_{p,n}$ s'il n'y a pas de confusion sur A. Une telle matrice fait correspondre à tout (i, j) l'image $M(i, j)$ et on écrit généralement

$$M = (a_{ij})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq n}}$$

ou simplement (a_{ij}) où $a_{ij} = a(i, j) = M(i, j)$. Si $p = n = 1$, l'ensemble des $(1, 1)$-matrices se réduit à A. Ce qui permet de voir les matrices comme une *généralisation des nombres*. Cependant, on convient par souci de cohérence de la théorie que si $p = 0$ ou $n = 0$, la (p, n)-matrice est l'application vide $\emptyset \longrightarrow A$ (qui n'associe rien à rien !). Ainsi, lorsque $p = 0$ ou $n = 0$, $M_{p,n}(A)$ contient un seul élément, la **matrice vide**.

Soit $M = (a_{ij}) \in M_{p,n}(A)$. Une telle matrice est représentée sous forme d'un

tableau rectangulaire comme suit

$$M = \begin{pmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ a_{i1} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & & \vdots & & \vdots \\ a_{p1} & \cdots & a_{pj} & \cdots & a_{pn} \end{pmatrix} \tag{5.1}$$

EXEMPLES **5.1**

$$M = \begin{pmatrix} 1 & 3 & -1 \\ 0 & 1 & 2 \end{pmatrix} \in M_{2,3}(\mathbb{R}); \quad N = \begin{pmatrix} 1 & 2-i & 3+i \\ 0 & 1+i & i \\ -i & 2 & 1 \end{pmatrix} \in M_{2,3}(\mathbb{C})$$

Dans la première, nous avons $a_{12} = 3$, et dans la seconde, $a_{23} = i$. ○

La représentation (5.1) justifie les appellations suivantes. Pour i fixé, la séquence $j \mapsto a_{ij}$ de $[\![1, n]\!]$ dans A est dite **ligne d'indice** i : c'est un élément de A^n que l'on note par $L_i(M)$. De même, pour j fixé, la séquence $i \mapsto a_{ij}$ de $[\![1, p]\!]$ dans A est dite **colonne d'indice** j : c'est un élément de A^n que l'on note par $C_i(M)$. Dans le cas fréquent où A est un corps commutatif K, $L_i(M)$ et $C_j(M)$ sont dits respectivement **vecteur ligne** et **vecteur colonne**.

EXEMPLES **5.2** Reprenons les Exemples 5.1. Nous avons alors

$$L_1(M) = \begin{pmatrix} 1 & 3 & -1 \end{pmatrix}, \quad C_2(N) = \begin{pmatrix} 2-i \\ 1+i \\ 2 \end{pmatrix}$$

○

A fortiori, quand $p = 1$, M est appelée **matrice ligne**. Les matrices de $M_{1,n}$ sont alors naturellement confondues avec les éléments de A^n par une bijection évidente. À l'opposé, on a $M_{p,1}$, l'ensemble des **matrices colonnes** associée bijectivement à A^p.

Si $p = n$, alors on dit que M est une **matrice carrée**. Pour n fixé, on écrit en l'occurrence $M_n(A) = M_{n,n}(A)$.

EXEMPLE **5.3** (**Matrice unitaire**) L'exemple basique d'une matrice carré, si 1_A existe, est la matrice dite **unitaire**, pour laquelle tous les éléments sont nuls sauf les diagonaux qui sont égaux à 1_A, i.e.

$$I_n = (\delta_{ij})$$

où

$$\delta_{ij} = \begin{cases} 1_A & \text{si } i = j \\ 0_A & \text{sinon} \end{cases}$$

En particulier, on a une matrice unitaire quand $A = K$. ○

e.v. des matrices

Maintenant, fixons $p, n \geq 1$ et soit $M = (a_{ij}), N = (b_{ij}) \in M_{p,n}(A)$. On définit naturellement l'**addition** des matrices en tant qu'applications comme celle des applications en ce sens que $M + N$ est la matrice de $M_{p,n}$ telle que son élément correspondant à la i-ème ligne et la j-ème colonne est $a_{ij} + b_{ij}$, autrement dit

$$(M + N)(i, j) = (M + N)_{ij} = a_{ij} + b_{ij}$$

Et par suite, $M_{p,n}$ est un **groupe abélien**. L'**élément neutre** est alors 0, la matrice dont tous coefficients sont nuls, et l'**opposé d'une matrice** M est $-M$, celle dont les éléments sont $-a_{ij}$.

Dans le cas particulier où $A = K$, K étant un corps commutatif, que nous emploierons le plus, on a en plus de l'addition la **multiplication externe** des matrices par K que l'on définit évidemment par

$$\lambda(a_{ij}) = (\lambda a_{ij})$$

Ainsi, $M_{p,n}(K)$ est un K**-e.v.** Considérons alors, pour $(i, j) \in [\![1, p]\!] \times [\![1, n]\!]$, les matrices $E^{ij} \in M_{p,n}(K)$ dont tous les coefficients sont nuls excepté $E^{ij}_{ij} = 1_K$:

$$E^{ij} = (\delta_{ik}\delta_{j\ell}) \tag{5.2}$$

où

$$\delta_{ik} = \begin{cases} 1_K & i = k \\ 0_K & \text{sinon} \end{cases}$$

idem pour $\delta_{j\ell}$. Nous avons alors

Théorème 5.4 *La famille $\{E^{ij}\}$ forme une base pour $M_{p,n}(K)$, appelée* ***base canonique****, et l'on a*

$$\dim\left(M_{p,n}(K)\right) = np \tag{5.3}$$

Extractions et permutations

Outre l'addition et la multiplication externe des matrices par des scalaires dans K, il y a d'autres opérations élémentaires possibles sur les matrices qui serviront à obtenir encore d'autres plus compliquées que nous verrons plus bas. On a l'**extraction** d'une matrice à partir d'une autre qui donne ce qu'on appelle **sous-matrice**. Explicitement, soit $M \in M_{m,n}$ et

$$I = \{i_1, \ldots, i_m\} \subset [\![1, p]\!]$$
$$J = \{j_1, \ldots, j_q\} \subset [\![1, n]\!]$$

Alors, la matrice

$$S_{IJ}(M) = (a_{i_k j_\ell})_{1 \leq k \leq m, 1 \leq \ell \leq q} \tag{5.4}$$

est appelée la sous-matrice de M indexée par I et J. Observons que ladite sous-matrice $S_{IJ}(M)$ est pratiquement obtenue en supprimant dans M les lignes correspondant aux indices dans $[\![1, p]\!] \setminus I$ et les colonnes associées aux indices dans $[\![1, n]\!] \setminus J$.

EXEMPLE **5.5** Si $m = n = 4$, $I = \{2, 3\}$ et que $J = \{1, 4\}$, alors on obtient de façon générale la sous-matrice

$$S_{IJ} = \begin{pmatrix} a_{21} & a_{24} \\ a_{31} & a_{34} \end{pmatrix}$$

○

D'autre part, nous avons la **permutation des lignes et des colonnes**. Soit σ une permutation sur $[\![1, n]\!]$ (cf. Exemple 2.9), i.e. une bijection de cet ensemble sur lui-même que l'on représente généralement par

$$\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix} \tag{5.5}$$

Nous rappelons que l'ensemble de telles permutations est notée $\mathcal{S}_n$. Soit deux permutations $\sigma \in \mathcal{S}_p, \tau \in \mathcal{S}_n$. Alors, pour $M \in M_{p,n}(A)$, on définit la matrice

$$(\sigma, \tau) * M = \left(a_{\sigma^{-1}(i)\tau^{-1}(j)}\right) \tag{5.6}$$

Observons alors que la nouvelle matrice est obtenue en permutant les lignes de la première M suivant σ et les colonnes suivant τ en ce sens que la ligne i passe à la

ligne $\sigma(i)$ dont les coefficients sont permutés suivant τ ou l'inverse : la colonne j passe à la colonne $\tau(j)$ dont les coefficients sont permutés suivant σ. Nous pouvons aussi procéder aux permutations de la manière suivante : on prend successivement les vecteurs lignes $\sigma^{-1}(i)$ pour le placer aux lignes i, ensuite, dans la matrice *intermédiaire* obtenue, on déplace les vecteurs colonnes $\tau^{-1}(j)$ aux colonnes j.

EXEMPLE **5.6** Soit

$$M = \begin{pmatrix} 1 & 0 & 3 & 5 \\ 2 & 6 & 0 & 8 \\ 7 & 0 & 4 & 9 \end{pmatrix}$$

Donnons-nous les deux permutations

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

Alors, nous avons

$$(\sigma, \tau) * M = \begin{pmatrix} a_{23} & a_{21} & a_{22} & a_{24} \\ a_{13} & a_{11} & a_{12} & a_{14} \\ a_{33} & a_{31} & a_{32} & a_{34} \end{pmatrix} = \begin{pmatrix} 0 & 2 & 6 & 8 \\ 3 & 1 & 0 & 5 \\ 4 & 7 & 0 & 9 \end{pmatrix}$$

○

Si Id est la permutation identité, i.e. $\mathrm{Id}(i) = i$, remarquons que

$$(\mathrm{Id}, \mathrm{Id}) * M = M$$

Et de plus, nous avons

$$(\sigma_1 \circ \sigma_2, \tau_1 \circ \tau_2) * M = (\sigma_1, \tau_1) * ((\sigma_2, \tau_2) * M))$$

5.2 Produit et transposition

Comment peut-on multiplier les matrices ? Nous allons maintenant connaître algébriquement cette opération qui vient de la composition des applications comme nous le verrons plus bas. De plus, nous aborderons une autre opération utile, à savoir la transposition de matrice. Ce qui établit clairement les bases du *calcul matriciel*.

Soit $M = (a_{ij}) \in M_{p,n}(A)$ et $N = (b_{ij}) \in M_{n,q}(A)$. On appelle **produit de** M **et** N, et on note $M \cdot N = MN$, la matrice $(c_{ij}) \in M_{p,q}(A)$ telle que

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \tag{5.7}$$

Remarquons que le produit MN n'est défini dans cet ordre que si le nombre de colonnes de la matrice à gauche est égal à celui du nombre de lignes de la matrice à droite. L'élément c_{ij} est ainsi obtenu en sommant les produits des coefficients ordonnés de la ligne $L_i(M)$ et de la colonne $C_j(N)$, lesquels sont au même nombre.

EXEMPLE **5.7** Soit

$$M = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \quad N = \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}$$

Alors,

$$MN = \begin{pmatrix} 1+\lambda\mu & \lambda \\ \mu & 1 \end{pmatrix} \quad NM = \begin{pmatrix} \mu & 1+\lambda\mu \\ 0 & 1 \end{pmatrix}$$

○

Nous avons les propriétés suivantes.

Théorème 5.8 *Le produit des matrices possède les propriétés suivantes. Soit* $m, n, p, q \in \mathbb{N}^*$ *fixés* :

(*i*) *Pour toutes* $M_1, M_2 \in M_{p,n}(A)$ *et toutes* $N_1, N_2 \in M_{n,q}(A)$, *on a*

$$\begin{aligned} (M_1 + M_2)N_1 &= M_1N_1 + M_2N_2 \\ M_1(N_1 + N_2) &= M_1N_1 + M_1N_2 \end{aligned} \tag{5.8}$$

(*ii*) *Pour toutes* $M \in M_{p,n}(A), N \in M_{n,q}(A), P \in M_{q,m}(A)$, *on a*

$$(MN)P = M(NP) \tag{5.9}$$

(*iii*) *Si* $A = K$, K *étant un corps, alors pour tout* $\lambda \in K$ *et toutes* $M \in M_{p,n}(K), N \in M_{n,q}(K)$, *on a*

$$\lambda(MN) = (\lambda M)N = M(\lambda N) \tag{5.10}$$

Remarque 5.9 *Le produit des matrices n'est clairement pas commutatif même pour les matrices carrées* (*Exemple 5.7*).

Intéressons-nous maintenant à une deuxième opération importante sur les matrices. Soit $M = (a_{ij}) \in M_{p,n}(A)$, on appelle **transposée** de M, la matrice dans $M_{n,p}(A)$, notée par ${}^tM$ telle que son coefficient à la position (i, j) est défini par

$${}^ta_{ij} = a_{ji} \tag{5.11}$$

La matrice ${}^tM$ s'obtient de M par échange des lignes et des colonnes, i.e. la i-ème ligne de ${}^tM$ est simplement la i-ème colonne de M, et la j-ème colonne de ${}^tM$ est la j-ème ligne de M.

À partir de la définition de la transposition des matrices, il vient que

Théorème 5.10 *L'application de transposition des matrice de $M_{p,n}(A)$ à $M_{n,p}(A)$ est bijective et l'on a*

$$^t(M+N) = {}^tM + {}^tN \tag{5.12}$$

et de plus, si A est commutatif,

$$^t(MN) = {}^tN\,{}^tM \tag{5.13}$$

5.3 Matrices carrées

Dans la suite, A désignera un anneau unitaire commutatif non nul et K un corps commutatif.

Soit $M = (a_{ij}) \in M_n(A)$. On dit que M est **triangulaire supérieure** (resp. **inférieure**) ssi $a_{ij} = 0$ pour $i > j$ (resp. pour $i < j$). On dit que M est **unipotente supérieure** (resp. **inférieure**) ssi $a_{ij} = 0$ pour $i > j$ (resp. pour $i < j$) et $a_{ii} = 1$. On dit que M est **diagonale** ssi $a_{ij} = 0$ pour $i \neq j$.

On note $T_n^+(A), T_n^-(A), U_n^+(A), U_n^-(A)$ et $D_n(A)$, l'ensemble des matrices triangulaires (trigonales) supérieures et inférieures, unipotentes supérieures et inférieures, et diagonales, respectivement. Une matrice diagonale (a_{ij}) est uniquement déterminée par ses coefficients diagonaux (a_{ii}), aussi on la note simplement $D(a_i)$. Notons qu'une matrice scalaire est une matrice diagonale, toutefois, quand $n \geq 2$, il est clair qu'il y a plus de matrices diagonales que de matrices scalaires.

Remarquons que les présentes définitions donnent

$$T_n^+(A) \cap T_n^-(A) = D_n(A)$$

et aussi

$$U_n^+(A) \cap T_n^-(A) = U_n^-(A) \cap T_n^+(A) = \{I_n\}$$

Théorème 5.11 *L'ensemble $M_n(A)$ muni des opérations d'addition et de produit de matrices est un anneau non nul unitaire dont l'élément unité est la matrice diagonale $I_n \coloneqq (\delta_{ij})$. De plus, le K-e.v. $M_n(K)$ est de dimension n^2, et la famille des matrices élémentaires $\{E^{ij}\}$ constitue une de ses bases.*

Remarque 5.12 *Les matrices de la forme aI_n, avec $a \in A$, sont dites **scalaires** : elles forment un sous-anneau de $M_n(A)$ isomorphe à A par l'application $a \longmapsto aI_n$. L'anneau $M_n(A)$ n'est généralement par commutatif (cf. Exemple 5.7). Cependant, les matrices scalaires sont permutables avec toute matrice.*

Les matrice inversibles de $M_n(A)$ forment un groupe que l'on note $G_n(A)$. Notons que si $a \in A$ est inversible, alors $aI_n \in G_n(A)$. De plus, par (5.13), on a que

${}^tM \in G_n(A)$ si $M \in G_n(A)$, et dans ce cas :

$$({}^tM)^{-1} = {}^t(M^{-1}) \tag{5.14}$$

D'où, si M et N sont inversibles, on a

$$({}^t(MN))^{-1} = ({}^tN{}^tM)^{-1} = ({}^tM)^{-1}({}^tN)^{-1} = {}^t(M^{-1}){}^t(N^{-1}) \tag{5.15}$$

La transposition des matrices entraîne géométriquement une nouvelle notion pour les matrices carrées ; on appelle $M = (a_{ij}) \in M_n(A)$ une **matrice symétrique** ssi $a_{ij} = a_{ji}$ pour tout (i, j). Ceci équivaut à ce que ${}^tM = M$. Par contre, M est dite **antisymétrique** ssi $a_{ij} = -a_{ji}$, i.e. ${}^tM = -M$.

L'ensemble des matrices symétriques (resp. antisymétriques) est notée par $S_n(A) = S_n$ (resp. $A_n(A) = A_n$). Ceux-ci forme clairement des sous-groupes additifs de A. De plus, $S_n(A)$ et $A_n(A)$ sont des e.v. si $A = K$.

Notons que $M \in S_n$ ssi

$$M = \sum_{i=1}^{n} a_{ii}E^{ii} + \sum_{i<j} a_{ij}(E^{ij} + E^{ji}) \tag{5.16}$$

Ainsi, la famille $\{E^{ii}\} \cup \{E^{ij} + E^{ji}, i < j\}$ forme une base de S_n. Et on a

$$\dim(S_n) = \frac{n(n+1)}{2}$$

En effet, le nombre des E^{ii} est de n, et le nombre des $E^{ij} + E^{ji}$, quand $i < j$, est clairement de $1 + \cdots + (n-1)$, ce qui donne

$$\dim(S_n) = 1 + \cdots + n = \frac{n(n+1)}{2}$$

D'autre par, si 2 est régulier dans A, alors $a_{ii} = 0$, d'où, il vient que

$$M \in A_n \Longleftrightarrow M = \sum_{i<j} a_{ij}(E^{ij} - E^{ji})$$

Dans ce cas, nous voyons que A_n est généré par $\{E^{ij} - E^{ji}, i < j\}$, d'où

$$\dim(A_n) = 1 + \cdots + (n-1) = \frac{(n-1)n}{2}$$

Considérons maintenant les matrices diagonales dans $M_n(A)$. Soit $M = D(a_i)$ et $N = D(b_i)$ dans M_n. Alors, par définition, nous avons

$$M + N = D(a_i + b_i), \quad MN = D(a_ib_i)$$

Ce qui entraîne clairement que

Proposition 5.13 *L'ensemble $D_n(A)$ est un sous-anneau de $M_n(A)$ et isomorphe à l'anneau A^n.*

Par ailleurs, au vu de l'expression du produit de deux matrices diagonales, nous voyons qu'une telle matrice est inversible ssi tous les éléments diagonaux sont inversibles dans A. En particulier, si $A = K$, un corps commutatif, alors $D(a_i) \in G_n(A)$ ssi $\forall i : a_i \neq 0$.

Quant aux matrices trigonales, le théorème suivant réunit leurs principales propriétés.

Théorème 5.14 *Dans $M_n(A)$, on a*

(i) $T_n^+(A)$ est un sous-anneau de $M_n(A)$.

(ii) Soit $M \in T_n^+(A)$. Alors, $M \in G_n(A)$ ssi M est inversible dans $T_n^+(A)$ ssi les éléments diagonaux de M sont inversibles dans A.

(iii) Si $A = K$, alors $T_n^+(K)$ est K-s.e.v. de $M_n(K)$ tel que

$$\dim\left(T_n^+(A)\right) = \frac{n(n+1)}{2}$$

De plus, une matrice $M \in T_n^+(K)$ est inversible dans $T_n^+(K)$ ssi $M \in G_n(K)$ ssi les éléments diagonaux de M sont dans K^*.

Remarque 5.15 *Il est évident que ce théorème est aussi vrai pour $T_n^-(A)$.*

Nous avons une conséquence immédiate du Théorème 5.14 :

Corollaire 5.16 *$U_n^+(A)$ (resp. $U_n^-(A)$) est un sous-groupe du groupe des matrices inversibles de $T_n^+(A)$ (resp. de $T_n^-(A)$).*

Les derniers résultats montrent que les diagonaux d'une matrice jouent un rôle important. Pour mieux les connaître, on utilise la caractéristique suivante : on appelle **trace** d'une matrice $M = (a_{ij}) \in M_n(A)$, la valeur de A donnée par

$$\mathrm{Tr}\,(M) = \sum_{i=1}^{n} a_{ii} \tag{5.17}$$

Proposition 5.17 *Soir $M, N \in M_n(K)$. Alors, on a*

$$\mathrm{Tr}\,(MN) = \mathrm{Tr}\,(NM) \tag{5.18}$$

En particulier, pour une permutation $\sigma \in \mathcal{S}_p$, on a

$$\mathrm{Tr}\,(M_1 \cdots M_p) = \mathrm{Tr}\,(M_{\sigma(1)} \cdots M_{\sigma(p)}) \tag{5.19}$$

Il résulte de la Proposition 5.17 que

Corollaire 5.18 *Si $M \in M_n(K)$ et que $P \in G_n(K)$, alors*

$$\mathrm{Tr}\,(M) = \mathrm{Tr}\,(P^{-1}MP) \tag{5.20}$$

5.4 Applications linéaires

Dans cette section *centrale*, nous allons établir le lien entre les matrices et les applications linéaires, et du coupe connaître l'origine de la notion de matrice.

Matrice ≡ a.l.

Soit K un corps commutatif et considérons deux K-e.v. E et F non nuls et de dimensions finies respective n et p. Soit $B = (e_i)$ et $C = (f_i)$ des bases de E et de F, respectivement. Soit $f \in \mathrm{Hom}_K(E, F)$. On appelle **matrice de f dans les bases B et C**, la matrice $(a_{ij}) \in M_{p,n}(K)$ telle que

$$\forall j : f(e_j) = \sum_{i=1}^{p} a_{ij} f_i \tag{5.21}$$

autrement dit , a_{ij} est la i-ème coordonnée de $f(e_j)$ dans la base C. Ladite matrice se note $M_{B,C}(f)$. Si, en particulier, $E = F$ et $B = C$, alors on dit que M est la **matrice de f dans B** et on écrit $M_B(f)$. S'il n'y a pas de risque confusion avec les bases, on écrit $M_f = M(f)$.

Si $y = (y_i) = f(x) = f((x_i))$, où les x_i et y_i sont les coordonnées respectives d'un vecteur v relativement aux bases B et C, les conditions (5.21) s'écrivent sous forme d'un système d'équations linéaires simples

$$\begin{cases} y_1 = a_{11}x_1 + \cdots + a_{1n}x_n \\ \vdots \\ y_p = a_{p1}x_1 + \cdots + a_{pn}x_n \end{cases} \tag{5.22}$$

En notation matricielle, cela donne

$$\begin{pmatrix} y_1 \\ \vdots \\ y_p \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{p1} & \cdots & a_{pn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \tag{5.23}$$

Ce que l'on écrit généralement sous la forme

$$Y = AX \tag{5.24}$$

où X et Y sont respectivement les matrices uni-colonnes dont les termes respectifs sont $(x_1, \ldots, x_n)$ et $(y_1, \ldots, y_p)$, i.e. $X \in M_{n,1}(K), Y \in M_{p,1}(K)$ et on écrit

$$X = M_B(v), \quad Y = M_C(v) \tag{5.25}$$

EXEMPLE **5.19** (**Identité**) Soit E un K-e.v. de dimension n muni d'une base B, et considérons sur E l'application identité $\mathrm{Id}_E(x) = x$. Comme $\mathrm{Id}_E(e_j) = e_j$, alors on a

$$M_B(\mathrm{Id}_E) = I_n$$

○

EXEMPLE **5.20** (**Homothétie**) Soit E un K-e.v. muni de la base et B. Alors, pour tout $\lambda \in K$, la matrice de l'homothétie $\lambda\mathrm{Id}_E$ dans B est λI_n. Remarquons que cette dernière ne dépend pas de B. Ce phénomène est toutefois exceptionnel ; en général $M_{B,C}(f)$ dépend de B et de C, même si $B = C$. ○

EXEMPLE **5.21** (**Projection**) Considérons le plan géométrique $\mathbb{R}^2$ muni de sa base canonique $B = \{(1,0),(0,1)\} = \{e_1, e_2\}$. Considérons la projection suivante (cf. Exemple 4.3)

$$\begin{array}{rccc} \mathrm{Pr}_1 : & \mathbb{R}^2 & \to \mathbb{R}^2 \\ & (x,y) & \mapsto (x,0) \end{array}$$

Nous avons $\mathrm{Pr}_1(e_1) = 1$ et $\mathrm{Pr}_1(e_2) = 0$, d'où

$$M_{\mathrm{Pr}_1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

○

EXEMPLE **5.22** Considérons les $\mathbb{R}$-e.v. munis de leurs bases canonique respectives $\{e_1, e_2, e_3\}$ et $\{\epsilon_1, \epsilon_2\}$ et soit $\mathbb{R}^3$ et $\mathbb{R}^2$ Soit $f \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^3, \mathbb{R}^2)$ telle que $(x,y,z) \mapsto (x-y, z-y)$. Alors, on a facilement que

$$\begin{aligned} f(e_1) &= \epsilon_1 \\ f(e_2) &= -\epsilon_1 - \epsilon_2 \\ f(e_3) &= \epsilon_2 \end{aligned}$$

Donc,

$$M_f = \begin{pmatrix} 1 & -1 & 0 \\ 0 & -1 & 1 \end{pmatrix}$$

○

Le lien entre les matrices et les a.l. est donné dans le théorème fondamental suivant.

Théorème 5.23 ($f \equiv M_f$) *Soit E, F deux K-e.v. de dimensions finies n et p, respectivement. Soit B et C des bases respectives de E et de F. Alors, l'application $\Phi : \mathrm{Hom}_K(E,F) \to M_{p,n}(K)$ telle que $\Phi(f) = M_{B,C}(f)$ est un isomorphisme, et l'on a*

$$\dim\left(\mathrm{Hom}_K(E,F)\right) = np = \dim\left(M_{p,n}(K)\right) \tag{5.26}$$

Remarque 5.24 *Le présent théorème montre en particulier que les espaces $\mathrm{Hom}_K(E)$ sont isomorphes entre eux étant donné qu'ils sont isomorphes à $M_n(K)$. En outre, nous obtenons avec les résultat qui vont suivre qu'une application linéaire peut être regardée comme une matrice et vice versa. Ce qui peut faciliter l'étude des a.l.*

Quelle est la matrice associée à une composition d'a.l. :

Théorème 5.25 *Soit E, F et G trois K-e.v. munis des bases respectives $B = \{e_1, \ldots, e_n\}, C = \{f_1, \ldots, f_p\}$ et $D = \{g_1, \ldots, g_q\}$. Soit $f \in \mathrm{Hom}_K(E,F)$ et $g \in \mathrm{Hom}_K(F,G)$. Alors, on a*

$$M_{B,D}(g \circ f) = M_{B,C}(f) M_{C,D}(g) \tag{5.27}$$

Remarque 5.26 *Si $f_M : K^n \to K^p, f_N : K^p \to K^q$ sont les deux a.l. associées aux matrices $M \in M_{p,n}$ et $N \in M_{q,p}$, respectivement, alors la formule (5.25) s'écrit comme suit*

$$f_N \circ f_M = f_{NM} \tag{5.28}$$

Matrice de passage

Soit $B = \{e_1, \ldots, e_n\}$ une base d'un K-e.v. E et $V = \{v_1, \ldots, v_n\}$ une famille de vecteurs de E. En vertu du Théorème 4.14, nous savons qu'il existe un unique $f \in \mathrm{Hom}_K(E)$ telle que $f(e_i) = v_i$ pour tout i. La matrice $M_B(f) =: (a_{ij})$ s'appelle **matrice des colonnes f_i dans la base** B que l'on peut noter en fonction des v_i :

$$M_B(v_1, \ldots, v_n) = M_B(V)$$

C'est là l'unique matrice telle que

$$\forall j : v_j = \sum_{i=1}^{n} a_{ij} e_i \tag{5.29}$$

L'observation ci-dessus conduit à la définition suivante. Si B et C sont deux bases d'un K-e.v. de dimension finie, on appelle $M_B(C)$ la **matrice de passage** de B à C, ce que l'on note par $P_{B,C}$.

La matrice de passage possède quelques propriété fondamentales. En premier, nous avons

Proposition 5.27 *Soit B et C deux bases d'un K-e.v. E de dimension finie. Alors, on a que*

(i)

$$P_{B,C} = M_{C,B}(\mathrm{Id}_E)$$

(ii) $P_{B,C}$ est inversible et son inverse est donné par

$$P_{B,C}^{-1} = P_{C,B}$$

(iii) si D est une troisième base de E,

$$P_{B,D} = P_{B,C} P_{C,D}$$

La matrice de passage donne lieu à une formule célèbre qui permet dans un e.v. de passer d'une base à une autre.

Proposition 5.28 (Formule de changement de coordonnées) *Soit B et C deux bases d'un K-e.v. E de dimension n. Soit $v \in E$ tel que*

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = M_B(v) \quad Y = M_C(v) = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

Alors, en posant $P = P_{B,C}$, on a

$$X = PY \tag{5.30}$$

Changement de base

Nous avons appris dans la section précédente comment passer d'une base à une autre dans un e.v. Ici, l'objectif est de connaître l'expression de la matrice d'une a.l. dans des bases différentes.

Théorème 5.29 *Soit E et F deux K-e.v. de dimensions finies. Soit B, B' des bases de E, et C, C' des bases de F. Soit $f \in \mathrm{Hom}_K(E,F)$. Alors, si $M = M_{B,C}(f), M' = M_{B',C'}(f)$ et que $P = P_{B,B'}, Q = P_{C,C'}$, on a que*

$$M' = Q^{-1}MP \tag{5.31}$$

EXEMPLE **5.30** Un bel exemple de changement de bases constitue à permuter l'ordre des bases données. Soit B et C des bases respectives des K-e.v. E et F de dimensions n et p, respectivement. Soit $\sigma \in \mathcal{S}_n$ et $\tau \in \mathcal{S}_p$. Appelons $B' = \{e_{\sigma(i)}\}$ et $C' = \{f_{\tau(i)}\}$ les nouvelles bases de E et F obtenues respectivement par permutations des deux premières suivant σ et τ. Posons $P = P_{B,B'} = P_\sigma$ et $Q = P_{C,C'} = Q_\tau$. Clairement, nous avons $Q^{-1} = Q_{\tau^{-1}}$, d'où, si $f \in \mathrm{Hom}_K(E,F)$, on a

$$M' = Q_{\tau^{-1}} M P_\sigma$$

Ce qui donne avec les notations de (5.6)

$$M' = (\tau^{-1}, \sigma^{-1}) * M$$

Donc,

$$Q_{\tau^{-1}} M P_\sigma = (\tau^{-1}, \sigma^{-1}) * M$$

○

Corollaire 5.31 (Formule de changement de base) *Soit B et B' deux bases d'un K-e.v. E de dimension finie. Soit $f \in \mathrm{Hom}_K(E)$. Alors, si $M = M_B(f), M' = M_{B'}(f)$ et que $P = P_{B,B'}$, on a*

$$M' = P^{-1}MP \tag{5.32}$$

5.5 Rang d'une Matrice

Nous savons maintenant qu'une matrice et une a.l. sont deux faces d'un même objet mathématique. Cela conduit à poser une définition équivalente à celle du rang d'une a.l. pour les matrices.

Soit K un corps commutatif et considérons ici des e.v. non nuls et de dimension finie, spécialement K^n et K^p munis de leurs bases canoniques respectives. Soit $M = (a_{ij}) \in M_{p,n}(K)$. Considérons $f_M : K^n \to K^p$ l'a.l. associée définie par (5.21) ; la notation matricielle (5.23) exprime le rapport entre les deux objets *équivalents*.

On appelle **rang** de M et l'on note $\mathrm{rg}\,(M)$, le rang de f_M, i.e.

$$\mathrm{rg}\,(M) = \mathrm{rg}\,(f_M) = \dim\left(\mathrm{Im}\,(f_M)\right) \tag{5.33}$$

Soit $(e_1, \ldots, e_n)$ la base canonique de K^n. Nous avons pour chaque $j = 1, \ldots, n$,

$$f_M(e_j) = C_j(M) \tag{5.34}$$

De ce fait, le rang de M n'est autre que le rang des vecteurs colonnes de M, i.e.

$$\mathrm{rg}\,(M) = \mathrm{rg}\,(\{C_j(M)\}) \tag{5.35}$$

En même temps, comme la décomposition des vecteurs $f_M(e_j)$ est unique dans K^p muni de sa base canonique, il y a une **correspondance bijective** entre $M_{p,n}(K)$ et $\mathrm{Hom}_K(K^n, K^p)$, le fait que nous avons déjà observé dans le Théorème 5.23.

Notons que $\mathrm{rg}\,(0) = 0$, de plus, $\mathrm{rg}\,(M)$ ne peut être supérieur aux dimensions de l'espace de départ et d'arrivé, d'où

$$\mathrm{rg}\,(M) \leq \min\{n, p\} \tag{5.36}$$

Cependant, le rang d'une matrice est indépendant de la base choisie :

Proposition 5.32 *Le rang d'une matrice $M \in M_{p,n}(K)$ est constant.*

Si nous considérons maintenant une matrice carrée $M \in M_n(K)$, nous savons (cf. (5.35)) que

$$\mathrm{rg}(M) = n \Longleftrightarrow \langle\{C_j(M)\}\rangle = K^n$$

Ce qui, par le Théorème 4.23, est équivalent à l'inversibilité de f_M, l'a.l. associée relativement à la base canonique. Donc, il vient que

Proposition 5.33 *Soit $M \in M_n(K)$. Alors, on a*

$$\mathrm{rg}(M) = n \Longleftrightarrow \mathrm{rg}({}^tM) = n \tag{5.37}$$

6 Déterminants*

En cours de préparation ...

Références

[1] J. M. Arnaudies, H. Fraysse. (1988). *Cours de mathématiques-1*, edition Dunod.

[2] O. Boukhadra. (2020). *Introduction à l'Algèbre*. En cours de préparation.

[3] J. Grifone. (2011). *Algèbre linéaire*, 4ème édition, Cépaduès-Édition.

[4] M. Queysanne. (1984). *Algèbre*, office des publications universitaires.