CHAPITRE 1

Préliminaires algébriques

Sommaire

Ce chapitre contient peu de démonstrations, son rôle est de fixer les notations et de rappeler les structures algébriques fondamentales, ainsi que les principaux résultats algébriques que nous utiliserons dans ce cours. Nous renvoyons le lecteur au cours de première année pour tout approfondissement.

§ 1 Ensembles et applications

1.1.1. Applications.— Soient A et B deux ensembles. Une *application* f de A dans B est un procédé qui à tout élement x de A associe un élément unique de B, noté $f(x)$. On note $f : A \longrightarrow B$, ou $A \xrightarrow{f} B$, ou encore

$$\begin{aligned} f : A &\longrightarrow B \\ x &\longrightarrow f(x). \end{aligned}$$

On note $f(A)$ l'*image* de l'ensemble A, définie par

$$f(A) = \{y \mid y \in B,\ \exists\, x \in A,\ \text{tel que } y = f(x)\}.$$

L'*image inverse* d'un sous-ensemble $Y \subset B$ est définie par

$$f^{-1}(Y) = \{x \mid x \in A,\ f(x) \in Y\}.$$

Une application $f : A \longrightarrow B$ est dite *injective* si, $f(x) = f(y)$ implique $x = y$. Elle est dite *surjective* si $f(A) = B$, *i.e.*, pour tout $y \in B$, il existe un élément $x \in A$ tel que $y = f(x)$. Une application est dite *bijective* si elle est à la fois injective et surjective.

Si $f : A \longrightarrow B$ et $g : B \longrightarrow C$ sont deux applications, on note $g \circ f$, ou encore gf, l'application, dite *composée*, définie par

$$\begin{aligned} g \circ f : A &\longrightarrow C \\ x &\longrightarrow g(f(x)). \end{aligned}$$

La composée des applications est une opération associative, *i.e.*, étant données trois applications $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$, on a

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

1.1.2. Quelques ensembles fondamentaux de nombres. — Dans tout ce cours, nous supposons connus les ensembles de nombres suivants et les opérations d'addition, de soustraction, de multiplication et de division sur ces ensembles.

- L'ensemble des *entiers naturels*, $0, 1, 2, \ldots$, noté $\mathbb{N}$.
- L'ensemble des *entiers relatifs*, noté $\mathbb{Z}$, formé des entiers naturels et de leurs opposés. Si p et q sont deux entiers relatifs, on notera

$$[\![p, q]\!] = \{a \in \mathbb{Z} \mid p \leq a \leq q\}.$$

- L'ensemble des *nombres rationnels*, noté $\mathbb{Q}$, formé des quotients $\dfrac{p}{q}$, où p et q sont des entiers relatifs, avec q non nul.
- L'ensemble des *nombres réels*, noté $\mathbb{R}$, qui contient les nombres rationnels et les nombres irrationnels.
- L'ensemble des *nombres complexes*, noté $\mathbb{C}$, formé des nombres $a+ib$, où a et b sont des réels et i un complexe vérifiant $i^2 = -1$.

§ 2 Les corps

Un *corps* est un objet algébrique constitué d'un ensemble et de deux opérations sur cet ensemble, une addition et une multiplication, qui satisfont à certaines relations. Intuitivement, cette structure est proche de notre intuition de nombres et des opérations que l'on peut leur appliquer. Avant d'énoncer les relations des deux opérations de la structure de corps, rappelons la structure de groupe.

1.2.1. Les groupes. — Un *groupe* est un ensemble G muni d'une opération $\star$, associant à deux éléments a et b de G un troisième élément de G, noté $a \star b$, satisfaisant les assertions suivantes

i) l'opération est *associative*, *i.e.*, pour tous éléments a, b et c de G,

$$a \star (b \star c) = (a \star b) \star c,$$

ii) il existe un élément e dans G, appelé *neutre*, tel que, pour tout élément a de G,

$$a \star e = e \star a = a,$$

iii) pour tout élément a de G, il existe un élément *inverse*, que nous noterons a^{-1}, tel que

$$a \star a^{-1} = e = a^{-1} \star a.$$

1.2.2 Exercice.— On définit sur l'ensemble des nombres réels l'opération $\star$ en posant

$$a \star b = 2a + 2b.$$

1. Cette opération est-elle associative ?
2. L'opération suivante est-elle associative

$$a \star b = 2a + b?$$

1.2.3 Exercice.—

1. Montrer qu'un groupe possède un unique élément neutre.
2. Montrer que dans un groupe, l'inverse d'un élément est unique.

1.2.4. Exemples.—

1) Le groupe *trivial* est le groupe à un seul élément, l'élément neutre.

2) L'ensemble des entiers $\mathbb{Z}$ forme un groupe pour l'addition usuelle. Il ne forme pas un groupe pour la multiplication.

3) L'ensemble des nombres rationnels $\mathbb{Q}$ forme un groupe pour l'addition. L'ensemble $\mathbb{Q} - \{0\}$ des nombres rationnels non nul est un groupe pour la multiplication.

4) L'ensemble des complexes non nuls $\mathbb{C} - \{0\}$, muni de la multiplication usuelle des complexes.

5) L'ensemble $\mathbb{R}^n$ des n-uplets ordonnées $(x_1, \ldots, x_n)$ de nombres réels, muni de l'opération

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

forme un groupe.

1.2.5 Exercice.— Justifier toutes les propriétés précédentes. Dans le cas de $\mathbb{R}^n$, déterminer l'élément neutre du groupe et l'inverse d'un n-uplet $(x_1, \ldots, x_n)$.

1.2.6. Les groupes abéliens.— Un groupe est dit *abélien*, ou *commutatif*, si tous éléments a et b vérifient

$$a \star b = b \star a.$$

Les groupes des exemples 1.2.4 sont abéliens.

1.2.7 Exercice.— Les opérations de l'exercice 1.2.2 sont-elles commutatives ?

1.2.8 Exercice.— Soit X un ensemble.

1. Montrer que l'ensemble des permutations de X, *i.e.*, des bijections de X dans lui-même, forment un groupe.
2. Montrer que ce groupe n'est pas commutatif lorsque X possède au moins trois éléments.

1.2.9. Les corps.— Un *corps* (commutatif) est un ensemble $\mathbb{K}$ sur lequel une opération d'addition $(a, b) \to a + b$ et une opération de multiplication $(a, b) \to ab$ sont définies et satisfont aux assertions suivantes :

i) $\mathbb{K}$ est un groupe abélien pour l'addition,

ii) $\mathbb{K} - \{0\}$ est un groupe abélien pour la multiplication,

iii) la multiplication est distributive par rapport à l'addition, *i.e.*, pour tous éléments a, b et c, on a

$$a(b + c) = ab + ac.$$

L'élément neutre pour l'addition, appelé *zero*, est noté 0, l'inverse de a est appelé l'*opposé* de a et noté $-a$, l'élement neutre pour la multiplication est appelé *unité* et noté 1, l'*inverse* de a pour la multiplication est noté a^{-1}.

1.2.10. Exemples.—

1) L'ensemble des nombres rationnels $\mathbb{Q}$, l'ensemble des nombres réels $\mathbb{R}$ et l'ensemble des nombres complexes $\mathbb{C}$, munis des opérations d'addition et de multiplication usuelles sont des corps.

2) L'ensemble $\mathbb{Z}$ des entiers relatifs n'est pas un corps.

3) Un exemple de corps fini, *i.e.*, avec un nombre fini d'éléments, est donné par l'ensemble, noté $\mathbb{Z}/p\mathbb{Z}$, des entiers modulo un entier premier p, muni des opérations d'addition et de multiplication induites de celles de $\mathbb{Z}$.

1.2.11 Exercice.— Montrer que $\mathbb{Z}/4\mathbb{Z}$ n'est pas un corps.

1.2.12 Exercice.— Montrer que dans un corps, l'élément neutre de l'addition joue le rôle d'*annulateur*, *i.e.*, pour tout élément a, on a :

$$a0 = 0.$$

Par définition, un groupe ne peut être vide, il contient au moins un élément. Un corps contient donc au moins deux éléments 0 et 1 qui sont nécessairement distincts.

1.2.13 Exercice.— Montrer qu'un corps ne contient pas de diviseur de zero, c'est-à-dire que si a et b sont deux éléments non nul d'un corps $\mathbb{K}$, alors leur produit ab est non nul.

Il n'existe qu'un seul corps à deux éléments.

1.2.14 Exercice.— Établir les tables d'addition et de multiplication du corps à deux éléments.

1.2.15. Extension de corps.— Un sous-ensemble $\mathbb{L}$ d'un corps $\mathbb{K}$ est un *sous-corps* de $\mathbb{K}$ si les opérations du corps $\mathbb{K}$ munissent $\mathbb{L}$ d'une structure de corps. On dit alors que $\mathbb{K}$ est une *extension* du corps $\mathbb{L}$. Par exemple, le corps des réels $\mathbb{R}$ est une extension du corps des rationnels $\mathbb{Q}$ et le corps des complexes $\mathbb{C}$ est une extension du corps $\mathbb{R}$.

§ 3 Les anneaux

La structure d'anneau généralise celle de corps. Un ensemble muni d'une opération d'addition et d'une opération de multiplication qui satisfont à tous les axiomes de corps, excepté l'existence d'un élément inverse a^{-1}, pour tout élément a non nul, est appelé un *anneau commutatif*. Pour que notre définition soit complète, on convient, qu'il existe un anneau qui possède un seul élément.

Par exemple, l'ensemble des entiers relatifs $\mathbb{Z}$, muni de l'addition et de la multiplication, n'est pas un corps - les éléments non nuls ne sont pas tous inversibles - mais il forme un anneau commutatif. Nous verrons que l'ensemble $A[x]$ des polynômes à une indéterminée à coefficients dans un anneau ou un corps A forme un anneau ; les principales constructions sur les anneaux de polynômes sont rappelées dans la section suivante.

1.3.1. Les anneaux. — Un *anneau* est un ensemble A muni d'une opération d'*addition* $(a, b) \to a + b$ et d'une opération de *multiplication* $(a, b) \to ab$ qui satisfont aux assertions suivantes

i) A est un groupe abélien pour l'addition,

ii) la multiplication est associative, *i.e.*, pour tous éléments a, b et c de A,

$$(ab)c = a(bc).$$

iii) la multiplication possède un élément neutre dans A, appelé *unité* et noté 1, vérifiant pour tout élément a de A,

$$1a = a1 = a.$$

iv) la multiplication est *distributive* par rapport à l'addition, *i.e.*, pour tous éléments a, b, c de A, on a :

$$a(b + c) = ab + ac, \qquad (b + c)a = ba + ca.$$

Un anneau est dit *commutatif* si sa multiplication est commutative.

1.3.2 Exercice. — Montrer que dans un anneau A, on a, pour tous éléments a et b,

1. $0a = a0 = 0$,
2. $(-1)a = -a$,
3. $-(ab) = (-a)b = a(-b)$,
4. $(-a)(-b) = ab$.

1.3.3. Exemples. —

1) L'ensemble des entiers relatifs $\mathbb{Z}$, muni de l'addition et de la multiplication usuelles, forme un anneau commutatif.

2) Un corps (commutatif) est un anneau $\mathbb{K}$ non réduit à $\{0\}$, tel que la multiplication muni $\mathbb{K} - \{0\}$ d'une structure de groupe abélien.

3) Si $1 = 0$ dans un anneau A, alors A est réduit à $\{0\}$, car pour tout élément a de A, $a = 1a = 0a = 0$.

FIGURE 1.1 – Emmy Noether (1882 - 1935)

La notion d'anneau a été introduite à la fin du XIX^{e} *siècle pour étudier les équations algébriques et les nombres algébriques. L'étude de cette structure a été initiée par les mathématiciens allemands Dedekind, Hilbert et Fraenkel. Emmy Noether développera ensuite la théorie des idéaux dans un anneau et introduira la notion d'anneau noethérien.*

1.3.4. Endomorphismes d'un groupe abélien.— Rappelons qu'un *endomorphisme* d'un groupe $(G, \star)$ est un morphisme de groupes de G dans lui-même, c'est-à-dire, une application $f : G \longrightarrow G$ vérifiant, pour tous $a, b \in G$,

$$f(a \star b) = f(a) \star f(b).$$

L'ensemble des endomorphismes d'un groupe abélien $(G, +)$, muni de l'addition induite de celle sur G et de la composition, est un anneau non commutatif en général.

1.3.5. Formule du binôme.— Dans un anneau, si deux éléments a et b commutent, *i.e.*, $ab = ba$, alors on a la formule dite du *binôme de Newton*, pour tout entier naturel n,

$$(a+b)^n = \sum_{p=0}^{n} \binom{n}{p} a^p b^{n-p}.$$

1.3.6 Exercice.— Démontrer la formule du binôme de Newton.

1.3.7. Caractéristique d'un anneau commutatif.— Soit A un anneau commutatif. La *caractéristique* de A est le plus petit entier naturel non nul q, tel que l'addition de q fois l'unité soit égale à zero :

$$q.1 = \underbrace{1 + 1 + \ldots + 1}_{q \text{ fois}} = 0.$$

Si un tel entier n'existe pas, on dit que l'anneau est de caractéristique nulle.

1.3.8 Exercice. —

1. Montrer qu'un anneau commutatif fini est de caractéristique non nulle.
2. Montrer que la caractéristique d'un corps fini est un nombre premier.

1.3.9 Exercice. — Construire un corps de caractéristique 3.

1.3.10 Exercice. — Montrer que dans un anneau commutatif de caractéristique un nombre premier p, alors, pour tous éléments a et b de A, on a

$$(a + b)^p = a^p + b^p.$$

1.3.11. Division euclidienne dans l'anneau $\mathbb{Z}$. — La *division euclidienne* est un résultat fondamental de l'arithmétique élémentaire sur les entiers ou les polynômes. Avant d'identifier les anneaux dans lesquels, un tel algorithme est disponible, rappelons la division euclidienne sur les entiers.

1.3.12 Théorème (division euclidienne). — Soient $a, b \in \mathbb{Z}$, avec $b > 0$. Il existe un couple unique (q, r) d'entiers dans $\mathbb{Z}$ tel que :

$$a = bq + r, \quad \text{avec } \ 0 \leq r < b.$$

L'entier q est appelé le *quotient* de la division euclidenne de a par b et l'entier r est appelé le *reste* de la division euclidenne de a par b.

Preuve. Montrons dans un premier temps l'unicité du couple. Supposons que (q, r) et (q', r') soient deux couples vérifiant la condition, alors

$$a = bq + r = bq' + r'.$$

D'où $r' - r = b(q - q')$, par suite b divise $r' - r$. Comme, par hypothèse, $0 \leq r < b$ et $0 \leq r' < b$, on a

$$b|q - q'| = |r' - r| < b.$$

Par suite, $|q - q'| = 0$, d'où $q = q'$ et $r = r'$.

Montrons l'existence du couple. Considérons l'ensemble $A = \{k \in \mathbb{Z} \mid bk \leq a\}$. C'est une partie non vide et majorée de $\mathbb{Z}$. En effet, si $a \geq 0$, alors $0 \in A$, d'où A est non vide, et comme $1 \leq b$, l'entier a majore A. Si $a < 0$, alors $a \in A$, d'où A est non vide et 0 majore A. Par suite, l'ensemble A admet un plus grand élément q. On a

$$bq \leq a < b(q + 1).$$

En posant $r = a - bq$, on a $0 \leq r < b$. $\square$

De l'unicité du quotient et du reste de la division eulcidienne, on déduit qu'un entier b divise un entier a si, et seulement si, le reste de division euclidienne de a par b est nul.

1.3.13 Exercice.— Soit n un entier naturel. Calculer la division euclidienne de

1. l'entier $n^3 + n^2 + 2n + 1$ par $n + 1$,
2. l'entier $n^4 + 4n^3 + 6n^2$ par $n^2 + 2$.

FIGURE 1.2 – Euclide de Samos (325 - 265 av. J.-C.)

Euclide est un mathématicien de la Grèce antique né vers 325 av. J.C. et mort vers 265 av. J.C.. Nous n'avons que très peu d'information sur la vie d'Euclide. L'article de Fabio Acerbi du site Image des mathématiques [1] *présente ce que nous savons à ce jour sur le personnage d'Euclide. Euclide est l'auteur des* Éléments *qui est un texte fondateur de la géométrie.*

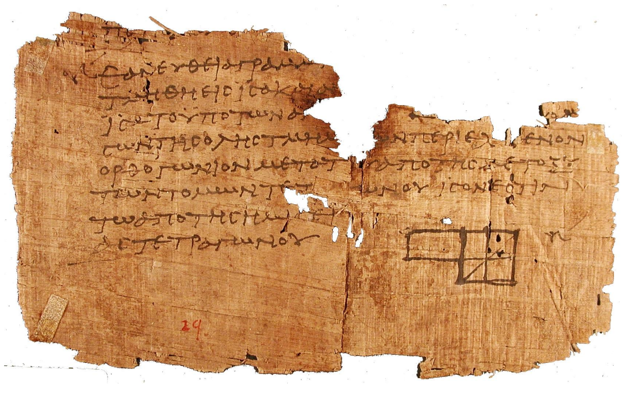


FIGURE 1.3 – Un fragment des éléments d'Euclide, papyrus daté d'entre 75 et 125 de notre ère.

1.3.14. Les anneaux euclidiens.— Soit A un anneau commutatif. On appelle *algorithme euclidien* sur A toute application

$$\varphi : A - \{0\} \longrightarrow \mathbb{N},$$

telle que, pour tout $a \in A$ et tout $b \in A - \{0\}$, il existe $q \in A$ et $r \in A$, tels que

$$a = bq + r, \quad \text{avec } \varphi(r) < \varphi(b) \text{ ou } r = 0.$$

1. Fabio Acerbi, « Euclide » - Images des Mathématiques, CNRS, 2010. En ligne, URL : `http://images.math.cnrs.fr/Euclide.html`

Un anneau commutatif A est dit *euclidien*, s'il vérifie les deux propriétés suivantes

i) A est *intègre*, *i.e.*, pour tous éléments a et b de A,

$$ab = 0 \Rightarrow (\ a = 0 \ \text{ ou } \ b = 0\ ).$$

ii) il existe sur A un algorithme euclidien.

1.3.15. Exemple.— L'anneau $\mathbb{Z}$ est euclidien. Il est en effet intègre et l'application valeur absolue $|\ | : \mathbb{Z}-\{0\} \longrightarrow \mathbb{N}$ est un algorithme euclidien, car, pour tout $a \in \mathbb{Z}$ et tout $b \in \mathbb{Z}-\{0\}$, il existe $q, r \in \mathbb{Z}$ tels que

$$a = bq + r, \quad \text{avec } |r| < |b| \ \text{ ou } \ r = 0.$$

Attention, le couple (q, r) n'est pas ici unique, par exemple, on a

$$5 = (-3)(-2) + (-1) \text{ avec } |-1| < |-3|,$$

et

$$5 = (-3)(-1) + 2 \text{ avec } |2| < |-3|.$$

Dans la suite, nous montrerons que si $\mathbb{K}$ est un corps, l'anneau $\mathbb{K}[x]$ est euclidien.

1.3.16 Exercice.— Montrer que l'anneau $\mathbb{D}$ des nombres décimaux, *i.e.*, le sous-anneau de $\mathbb{Q}$, engendré par $1/10$, est euclidien.

§ 4 Les polynômes à une indéterminée

1.4.1. Polynômes sur un corps.— Avant d'aborder la notion de polynôme, rappelons qu'il est important de distinguer les polynômes des fonctions polynomiales. En effet, considérons le polynôme $f = x^2 - x$ à coefficients dans le corps $\mathbb{Z}/2\mathbb{Z}$. La fonction polynomiale associée $\widetilde{f} : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$, définie par

$$\widetilde{f}(a) = a^2 - a, \quad \text{pour tout } a \in \mathbb{Z}/2\mathbb{Z},$$

est nulle, car $\widetilde{f}(0) = 0$ et $\widetilde{f}(1) = 0$, alors que le polynôme f n'est pas nul.

1.4.2 Exercice.— Montrer qu'il n'existe que quatre fonctions polynomiales à coefficients dans le corps $\mathbb{Z}/2\mathbb{Z}$ et une infinité de polynômes à coefficients dans ce corps.

La situation est différente pour les polynômes à coefficients dans les corps infinis, dans ce cas, il existe une correspondance biunivoque entre les polynômes et les fonctions polynomiales, cf. section 1.4.6.

1.4.3. Les polynômes.— Soit $\mathbb{K}$ un corps. On appelle *polynôme* à coefficients dans $\mathbb{K}$, toute suite $f = (a_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}$, nulle à partir d'un certain rang. On note $\mathbb{K}^{(\mathbb{N})}$ l'ensemble de ces suites.

On définit sur l'ensemble $\mathbb{K}^{(\mathbb{N})}$ une addition et un produit externe par un scalaire en posant, pour tous $f = (a_n)_{n\in\mathbb{N}}$, $g = (b_n)_{n\in\mathbb{N}}$ et $\lambda \in \mathbb{K}$,

$$f + g = (a_n + b_n)_{n\in\mathbb{N}}, \qquad \lambda f = (\lambda a_n)_{n\in\mathbb{N}}.$$

En outre, on définit une multiplication en posant, pour tous $f = (a_n)_{n\in\mathbb{N}}$, $g = (b_n)_{n\in\mathbb{N}}$,

$$fg = (c_n)_{n\in\mathbb{N}}, \qquad \text{avec} \qquad c_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

1.4.4. L'algèbre des polynômes. — Ces trois opérations munissent l'ensemble $\mathbb{K}^{(\mathbb{N})}$ d'une structure de $\mathbb{K}$-*algèbre* associative, commutative et unitaire, c'est-à-dire,

i) $\mathbb{K}^{(\mathbb{N})}$ muni de l'addition et du produit par un scalaire est un $\mathbb{K}$-espace vectoriel,

ii) $\mathbb{K}^{(\mathbb{N})}$ muni de l'addition et de la multiplication est un anneau commutatif,

iii) pour tous $f, g \in \mathbb{K}^{(\mathbb{N})}$ et tous scalaires $\lambda, \mu \in \mathbb{K}$, on a

$$(\lambda f)(\mu g) = (\lambda\mu)(fg).$$

1.4.5. Notion d'indéterminée. — L'écriture des polynômes sous forme de suite est peu manipulable, aussi, on préfère la notation basée sur la notion d'*indéterminée*. Notons x le polynôme de $\mathbb{K}^{(\mathbb{N})}$ dont tous les termes sont nuls, sauf celui de degré 1 :

$$x = (0, 1, 0, \ldots).$$

Par convention, on pose $x^0 = 1$. On définit les puissances de x par récurrence, pour tout entier k, $x^{k+1} = x\,x^k$. Ainsi, si $f = (a_n)_{n\in\mathbb{N}}$, on montre que

$$f = \sum_{i=0}^{+\infty} a_i x^i.$$

Les scalaires a_i sont appelés les *coefficients* du polynôme f. On montre que deux polynômes sont égaux si, et seulement si, ils ont les mêmes coefficients :

$$\sum_{k=0}^{+\infty} a_k x^k = \sum_{k=0}^{+\infty} b_k x^k \quad \text{si, et seulement si,} \quad a_k = b_k, \ \text{pour tout } k \in \mathbb{N}.$$

On notera alors $\mathbb{K}[x]$ l'ensemble des *polynômes à une indéterminée* à coefficients dans le corps $\mathbb{K}$. Avec ces notations, l'addition des polynômes est définie de la façon suivante, pour $f = \sum_{i=0}^{m} a_i x^i$ et $g = \sum_{j=0}^{n} b_j x^j$, alors

$$f + g = \sum_{k=0}^{\max\{m,n\}} (a_k + b_k) x^k,$$

avec $a_k = 0$, pour $k > m$ et $b_k = 0$ pour $k > n$. Par ailleurs, pour la multiplication, on a

$$fg = \sum_{k=0}^{m+n} \left(\sum_{\substack{i,j\geq 0\\ i+j=k}} (a_i b_j) \right) x^k$$

1.4.6. Fonction polynomiale. — Étant donné un polynôme $f = \sum_{i=0}^{n} a_i x^i$ de $\mathbb{K}[x]$, on définit la *fonction polynomiale* associée comme l'application

$$\widetilde{f} : \mathbb{K} \longrightarrow \mathbb{K},$$

qui, à tout $a \in \mathbb{K}$, associe le scalaire $f(a) \in \mathbb{K}$, obtenu en remplaçant dans l'expression de f l'indéterminée x par a.

Nous avons vu en 1.4.1 que sur un corps fini, les notions de polynômes et de fonction polynomiale ne coïncident pas. Nous allons voir que c'est le cas lorsque le corps est infini, par exemple lorsque $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$.

1.4.7 Exercice.— Supposons que $\mathbb{K}$ est le corps $\mathbb{R}$ ou $\mathbb{C}$.

1. Montrer que l'application
$$\varphi : \mathbb{K}[x] \longrightarrow \mathbb{K}^{\mathbb{K}}$$
définie par $\varphi(f) = \widetilde{f}$ est injective.

2. Montrer que deux polynômes à coefficients dans $\mathbb{K}$ sont égaux si, et seulement si leurs fonctions polynomiales associées sont égales.

1.4.8. Degré d'un polynôme.— Soit f un polynôme de $\mathbb{K}[x]$. Si $f = 0$, on pose $\deg f = -\infty$, si $f = \sum_{i=0}^{m} a_i x^i$ est non nul, on note $\deg f$ le plus grand entier naturel n tel que a_n soit non nul. L'entier $\deg f$ est appelé le *degré* du polynôme f.

Un polynôme non nul f de degré $n \geq 0$ s'écrit de façon unique sous la forme
$$f = a_0 + a_1 x + \ldots + a_n x^n,$$
où a_n est non nul. Le degré de f est le plus grand exposant de x apparaissant dans f.

1.4.9. Les monômes.— On appelera *monôme* un polynôme de la forme x^k, où k est un entier naturel. La famille de monômes $(x^n)_{n\in N}$ forme une base du $\mathbb{K}$-espace vectoriel $\mathbb{K}[x]$. On l'appelle base canonique de $\mathbb{K}[x]$.

1.4.10. Terme de plus haut degré.— Le *coefficient de plus haut degré* (*leading coefficient*) d'un polynôme f de $\mathbb{K}[x]$, noté $\mathrm{lc}(f)$, est le coefficient du monôme de plus grand exposant. Le *terme de plus haut degré* d'un polynôme f (*leading term*), noté $\mathrm{lt}\,(f)$, est le terme de plus haut degré de f. Par exemple, pour le polynôme $f = a_0 + a_1 x + \ldots + a_n x^n$, on a
$$\deg f = n, \quad \mathrm{lt}\,(f) = a_n x^n, \quad \mathrm{lc}(f) = a_n.$$
Un polynôme est dit *unitaire*, si le coefficient de son terme de plus haut degré est égal à 1.

1.4.11 Exercice.— Montrer que pour tous polynômes f et g de $\mathbb{K}[x]$, on a

1. $\mathrm{lc}(fg) = \mathrm{lc}(f)\mathrm{lc}(g)$,

2. $\mathrm{lt}\,(fg) = \mathrm{lt}\,(f)\,\mathrm{lt}\,(g)$.

§ 5 Arithmétique des polynômes

1.5.1. Divisibilité.— Soient f et g deux polynômes de $\mathbb{K}[x]$. On dit que g *divise* f, ou que f est *divisible* par g, ou encore que f est un multiple de g, s'il existe un polynôme q de $\mathbb{K}[x]$ tel que $f = gq$. On note alors $g|f$.

1.5.2 Exercice.— Montrer que le polynôme $x + 3$ divise le polynôme $x^3 + 27$.

1.5.3 Exercice.— Montrer que pour deux polynômes f et g non nuls de $\mathbb{K}[x]$, $\deg f \leq \deg g$ si, et seulement si, $\mathrm{lt}\,(f) \mid \mathrm{lt}\,(g)$.

1.5.4 Exercice.— Soient f et g deux polynômes de $\mathbb{K}[x]$. Montrer que $f|g$ et $g|f$ si, et seulement si, il existe un scalaire non nul λ de $\mathbb{K}$ te que $f = \lambda g$.

1.5.5. La division euclidienne dans $\mathbb{K}[x]$. — Il existe sur l'anneau $\mathbb{K}[x]$ une division euclidienne comme celle que nous avons vue sur l'anneau $\mathbb{Z}$. Par exemple, considérons deux polynomes

$$f = x^3 - 3x^2 + 4x + 7, \qquad g = 2x^2 + 4x + 6,$$

de $\mathbb{Q}[x]$. La division de f par g a pour quotient $\frac{1}{2}x - \frac{5}{2}$ et pour reste $11x + 22$. On les obtient en procédant de la même façon que la division des entiers :

$$\begin{array}{rrrr|lll}
x^3 & -3x^2 & +4x & +7 & 2x^2 & +4x & +6 \\ \cline{5-7}
x^3 & +2x^2 & +3x & & \frac{1}{2}x & -\frac{5}{2} & \\ \cline{1-4}
& -5x^2 & +x & +7 & & & \\
& -5x^2 & -10x & -15 & & & \\ \cline{2-4}
& & 11x & +22 & & &
\end{array}$$

La première étape consiste à multiplier le polynôme g par $\frac{1}{2}x$, puis à soustraire le résultat à f, soit

$$f - \frac{x^3}{2x^2}g = f - \frac{1}{2}xg = -5x^2 + x + 7.$$

L'idée consiste à multiplier g par un terme, ici $\frac{x^3}{2x^2}$, de telle façon que le terme de plus haut degré de g multiplié par ce terme annule le terme de plus haut degré de f. On obtient ainsi un nouveau polynôme $h = -5x^2 + x + 7$, on dit que h est une *reduction* de f par g, on note

$$f \xrightarrow{g} h.$$

On répète alors ce processus, jusqu'à obtenir le reste

$$r = h - (-\frac{5}{2})g = 11x + 22.$$

La division se compose ainsi d'une suite de réductions par g :

$$f \xrightarrow{g} h \xrightarrow{g} r.$$

1.5.6. Le cas général. — Plus généralement, considérons deux polynômes

$$f = a_n x^n + \ldots + a_1 x + a_0, \quad g = b_m x^m + \ldots + b_1 x + b_0,$$

avec $\deg f = n \geq \deg g = m$. La première étape dans la division de f par g consiste à soustraire à f le produit

$$\frac{a_n}{b_m} x^{n-m} g,$$

qui, avec les notations définies en 1.4.10, s'écrit

$$\frac{\mathrm{lt}\,(f)}{\mathrm{lt}\,(g)} g.$$

On obtient ainsi comme premier reste le polynôme

$$h = f - \frac{\mathrm{lt}\,(f)}{\mathrm{lt}\,(g)} g.$$

On dit que f se *réduit* en h par g, on note

$$f \xrightarrow{g} h.$$

On répète alors l'opération de réduction par g, pour obtenir un nouveau reste :

$$h' = h - \frac{\mathrm{lt}\,(h)}{\mathrm{lt}\,(g)} g.$$

Dans la réduction $f \xrightarrow{g} h$, on notera que le reste h a un degré strictement inférieur au degré de f. On peut alors poursuivre le processus de réduction, jusqu'à obtenir un reste, dont le degré est strictement inférieur au degré du polynôme g. On obtient ainsi une suite de réductions par g qui termine sur un reste r, tel que $\deg r < \deg g$:

$$f \xrightarrow{g} h \xrightarrow{g} h' \xrightarrow{g} \ldots \xrightarrow{g} r.$$

On montre ainsi l'existence du quotient et du reste dans le théorème de la division euclidienne :

1.5.7 Théorème (de la division euclidienne).— Soient f et g deux polynômes de $\mathbb{K}[x]$, avec $g \neq 0$. Il existe un couple unique (q, r) de polynômes de $\mathbb{K}[x]$ tel que :

$$f = gq + r,$$

avec $\deg r < \deg g$.

Le polynôme q est appelé le *quotient* de la division euclidenne de f par g et le polynôme r est appelé le *reste* de la division euclidenne de f par g. Si le reste de la division euclidienne de f par g est nul, alors le polynôme g divise f.

1.5.8 Exercice.— Montrer l'unicité des polynômes q et r.

1.5.9 Exercice.— Étant donnés deux élements distincts a et b d'un corps $\mathbb{K}$. Calculer le reste de la division euclidienne d'un polynôme f de $\mathbb{K}[x]$ par le polynôme $(x-a)(x-b)$ en fonction de $f(a)$ et $f(b)$.

1.5.10 Exercice.— Calculer le reste de la division de f par g avec

1. $f = x^3 + x^2 + x + 1,\ \ g = x + 1,$
2. $f = x^3 + x^2 + x + 1,\ \ g = x - 1,$
3. $f = x^3 + 3x^2 - 7x + 5,\ \ g = x^2 - 3,$
4. $f = x^4 + 2x^3 - 4x^2 + 5,\ \ g = x^3 + 5.$

1.5.11 Théorème.— Si $\mathbb{K}$ est un corps, l'anneau $\mathbb{K}[x]$ est euclidien.

Preuve. D'après le théorème 1.5.7, l'application $\deg : \mathbb{K}[x] - \{0\} \longrightarrow \mathbb{N}$ est un algorithme euclidien sur $\mathbb{K}[x]$. $\square$

ENTRÉE : $f, g \in \mathbb{K}[x]$ avec $g \neq 0$,
SORTIE : $q, r \in \mathbb{K}[x]$ tels que $f = gq + r$ avec $\big(r = 0$ ou $\deg r < \deg g\big)$.
INITIALISATION : $q := 0$; $r := f$
TANT QUE : $r \neq 0$ **ET** $\deg g \leq \deg r$ **FAIRE**

$$q := q + \frac{\mathrm{lt}\,(r)}{\mathrm{lt}\,(g)}$$

$$r := r - \frac{\mathrm{lt}\,(r)}{\mathrm{lt}\,(g)}g.$$

Algorithme de la division des polynômes d'une indéterminée.

Nous reviendrons sur cet algorithme de la division dans un prochain chapitre, en particulier pour ses nombreuses applications.

1.5.12. Polynômes premiers entre eux.— Deux polynômes sont dits *premiers entre eux*, si leurs seuls diviseurs communs sont les polynômes de degré nul. Plus généralement, des polynômes $f_1, \ldots, f_s$ de $\mathbb{K}[x]$ sont dits

- *premiers entre eux dans leur ensemble*, si les seuls polynômes qui divisent simultanément les polynômes $f_1, \ldots, f_s$ sont de degré nul,
- *premiers entre eux deux à deux*, si, pour tout i différent de j, les polynômes f_i et f_j sont premiers entre eux.

Si f_i et f_j sont premiers entre eux, alors les polynômes $f_1, \ldots, f_i, \ldots, f_j, \ldots, f_s$ sont premier entre eux dans leur ensemble. Attention, les polynômes $f_1 = x - 1$, $f_2 = (x-1)(x-2)$ et $f_3 = x - 3$ sont premiers entre eux dans leur ensemble, alors que les polynômes f_1 et f_2 ne sont pas premiers entre eux.

1.5.13 Théorème (Identité de Bézout).— Les polynômes $f_1, \ldots, f_s \in \mathbb{K}[x]$ sont premiers entre eux dans leur ensemble si, et seulement si, il existe des polynômes $u_1, \ldots, u_s$ de $\mathbb{K}[x]$, tels que

$$f_1h_1 + \cdots + f_sh_s = 1.$$

L'égalité $f_1h_1 + \cdots + f_sh_s = 1$ s'appelle une *identité de Bézout*.

1.5.14. Exemples.— Les polynômes $x - 1$ et $x + 2$ sont premiers entre eux, on a l'identité de Bézout

$$-\frac{1}{3}(x-1) + \frac{1}{3}(x+2) = 1.$$

Les polynômes $x^2 - 1$ et $x + 2$ sont premiers entre eux, une identité de Bézout est donnée par

$$\frac{1}{3}(x^2-1) + (-\frac{1}{3}x + \frac{2}{3})(x+2) = 1.$$

1.5.15. Calculer une identité de Bézout. — L'algorithme d'Euclide permet de calculer une identité de Bézout. Étant donnés deux polynômes f_1 et f_2, premiers entre eux, l'algorithme suivant permet de calculer une identité de Bézout

$$f_1h_1 + f_2h_2 = 1.$$

Soient $f_1, f_2 \in \mathbb{K}[x] - \{0\}$ deux polynômes premiers entre eux. On pose $r_0 = f_1$, $r_1 = f_2$. On calcule les divisions euclidiennes

$$\begin{aligned}
r_0 &= r_1q_1 + r_2, \quad \deg r_2 < \deg r_1,\\
r_1 &= r_2q_2 + r_3, \quad \deg r_3 < \deg r_2,\\
&\vdots\\
r_{n-2} &= r_{n-1}q_{n-1} + r_n, \quad \deg r_n < \deg r_{n-1},
\end{aligned}$$

Alors, il existe $n_0 \geq 0$ tel que, pour tout $n \geq n_0$, $r_n = 0$. Les polynômes f_1 et f_2 sont premiers entre eux, par suite le dernier reste non nul r_{n_0-1} est une constante $b \in \mathbb{K}-\{0\}$. Pour déterminer les polynômes h_1 et h_2 dans l'identité de Bézout, il suffit de partir de

$$r_{n_0-1} = b = r_{n_0-3} - r_{n_0-2}q_{n_0-2},$$

et en utilisant toutes les relations entre les restes, obtenir une relation de Bézout entre r_0 et r_1, comme dans l'exemple suivant.

1.5.16. Exemple. — Les polynômes $x^4 + 1$ et $x^3 + 1$ sont premiers entre eux. On calcule la division euclidienne de $x^4 + 1$ par $x^3 + 1$:

$$x^4 + 1 = (x^3 + 1)(x) + (-x + 1),$$

on calcule alors la division euclidienne de $x^3 + 1$ par $-x + 1$:

$$x^3 + 1 = (-x + 1)(-x^2 - x - 1) + 2.$$

Le dernier reste non nul est 2, on a alors

$$\begin{aligned}
2 &= (x^3 + 1) - (-x + 1)(-x^2 - x - 1),\\
&= (x^3 + 1) - ((x^4 + 1) - (x^3 + 1)(x))(-x^2 - x - 1),\\
&= (x^3 + 1) - (x^4 + 1)(-x^2 - x - 1) + (x^3 + 1)x(-x^2 - x - 1),\\
&= (x^3 + 1)(1 - x - x^2 - x^3) + (x^4 + 1)(1 + x + x^2).
\end{aligned}$$

On obtient ainsi une relation de Bézout :

$$1 = \frac{1}{2}(1 - x - x^2 - x^3)(x^3 + 1) + \frac{1}{2}(1 + x + x^2)(x^4 + 1).$$

1.5.17 Exercice. — Trouver une relation de Bézout entre les polynômes f_1 et f_2, avec

1. $f_1 = x^2 + 2x - 1, \quad f_2 = x + 2,$
2. $f_1 = x^4 + 2x^3 - x, \quad f_2 = x^3 + 5,$
3. $f_1 = x^2 + 2x - 1, \quad f_2 = x + 2.$

1.5.18 Exercice (Lemme de Gauss). — Soient f, g, h des polynômes de $\mathbb{K}[x]$. Montrer que si f et g sont premiers entre eux et que f divise gh, alors f divise h.

FIGURE 1.4 – Étienne Bézout (1730 - 1783)

Étienne Bézout est un mathématicien français, auteur d'une Théorie générale des équations algébriques sur la théorie de l'élimination et des fonctions symétriques sur les racines d'une équation. Examinateur des élèves du corps de l'artillerie, il rédige un cours de mathématiques à l'usage de la marine et de l'artillerie, qui deviendra un ouvrage de référence pour les candidats au concours d'entrée à l'École polytechnique.

1.5.19. Racine d'un polynôme.— Soit f un polynôme de $\mathbb{K}[x]$. Un scalaire $a \in \mathbb{K}$ est dit *racine* de f si $f(a) = 0$, c'est-à-dire, lorsque a est un zéro de la fonction polynomiale $\widetilde{f}$. On peut dire aussi que a est racine de f si, et seulement si, $x - a$ divise f.

Si $a_1, \ldots, a_p$ sont p racines distinctes de f, alors f est divisible par le polynôme

$$(x - a_1) \ldots (x - a_p).$$

Un polynôme non nul f de degré n admet au plus n racines distinctes. Si f admet n racines distinctes $a_1, \ldots, a_n$, alors, il se décompose sous la forme

$$f = \mathrm{lc}(f)(x - a_1) \ldots (x - a_n).$$

1.5.20. Racines multiples.— Soient f un polynôme de $\mathbb{K}[x]$ et a une racine de f. On appelle *ordre de multiplicité* de la racine a l'exposant de la plus grande puissance de $x - a$ qui divise f. Autrement dit, c'est l'entier h tel que $(x - a)^h$ divise f et $(x - a)^{h+1}$ ne divise pas f. Soit f un polynôme tel que

$$f = (x - a)^h q.$$

Alors a est racine d'ordre de multiplicité h si, et seulement si, a n'est pas racine du polynôme q.

1.5.21. Polynômes scindés.— Soit $f \in \mathbb{K}[x]$ un polynôme. On dit que f est *scindé* sur $\mathbb{K}$ s'il admet des racines $a_1, \ldots, a_p$ dans $\mathbb{K}$ d'ordre de multiplicité respectifs $m_1, \ldots, m_p$ telles que $m_1 + \ldots + m_p = \deg f$. On a alors

$$f = \mathrm{lc}(f)(x - a_1)^{m_1} \ldots (x - a_p)^{m_p},$$

avec $a_i \neq a_j$ si $i \neq j$ et $m_1 + \cdots + m_p = \deg f$.

1.5.22 Théorème (de D'Alembert-Gauss).— Tout polynôme non constant à coefficients dans $\mathbb{C}$ possède au moins une racine dans $\mathbb{C}$.

Ce théorème est appelé aussi théorème de D'Alembert-Gauss, ou encore *théorème fondamental de l'algèbre*.

1.5.23 Corollaire.— Tout polynôme non nul de $\mathbb{C}[x]$ est scindé sur $\mathbb{C}$.

On dit qu'un corps $\mathbb{K}$ est *algébriquement clos*, si tout polynôme non constant de $\mathbb{K}[x]$ possède une racine dans $\mathbb{K}$.

1.5.24 Exercice.— Montrer que le corps $\mathbb{R}$ n'est pas algébriquement clos.

Le théorème fondamental de l'algèbre entraîne que le corps $\mathbb{C}$ est algébriquement clos. Plus généralement, on peut montrer que, pour tout corps $\mathbb{K}$, il existe une extension $\mathbb{L}$ telle que tout polynôme de $\mathbb{K}[x]$ soit scindé sur $\mathbb{L}$. Le corps $\mathbb{L}$ est appelé la *clôture algèbrique* de $\mathbb{K}$. Par exemple $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$.

FIGURE 1.5 – Jean Le Rond D'Alembert (1717 - 1783)

Jean Le Rond D'Alembert est un mathématicien, philosophe et encyclopédiste français. Il énonce le théorème de D'Alembert-Gauss dans le Traité de dynamique, qui ne sera démontré qu'un siècle après par Carl Friedrich Gauss. D'Alembert est célèbre pour ses nombreux travaux mathématiques, notamment sur les équations différentielles et les équations aux dérivées partielles. Il aborda des problèmes difficiles en physique avec le Traité de dynamique des systèmes, en astronomie avec le problème des trois corps, ou encore en musique avec la vibration des cordes.

§ 6 Les fractions rationnelles

Nous connaissons la construction du corps $\mathbb{Q}$ des nombres rationnels à partir de l'anneau des entiers relatifs $\mathbb{Z}$. Le corps des fractions rationnelles $\mathbb{K}(x)$ se construit de façon similaire à partir de l'anneau des polynômes $\mathbb{K}[x]$.

1.6.1. Le corps des fractions rationnelles. — Soit $\mathcal{E}$ l'ensemble $\mathbb{K}[x]\times(\mathbb{K}[x]\setminus\{0\})$. On définit sur $\mathcal{E}$ une relation $\approx$ définie par, pour tous $(f,g),(f',g')\in\mathcal{E}$,

$$(f,g)\approx(f',g') \quad \text{si, et seulement si,} \quad fg' = f'g.$$

La relation $\approx$ forme une relation d'équivalence sur $\mathcal{E}$. L'ensemble $\mathcal{E}/\approx$ des classes d'équivalence est noté $\mathbb{K}(x)$. Un élément de $\mathbb{K}(x)$ représenté par $(f,g)\in\mathcal{E}$ est noté $\dfrac{f}{g}$. et appelé *fraction rationnelle*.

On définit sur $\mathbb{K}(x)$ une addition et une multiplication définies de la façon suivante, pour toutes fractions rationnelles $\dfrac{f}{g}$ et $\dfrac{f'}{g'}$,

$$\frac{f}{g}+\frac{f'}{g'}=\frac{fg'+f'g}{gg'}, \qquad \frac{f}{g}.\frac{f'}{g'}=\frac{ff'}{gg'}.$$

1.6.2 Proposition. — Ces opérations sont bien définies et munissent l'ensemble $\mathbb{K}(x)$ des fractions rationnelles d'une structure de corps.

Le corps $\mathbb{K}(x)$ est appelé *corps des fractions rationnelles*.

1.6.3 Exercice. — Montrer que la relation $\approx$ est une relation d'équivalence.

1.6.4 Exercice. — Montrer la proposition 1.6.2.

On appelle *représentant irréductibe* d'une fraction rationnelle F, tout représentant (f,g) de F où les polynômes f et g sont premiers entre eux.

On appelle *degré* d'une fraction rationnelle F, la quantité $\deg f - \deg g \in \mathbb{Z}\cup\{-\infty\}$, où (f,g) est un représentant de F. Cette quantité ne dépend pas du représentant et est notée $\deg F$. On a $\deg 0 = -\infty$.

Soit F une fraction rationnelle de forme irréductible $\dfrac{f}{g}$. On appelle *racine* de F toute racine de f. On appelle *pôle* de F toute racine de g. L'*ordre de multiplicité* d'une racine ou d'un pôle est l'ordre de multiplicité de la racine dans le polynôme correspondant.

1.6.5. Décomposition en éléments simples. —

1.6.6 Proposition. — Toute fraction rationnelle F s'écrit de façon unique comme la somme d'un polynôme, appelé *partie entière* de F, et d'une fraction rationnelle de degré strictement négatif.

On considère la fraction rationnelle $\frac{f}{g}$. En notant E le quotient et R le reste de la division euclidienne de f par g, alors

$$\frac{f}{g} = E + \frac{r}{q}, \quad \text{avec } \deg r < \deg q.$$

Par exemple, on a

$$\frac{x^5+1}{x(x-1)^2} = x^2 + 2x + 3 + \frac{4x^2 - 3x + 1}{x(x-1)^2}.$$

Le polynôme $x^2 + 2x + 3$ est la partie entière de la fraction rationnelle $\frac{x^5+1}{x(x-1)^2}$.

1.6.7 Proposition. — Soit F un fraction rationnelle admettant un pôle λ d'ordre k. Il existe un unique k-uplet de scalaires $(\beta_1, \ldots, \beta_k)$ et une unique fraction F_0 n'admettant pas λ pour pôle, tels que :

$$F = F_0 + \sum_{i=1}^{k} \frac{\beta_i}{(x-\lambda)^i}.$$

1.6.8. Exemple. — La fraction $\frac{x^5+1}{x(x-1)^2}$ admet pour pôles 0 et 1 d'ordre 1 et 2 respectivement. On a une *décomposition en éléments simples* :

$$\frac{x^5+1}{x(x-1)^2} = x^2 + 2x + 3 + \frac{1}{x} + \frac{2}{(x-1)^2} + \frac{3}{x-1}.$$

1.6.9 Proposition (décomposition en éléments simples dans $\mathbb{C}(x)$). — Soit F une fraction rationnelle de $\mathbb{C}(x)$ de pôles $\lambda_1, \ldots, \lambda_p$ distincts deux à deux et d'ordre de multiplicité respectifs $k_1, \ldots, k_p$. Il existe un polynôme E de $\mathbb{C}[x]$ et une unique famille de scalaires $(\beta_{i,j})$ tels que :

$$F = E + \sum_{i=1}^{p} \sum_{j=1}^{k_i} \frac{\beta_{i,j}}{(x-\lambda_i)^j}.$$

La décomposition précédente est appelée la *décomposition en éléments simples* dans $\mathbb{C}(x)$ de la fraction rationnelle F.

1.6.10 Exercice. — Déterminer une identité de Bézout entre les polynômes suivants

1. $x-1$ et $x+2$,
2. $x+1$ et x^2-2x+1,
3. x^4-1 et x^3+2.

1.6.11 Exercice. — Décomposer en éléments simples dans $\mathbb{C}(x)$ les fractions suivantes

1. $\frac{10x^3}{(x^2+1)(x^2-4)}$,

2. $\dfrac{x^3-1}{(x-1)(x-2)(x-3)}$,

3. $\dfrac{x^2}{(x^2+x+1)^2}$,

4. $\dfrac{(x^2+4)^2}{(x^2+1)(x^2-2)^2}$.

CHAPITRE
2

Les espaces vectoriels

Sommaire

Nous rappelons dans ce chapitre les notions d'algèbre linéaire abordées en première année. Pour une bonne compréhension des prochains chapitres, il est important que ces notions soient bien assimilées. Ce chapitre constitue un recueil de résultats sans démonstration. Le lecteur est renvoyé à son cours de première année.

§ 1 La structure d'espace vectoriel

2.1.1. Un prototype.— L'espace vectorie réel $\mathbb{R}^n$ est le prototype d'espace vectoriel réel de dimension finie. Ses éléments sont les n-uplets ordonnées de nombres réels $(x_1, x_2, \ldots, x_n)$, que nous écrirons sous la forme de *vecteur colonne* :

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}.$$

Les opérations d'addition et de multiplication de nombre réels permettent de définir deux opérations sur $\mathbb{R}^n$, l'addition de vecteurs :

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{bmatrix}$$

et la multiplication d'un vecteur par un nombre réel, pour tout réel λ,

$$\lambda \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \lambda x_1 \\ \lambda x_2 \\ \vdots \\ \lambda x_n \end{bmatrix}.$$

Ces deux opérations ont des propriétés héritées de celles satisfaites par les opérations d'addition et de multiplication sur les nombres réels. On peut vérifier ainsi que, l'addition de n-uplets satisfait les relations suivantes :

i) pour tous $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{R}^n$, on a $(\mathbf{x} + \mathbf{y}) + \mathbf{z} = \mathbf{x} + (\mathbf{y} + \mathbf{z})$,

ii) pour tous $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, on a $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$,

iii) si $\mathbf{0}$ désigne le n-uplet $(0, 0, \ldots, 0)$, on a $\mathbf{x} + \mathbf{0} = \mathbf{x}$,

iv) en notant $-(x_1, x_2, \ldots, x_n)$, le n-uplet $(-x_1, -x_2, \ldots, -x_n)$, on a $\mathbf{x} + (-\mathbf{x}) = \mathbf{0}$.

D'autre part, la mupliplication par un nombre réel satisfait les relations suivantes :

v) pour tous $\lambda, \mu \in \mathbb{R}$ et tout $\mathbf{x} \in \mathbb{R}^n$, on a $\lambda(\mu\mathbf{x}) = (\lambda\mu)\mathbf{x}$,

vi) pour tout $\mathbf{x} \in \mathbb{R}^n$, on a $1\mathbf{x} = \mathbf{x}$.

Enfin, les opérations d'addition et de multiplication par un réel vérifient des relations de compatibilités entre elles :

vii) pour tout $\lambda \in \mathbb{R}$ et tous $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, on a $\lambda(\mathbf{x} + \mathbf{y}) = \lambda\mathbf{x} + \lambda\mathbf{y}$,

viii) pour tous $\lambda, \mu \in \mathbb{R}$ et tout $\mathbf{x} \in \mathbb{R}^n$, on a $(\lambda + \mu)\mathbf{x} = \lambda\mathbf{x} + \mu\mathbf{x}$.

2.1.2. D'autres exemples. — Il existe d'autres ensembles qui, munis d'une opération d'addition et de multiplication par un réel, satisfont les mêmes relations.

1) Considérons l'ensemble $\mathcal{C}([0, 1], \mathbb{R})$ des fonctions continues sur l'intervale réel $[0, 1]$ et à valeurs réelles. Si f et g sont deux telles fonctions, on définit leur addition en posant, pour tout réel $x \in [0, 1]$,

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

et la multiplication d'une fonction f par un réel λ, en posant

$$(\lambda f)(x) = \lambda f(x).$$

Ces opérations ainsi définies statisfont les propriétés **i)-viii)** ci-dessus, en prenant pour zéro dans **iii)** la fonction nulle et en notant dans **iv)** $-f$, la fonction définie par

$$(-f)(x) = -f(x).$$

2) On vérifiera que les mêmes opérations sur l'ensemble des fonctions deux fois différentiables qui satisfont

$$\frac{d^2 f}{dt^2} + \lambda \frac{df}{dt} + \mu f = 0, \qquad \lambda, \mu \in \mathbb{R},$$

satisfont les propriétés **i)-viii)**.

3) De la même façon, les suites réelles $(x_n)_{n \in \mathbb{N}}$, satisfaisant la relation de récurrence

$$x_{n+2} = \lambda x_{n+1} + \mu x_n, \qquad \lambda, \mu \in \mathbb{R},$$

satisfont les propriétés **i)-viii)**.

En remplaçant le corps des réels par un corps quelconque $\mathbb{K}$, on obtient la struture d'espace vectoriel sur un corps $\mathbb{K}$, tel que $\mathbb{K}$ lui-même ou bien $\mathbb{K}^n$.

2.1.3. Définition.— Un *espace vectoriel* sur un corps $\mathbb{K}$, ou $\mathbb{K}$-espace vectoriel, est un ensemble E muni d'une addition $+ : E \times E \longrightarrow E$ et d'une application

$$\begin{aligned} . : \mathbb{K} \times E &\longrightarrow E \\ (\lambda, \mathbf{x}) &\longmapsto \lambda.\mathbf{x} \end{aligned}$$

appelée loi externe, on notera aussi $\lambda\mathbf{x}$ pour $\lambda.\mathbf{x}$, qui vérifient les propriétés suivantes,

i) l'ensemble E muni de l'addition est un groupe abélien,

ii) pour tout $\mathbf{x} \in E$, $1\mathbf{x} = \mathbf{x}$,

iii) pour tous $\lambda, \mu \in \mathbb{K}$ et tous $\mathbf{x}, \mathbf{y} \in E$:

$$\begin{aligned} \lambda(\mu\mathbf{x}) &= (\lambda\mu)\mathbf{x}, \\ (\lambda + \mu)\mathbf{x} &= \lambda\mathbf{x} + \mu\mathbf{x}, \\ \lambda(\mathbf{x} + \mathbf{y}) &= \lambda\mathbf{x} + \lambda\mathbf{y}. \end{aligned}$$

Les éléments d'un espace vectoriel E sont appelés *vecteurs* et les éléments du corps $\mathbb{K}$ sont appelés *scalaires*.

2.1.4. L'espace nul.— Le $\mathbb{K}$-espace vectoriel qui comporte un seul élément, l'élément nul $\mathbf{0}$, est appelé l'*espace vectoriel nul*.

2.1.5 Exercice.— Soit E un $\mathbb{K}$-espace vectoriel. Montrer que, pour tout vecteur $\mathbf{x}$ et tout scalaire λ, on a les relations :

a) $\mathbf{0} + \mathbf{x} = \mathbf{x}$,

b) $\lambda\mathbf{0} = \mathbf{0}$,

c) $0\mathbf{x} = \mathbf{0}$,

d) $\lambda\mathbf{x} = \mathbf{0}$ si, et seulement si, $\lambda = 0$ ou $\mathbf{x} = \mathbf{0}$,

e) $-(\lambda\mathbf{x}) = \lambda(-\mathbf{x}) = (-\lambda)\mathbf{x}$.

2.1.6. Combinaisons linéaires.— Soit E un $\mathbb{K}$-espace vectoriel. Soient $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_p$ des vecteurs de E. On appelle *combinaison linéaire* des vecteurs $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_p$ tout vecteur de la forme

$$\lambda_1\mathbf{x}_1 + \lambda_2\mathbf{x}_2 + \ldots + \lambda_p\mathbf{x}_p,$$

où $\lambda_1, \ldots, \lambda_p \in \mathbb{K}$.

Plus généralement, si $(\mathbf{x}_i)_{i\in I}$ est une famille de vecteurs de E, on appele *combinaison linéaire* des $(\mathbf{x}_i)_{i\in I}$ toute somme

$$\sum_{i\in I} \lambda_i\mathbf{x}_i,$$

dans laquelle, pour tout $i \in I$, $\lambda_i \in \mathbb{K}$ et où les λ_i sont tous nuls sauf un nombre fini.

2.1.7. Sous-espaces vectoriels.— Soit E un $\mathbb{K}$-espace vectoriel. Un *sous-espace vectoriel* de E est un sous ensemble F de E tel que les opérations de E induisent sur F une structure de $\mathbb{K}$-espace vectoriel. Un sous-ensemble F de E est donc un sous-espace vectoriel si les assertions suivantes sont vérifiées :

i) $\mathbf{0} \in F$,

ii) pour tous $\mathbf{x}, \mathbf{y} \in F$, $\mathbf{x} + \mathbf{y} \in F$,

iii) pour tout $\mathbf{x} \in F$ et tout $\lambda \in \mathbb{K}$, $\lambda\mathbf{x} \in F$.

2.1.8. Exemples. —

a) Le sous-ensemble $\{\mathbf{0}\}$ réduit au vecteur nul et E sont des sous-espaces vectoriel de E.

b) Soit $\mathbb{K}[x]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$. Le sous-ensemble $\mathbb{K}_n[x]$ de $\mathbb{K}[x]$ formé des polynômes de degré au plus n est un sous-espace vectoriel de $\mathbb{K}[x]$.

2.1.9 Exercice. — Montrer qu'une intersection de sous-espaces vectoriels de E est un sous-espace vectoriel de E.

2.1.10. Remarques. — Un sous-ensemble F de E est un sous-espace vectoriel si, et seulement si, toute combinaison linéaire de vecteurs de F est un vecteur de F. Pour montrer qu'un sous-ensemble F de E est un sous-espace vectoriel, il suffit alors de montrer que $\mathbf{0} \in F$ et que $\lambda\mathbf{x} + \mu\mathbf{y}$, pour tous vecteurs $\mathbf{x}, \mathbf{y} \in F$ et scalaires $\lambda, \mu \in \mathbb{K}$.

2.1.11 Exercice. — Soit α un réel. On considère le sous-ensemble suivant de $\mathbb{R}^3$:

$$F_\alpha = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \;\mid\; x_1 + x_2 + x_3 = \alpha\}$$

Montrer que F_α est un sous-espace vectoriel de $\mathbb{R}^3$, si et seulement si, $\alpha = 0$.

§ 2 Bases et dimension d'un espace vectoriel

2.2.1. Sous-espace vectoriel engendré par une partie. — Une intersection de sous-espaces vectoriels de E est un sous-espace vectoriel de E.

Soient E un $\mathbb{K}$-espace vectoriel et A une partie de E. L'intersection de tous les sous-espaces vectoriels de E qui contiennent A est le plus petit sous-espace vectoriel de E, au sens de l'inclusion, contenant A. On l'appelle *sous-espace vectoriel engendré* par A et on le note $\mathrm{Vect}(A)$.

Le sous-espace vectoriel $\mathrm{Vect}(A)$ est formé de toutes les combinaisons linéaires de vecteurs de A.

2.2.2. Exemples. — Le sous-espace vectoriel engendré par l'ensemble vide est l'espace vectoriel nul :

$$\mathrm{Vect}(\{\mathbf{0}\}) = \{\mathbf{0}\}.$$

Pour tous vecteurs $\mathbf{x}, \mathbf{y}$ de E, on a

$$\mathrm{Vect}(\mathbf{x}, \mathbf{y}) = \mathrm{Vect}(\mathbf{x} + \mathbf{y}, \mathbf{x} - \mathbf{y}).$$

2.2.3 Exercice. —

1. Montrer que l'ensemble $A = \{(1, 0), (0, 1)\}$ engendre $\mathbb{R}^2$.
2. Montrer que l'ensemble $A = \{(x, x^2, x^3) \mid x \in \mathbb{R}\}$ n'engendre pas $\mathbb{R}^3$.

2.2.4. Famille génératrice. — Une famille $(\mathbf{x}_i)_{i\in I}$ de vecteurs d'un $\mathbb{K}$-espace vectoriel E est dite *génératrice* si $E = \mathrm{Vect}((\mathbf{x}_i)_{i\in I})$.

2.2.5. Famille libre.— Une famille $(\mathbf{x}_i)_{i\in I}$ de vecteurs d'un $\mathbb{K}$-espace vectoriel E est dite *libre*, ou *linéairement indépendante*, si pour toute combinaison linéaire vérifiant

$$\sum_{i\in I} \lambda_i \mathbf{x}_i = \mathbf{0},$$

alors, pour tout $i \in I$, $\lambda_i = 0$. Autrement dit, aucun des vecteurs de la famille $(\mathbf{x}_i)_{i\in I}$ n'est combinaison linéaire des autres. Un famille qui n'est pas libre est dite *liée*.

Les éléments d'une famille libre sont non nuls et tous distincts. Toute sous-famille d'une famille libre est libre

2.2.6 Exercice.— Montrer cette propriété.

2.2.7. Base d'un espace vectoriel.— Une famille libre et génératrice d'un $\mathbb{K}$-espace vectoriel E est appelée un *base* de E. Si $(\mathbf{e}_i)_{i\in I}$ une base de E, tout vecteur $\mathbf{x}$ de E s'écrit de façon unique

$$\mathbf{x} = \sum_{i\in I} \lambda_i \mathbf{e}_i.$$

Les scalaires λ_i s'appellent les *coordonnées* de $\mathbf{x}$ dans la base $(\mathbf{e}_i)_{i\in I}$.

2.2.8. Exemples.— Tout élément non nul de $\mathbb{K}$ forme une base du $\mathbb{K}$-espace vectoriel $\mathbb{K}$. Le couple $(1, i)$ forme une base du $\mathbb{R}$-espace vectoriel $\mathbb{C}$.

2.2.9. Base canonique.— Lorsqu'un espace est muni naturellement d'une base particulière, elle est dite *canonique*. Par exemple, la famille $(x^n)_{n\in\mathbb{N}}$ est la base canonique de l'espace vectoriel $\mathbb{K}[x]$ des polynômes en l'indéterminée x.

La famille $(0, \ldots, 1, \ldots, 0)$, $1 \leq i \leq n$, est la base canonique de l'espace vectoriel $\mathbb{K}^n$.

2.2.10. Le concept de dimension.— Un espace vectoriel est dit de *dimension finie*, s'il admet une famille génératrice finie. Dans le cas contraire, on dit qu'il est de *dimension infinie*. Le théorème fondamental d'existence de base dans les espaces vectoriels de dimension finie se formule de la façon suivante.

2.2.11 Théorème.— Soit E un $\mathbb{K}$-espace vectoriel non nul de dimension finie. Soient $\mathcal{G}$ une famille génératrice de E et $\mathcal{L} \subset \mathcal{G}$ une famille libre. Alors, il existe une base $\mathcal{B}$ de E vérifiant $\mathcal{L} \subset \mathcal{B} \subset \mathcal{G}$.

De ce résultat on déduit que, pour tout espace vectoriel de dimension finie E

i) de toute famille génératrice de E, on peut extraire une base de E,

ii) (théorème de la base incomplète) toute famille libre peut être complétée en une base.

Enfin, on a le théorème de la dimension d'un espace vectoriel de dimension finie.

2.2.12 Théorème.— Dans un $\mathbb{K}$-espace vectoriel E de dimension finie, toutes les bases ont le même nombre d'éléments.

Ce nombre est appelé la *dimension* de E et est noté $\dim_{\mathbb{K}}(E)$, ou $\dim(E)$, s'il n'y a pas de confusion.

2.2.13 Proposition.— Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et F un sous-espace vectoriel de E. Alors F est de dimension finie et $\dim(F) \leq \dim(E)$. De plus, F est égal à E si, et seulement si, $\dim(F) = \dim(E)$.

Par exemple, l'espace $\mathbb{K}^n$ est de dimension n. L'espace $\mathbb{K}_n[x]$ des polynômes à coefficients dans $\mathbb{K}$ et de degré inférieur ou égal à n admet comme base canonique $(1, x, \ldots, x^n)$ et est donc de dimension $n+1$. L'espace vectoriel $\mathbb{K}[x]$ est de dimension infinie.

§ 3 Somme de sous-espaces vectoriels

2.3.1. Somme de sous-espaces.— Soit E un $\mathbb{K}$-espace vectoriel et soient F et G deux sous-espaces vectoriels de E. La réunion de F et G n'est pas en général un sous-espace vectoriel de E

2.3.2 Exercice.— Donner des contre-exemples.

Le plus petit sous-espace vectoriel contenant F et G est le sous-espace vectoriel $\mathrm{Vect}(F \cup G)$. Ce sous-espace vectoriel est décrit par

$$\mathrm{Vect}(F \cup G) = \{\mathbf{x} + \mathbf{y} \ \mid \ \mathbf{x} \in F \ \text{ et } \ \mathbf{y} \in G\},$$

et est appelé la *somme de* F *et* G. On le notera $F + G$.

Plus généralement, si $(E_i)_{i \in I}$ une famille de sous-espaces vectoriel de E, on note $\sum\limits_{i \in I} E_i$ le sous-espace vectoriel de E formé des combinaisons linéaires

$$\sum_{i \in I} \mathbf{x}_i,$$

où les $\mathbf{x}_i \in E_i$, $i \in I$, sont tous nuls sauf une nombre fini. L'espace $\sum\limits_{i \in I} E_i$ est appelé la *somme* des sous-espaces vectoriels E_i, $i \in I$.

2.3.3 Exercice.— Soient E un espace vectoriel et F, G deux sous-espaces vectoriels de E.

1. Montrer que $F \cap G = F + G$ si, et seulement si, $F = G$.
2. Montrer que la réunion $F \cup G$ est un sous-espace vectoriel de E si, et seulement si, $F \subset G$ ou $G \subset F$.

2.3.4. Somme de sous-espaces supplémentaires.— Soient E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels de E. Les deux assertions suivantes sont équivalentes :

i) pour tout vecteur $\mathbf{x} \in E$, il existe un unique couple $(\mathbf{y}, \mathbf{z}) \in F \times G$ tel que

$$\mathbf{x} = \mathbf{y} + \mathbf{z}.$$

ii) E est égal à la somme $F + G$ des sous-espaces F et G et $F \cap G = \{\mathbf{0}\}$.

On dit que F et G sont deux *sous-espaces vectoriels supplémentaires* de E lorsqu'ils satisfont ces propriétés. On dit aussi que E est la *somme directe* des sous-espaces F et G et on écrit :

$$E = F \oplus G.$$

2.3.5 Exercice.— Montrer l'équivalence des assertions **i)** et **ii)**.

En résumé :

2.3.6 Proposition.— Soient F et G deux sous-espaces vectoriels de E. Alors $E = F \oplus G$ si, et seulement si, les deux propriétés suivantes sont vérifiées :

i) $E = F + G$,

ii) $F \cap G = \{\mathbf{0}\}$.

2.3.7 Proposition.— Tout sous-espace vectoriel d'un espace vectoriel de dimension finie admet au moins un supplémentaire.

2.3.8 Exercice.— On considère les trois sous-espaces vectoriels suivants de $\mathbb{R}^2$:

$$F = \mathbb{R} \times \{\mathbf{0}\}, \qquad G = \{\mathbf{0}\} \times \mathbb{R}, \qquad H = \{(\mathbf{x}, \mathbf{x}) \mid \mathbf{x} \in \mathbb{R}\}.$$

Montrer que $F \cap G = F \cap H = G \cap H = \{\mathbf{0}\}$ et que la somme $F + G + H$ n'est pas directe.

2.3.9. Somme directe d'une famille de sous-espaces.— Plus généralement, soient $E_1, \ldots, E_p$ des sous-espaces vectoriel de E. On dit que E est *somme directe* des sous-espaces vectoriels $E_1, \ldots, E_p$, si tout vecteur $\mathbf{x}$ de E s'écrit de façon unique sous la forme

$$\mathbf{x} = \mathbf{x}_1 + \ldots + \mathbf{x}_p,$$

où, pour tout $i \in [\![1, p]\!]$, $\mathbf{x}_i \in E_i$. On note alors $E = E_1 \oplus \ldots \oplus E_p$.

Pour montrer que E se décompose en la somme directe de p espaces vectoriels :

$$E = E_1 \oplus \ldots \oplus E_p,$$

il suffit de montrer que $E = E_1 + \ldots + E_p$ et que pour tout $i \in [\![2, p]\!]$, on a

$$E_i \cap (E_1 + \ldots + E_{i-1}) = \{\mathbf{0}\}.$$

En pratique, on peut aussi utiliser la caractérisation suivante. Les sous-espaces $E_1, \ldots, E_p$ sont en somme directe si, et seulement si, l'égalité

$$\mathbf{x}_1 + \ldots + \mathbf{x}_p = \mathbf{0}, \quad \text{où} \quad \mathbf{x}_i \in E_i,$$

implique que $\mathbf{x}_i = \mathbf{0}$, pour tout $i \in [\![1, p]\!]$.

2.3.10 Proposition.— Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et $E_1, \ldots, E_p$ des sous-espaces de E de bases respectives $\mathcal{B}_1, \ldots, \mathcal{B}_p$. Alors $E = E_1 \oplus \ldots \oplus E_p$ si, et seulement si, la réunion $\mathcal{B}_1 \cup \ldots \cup \mathcal{B}_p$ est une base de E.

Considérons le $\mathbb{R}$-espace vectoriel $\mathbb{C}$ des nombres complexes. L'ensemble $\mathbb{R}$ des nombres réels et l'ensemble $i\mathbb{R}$ des nombres imaginaires purs, auquel on ajoute 0, sont deux sous-espaces vectoriel de $\mathbb{C}$. On a $\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$.

2.3.11 Exercice.— Montrer que l'ensemble $\mathcal{F}(\mathbb{R}, \mathbb{R})$ des fonctions réelles à valeurs réelles se décompose en la somme directe de l'ensemble des fonctions paires et de l'ensemble des fonctions impaires.

2.3.12 Proposition (une formule de Grassmann).— Soient F et G deux sous-espaces vectoriels de E. On a

$$\dim(F + G) = \dim(F) + \dim(G) - \dim(F \cap G).$$

On en déduit que si $E_1, \ldots, E_p$ sont des sous-espaces vectoriels de E, alors

$$\dim(E_1 \oplus \ldots \oplus E_p) = \dim(E_1) + \ldots + \dim(E_p).$$

§ 4 Les applications linéaires

2.4.1. Définition.— Soient E et E' deux $\mathbb{K}$-espaces vectoriels. Une application

$$u : E \longrightarrow E'$$

est dite *linéaire* si, pour tous vecteurs $\mathbf{x}, \mathbf{y} \in E$ et scalaires $\lambda, \mu \in \mathbb{K}$,

$$u(\lambda\mathbf{x} + \mu\mathbf{y}) = \lambda u(\mathbf{x}) + \mu u(\mathbf{y}).$$

Il découle de cette définition que $u(\mathbf{0}) = \mathbf{0}$.

2.4.2. Espace vectoriel des applications linéaires.— On notera $\mathcal{L}(E, E')$ l'ensemble des applications linéaires de E dans E'. Si u et v sont deux applications linéaires de E dans E' et $\lambda \in \mathbb{K}$ un scalaire, alors les applications $u + v$ et λu définies, pour tout $\mathbf{x} \in E$, par

$$(u + v)(\mathbf{x}) = u(\mathbf{x}) + v(\mathbf{x}),$$
$$(\lambda u)(\mathbf{x}) = \lambda u(\mathbf{x}),$$

sont aussi des applications linéaires de E dans E'. L'addition et la multplication par un scalaire sur l'espace vectoriel E' induisent ainsi une structure de $\mathbb{K}$-espace vectoriel sur $\mathcal{L}(E, E')$.

Une application linéaire de E dans E est appelée un *endomorphisme* de E. On notera $\mathcal{L}(E)$ l'espace vectoriel des endomorphismes de E. Une application linéaire de E dans $\mathbb{K}$ est appelée une *forme linéaire*. Une application linéaire et bijective est appelée un *isomorphisme*. Les endomorphismes bijectifs de E sont encore appelés les *automorphismes* de E. Les automorphismes de E, muni de la composition, forment un groupe, noté $\mathrm{GL}(E)$ et appelé le *groupe linéaire* de E.

2.4.3. Exemples. —

1) L'homothétie $h : E \longrightarrow E$, de rapport λ, définie par $h(\mathbf{x}) = \lambda\mathbf{x}$ est un endomorphisme de E.

2) Soit $E = \mathcal{C}([a,b],\mathbb{R})$ l'espace vectoriel réel formé des fonctions continues de l'intervalle réel $[a,b]$ à valeurs réelles. L'application $\varphi : E \longrightarrow \mathbb{R}$ définie par

$$\varphi(f) = \int_a^b f(t)dt$$

est une forme linéaire.

3) Soit p l'application de $\mathbb{R}^3$ dans $\mathbb{R}^3$ qui envoie un vecteur sur sa projection orthognonale sur le plan xy :

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} \longmapsto \begin{bmatrix} x \\ y \\ 0 \end{bmatrix}$$

est une application linéaire.

2.4.4. Endomorphismes nilpotents. — Un endomorphisme u de $\mathbb{K}^n$ est dit *nilpotent* s'il existe un entier naturel q tel que $u^q = 0$. Le plus petit entier non nul r tel que $u^r = 0$ est appelé l'*indice de nilpotence* de u.

2.4.5. Image d'une application linéaire. — Soient $u : E \longrightarrow E'$ une application linéaire et F un sous-espace vectoriel de E. Alors l'image directe par u du sous-espace F, donnée par

$$u(F) = \{\mathbf{y} \in E' \mid \exists \mathbf{x} \in F,\ \mathbf{y} = u(\mathbf{x})\}$$

est un sous-espace vectoriel de E'

2.4.6 Exercice. — Montrer que $u(F)$ est un sous-espace vectoriel.

On appelle *image* de u, et on note $\mathrm{Im}(u)$, le sous-espace vectoriel $u(E)$.
L'application u est surjective si, et seulement si, $\mathrm{Im}(u) = E'$.

2.4.7. Sous-espace vectoriel stable. — Soient u un endomorphisme de E et F un sous-espace vectoriel de E. On dit que u laisse *stable* F si $u(F)$ est un sous-espace vectoriel de F.

Par exemple, étant donné $\mathbf{x} \in E$, un endomorphisme u de E laisse stable la droite vectorielle $\mathrm{Vect}(\mathbf{x})$ si, et seulement si, les vecteurs $u(\mathbf{x})$ et $\mathbf{x}$ sont colinéaires. Autrement dit, si u est une homothétie.

2.4.8. Noyau d'une application linéaire. — Soient $u : E \longrightarrow E'$ une application linéaire et F' un sous-espace vectoriel de E'. Alors, l'image réciproque par u de F'

$$u^{-1}(F') = \{\mathbf{x} \in E \mid u(\mathbf{x}) \in F'\}$$

est un sous-espace vectoriel de E.

2.4.9 Exercice. — Montrer que $u^{-1}(F')$ est un sous-espace vectoriel de E.

On appelle *noyau* de u, et on note $\mathrm{Ker}(u)$, le sous-espace vectoriel $u^{-1}(\mathbf{0})$.

2.4.10 Proposition.— Une application linéaire u est injective si, et seulement si, $\mathrm{Ker}(u) = \{\mathbf{0}\}$.

2.4.11 Exercice.— Montrer la proposition 2.4.10.

2.4.12. Rang d'une application linéaire.— Soit E un $\mathbb{K}$-espace vectoriel. Le rang d'une famille finie $\mathcal{V}$ de vecteurs de E est la dimension du sous-espace vectoriel $\mathrm{Vect}(\mathcal{V})$ engendré par les vecteurs de $\mathcal{V}$, on le note $\mathrm{rg}(\mathcal{V})$.

Par exemple, si

$$\mathcal{V} = \left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$$

on a $\mathrm{rg}(\mathcal{V}) = 2$.

Soit $u : E \longrightarrow E'$ une application linéaire. L'application u est dite de rang fini si le sous-espace vectoriel $\mathrm{Im}(u)$ est de dimension finie. L'entier $\dim(\mathrm{Im}(u))$ est alors appelé le *rang* de u et est noté $\mathrm{rg}(u)$.

2.4.13. Le théorème du rang.— Étant donnée une application linéaire $u : E \longrightarrow E'$, on considère les ensembles $\mathrm{Ker}(u)$ et $\mathrm{Im}(u)$ qui sont respectivement sous-espaces vectoriels de E et E'. Soit $\mathcal{B} = (\mathbf{e}_1, \ldots, \mathbf{e}_k)$ une base de $\mathrm{Ker}(u)$. D'après le théorème de la base incomplète, on peut compléter cette base en une base $(\mathbf{e}_1, \ldots, \mathbf{e}_k, \mathbf{e}_{k+1}, \ldots, \mathbf{e}_n)$ de E. Alors la famille $(u(\mathbf{e}_{k+1}), \ldots, u(\mathbf{e}_n))$ est une base du sous-espace $\mathrm{Im}(u)$, cf. exercice 2.4.15. On en déduit une formule très utile reliant les dimensions des sous-espaces $\mathrm{Ker}(u)$, $\mathrm{Im}(u)$ avec celle de E :

2.4.14 Théorème (La formule du rang).— Soient E un espace vectoriel de dimension finie et $u : E \longrightarrow E'$ une application linéaire à valeurs dans un espace vectoriel E'. Alors

$$\dim(E) = \dim(\mathrm{Ker}(u)) + \mathrm{rg}(u).$$

2.4.15 Exercice.— Soient E et E' des espaces vectoriels et $u : E \longrightarrow E'$ une application linéaire. On suppose que E est de dimension finie. D'après la proposition 2.3.7, il existe alors un supplémentaire F du sous-espace $\mathrm{Ker}(u)$ dans E.

Montrer que la restriction de l'application u à F

$$\begin{aligned} u_{|F} : F &\longrightarrow \mathrm{Im}(u) \\ \mathbf{x} &\longmapsto u(\mathbf{x}) \end{aligned}$$

est un isomorphisme de F sur $\mathrm{Im}(u)$.

On déduit du théorème 2.4.14, le résultat suivant :

2.4.16 Proposition.— Soit $u : E \longrightarrow E'$ une application linéaire entre deux $\mathbb{K}$-espaces vectoriel de même dimension finie. Les assertions suivantes sont équivalentes :

i) u est injective,

ii) u est surjective,

iii) u est bijective

iv) $\mathrm{Ker}(u) = \{\mathbf{0}\}$,

v) $\mathrm{Im}(u) = E'$,

vi) $\mathrm{rg}(u) = \dim(E)$.

2.4.17. Remarque.— Attention, ce résultat est faux en dimension infinie. En effet, l'application

$$\begin{aligned} u : \mathbb{R}[x] &\longrightarrow \mathbb{R}[x] \\ f(x) &\longmapsto f'(x) \end{aligned}$$

est un endomorphisme de $\mathbb{R}[x]$. Son noyau est le sous-espace vectoriel de $\mathbb{R}[x]$ formé des polynômes constants. L'endomorphisme u n'est donc pas injectif, alors qu'il est surjective. En effet $\mathrm{Im}(u) = \mathbb{R}[x]$, car, pour tout polynôme f de $\mathbb{R}[x]$, il existe un polynôme g défini par

$$g(x) = \int_0^x f(t)dt$$

tel que $u(g) = f$. Par exemple, si

$$f(x) = \sum_{i=0}^{n} a_i x^i,$$

on pose

$$g(x) = \sum_{i=0}^{n} \frac{a_i}{i+1} x^{i+1}.$$

On a alors $u(g) = f$.

2.4.18 Exercice.— Montrer que l'application

$$\begin{aligned} u : \mathbb{R}[x] &\longrightarrow \mathbb{R}[x] \\ f(x) &\longmapsto xf(x) \end{aligned}$$

est un endomorphisme injectif de $\mathbb{R}[x]$, mais pas surjectif.

§ 5 Projections sur un sous-espace

2.5.1. Les projecteurs.— Soit E un $\mathbb{K}$-espace vectoriel. Un endomorphisme p de E tel que $p^2 = p$ est appelé *projecteur* de E.

Soient F et G deux sous-espaces vectoriels de E tels que $E = F \oplus G$. Alors tout vecteur $\mathbf{x}$ de E s'écrit de façon unique en $\mathbf{x} = \mathbf{y}+\mathbf{z}$, avec $\mathbf{y} \in F$ et $\mathbf{z} \in G$. On considère l'endomorphisme p_F de E défini par $p_F(\mathbf{x}) = \mathbf{y}$. On dit que p_F est la *projection sur F parallèlement à G*. On définit de la même façon, la *projection sur G parallèlement à F*, comme l'endomorphisme p_G de E défini par $p_G(\mathbf{x}) = \mathbf{z}$. Pour tout vecteur $\mathbf{x}$ de E, on a

$$\mathbf{x} = p_F(\mathbf{x}) + p_G(\mathbf{x}).$$

Ainsi définis, les endomorphismes p_F et p_G vérifient les assertions suivantes

i) p_F et p_G sont des projecteurs, *i.e.*, $p_F^2 = p_F$ et $p_G^2 = p_G$,

ii) $\mathrm{Im}(p_F) = F$ et $\mathrm{Im}(p_G) = F$,

iii) $\mathrm{Ker}(p_F) = G$ et $\mathrm{Ker}(p_G) = F$.

iv) $p_F + p_G = \mathrm{Id}_E$,

v) $p_F p_G = p_G p_F = 0$.

L'assertion **i)** découle de la définition de p_F et p_G. Si $\mathbf{x} \in E$, alors $p_F(\mathbf{x})$ est un vecteur de F d'où $p_F(p_F(\mathbf{x})) = p_F(\mathbf{x}) + \mathbf{0}$. On montre de la même façon que $p_G^2 = p_G$. L'assertion **ii)** est une conséquence immédiate de la définition de p_F et p_G.

Pour montrer **iii)**, considérons $\mathbf{x} \in \mathrm{Ker}(p_F)$, alors $\mathbf{x} = p_G(\mathbf{x})$ donc $\mathbf{x} \in G$. Inversement, si $\mathbf{x} \in G$, on a $p_F(\mathbf{x}) = \mathbf{0}$. On montre de la même façon que $\mathrm{Ker}(p_G) = F$.

L'assertion **iv)** correspond à la décomposition $\mathbf{x} = p_F(\mathbf{x}) + p_G(\mathbf{x})$. L'assertion **v)** est obtenue en composant la relation $\mathrm{Id}_E = p_F + p_G$ par p_F et p_G.

Inversement, supposons qu'il existe deux applications linéaires

$$p : E \longrightarrow F, \quad q : E \longrightarrow G,$$

telles que $\mathrm{Id}_E = p + q$ et $pq = qp = 0$. On montre alors que $E = F \oplus G$. Plus généralement, on a :

2.5.2 Proposition. — Soit E un $\mathbb{K}$-espace vectoriel et soient $E_1, \ldots, E_k$ des sous-espaces vectoriel de E. Une condition nécessaire et suffisante pour que $E = E_1 \oplus \ldots \oplus E_k$ est qu'il existe des applications linéaires $p_i : E \longrightarrow E_i$, $i \in [\![1, k]\!]$ vérifiant les deux assertions suivantes :

i) $\mathrm{Id}_E = p_1 + \ldots + p_k$,

ii) $p_i p_j = 0$, pour tout $i \neq j$.

Pour tout $i \in [\![1, k]\!]$, p_i est appelé la projection sur le sous-espace E_i parallèlement au sous-espace $\bigoplus_{\substack{j=1 \\ j \neq i}}^{k} E_j$.

Les projection p_i sont des projecteurs, $p_i^2 = p_i$, et satisfont

$$\mathrm{Ker}(p_i) = \bigoplus_{\substack{j=1 \\ j \neq i}}^{k} E_j, \qquad \mathrm{Im}(p_i) = E_i.$$

2.5.3 Exercice. — Établir les deux propriétés précédentes.

2.5.4 Exercice. — Soit E un $\mathbb{K}$-espace vectoriel et soient p et q deux projecteurs de E. On suppose que le corps $\mathbb{K}$ n'est pas de caractéristique 2.

1. Montrer que $p+q$ est un projecteur si, et seulement si, $p \circ q = q \circ p = 0$.
2. Supposons que $p+q$ est un projecteur de E. Montrer l'égalité :

$$\mathrm{Im}(p+q) = \mathrm{Im}(p) + \mathrm{Im}(q).$$

3. Supposons que $p+q$ est un projecteur de E. Montrer l'égalité :

$$\mathrm{Ker}(p+q) = \mathrm{Ker}(p) \cap \mathrm{Ker}(q).$$

2.5.5 Exercice.— Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n et soient p et q deux endomorphismes de E vérifiant

$$p+q = \mathrm{Id}_E, \quad \text{et} \quad \mathrm{rg}(p) + \mathrm{rg}(q) \leq n.$$

1. Montrer que $\mathrm{Im}(p)$ et $\mathrm{Im}(q)$ sont supplémentaires dans E.
2. Montrer que $\mathrm{rg}(p) + \mathrm{rg}(q) = n$.
3. Montrer que p et q sont des projecteurs.

2.5.6 Exercice.— Soit p un projecteur d'un $\mathbb{K}$-espace vectoriel E.

1. Montrer que $E = \mathrm{Ker}(p) \oplus \mathrm{Im}(p)$.
2. La réciproque est-elle vraie ?

2.5.7 Exercice.— Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Montrer que si p est un projecteur de E, alors

$$\mathrm{rang}(p) = \mathrm{trace}(p).$$

§ 6 Exercices

2.6.1 Exercice.— Soient E un $\mathbb{K}$-espace vectoriel et u un endomorphisme de E. Montrer que u est une homothétie si, et seulement si, pour tout vecteur $\mathbf{x}$ de E, la famille $(\mathbf{x}, u(\mathbf{x}))$ est liée.

2.6.2 Exercice.— Soit E un $\mathbb{K}$-espace vectoriel, pas nécessairement de dimension finie et soit u un endomorphisme de E.

1. Montrer que $\mathrm{Ker}(u) \subseteq \mathrm{Ker}(u^2)$ et $\mathrm{Im}(u^2) \subseteq \mathrm{Im}(u)$.
2. Montrer que $\mathrm{Ker}(u) = \mathrm{Ker}(u^2)$ si, et seulement si, $\mathrm{Ker}(u) \cap \mathrm{Im}(u) = \{\mathbf{0}\}$.
3. Montrer que $\mathrm{Im}(u) = \mathrm{Im}(u^2)$ si, et seulement si, $E = \mathrm{Ker}(u) + \mathrm{Im}(u)$.

2.6.3 Exercice.— Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et soit u un endomorphisme de E. D'après le théorème du rang, on a l'égalité

$$\dim(E) = \dim(\mathrm{Ker}(u)) + \dim(\mathrm{Im}(u)).$$

Ce qui n'entraîne pas en général que $E = \mathrm{Ker}(u) \oplus \mathrm{Im}(u)$.

1. Soit u l'endomorphisme de $\mathbb{R}^3$ dont la matrice dans la base canonique est

$$[u]_{can} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

Déterminer $\mathrm{Ker}(u)$, $\mathrm{Ker}(u^2)$, $\mathrm{Im}(u)$, $\mathrm{Im}(u^2)$.

2. Montrer que les assertions suivantes sont équivalentes

a) $E = \mathrm{Ker}(u) \oplus \mathrm{Im}(u)$,

b) $E = \mathrm{Ker}(u) + \mathrm{Im}(u)$

c) $\mathrm{Im}(u) = \mathrm{Im}(u^2)$,

d) $\mathrm{rg}(u) = \mathrm{rg}(u^2)$

e) $\mathrm{Ker}(u) = \mathrm{Ker}(u^2)$,

f) $\mathrm{Ker}(u) \cap \mathrm{Im}(u) = \{\mathbf{0}\}$

2.6.4 Exercice.— Soit u un endomorphisme d'un espace vectoriel E de dimension finie n. Montrer que les deux assertions suivantes sont équivalentes

a) $\mathrm{Ker}(u) = \mathrm{Im}(u)$,

b) $u^2 = 0$ et $n = 2.\mathrm{rg}(u)$.

2.6.5 Exercice.— Soient E, F et G trois $\mathbb{K}$-espaces vectoriels et $u : E \longrightarrow F$, $v : F \longrightarrow G$ deux applications linéaires.

1. Montrer que $u(\mathrm{Ker}(v \circ u)) = \mathrm{Ker}(v) \cap \mathrm{Im}(u)$.

2. Montrer que $v^{-1}(\mathrm{Im}(v \circ u)) = \mathrm{Ker}(v) + \mathrm{Im}(u)$.

CHAPITRE
3

Les matrices

Sommaire

§ 1 Définitions

3.1.1. Définitions.— Soient m et n deux entiers naturels non nuls. Une famille $(a^i_j)^{1\leq i\leq n}_{1\leq j\leq m}$, où, pour tous entiers i et j, a^i_j est un scalaire dans $\mathbb{K}$, est appelée une *matrice* de type (m, n) à coefficients dans $\mathbb{K}$.

S'il n'y a pas de confusion, une telle matrice sera notée $[a^i_j]$ et représentée par un tableau de scalaires à n colonnes et m lignes :

$$\begin{bmatrix} a^1_1 & a^2_1 & \cdots & a^n_1 \\ a^1_2 & a^2_2 & \cdots & a^n_2 \\ \vdots & \vdots & & \vdots \\ a^1_m & a^2_m & \cdots & a^n_m \end{bmatrix}$$

On note $\mathcal{M}_{m,n}(\mathbb{K})$ l'ensemble des matrices carrées de type (m, n) à coefficients dans $\mathbb{K}$. Si

$\mathbf{A} \in \mathcal{M}_{m,n}(\mathbb{K})$, on notera $\mathbf{A}^i_j$, le coefficient de $\mathbf{A}$ de la j-ième ligne de la i-ième colonne :

$$\mathbf{A} = \begin{array}{cc} \begin{array}{ccc} & i & \\ \end{array} & \\ \begin{bmatrix} & \vdots & \\ & \mathbf{A}^i_j & \cdots \\ & & \end{bmatrix} & j \end{array}$$

Une matrice de type (n, n) est dite *carrée*. On note $\mathcal{M}_n(\mathbb{K})$ l'ensemble des matrices carrées de type (n, n). Une matrice de type $(m, 1)$ est dite *colonne* et une matrice de type $(1, n)$ est dite *ligne*.

La *diagonale* d'une matrice carrée $\mathbf{A} = [a^i_j]$ de type (n, n) est formée des coefficients a^i_i, pour $i \in [\![1, n]\!]$; on note

$$\operatorname{diag}(\mathbf{A}) = (a^1_1, a^2_2, \ldots, a^n_n).$$

Une matrice est dite *diagonale* , si tous ses coefficients non diagonaux sont nuls, *i.e.*, $a^j_i = 0$, pour tout $i \neq j$. On notera

$$\mathbf{Diag}\,(a_1, \ldots, a_n) = \begin{bmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & a_n \end{bmatrix}.$$

La *matrice identité* de $\mathcal{M}_n(\mathbb{K})$ est la matrice diagonale $\mathbf{1}_n$, où tous les éléments de la diagonale sont égaux à 1 :

$$\mathbf{1}_n = \mathbf{Diag}\,(1, \ldots, 1).$$

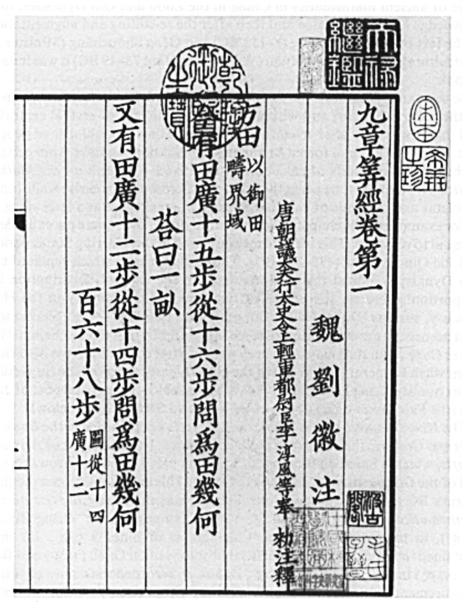


FIGURE 3.1 – Les Neuf Chapitres sur l'art mathématique (IIe siècle av. J.-C.)

Le calcul algébrique sur les matrices se développa à partir du début du XIXe *siècle. Les matrices sont alors utilisées pour la résolution d'équations linéaires. La notion de* ≪ *tableau de nombres* ≫ *pour noter un ensemble de données d'un système linéaire apparaît dès le* IIe *siècle av. J.-C. dans le texte mathématique chinois* ≪ Les Neuf Chapitres sur l'art mathématique ≫.

3.1.2. Matrices triangulaires.— Une matrice est dite *triangulaire supérieure* (resp. *triangulaire inférieure*), si tous ses coefficients en dessous (resp. au dessus) de la diagonale sont nuls, *i.e.*, $a^i_j = 0$, pour tout $j > i$ (resp. $i < j$). Une matrice triangulaire supérieure (resp. inférieure) sera notée

$$\begin{bmatrix} * & * & \dots & * \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & * \end{bmatrix} \quad \text{(resp. } \begin{bmatrix} * & 0 & \dots & 0 \\ * & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ * & \dots & * & * \end{bmatrix}\text{)}.$$

3.1.3. Matrices élémentaires.— Les *matrices élémentaires* de $\mathcal{M}_{m,n}(\mathbb{K})$ sont les matrices $\mathbf{e}_{(i,j)}$, où $(\mathbf{e}_{(i,j)})^l_k$ égale 1 si $k = j$ et $l = i$ et 0 sinon :

$$\mathbf{e}_{(i,j)} = \begin{array}{cc} \begin{matrix} & & i & & \end{matrix} & \\ \begin{bmatrix} 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{bmatrix} & \begin{matrix} \\ \\ j \\ \\ \\ \end{matrix} \end{array}$$

3.1.4. Espace vectoriel des matrices.— Soient m et n deux entiers naturels non nuls. On définit sur l'ensemble $\mathcal{M}_{m,n}(\mathbb{K})$ les opération

i) d'*addition*, pour toutes matrices $\mathbf{A} = [a^i_j]$ et $\mathbf{B} = [b^i_j]$ de $\mathcal{M}_{m,n}(\mathbb{K})$,

$$\mathbf{A} + \mathbf{B} = [a^i_j + b^i_j].$$

ii) la multiplication par un scalaire, pour toute matrice $\mathbf{A} = [a^j_i]$ de $\mathcal{M}_{m,n}(\mathbb{K})$ et tout scalaire α de $\mathbb{K}$,

$$\alpha\mathbf{A} = [\alpha a^i_j].$$

3.1.5 Proposition.— Muni de l'addition et de la multiplication par un scalaire l'ensemble $\mathcal{M}_{m,n}(\mathbb{K})$ des matrices de type (m, n) forme un $\mathbb{K}$-espace vectoriel de dimension mn.

La famille des mn matrices élémentaires

$$\{\mathbf{e}_{(i,j)} \quad | \quad i \in [\![1, n]\!],\ j \in [\![1, m]\!]\}$$

de $\mathcal{M}_{m,n}(\mathbb{K})$ forme une base canonique du $\mathbb{K}$-espace vectoriel $\mathcal{M}_{m,n}(\mathbb{K})$.

3.1.6. Sous-espaces vectoriels remarquables de $\mathcal{M}_{m,n}(\mathbb{K})$.— L'ensemble des matrices diagonales de $\mathcal{M}_n(\mathbb{K})$ forme un sous-espace vectoriel de dimension n.

L'ensemble des matrices triangulaires supérieures (resp. inférieures) de $\mathcal{M}_n(\mathbb{K})$ forme un sous-espace vectoriel de dimension $n(n+1)/2$.

3.1.7. Transposition.— La matrice *transposée* d'une matrice $\mathbf{A}$ de $\mathcal{M}_{m,n}(\mathbb{K})$ est la matrice de $\mathcal{M}_{n,m}(\mathbb{K})$, notée $\mathbf{A}^\top$ définie par

$$(\mathbf{A}^\top)^i_j = \mathbf{A}^j_i,$$

pour tous $i \in [\![1, n]\!]$ et $j \in [\![1, m]\!]$. Pour toute matrice $\mathbf{A}$, on a

$$(\mathbf{A}^\top)^\top = \mathbf{A}.$$

La transposition est une application linéaire

$$\begin{aligned} {}^\top : \mathcal{M}_{m,n}(\mathbb{K}) &\longrightarrow \mathcal{M}_{n,m}(\mathbb{K}) \\ \mathbf{A} &\longmapsto \mathbf{A}^\top \end{aligned}$$

On vérifie que pour toutes matrices $\mathbf{A}$, $\mathbf{B}$ et scalaire λ, on a

i) $(\mathbf{A} + \mathbf{B})^\top = \mathbf{A}^\top + \mathbf{B}^\top$,

ii) $(\lambda\mathbf{A})^\top = \lambda\mathbf{A}^\top$.

3.1.8 Exercice.— Établir ces relations.

3.1.9. Matrices symétriques et antisymétrique.— Une matrice carrée s est dite *symétrique* si $\mathrm{s}^\top = \mathrm{s}$. Une matrice carrée $\mathbf{A}$ est dite *antisymétrique* si $\mathbf{A}^\top = -\mathbf{A}$.

On note $\mathcal{S}_n(\mathbb{K})$ (resp. $\mathcal{A}_n(\mathbb{K})$) le sous-ensemble de $\mathcal{M}_n(\mathbb{K})$ formé des matrices symétriques (resp. antisymétriques).

3.1.10 Proposition.— Les sous-ensembles $\mathcal{S}_n(\mathbb{K})$ et $\mathcal{A}_n(\mathbb{K})$ forment des sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{K})$, avec

$$\dim(\mathcal{A}_n(\mathbb{K})) = \frac{n^2 - n}{2}, \quad \dim(\mathcal{S}_n(\mathbb{K})) = \frac{n^2 + n}{2}.$$

De plus, on a

$$\mathcal{M}_n(\mathbb{K}) = \mathcal{A}_n(\mathbb{K}) \oplus \mathcal{S}_n(\mathbb{K})$$

3.1.11 Exercice.— Soit $u : \mathcal{M}_n(\mathbb{R}) \longrightarrow \mathcal{M}_n(\mathbb{R})$ l'application définie par

$$u(\mathbf{A}) = \mathbf{A} + \mathbf{A}^\top,$$

pour tout $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$.

1. Montrer que l'application u est un endomorphisme de $\mathcal{M}_n(\mathbb{R})$.
2. Déterminer le noyau de u.
3. Déterminer l'image de u.
4. Montrer que $\mathcal{M}_n(\mathbb{R}) = \mathrm{Ker}(u) \oplus \mathrm{Im}(u)$.

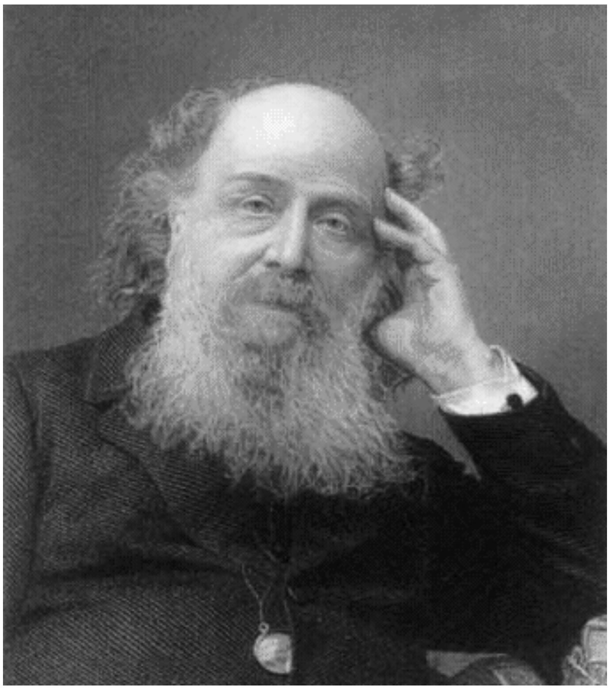


FIGURE 3.2 – James Joseph Sylvester (1814 - 1897)

Joseph Sylvester est un mathématicien anglais. Il introduit en 1851 le terme de matrice dans ses travaux géométriques. Il publie plusieurs mémoires dans lesquels il traduit des propriétés géométriques en terme de calcul de déterminant. Sylvester entretiendra une collaboration mathématique fructueuse avec le mathématicien Arthur Cayley. Ils travaillent notamment sur les invariants des formes quadratiques et les déterminants.

§ 2 Produit de matrices

3.2.1. Produit de matrices.— On définit le *produit* (ou *multiplication*) d'une matrice $\mathbf{A}$ de type (m,n) par une matrice $\mathbf{B}$ de type (n,p), comme la matrice

$$\mathbf{AB} = [c_i^j], \quad \text{avec} \quad c_i^j = \sum_{k=1}^{n} a_i^k b_k^j.$$

Le produit de matrices vérifie les propriétés suivantes :

i) (associativité) pour toute matrices compatibles, $\mathbf{A}$, $\mathbf{B}$ et $\mathbf{C}$,

$$\mathbf{A}(\mathbf{BC}) = (\mathbf{AB})\mathbf{C}.$$

ii) (matrices unitées) pour toute matrice $\mathbf{A}$ de $\mathcal{M}_{m,n}(\mathbb{K})$,

$$\mathbf{1}_m\mathbf{A} = \mathbf{A} = \mathbf{A}\mathbf{1}_n.$$

iii) (distributivité), pour toutes matrices compatibles $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ et $\mathbf{D}$, on a

$$\mathbf{A}(\mathbf{B}+\mathbf{C}) = \mathbf{AB}+\mathbf{AC}, \qquad (\mathbf{B}+\mathbf{C})\mathbf{D} = \mathbf{BD}+\mathbf{CD}.$$

On en déduit que

3.2.2 Proposition. — L'ensemble $\mathcal{M}_n(\mathbb{K})$ des matrices carrées de type (n, n), muni de l'addition et de la multiplication, forme un anneau non commutatif.

L'unité de l'anneau est la matrice identité $\mathbf{1}_n$.

3.2.3 Exercice. — Montrer que l'anneau $\mathcal{M}_n(\mathbb{K})$ n'est pas commutatif pour $n \geq 2$.

3.2.4 Exercice. — Montrer que, pour toutes matrices compatibles $\mathbf{A}$ et $\mathbf{B}$, on a

$$(\mathbf{AB})^\top = \mathbf{B}^\top \mathbf{A}^\top.$$

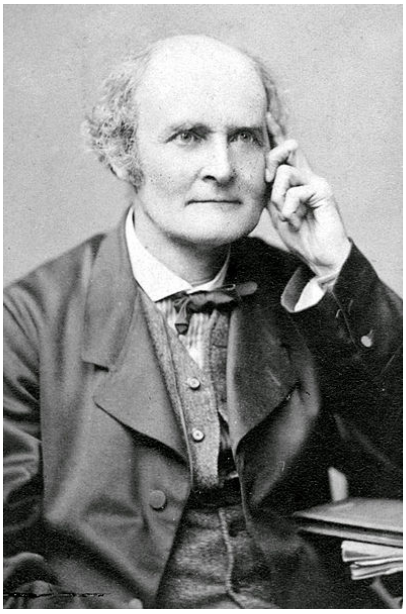


FIGURE 3.3 – Arthur Cayley (1821 - 1895)

Arthur Cayley est un mathématicien anglais auteur de nombreux travaux. Dans un article de 1855 publié dans le Journal de Crelle, il utilise la notion de matrice pour représenter des systèmes d'équations linéaires et des formes quadratiques. Les problèmes géométriques, comme les types d'intersection de coniques ou quadriques, exprimés en terme de déterminant, sont à l'origine de l'intérêt de Cayley pour la notion de matrice. Ses travaux sur les matrices conduisent à un mémoire intitulé « A memoir on the Theory of Matrices », publié en 1858 dans Philosophical Transactions of the Royal Society of London *dans lequel la notion de matrice fait l'objet d'une étude théorique indépendamment du contexte géométrique dans lequels elles apparaissent jusqu'alors.*

Ce mémoire conporte des résultats importants, en particulier, il formule le théorème dit de Cayley-Hamilton pour les matrices carrées d'ordre 3 sans toutefois en publier de preuve

3.2.5 Exercice.— Soient

$$\mathbf{B} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 5 & 0 & 1 \end{bmatrix}$$

et $\mathbf{A}$ des matrices de $\mathcal{M}_3(\mathbb{R})$. Décrire les lignes de la matrice $\mathbf{bA}$ en terme des lignes de $\mathbf{A}$ et les colonnes de la matrice $\mathbf{Ab}$ en terme des colonnes de $\mathbf{A}$.

3.2.6 Exercice.— Soit $\mathbf{e}_i$ le vecteur colonne de $\mathcal{M}_{n,1}(\mathbb{K})$ contenant 1 à la i-ième ligne et 0 sur les autres lignes. Étant donnée une matrice $\mathbf{A}$ de $\mathcal{M}_n(\mathbb{K})$, décrire les produits suivants :

$$\mathbf{Ae}_i, \qquad \mathbf{e}_i^\top \mathbf{A}, \qquad \mathbf{e}_i^\top \mathbf{A}\mathbf{e}_j.$$

3.2.7 Exercice.— Soient $\mathbf{A}$ et $\mathbf{B}$ deux matrices de $\mathcal{M}_{n,m}(\mathbb{K})$. Montrer que si $\mathbf{Ax} = \mathbf{Bx}$, pour tout vecteur colonne $\mathbf{x}$, alors $\mathbf{A} = \mathbf{B}$.

3.2.8 Exercice.— Soit

$$\mathbf{A} = \begin{bmatrix} 1/2 & a \\ 0 & 1/2 \end{bmatrix}$$

une matrice à coefficients réels.

1. Calculer $\mathbf{A}^2$, $\mathbf{A}^3$ et $\mathbf{A}^4$.
2. Donner l'expression de $\mathbf{A}^k$, pour tout entier naturel k.

3.2.9 Exercice.— Soient $\mathbf{T}$ et $\mathbf{T}'$ deux matrices triangulaires supérieures.

1. Montrer que le produit $\mathbf{TT}'$ est une matrice triangulaire supérieure.
2. Déterminer la diagonale de la matrice $\mathbf{TT}'$.

3.2.10 Exercice.— Soient $\mathbf{A}$ et $\mathbf{B}$ deux matrices symétriques de $\mathcal{M}_n(\mathbb{K})$ qui commutent, *i.e.*, $\mathbf{AB} = \mathbf{BA}$. Montrer que le produit $\mathbf{AB}$ est une matrice symétrique.

3.2.11. Matrices nilpotentes.— Une matrice $\mathbf{A}$ de $\mathcal{M}_n(\mathbb{K})$ est dite *nilpotente*, s'il existe un entier naturel q tel que $\mathbf{A}^q = 0$. Le plus petit entier non nul r tel que $\mathbf{A}^r = 0$ est appelé l'*indice de nilpotence* de $\mathbf{A}$.

3.2.12. Exemples.— Toute matrice nulle est nilpotente d'indice de nilpotence 1. Les matrices suivantes

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

sont nilpotentes d'indice de nilpotence 2, 3, 3, 3 et 4 respectivement.

3.2.13. Matrices inversibles.— Une matrice carrée $\mathbf{A}$ de $\mathcal{M}_n(\mathbb{K})$ est dite *inversible*, s'il existe une matrice $\mathbf{B}$ de $\mathcal{M}_n(\mathbb{K})$ telle que

$$\mathbf{AB} = \mathbf{1}_n \quad \text{et} \quad \mathbf{BA} = \mathbf{1}_n.$$

La matrice $\mathbf{B}$ est alors appelée la *matrice inverse* de $\mathbf{A}$, on note alors $\mathbf{B} = \mathbf{A}^{-1}$. On déduit immédiatement de cette définition que l'inverse d'une matrice est unique.

L'opération d'inversion vérifie les propriétés suivantes :

i) si $\mathbf{A}$ est inversible, $(\mathbf{A}^{-1})^{-1} = \mathbf{A}$,

ii) si $\mathbf{A}$ et $\mathbf{B}$ sont inversibles, alors $\mathbf{AB}$ est inversible et

$$(\mathbf{AB})^{-1} = \mathbf{B}^{-1}\mathbf{A}^{-1},$$

iii) si $\mathbf{A}$ est inversible, alors sa transposée est inversible et

$$(\mathbf{A}^{\top})^{-1} = (\mathbf{A}^{-1})^{\top}.$$

3.2.14 Exercice. — Montrer ces trois propriétés.

On désigne par $\mathrm{GL}_n(\mathbb{K})$ l'ensemble des matrices inversibles de $\mathcal{M}_n(\mathbb{K})$:

$$\mathrm{GL}_n(\mathbb{K}) = \{\mathbf{A} \in \mathcal{M}_n(\mathbb{K}) \mid \mathbf{A} \text{ est inversible}\}.$$

3.2.15 Proposition. — La multiplication des matrices munit l'ensemble $\mathrm{GL}_n(\mathbb{K})$ des matrices inversibles de $\mathcal{M}_n(\mathbb{K})$ d'une structure de groupe.

Le groupe $\mathrm{GL}_n(\mathbb{K})$, est appelé le *groupe linéaire* des matrices d'ordre n.

3.2.16. Calcul de l'inverse. — Déterminer si une matrice est inversible et le calcul des inverses sont des problèmes importants d'algèbre linéaire. Par exemple, considérons la matrice suivante de $\mathcal{M}_3(\mathbb{R})$

$$\mathbf{A} = \begin{bmatrix} 1 & 1 & 3 \\ 2 & 0 & 1 \\ 1 & 1 & 2 \end{bmatrix}.$$

La matrice $\mathbf{A}$ est-elle inversible ? L'équation matricielle suivante dans $\mathbb{R}^3$:

$$\mathbf{Ax} = \mathbf{b} \quad \text{avec} \quad \mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \quad \text{et } \mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

peut s'écrire sous la forme du système d'équations suivant

$$\left|\begin{array}{lcl} x_1 + x_2 + 3x_3 &=& b_1 \\ 2x_1 + x_3 &=& b_2 \\ x_1 + x_2 + 2x_3 &=& b_3 \end{array}\right.$$

Pour résoudre ce systèmes, *i.e.*, exprimer les coefficients du vecteur $\mathbf{x}$ en terme de ceux du vecteur $\mathbf{b}$ on procède en appliquant des opérations sur les lignes. Retranchons 3 fois la seconde équation à la première et 2 fois à la dernière, le système devient :

$$\left|\begin{array}{lcl} -5x_1 + x_2 &=& b_1 - 3b_2 \\ 2x_1 + x_3 &=& b_2 \\ -3x_1 + x_2 &=& -2b_2 + b_3 \end{array}\right.$$

Retranchons la dernière équation à la première, on obtient :

$$\left|\begin{array}{lcl} -2x_1 &=& b_1 - b_2 - b_3 \\ 2x_1 + x_3 &=& b_2 \\ -3x_1 + x_2 &=& -2b_2 + b_3 \end{array}\right.$$

On additionne la première équation à la seconde et on retranche $\frac{3}{2}$ de la première à la troisième, il reste :

$$\left|\begin{array}{lll} -2x_1 & = & b_1 - b_2 - b_3 \\ x_3 & = & b_1 - b_3 \\ x_2 & = & -\frac{3}{2}b_1 - \frac{1}{2}b_2 + \frac{5}{2}b_3 \end{array}\right.$$

On obtient ainsi le système

$$\left|\begin{array}{lll} x_1 & = & -\frac{1}{2}b_1 + \frac{1}{2}b_2 + \frac{1}{2}b_3 \\ x_2 & = & -\frac{3}{2}b_1 - \frac{1}{2}b_2 + \frac{5}{2}b_3 \\ x_3 & = & b_1 - b_3 \end{array}\right.$$

L'équation $\mathbf{Ax} = \mathbf{b}$ admet une unique solution $\mathbf{x}$ donnée par le système précédent, ce qui s'écrit matriciellement sous la forme

$$\mathbf{x} = \mathbf{A}^{-1}\mathbf{b},$$

avec

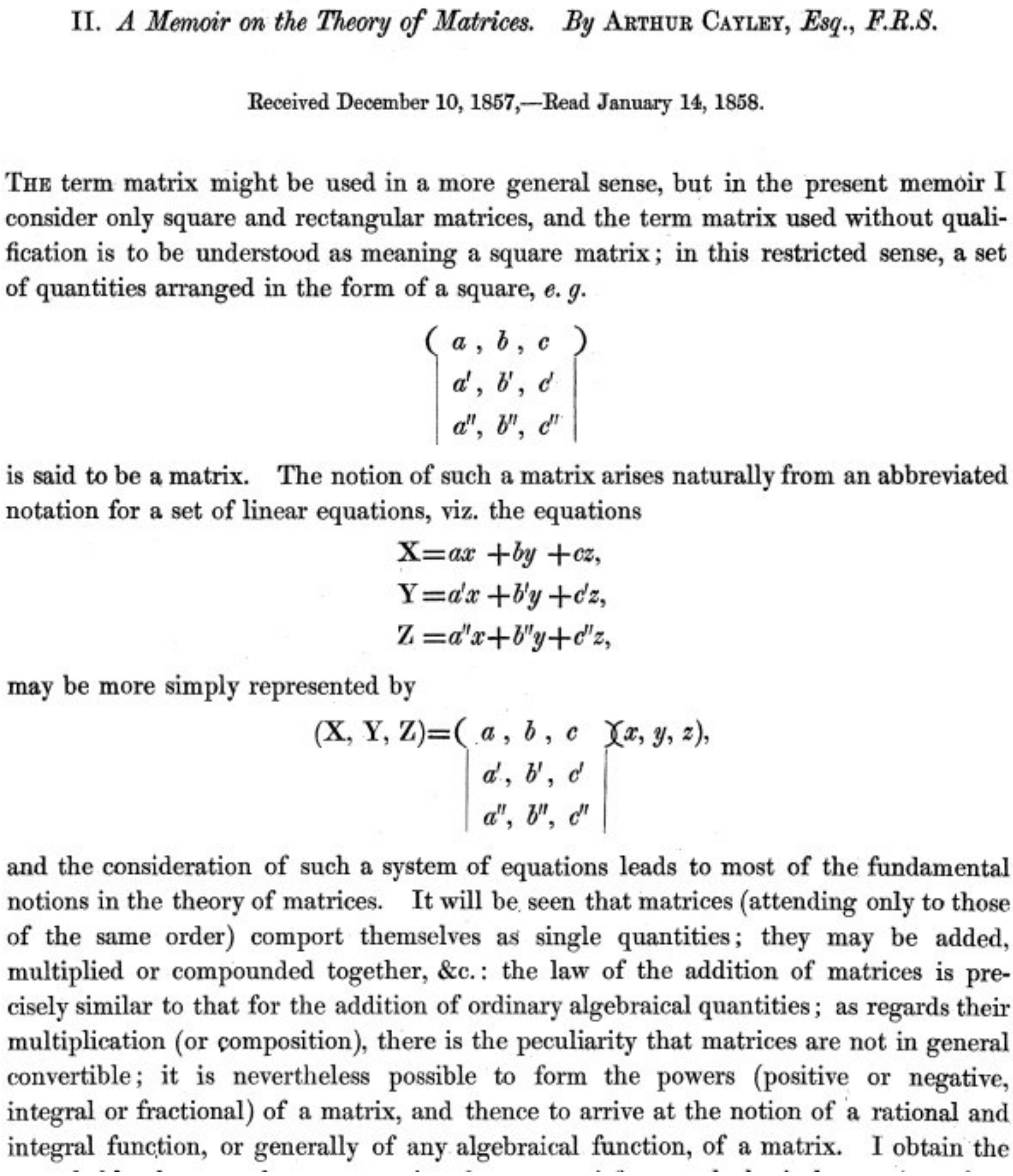
$$\mathbf{A}^{-1} = \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ -\frac{3}{2} & -\frac{1}{2} & \frac{5}{2} \\ 1 & 0 & -1 \end{bmatrix}.$$

On vérifie que $\mathbf{AA}^{-1} = \mathbf{A}^{-1}\mathbf{A} = \mathbf{1}_n$, la matrice $\mathbf{A}$ est donc inversible. Cet exemple illustre le calcul de l'inverse d'une matrice en effectuant la résolution d'un système linéaire à seconds membres. On notera cependant, que les matrices carrées ne sont pas toujours inversibles. Nous verrons plus loin d'autres méthodes permettant de déterminer si une matrice est inversible et de calculer l'inverse d'une matrice.

3.2.17 Exercice.— Montrer que les matrices suivantes ne sont pas inversibles

$$\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \qquad \mathbf{B} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \qquad \mathbf{C} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 7 \\ 1 & 1 & 2 \end{bmatrix}.$$

3.2.18 Exercice.— Soit $\mathbf{A}$ un matrice de $\mathcal{M}_n(\mathbb{K})$ telle que $\mathbf{A}^2$ est inversible. Montrer que $\mathbf{A}$ est inversible.



II. *A Memoir on the Theory of Matrices.* *By* ARTHUR CAYLEY, *Esq., F.R.S.*

Received December 10, 1857,—Read January 14, 1858.

THE term matrix might be used in a more general sense, but in the present memoir I consider only square and rectangular matrices, and the term matrix used without qualification is to be understood as meaning a square matrix; in this restricted sense, a set of quantities arranged in the form of a square, *e. g.*

$$\begin{pmatrix} a\ , & b\ , & c \\ a'\ , & b'\ , & c' \\ a''\ , & b''\ , & c'' \end{pmatrix}$$

is said to be a matrix. The notion of such a matrix arises naturally from an abbreviated notation for a set of linear equations, viz. the equations

$$\begin{aligned} \mathrm{X} &= ax + by + cz, \\ \mathrm{Y} &= a'x + b'y + c'z, \\ \mathrm{Z} &= a''x + b''y + c''z, \end{aligned}$$

may be more simply represented by

$$(\mathrm{X}, \mathrm{Y}, \mathrm{Z}) = \begin{pmatrix} a\ , & b\ , & c \\ a'\ , & b'\ , & c' \\ a''\ , & b''\ , & c'' \end{pmatrix}(x, y, z),$$

and the consideration of such a system of equations leads to most of the fundamental notions in the theory of matrices. It will be seen that matrices (attending only to those of the same order) comport themselves as single quantities; they may be added, multiplied or compounded together, &c.: the law of the addition of matrices is precisely similar to that for the addition of ordinary algebraical quantities; as regards their multiplication (or composition), there is the peculiarity that matrices are not in general convertible; it is nevertheless possible to form the powers (positive or negative, integral or fractional) of a matrix, and thence to arrive at the notion of a rational and integral function, or generally of any algebraical function, of a matrix. I obtain the

FIGURE 3.4 – A Memoir on the Theory of Matrices

§ 3 Matrice d'une application linéaire

Soient E et E' deux $\mathbb{K}$-espaces vectoriel de dimensions n et m respectivement. Considérons une base $\mathcal{B} = (\mathbf{e}_1, \ldots, \mathbf{e}_n)$ de E et une base $\mathcal{B}' = (\mathbf{f}_1, \ldots, \mathbf{f}_m)$ de E'.

Soit $u : E \longrightarrow E'$ une application linéaire. On peut exprimer l'image par u de chaque vecteur de la base $\mathcal{B}$ dans la base $\mathcal{B}'$, on a :

$$\begin{aligned} u(\mathbf{e}_1) &= a_1^1\mathbf{f}_1 + a_2^1\mathbf{f}_2 + \cdots + a_m^1\mathbf{f}_m, \\ u(\mathbf{e}_2) &= a_1^2\mathbf{f}_1 + a_2^2\mathbf{f}_2 + \cdots + a_m^2\mathbf{f}_m, \\ \cdots & \\ u(\mathbf{e}_n) &= a_1^n\mathbf{f}_1 + a_2^n\mathbf{f}_2 + \cdots + a_m^n\mathbf{f}_m, \end{aligned}$$

avec $a_j^i \in \mathbb{K}$. La matrice

$$[a_j^i]_{1\leq j\leq m}^{1\leq i\leq n}$$

est appelée la *matrice de l'application linéaire* u exprimée dans les bases $\mathcal{B}$ et $\mathcal{B}'$, on la notera

$$[u]_{\mathcal{B}}^{\mathcal{B}'}.$$

En résumé :

$$[u]_{\mathcal{B}}^{\mathcal{B}'} = \begin{array}{c} \begin{array}{cccc} u(\mathbf{e}_1) & u(\mathbf{e}_2) & \cdots & u(\mathbf{e}_n) \end{array} \\ \left[\begin{array}{cccc} a_1^1 & a_1^2 & \cdots & a_1^n \\ a_2^1 & a_2^2 & \cdots & a_2^n \\ \vdots & \vdots & & \vdots \\ a_m^1 & a_m^2 & \cdots & a_m^n \end{array}\right] \begin{array}{c} \mathbf{f}_1 \\ \mathbf{f}_2 \\ \vdots \\ \mathbf{f}_m \end{array} \end{array}.$$

Pour un endomorphisme $u : E \longrightarrow E$ de E et $\mathcal{B}$ une base de E, nous noterons $[u]_{\mathcal{B}}$ la matrice $[u]_{\mathcal{B}}^{\mathcal{B}}$.

3.3.1. Exemple.— Soit p l'application linéaire de $\mathbb{R}^3$ dans $\mathbb{R}^3$ qui envoie un vecteur $\mathbf{x}$, sur sa projection orthogonale $p(\mathbf{x})$ sur le plan (Oxy) :

$$\begin{aligned} p : \mathbb{R}^3 &\longrightarrow \mathbb{R}^3 \\ \begin{bmatrix} x \\ y \\ z \end{bmatrix} &\longmapsto \begin{bmatrix} x \\ y \\ 0 \end{bmatrix}. \end{aligned}$$

On considère la base de $\mathbb{R}^3$ donnée par

$$\mathcal{B} = \left\{ \mathbf{e}_1 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \quad \mathbf{e}_2 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \quad \mathbf{e}_3 = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} \right\}$$

On a

$$p(\mathbf{e}_1) = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \mathbf{e}_2, \quad p(\mathbf{e}_2) = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \mathbf{e}_2, \quad p(\mathbf{e}_3) = \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix} = -3\mathbf{e}_1 + 3\mathbf{e}_2 + \mathbf{e}_3.$$

Ainsi, la matrice de l'application p, exprimée dans la base $\mathcal{B}$ de $\mathbb{R}^3$, est

$$[p]_{\mathcal{B}} = \begin{bmatrix} 0 & 0 & -3 \\ 1 & 1 & 3 \\ 0 & 0 & 1 \end{bmatrix}.$$

3.3.2 Proposition.— Soient E et E' deux $\mathbb{K}$-espaces vectoriels de dimension finie respectives n et m. L'application $\Phi : \mathcal{L}(E, E') \longrightarrow \mathcal{M}_{m,n}(\mathbb{K})$ définie par

$$\Phi(u) = [u]_{\mathcal{B}}^{\mathcal{B}'}$$

est un isomorphisme de $\mathbb{K}$-espaces vectoriels. En particulier, les espaces vectoriels $\mathcal{L}(E, E')$ et $\mathcal{M}_{m,n}(\mathbb{K})$ ont la même dimension, égale à mn.

Soient $u : E \longrightarrow E'$ et $v : E' \longrightarrow E''$ deux applications linéaires et $\mathcal{B}, \mathcal{B}', \mathcal{B}''$ des bases des $\mathbb{K}$-espaces vectoriels E, E' et E'' respectivement. Alors

$$[vu]_{\mathcal{B}}^{\mathcal{B}''} = [v]_{\mathcal{B}'}^{\mathcal{B}''}\, [u]_{\mathcal{B}}^{\mathcal{B}'}.$$

Soit $\mathbf{x}$ un vecteur de E de coordonnées $x_1, \ldots, x_n$ dans la base $\mathcal{B}$, on note $[\mathbf{x}]_{\mathcal{B}}$ le vecteur colonne correspondant :

$$[\mathbf{x}]_{\mathcal{B}} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}.$$

Avec les notations précédentes, on a :

$$[u(\mathbf{x})]_{\mathcal{B}'} = [u]_{\mathcal{B}}^{\mathcal{B}'}[\mathbf{x}]_{\mathcal{B}}.$$

3.3.3. Matrices de passage.— Soient E un $\mathbb{K}$-espace vectoriel de dimension n. Considérons $\mathcal{B} = (\mathbf{e}_1, \ldots, \mathbf{e}_n)$ et $\mathcal{B}' = (\mathbf{f}_1, \ldots, \mathbf{f}_n)$ deux bases de E. Tout vecteur $\mathbf{f}_i$, pour $i \in [\![1, n]\!]$, se décompose de façon unique dans la base $\mathcal{B}$:

$$\mathbf{f}_i = p_1^i \mathbf{e}_1 + \ldots + p_n^i \mathbf{e}_n, \quad \text{où } p_j^i \in \mathbb{K}.$$

La *matrice de passage* de la base $\mathcal{B}$ à la base $\mathcal{B}'$, est la matrice, notée $\mathbf{P}_{\mathcal{B}}^{\mathcal{B}'}$, dont les colonnes sont les composantes des vecteurs $\mathbf{F}_i$ exprimés dans la base $\mathcal{B}$:

$$\mathbf{P}_{\mathcal{B}}^{\mathcal{B}'} = \begin{bmatrix} p_1^1 & \ldots & p_1^n \\ p_2^1 & & p_2^n \\ \vdots & & \vdots \\ p_n^1 & \ldots & p_n^n \end{bmatrix}$$

La matrice de passage $\mathbf{P}_{\mathcal{B}}^{\mathcal{B}'}$ vérifie les propriétés suivantes :

i) $\mathbf{P}_{\mathcal{B}}^{\mathcal{B}'} = [\mathrm{Id}_E]_{\mathcal{B}'}^{\mathcal{B}}$,

ii) $\mathbf{P}_{\mathcal{B}}^{\mathcal{B}'}$ est inversible et $(\mathbf{P}_{\mathcal{B}}^{\mathcal{B}'})^{-1} = \mathbf{P}_{\mathcal{B}'}^{\mathcal{B}}$.

Soit $\mathbf{x}$ un vecteur de E de coordonnées $x_1, \ldots, x_n$ dans la base $\mathcal{B}$ et de coordonnées $x'_1, \ldots, x'_n$ dans la base $\mathcal{B}'$. En notant

$$[\mathbf{x}]_{\mathcal{B}} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \quad \text{et} \quad [\mathbf{x}]_{\mathcal{B}'} = \begin{bmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{bmatrix},$$

on a :

$$[\mathbf{x}]_{\mathcal{B}} = \mathbf{P}_{\mathcal{B}}^{\mathcal{B}'}[\mathbf{x}]_{\mathcal{B}'},$$

ou de façon équivalente :

$$[\mathbf{x}]_{\mathcal{B}'} = (\mathbf{P}_{\mathcal{B}}^{\mathcal{B}'})^{-1}[\mathbf{x}]_{\mathcal{B}} = \mathbf{P}_{\mathcal{B}'}^{\mathcal{B}}[\mathbf{x}]_{\mathcal{B}}.$$

3.3.4 Proposition.— Soient E et E' deux $\mathbb{K}$-espaces vectoriels de dimension finie et $u : E \longrightarrow E'$ une application linéaire. Soient $\mathcal{B}, \mathcal{B}'$ deux bases de E, $\mathcal{C}, \mathcal{C}'$ deux bases de E' et $\mathbf{P}_{\mathcal{B}}^{\mathcal{B}'}$, $\mathbf{P}_{\mathcal{C}}^{\mathcal{C}'}$ les matrices de changements de bases associées. Alors,

$$[u]_{\mathcal{B}'}^{\mathcal{C}'} = (\mathbf{P}_{\mathcal{C}}^{\mathcal{C}'})^{-1}[u]_{\mathcal{B}}^{\mathcal{C}}\mathbf{P}_{\mathcal{B}}^{\mathcal{B}'}.$$

En particulier, si u est un endomorphisme de E :

$$[u]_{\mathcal{B}'} = (\mathbf{P}_{\mathcal{B}}^{\mathcal{B}'})^{-1}[u]_{\mathcal{B}}\mathbf{P}_{\mathcal{B}}^{\mathcal{B}'}.$$

3.3.5. Exemple.— Soit $u : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ l'endomorphisme défini par

$$u\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x - z \\ y - z \\ 0 \end{bmatrix}.$$

La matrice de u dans la base canonique can $= (\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$ de $\mathbb{R}^3$ est

$$[u]_{\text{can}} = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{bmatrix}$$

On considère une nouvelle base de $\mathbb{R}^3$:

$$\mathcal{B} = \left\{ \mathbf{e}_1 = \mathbf{c}_1,\ \mathbf{e}_2 = \mathbf{c}_2,\ \mathbf{e}_3 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right\}.$$

La matrice de passage de la base canonique à la base $\mathcal{B}$ est

$$\mathbf{P}_{\text{can}}^{\mathcal{B}} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

On calcule l'inverse de la matrice de $\mathbf{P}_{\text{can}}^{\mathcal{B}}$:

$$\mathbf{P}_{\text{can}}^{\mathcal{B}\ -1} = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}.$$

L'expression de la matrice de u exprimée dans la base $\mathcal{B}$ est

$$\begin{aligned} [u]_{\mathcal{B}} &= \mathbf{P}_{\text{can}}^{\mathcal{B}\ -1}[u]_{\text{can}}\mathbf{P}_{\text{can}}^{\mathcal{B}} \\ &= \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}. \end{aligned}$$

D'où

$$[u]_{\mathcal{B}} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

On constate que cette nouvelle base permet d'exprimer plus simplement l'endomorphisme u. Nous retrouverons cet exemple en 5.3.4.

3.3.6 Exercice.— Écrire la matrice de passage de la base $\mathcal{B}$ de l'espace $\mathbb{R}^3$ donnée dans l'exemple 3.3.1 à la base canonique de $\mathbb{R}^3$. Soit p la projection donnée en 3.3.1. À l'aide de cette matrice de passage et de la matrice de l'endomorphisme p exprimée dans la base $\mathcal{B}$, calculer la matrice de p exprimée dans la base canonique de $\mathbb{R}^3$.

3.3.7. Matrices semblables.— Deux matrices $\mathbf{A}$ et $\mathbf{B}$ de $\mathcal{M}_n(\mathbb{K})$ sont dites *semblables*, s'il existe une matrice inversible $\mathbf{P}$ de $\mathcal{M}_n(\mathbb{K})$ telle que

$$\mathbf{B} = \mathbf{P}^{-1}\mathbf{A}\mathbf{P}.$$

La relation « être semblable à » , dite relation de *similitude*, est une relation d'équivalence sur l'ensemble $\mathcal{M}_n(\mathbb{K})$.

3.3.8 Exercice.— Montrer cette propriété.

Deux matrices semblables représentent le même endomorphisme dans des bases différentes.

3.3.9 Proposition.— Deux matrices semblables ont même trace, même déterminant, même rang.

3.3.10. Matrices équivalentes.— Deux matrices $\mathbf{A}$ et $\mathbf{B}$ de $\mathcal{M}_n(\mathbb{K})$ sont dites *équivalentes*, s'il existe deux matrice inversibles $\mathbf{P}$ et $\mathbf{Q}$ de $\mathcal{M}_n(\mathbb{K})$ telles que

$$\mathbf{B} = \mathbf{P}\mathbf{A}\mathbf{Q}.$$

La relation d'*équivalence* est une relation d'équivalence sur $\mathcal{M}_n(\mathbb{K})$. Deux matrices semblables sont équivalentes.

§ 4 Trace d'une matrice

3.4.1. Définition.— La *trace* d'une matrice carrée $\mathbf{A} = [a^i_j]$ de $\mathcal{M}_n(\mathbb{K})$ est la somme des coefficients de sa diagonale :

$$\operatorname{trace}(\mathbf{A}) = \sum_{i=1}^{n} a^i_i.$$

3.4.2 Proposition.— L'application $\operatorname{trace} : \mathcal{M}_n(\mathbb{K}) \longrightarrow \mathbb{K}$ est une forme linéaire vérifiant, pour toutes matrices $\mathbf{A}$ et $\mathbf{B}$ de $\mathcal{M}_n(\mathbb{K})$,

$$\operatorname{trace}(\mathbf{AB}) = \operatorname{trace}(\mathbf{BA}).$$

3.4.3 Exercice.— Étant donné deux matrices $\mathbf{A}$ et $\mathbf{B}$ de $\mathcal{M}_n(\mathbb{K})$, déterminer toutes les matrices $\mathbf{X}$ de $\mathcal{M}_n(\mathbb{K})$ telles que

$$\mathbf{X} + \mathrm{trace}(\mathbf{X})\mathbf{A} = \mathbf{B}.$$

3.4.4 Exercice.— Montrer qu'il n'existe pas de matrices $\mathbf{A}$ et $\mathbf{B}$ de $\mathcal{M}_n(\mathbb{K})$ telles que

$$\mathbf{AB} - \mathbf{BA} = \mathbf{1}_n.$$

3.4.5. Trace d'un endomorphisme.— De la proposition 3.4.2, on déduit que

3.4.6 Proposition.— Deux matrices semblables ont la même trace.

3.4.7 Exercice.— Soient $\mathbf{A}$ et $\mathbf{B}$ deux matrices carrées.
1. Montrer la relation $\mathrm{trace}(\mathbf{AB}) = \mathrm{trace}(\mathbf{BA})$.
2. En déduire la proposition 3.4.6 : deux matrices semblables ont la même trace.

§ 5 Noyau et image d'une matrice

Nous avons vu dans le chapitre précédent les notions de noyau et d'image d'une application linéaire. On peut définir de la même façon, le noyau et l'image d'une matrice.

3.5.1. Image d'une matrice.— Si $u : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ est une application linéaire, l'image de u est le sous-espace vectoriel de $\mathbb{K}^m$ défini par

$$\mathrm{Im}(u) = \{u(\mathbf{x}) \mid \mathbf{x} \in \mathbb{K}^n\}.$$

De la même façon, si $\mathbf{A}$ est une matrice de $\mathcal{M}_{m,n}(\mathbb{K})$, on définit l'*image* de $\mathbf{A}$ comme le sous-espace vectoriel de $\mathbb{K}^m$ engendré par les vecteurs $\mathbf{Ax}$, où $\mathbf{x} \in \mathbb{K}^n$. Soit

$$\mathrm{Im}(\mathbf{A}) = \{\mathbf{Ax} \mid \mathbf{x} \in \mathbb{K}^n\}.$$

3.5.2 Proposition.— L'image d'une matrice $\mathbf{A}$ de $\mathcal{M}_{m,n}(\mathbb{K})$ est le sous-espace vectoriel de $\mathbb{K}^m$ engendré par les vecteurs colonnes de $\mathbf{A}$.

Preuve. Écrivons $\mathbf{A}$ selon ses vecteurs colonnes :

$$\mathbf{A} = \left[\ \mathbf{a}^1_* \mid \mathbf{a}^2_* \mid \ldots \mid \mathbf{a}^n_*\ \right].$$

Pour tout vecteur

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

de $\mathbb{K}^n$, on a

$$\mathbf{Ax} = \left[\ \mathbf{a}^1_* \mid \mathbf{a}^2_* \mid \ldots \mid \mathbf{a}^n_*\ \right] \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = x_1\mathbf{a}^1_* + x_2\mathbf{a}^2_* + \ldots + x_n\mathbf{a}^n_*.$$

Ainsi, $\mathbf{Ax}$ est une combinaison linéaire des vecteurs colonnes de $\mathbf{A}$, autrement dit $\mathrm{Im}(\mathbf{A})$ est le sous-espace vectoriel de $\mathbb{K}^m$ engendré par les vecteurs colonnes de $\mathbf{A}$. $\square$

3.5.3 Exercice.— Soit $\mathbf{A}$ une matrice de $\mathcal{M}_n(\mathbb{K})$ telle que $\mathrm{Im}(\mathbf{A})$ soit égal à $\mathbb{K}^n$. Justifier que la matrice $\mathbf{A}$ est inversible.

3.5.4 Exercice.— Soit $\mathbf{A}$ une matrice de $\mathcal{M}_{n,m}(\mathbb{K})$. Soit $\mathcal{E}$ un sous-ensemble de vecteurs colonnes de $\mathcal{M}_{m,1}(\mathbb{K})$, identifié à $\mathbb{K}^m$. L'*image de $\mathcal{E}$ par* $\mathbf{A}$ est l'ensemble, noté $\mathbf{A}(\mathcal{E})$, formé de tous les produits de $\mathbf{A}$ par un vecteur de $\mathcal{E}$, *i.e.*,

$$\mathbf{A}(\mathcal{E}) = \{\mathbf{Ax} \mid \mathbf{x} \in \mathcal{E}\}.$$

1. Montrer que si $\mathcal{E}$ est un sous-espace vectoriel de $\mathbb{K}^m$, alors $\mathbf{A}(\mathcal{E})$ est un sous-espace vectoriel de $\mathbb{K}^n$.
2. Montrer que si $\mathcal{E} = \mathrm{Vect}(\mathbf{x}_1, \ldots, \mathbf{x}_p)$, alors $\mathbf{A}(\mathcal{E}) = \mathrm{Vect}(\mathbf{Ax}_1, \ldots, \mathbf{Ax}_p)$.

3.5.5 Exercice.— Soient $\mathbf{A}$ et $\mathbf{B}$ deux matrices compatibles. Montrer que $\mathrm{Im}(\mathbf{AB})$ est un sous-espace vectoriel de $\mathrm{Im}(\mathbf{A})$.

3.5.6 Exercice.— Soit $\mathbf{A} \in \mathcal{M}_{n,m}(\mathbb{K})$ et $\mathbf{B} \in \mathcal{M}_{n,p}(\mathbb{K})$ deux matrices. Montrer que

$$\mathrm{Im}([\mathbf{A} \ \ \mathbf{B}]) = \mathrm{Im}(\mathbf{A}) + \mathrm{Im}(\mathbf{B}),$$

où $[\mathbf{A} \ \ \mathbf{B}]$ désigne la matrice constituée des blocs $\mathbf{A}$ et $\mathbf{B}$.

3.5.7. Noyau d'une matrice.— Si $u : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ est une application linéaire, le noyau de u est le sous-espace vectoriel de $\mathbb{K}^n$ défini par

$$\mathrm{Ker}(u) = \{\mathbf{x} \in \mathbb{K}^n \mid u(\mathbf{x}) = \mathbf{0}\}.$$

De la même façon, si $\mathbf{A}$ est une matrice de $\mathcal{M}_{m,n}(\mathbb{K})$, on définit le *noyau* de $\mathbf{A}$ comme le sous-espace vectoriel suivant de $\mathbb{K}^n$

$$\mathrm{Ker}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{K}^n \mid \mathbf{Ax} = \mathbf{0}\}.$$

Le noyau $\mathrm{Ker}(\mathbf{A})$ est formé des solutions de l'équation

$$\mathbf{Ax} = \mathbf{0}.$$

3.5.8 Exercice.— Soit $\mathbf{A}$ une matrice inversible de $\mathcal{M}_n(\mathbb{K})$. Décrire les sous-espaces

$$\mathrm{Ker}(\mathbf{A}), \qquad \mathrm{Ker}(\mathbf{A}^\top), \qquad \mathrm{Im}(\mathbf{A}), \qquad \mathrm{Im}(\mathbf{A}^\top).$$

3.5.9 Exercice.— Soient $\mathbf{A}$ et $\mathbf{B}$ deux matrices compatibles. Montrer que $\mathrm{Ker}(\mathbf{B})$ est un sous-espace vectoriel de $\mathrm{Ker}(\mathbf{AB})$.

§ 6 Le rang d'une matrice

3.6.1. Définition.— Soient E un $\mathbb{K}$-espace vectoriel. On appelle *rang* d'une famille de vecteurs $(\mathbf{x}_i)_i$ de E, la dimension du sous-$\mathbb{K}$-espace vectoriel de E engendré par $(\mathbf{x}_i)_i$. En d'autres termes, le rang de la famille $(\mathbf{x}_i)_i$ est le nombre maximal de vecteurs linéairement indépendants que l'on peut extraire de $(\mathbf{x}_i)_i$.

3.6.2. Rang d'une matrice.— Le *rang* d'une matrice $\mathbf{A}$ de $\mathcal{M}_{m,n}(\mathbb{K})$ est le rang de la famille de ses vecteurs colonnes dans $\mathbb{K}^m$. On le note $\mathrm{rg}(\mathbf{A})$. Autrement dit,

$$\mathrm{rg}(\mathbf{A}) = \dim(\mathrm{Im}(\mathbf{A})).$$

3.6.3 Proposition.— Soit $\mathbf{A}$ une matrice de $\mathcal{M}_{m,n}(\mathbb{K})$. Le rang de $\mathbf{A}$ vérifie les propriétés suivantes :

i) $\mathrm{rg}(\mathbf{A}) \leq \inf\{m, n\}$,

ii) $\mathrm{rg}(\mathbf{A}) = \mathrm{rg}(\mathbf{A}^\top)$ (en particulier le rang de $\mathbf{A}$ est aussi le rang des vecteurs lignes),

iii) $\mathrm{Ker}(\mathbf{A}) = \{\mathbf{0}\}$ si, et seulement si, $\mathrm{rg}(\mathbf{A}) = n$,

iv) $\mathrm{Ker}(\mathbf{A}^\top) = \{\mathbf{0}\}$ si, et seulement si, $\mathrm{rg}(\mathbf{A}) = m$,

v) si $m = n$, alors $\mathbf{A}$ est inversible si, et seulement si, $\mathrm{rg}(\mathbf{A}) = n$.

Soit $\mathbf{A} \in \mathcal{M}_{p,q}(\mathbb{K})$ et $\mathbf{Q} \in \mathcal{M}_p(\mathbb{K})$, $\mathbf{P} \in \mathcal{M}_p(\mathbb{K})$ deux matrices inversibles, on a

$$\mathrm{rg}(\mathbf{A}) = \mathrm{rg}(\mathbf{QAP}).$$

En particulier si $\mathrm{rg}(\mathbf{A}) = r$, il existe deux matrices inversibles $\mathbf{P}$ et $\mathbf{Q}$ telles que

$$\mathbf{A} = \mathbf{Q}\begin{bmatrix} \mathbf{1}_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}\mathbf{P}.$$

3.6.4 Proposition.— Soit $\mathbf{A}$ une matrice de $\mathcal{M}_{p,q}(\mathbb{K})$ de rang r. Alors la matrice $\mathbf{A}$ est équivalente à la matrice

$$\mathbf{J}_r = \begin{bmatrix} \mathbf{1}_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}.$$

En particulier, deux matrices de $\mathcal{M}_{p,q}(\mathbb{K})$ sont équivalentes si, et seulement si, elles ont même rang.

3.6.5. Remarque.— Soit $u : E \longrightarrow E'$ une application linéaire. On a défini le rang de u comme la dimension du sous-espace $\mathrm{Im}(u)$. Soient $\mathcal{B}$ et $\mathcal{B}'$ des bases de E et E' respectivement. On a

$$\mathrm{rg}(u) = \dim(\mathrm{Im}(u)) = \dim(\mathrm{Vect}(u(\mathcal{B}))).$$

Autrement dit le rang de u est le rang de la matrice $[u]_{\mathcal{B}}^{\mathcal{B}'}$.

3.6.6 Exercice.— Soient $\mathbf{A}$ et $\mathbf{B}$ deux matrices de $\mathcal{M}_{n,m}(\mathbb{K})$.

1. Montrer que $\mathrm{Im}(\mathbf{A}+\mathbf{B})$ est un sous-espace de $\mathrm{Im}(\mathbf{A}) + \mathrm{Im}(\mathbf{B})$.
2. En déduire que $\mathrm{rg}(\mathbf{A}+\mathbf{B}) \leq \mathrm{rg}(\mathbf{A}) + \mathrm{rg}(\mathbf{B})$.

3.6.7 Exercice.— Soit $\mathbf{A} \in \mathcal{M}_{n,m}(\mathbb{K})$ et $\mathbf{B} \in \mathcal{M}_{n,p}(\mathbb{K})$ deux matrices. Montrer que

$$\mathrm{rg}([\mathbf{A}\ \ \mathbf{B}]) \leq \mathrm{rg}(\mathbf{A}) + \mathrm{rg}(\mathbf{B}) - \dim(\mathrm{Im}(\mathbf{A}) \cap \mathrm{Im}(\mathbf{B})).$$

§ 7 Opérations matricielles par blocs

Dans certaines situations, nous rencontrerons des matrices partionnées par blocs. Les opérations sur les matrices définies sur les scalaires, comme l'addition et la multiplication, se généralisent aux matrices partitionnées par blocs.

3.7.1. Matrices par blocs. — Exprimer une matrice par colonnes ou par lignes et un cas particulier de partitionnement de matrice. Plus généralement, soit $\mathbf{A}$ une matrice de $\mathcal{M}_{m,n}(\mathbb{K})$, une partitionner $\mathbf{A}$ consiste à l'écire sous la forme

$$\begin{array}{cc} \begin{array}{ccc} n_1 & \cdots & n_k \end{array} & \\ \begin{bmatrix} \mathbf{A}_1^1 & \cdots & \mathbf{A}_1^k \\ \vdots & & \vdots \\ \mathbf{A}_l^1 & \cdots & \mathbf{A}_l^k \end{bmatrix} & \begin{array}{c} m_1 \\ \vdots \\ m_l \end{array} \end{array}$$

où $n_1 + n_2 + \ldots + n_k = n$, $m_1 + m_2 + \ldots + m_l = m$ et où $\mathbf{A}_i^j$ est une matrice de $\mathcal{M}_{n_j,m_i}(\mathbb{K})$, appelée *bloc* (i,j) ou *sous-matrice* (i,j) de la matrice $\mathbf{A}$.

Les opérations sur les matrices par blocs se définissent comme dans le cas des matrices définies par des scalaires ; il faut cependant tenir compte des compatibilités des tailles des blocs.

3.7.2. Addition par blocs. — Considérons deux matrices par blocs, partitionnées de la même façon :

$$\mathbf{A} = \begin{array}{cc} \begin{array}{ccc} n_1 & \cdots & n_k \end{array} & \\ \begin{bmatrix} \mathbf{A}_1^1 & \cdots & \mathbf{A}_1^k \\ \vdots & & \vdots \\ \mathbf{A}_l^1 & \cdots & \mathbf{A}_l^k \end{bmatrix} & \begin{array}{c} m_1 \\ \vdots \\ m_l \end{array} \end{array}, \qquad \mathbf{B} = \begin{array}{cc} \begin{array}{ccc} n_1 & \cdots & n_k \end{array} & \\ \begin{bmatrix} \mathbf{B}_1^1 & \cdots & \mathbf{B}_1^k \\ \vdots & & \vdots \\ \mathbf{B}_l^1 & \cdots & \mathbf{B}_l^k \end{bmatrix} & \begin{array}{c} m_1 \\ \vdots \\ m_l \end{array} \end{array}.$$

La somme des matrices $\mathbf{A}$ et $\mathbf{B}$ est une matrice $\mathbf{C}$ de même partion :

$$\mathbf{C} = \mathbf{A} + \mathbf{B} = \begin{array}{cc} \begin{array}{ccc} n_1 & \cdots & n_k \end{array} & \\ \begin{bmatrix} \mathbf{C}_1^1 & \cdots & \mathbf{C}_1^k \\ \vdots & & \vdots \\ \mathbf{C}_l^1 & \cdots & \mathbf{C}_l^k \end{bmatrix} & \begin{array}{c} m_1 \\ \vdots \\ m_l \end{array} \end{array} = \begin{bmatrix} \mathbf{A}_1^1 + \mathbf{B}_1^1 & \cdots & \mathbf{A}_1^k + \mathbf{B}_1^k \\ \vdots & & \vdots \\ \mathbf{A}_l^1 + \mathbf{B}_l^1 & \cdots & \mathbf{A}_l^k + \mathbf{B}_l^k \end{bmatrix}.$$

3.7.3. Multiplication par blocs. — La multiplication par blocs est moins évidente. Considérons deux matrices par blocs

$$\mathbf{A} = \begin{array}{cc} \begin{array}{ccc} n_1 & \cdots & n_i \end{array} & \\ \begin{bmatrix} \mathbf{A}_1^1 & \cdots & \mathbf{A}_1^i \\ \vdots & & \vdots \\ \mathbf{A}_j^1 & \cdots & \mathbf{A}_j^i \end{bmatrix} & \begin{array}{c} m_1 \\ \vdots \\ m_l \end{array} \end{array} \quad \text{et} \quad \mathbf{B} = \begin{array}{cc} \begin{array}{ccc} p_1 & \cdots & p_k \end{array} & \\ \begin{bmatrix} \mathbf{B}_1^1 & \cdots & \mathbf{B}_1^k \\ \vdots & & \vdots \\ \mathbf{B}_i^1 & \cdots & \mathbf{B}_i^k \end{bmatrix} & \begin{array}{c} n_1 \\ \vdots \\ n_i \end{array} \end{array}.$$

Avec ces notations, on montre que (ce n'est pas immédiat)

3.7.4 Proposition. — Si la matrice produit $\mathbf{C} = \mathbf{AB}$ est partionnée de la façon suivante

$$\mathbf{C} = \begin{array}{cc} \begin{array}{ccc} p_1 & \cdots & p_k \end{array} & \\ \begin{bmatrix} \mathbf{C}_1^1 & \cdots & \mathbf{C}_1^k \\ \vdots & & \vdots \\ \mathbf{C}_j^1 & \cdots & \mathbf{C}_j^k \end{bmatrix} & \begin{array}{c} m_1 \\ \vdots \\ m_l \end{array} \end{array}$$

alors, pour tous $r \in [\![1, l]\!]$ et $s \in [\![1, k]\!]$,

$$\mathbf{C}_r^s = \sum_{t=1}^{i} \mathbf{A}_r^t \mathbf{B}_t^s.$$

En particulier, on a par exemple,

$$\mathbf{C}_1^1 = \mathbf{A}_1^1\mathbf{B}_1^1 + \mathbf{A}_1^2\mathbf{B}_2^1 + \ldots + \mathbf{A}_1^i\mathbf{B}_i^1.$$

3.7.5. Exemples. —

a) Soient $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ dans $\mathcal{M}_{m,n_1}(\mathbb{K})$, $\mathcal{M}_{m,n_2}(\mathbb{K})$, $\mathcal{M}_{m,n_3}(\mathbb{K})$ respectivement et $\mathbf{D}$, $\mathbf{E}$, $\mathbf{F}$ dans $\mathcal{M}_{n_1,p}(\mathbb{K})$, $\mathcal{M}_{n_2,p}(\mathbb{K})$, $\mathcal{M}_{n_3,p}(\mathbb{K})$ respectivement, alors

$$\begin{bmatrix} \mathbf{A} & \mathbf{B} & \mathbf{C} \end{bmatrix} \begin{bmatrix} \mathbf{D} \\ \mathbf{E} \\ \mathbf{F} \end{bmatrix} = \mathbf{AD} + \mathbf{BE} + \mathbf{CF}.$$

b) Soient $\mathbf{A} \in \mathcal{M}_{m_1,n_1}(\mathbb{K})$, $\mathbf{B} \in \mathcal{M}_{m_1,n_2}(\mathbb{K})$, $\mathbf{C} \in \mathcal{M}_{m_2,n_1}(\mathbb{K})$, $\mathbf{D} \in \mathcal{M}_{m_2,n_2}(\mathbb{K})$ et $\mathbf{e} \in \mathcal{M}_{n_1,p_1}(\mathbb{K})$, $\mathbf{F} \in \mathcal{M}_{n_1,p_2}(\mathbb{K})$, $\mathbf{G} \in \mathcal{M}_{n_2,p_1}(\mathbb{K})$, $\mathbf{H} \in \mathcal{M}_{n_2,p_2}(\mathbb{K})$, alors

$$\begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{bmatrix} \begin{bmatrix} \mathbf{E} & \mathbf{F} \\ \mathbf{G} & \mathbf{H} \end{bmatrix} = \begin{bmatrix} \mathbf{AE} + \mathbf{BG} & \mathbf{AF} + \mathbf{BH} \\ \mathbf{CE} + \mathbf{DG} & \mathbf{CF} + \mathbf{DH} \end{bmatrix}$$

c) Soient

$$\mathbf{A} = \begin{array}{cc} \begin{array}{cc} p_1 & p_2 \end{array} & \\ \begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{bmatrix} & \begin{array}{c} n_1 \\ n_2 \end{array} \end{array} \quad \text{et} \quad \mathbf{x} = \begin{array}{cc} 1 & \\ \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix} & \begin{array}{c} p_1 \\ p_2 \end{array} \end{array}$$

une matrice par blocs de $\mathcal{M}_{n_1+n_2,p_1+p_2}(\mathbb{K})$ et un vecteur de $\mathbb{K}^{p_1+p_2}$. On a

$$\begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{bmatrix} \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{A}\mathbf{x}_1 + \mathbf{B}\mathbf{x}_2 \\ \mathbf{C}\mathbf{x}_1 + \mathbf{D}\mathbf{x}_2 \end{bmatrix}.$$

3.7.6 Exercice. — Soient $\mathbf{A} \in \mathcal{M}_{n,m}(\mathbb{K})$ et $\mathbf{B} \in \mathcal{M}_{m,p}(\mathbb{K})$ deux matrices partionnées en blocs de la façon suivante

$$\mathbf{A} = \begin{bmatrix} \mathbf{C} & \mathbf{1}_2 \\ \mathbf{1}_2 & \mathbf{0} \end{bmatrix} \qquad \mathbf{B} = \begin{bmatrix} \mathbf{1}_2 & \mathbf{0} \\ \mathbf{C} & \mathbf{C} \end{bmatrix},$$

où

$$\mathbf{C} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}.$$

Exprimer le produit $\mathbf{AB}$ par blocs, puis calculer $\mathbf{AB}$.

3.7.7 Exercice. — Soient $\mathbf{A} \in \mathcal{M}_{n,n}(\mathbb{K})$, $\mathbf{B} \in \mathcal{M}_{m,m}(\mathbb{K})$ et $\mathbf{C} \in \mathcal{M}_{m,n}(\mathbb{K})$, telles que les matrices $\mathbf{A}$ et $\mathbf{B}$ sont inversibles. Montrer que les matrices suivantes sont inversibles et calculer leur inverse

$$\begin{bmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{bmatrix}, \qquad \begin{bmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{0} & \mathbf{B} \end{bmatrix}.$$

§ 8 Exercices

3.8.1 Exercice.— Parmi les sous-ensembles de matrices de $\mathcal{M}_n(\mathbb{K})$ suivants, lesquels sont des sous-espaces vectoriels :

a) les matrices symétriques,

b) les matrices diagonales,

c) les matrices inversibles,

d) les matrices non inversibles,

e) les matrices triangulaires,

f) les matrices triangulaires supérieures,

g) les matrices qui commutent avec une matrice donnée $\mathbf{A}$,

h) les matrices $\mathbf{A}$ telles que $\mathbf{A}^2 = \mathbf{A}$,

i) les matrices de trace nulle.

3.8.2 Exercice.— Donner les dimensions des sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{K})$ suivants

a) le sous-espace vectoriel des matrices à coefficients constants,

b) le sous-espace vectoriel des matrices diagonales,

c) le sous-espace vectoriel des matrices symétriques,

d) le sous-espace vectoriel des matrices antisymétriques.

3.8.3 Exercice.— Trouver des bases de l'espace des lignes et de l'espace des colonnes de la matrice

$$\mathbf{A} = \begin{bmatrix} 1 & 2 & 3 \\ 4 & -1 & 3 \\ 5 & 3 & 8 \end{bmatrix}.$$

Quelles sont les dimensions des noyaux de l'application linéaire représentée par $\mathbf{A}$ et de celle représentée par sa transposée. Déterminer des bases de ces noyaux.

3.8.4 Exercice.— Soit u l'application de $\mathbb{R}^3$ à valeurs dans $\mathbb{R}^3$ définie par

$$u \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x-y \\ y-x \\ x-z \end{bmatrix}.$$

1. Montrer que u est une application linéaire.

2. Exprimer la matrice de u dans la base suivante de $\mathbb{R}^3$:

$$\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \right\}$$

3. Écrire la matrice de passage de la base $\mathcal{B}$ à la base canonique de $\mathbb{R}^3$.

4. Donner la matrice de u exprimée dans la base canonique.

3.8.5 Exercice.— Mêmes questions avec l'application u définie par

$$u \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x+y \\ y+x \\ x+z \end{bmatrix}.$$

3.8.6 Exercice.— Pour chacune des applications de $\mathbb{R}^3$ à valeurs dans $\mathbb{R}^3$ définies par

$$\mathbf{a})\ u\begin{bmatrix} x\\ y\\ z\end{bmatrix} = \begin{bmatrix} 2x-y\\ -x+2y-z\\ z-y\end{bmatrix}, \qquad \mathbf{b})\ u\begin{bmatrix} x\\ y\\ z\end{bmatrix} = \begin{bmatrix} x-2y\\ x-2z\\ 2y+z\end{bmatrix},$$

$$\mathbf{c})\ u\begin{bmatrix} x\\ y\\ z\end{bmatrix} = \begin{bmatrix} x-y\\ y-z\\ x+z\end{bmatrix}, \qquad \mathbf{d})\ u\begin{bmatrix} x\\ y\\ z\end{bmatrix} = \begin{bmatrix} x-y+z\\ x+y-z\\ x+y+z\end{bmatrix}.$$

1. Montrer que u est une application linéaire.
2. Exprimer la matrice de u dans la base canonique de $\mathbb{R}^3$.
3. Montrer que l'application linéaire u est inversible.
4. Déterminer $u^{-1}(x,y,z)$, pour tout vecteur (x,y,z) de $\mathbb{R}^3$.

3.8.7 Exercice.— Soit $\mathcal{T}^s$ (resp. $\mathcal{T}^i$) l'ensemble des matrices triangulaires supérieures (resp. inférieures) de $\mathcal{M}_n(\mathbb{K})$.

1. Montrer que $\mathcal{T}^s$ et $\mathcal{T}^i$ sont des sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{K})$.
2. Montrer que $\mathcal{M}_n(\mathbb{K}) = \mathcal{T}^s + \mathcal{T}^i$. Cette somme est-elle directe ?
3. Quels sont les dimensions des sous-espaces $\mathcal{T}^s$ et $\mathcal{T}^i$?

3.8.8 Exercice.— Montrer que toute matrice triangulaire supérieure est semblable à une matrice triangulaire inférieure.

3.8.9 Exercice.— Soit u l'endomorphisme de $\mathbb{R}^2$ représenté dans une base $\mathcal{B}$ de $\mathbb{R}^2$ par la matrice

$$[u]_{\mathcal{B}} = \begin{bmatrix} 1 & 1\\ -1 & -1\end{bmatrix}.$$

1. Montrer que $u^2 = 0$.
2. Déterminer le rang, l'image et le noyau de u.
3. Montrer qu'il existe une base de $\mathbb{R}^2$ dans laquelle la matrice de u est

$$\begin{bmatrix} 0 & 2\\ 0 & 0\end{bmatrix}.$$

3.8.10 Exercice.— Soit $\mathbf{A} \in \mathcal{M}_2(\mathbb{K})$.

1. Montrer que

$$\mathbf{A}^2 - \mathrm{tr}(\mathbf{A})\mathbf{A} + \det(\mathbf{A})\mathbf{1}_2 = \mathbf{0}.$$

2. On suppose que le déterminant de $\mathbf{A}$ est non nul. Calculer l'inverse de $\mathbf{A}$.

3.8.11 Exercice.— Soient $\mathbf{A} \in \mathcal{M}_n(\mathbb{K})$ et $\lambda, \mu \in \mathbb{K}$ tels que

$$\mathbf{A}^2 = \lambda\mathbf{A} + \mu\mathbf{1}_n.$$

1. Montrer que si μ est non nul, la matrice $\mathbf{A}$ est inversible et que

$$\mathbf{A}^{-1} = \mu^{-1}(\mathbf{A} - \lambda\mathbf{1}_n).$$

2. Montrer que pour tout entier k, la matrice $\mathbf{A}^k$ s'écrit comme une combinaison linéaire des matrices $\mathbf{A}$ et $\mathbf{1}_n$.

3.8.12 Exercice.— Soient E un $\mathbb{K}$-espace vectoriel et u un endomorphisme non nul de E tel que $u^2 = 0$.

1. Montrer que $\mathrm{Im}(u) \subset \mathrm{Ker}(u)$.
2. Déterminer la dimension du noyau de u et de l'image de u.
3. Montrer qu'il existe une base de $\mathbb{R}^3$ dans laquelle l'endomorphisme u a pour matrice

$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

CHAPITRE 4

Les déterminants

Sommaire

Dans tout ce chapitre, $\mathbb{K}$ désignera un corps commutatif.

§ 1 Définition récursive du déterminant

4.1.1. Notation.— Soit $\mathbf{A} = [a_i^j]$ une matrice de $\mathcal{M}_n(\mathbb{K})$ et soient $i, j \in [\![1, n]\!]$. On notera $\mathbf{A}_{\check{i}\check{j}}$ la matrice obtenue en supprimant la i-ème ligne et j-ème colonne de la matrice $\mathbf{A}$:

$$\mathbf{A}_{\check{i}\check{j}} = \begin{bmatrix} a_1^1 & \cdots & a_1^j & \cdots & a_1^n \\ \vdots & & \vdots & & \vdots \\ a_i^1 & \cdots & a_i^j & \ldots & a_i^n \\ \vdots & & \vdots & & \vdots \\ a_n^1 & \cdots & a_n^j & \cdots & a_n^n \end{bmatrix} \in \mathcal{M}_{n-1}(\mathbb{K})$$

4.1.2. Définition.— Soit $\mathbf{A} = [a_i^j]$ une matrice de $\mathcal{M}_n(\mathbb{K})$. On définit une application

$$\det : \mathcal{M}_n(\mathbb{K}) \longrightarrow \mathbb{K}$$

par récurrence sur l'entier n en posant, pour $n = 1$,

$$\det(\mathbf{A}) = a_1^1,$$

et, pour tout $n > 1$,

$$\det(\mathbf{A}) = \sum_{k=1}^{n} (-1)^{k+1} a_1^k \det \mathbf{A}_{\check{1}\check{k}}.$$

Le scalaire $\det(\mathbf{A})$ ainsi défini est appelé le *déterminant* de la matrice $\mathbf{A}$

4.1.3. Notation.— Le déterminant d'une matrice $\begin{bmatrix} a_1^1 & \dots & a_1^n \\ \vdots & & \vdots \\ a_n^1 & \dots & a_n^n \end{bmatrix}$ sera aussi noté

$$\begin{vmatrix} a_1^1 & \dots & a_1^n \\ \vdots & & \vdots \\ a_n^1 & \dots & a_n^n \end{vmatrix}.$$

4.1.4. Exemples.— Pour une matrice de $\mathcal{M}_2(\mathbb{K})$, on a

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

Pour une matrice de $\mathcal{M}_3(\mathbb{K})$, on a

$$\begin{aligned} \begin{vmatrix} a_1^1 & a_1^2 & a_1^3 \\ a_2^1 & a_2^2 & a_2^3 \\ a_3^1 & a_3^2 & a_3^3 \end{vmatrix} &= a_1^1 \begin{vmatrix} a_2^2 & a_2^3 \\ a_3^2 & a_3^3 \end{vmatrix} - a_1^2 \begin{vmatrix} a_2^1 & a_2^3 \\ a_3^1 & a_3^3 \end{vmatrix} + a_1^3 \begin{vmatrix} a_2^1 & a_2^2 \\ a_3^1 & a_3^2 \end{vmatrix} \\ &= a_1^1(a_2^2 a_3^3 - a_3^2 a_2^3) - a_1^2(a_2^1 a_3^3 - a_3^1 a_2^3) + a_1^3(a_2^1 a_3^2 - a_3^1 a_2^2) \\ &= a_1^1 a_2^2 a_3^3 - a_1^1 a_3^2 a_2^3 - a_1^2 a_2^1 a_3^3 + a_1^2 a_3^1 a_2^3 + a_1^3 a_2^1 a_3^2 - a_1^3 a_3^1 a_2^2. \end{aligned}$$

4.1.5 Exercice.— Montrer que le déterminant d'une matrice triangulaire est égal au produit des coefficients de la diagonale.

4.1.6. Déterminant d'une famille de vecteurs.— Soient E un $\mathbb{K}$-espace vectoriel de dimension n et $\mathcal{B} = (\mathbf{e}_1, \dots, \mathbf{e}_n)$ une base de E.

Étant donnée une famille $(\mathbf{x}_1, \dots, \mathbf{x}_n)$ de vecteurs de E, on forme la matrice de $\mathcal{M}_n(\mathbb{K})$, notée

$$[\mathbf{x}_1 \,|\, \mathbf{x}_2 \,|\, \dots \,|\, \mathbf{x}_n]_{\mathcal{B}},$$

dont la j-ème colonne est constituée des coordonnées du vecteur $\mathbf{x}_j$ exprimé dans la base $\mathcal{B}$.

Le scalaire $\det [\mathbf{x}_1 \,|\, \mathbf{x}_2 \,|\, \dots \,|\, \mathbf{x}_n]_{\mathcal{B}}$ est appelé le *déterminant de la famille de vecteurs* par rapport à la base $\mathcal{B}$. On le note $\det_{\mathcal{B}}(\mathbf{x}_1, \dots, \mathbf{x}_n)$.

§ 2 Premières propriétés du déterminant

Soit $\mathbf{A} = [a_i^j]$ une matrice de $\mathcal{M}_n(\mathbb{K})$. On notera $\mathbf{a}_*^j$ la j-ème colonne de la matrice $\mathbf{A}$. Avec cette notation, on peut écrire la matrice $\mathbf{A}$ par colonnes sous la forme

$$\mathbf{A} = [\ \mathbf{a}_*^1 \,|\, \mathbf{a}_*^2 \,|\, \dots \,|\, \mathbf{a}_*^n\ ].$$

FIGURE 4.1 – Gottfried Wilhelm Leibniz (1646 - 1716)

Gottfried Wilhelm Leibniz est un mathématicien, philosophe, juriste, diplomate allemand. En mathématiques, l'influence de Leibniz est considérable, dans le domaine de l'algébrisation de la géométrie, en calcul différentiel, calcul infinitésimal. Leibniz travaille aussi sur la résolution des systèmes d'équations. Il introduit la notion de déterminant d'un système d'équation. Ses travaux sur les déterminants ne sont pas publiés, mais se retrouvent dans une lettre au mathématicien Guillaume François Antoine de L'Hôpital datée du 28 avril 1693. Dans cette lettre, il écrit la condition de compatibilité d'un système de trois équations linéaires à deux inconnues sous forme de déterminant. Le terme de ≪ déterminant ≫ne sera introduit que plus tard, par Carl Friedrich Gauss en 1801 dans l'ouvrage ≪ Disquisitiones Arithmeticae ≫.

Les résultats suivants résument les principales propriétés de l'application déterminant.

4.2.1 Proposition. — Le déterminant est une application linéaire par rapport à chaque colonne, *i.e.*, pour toute matrice $\mathbf{A} = [a_i^j]$ de $\mathcal{M}_n(\mathbb{K})$, on a, pour tout $j \in [\![1, n]\!]$,

i) si $\mathbf{a}_*^j = \mathbf{b}_*^j + \mathbf{c}_*^j$,

$$\begin{aligned}\det\left[\ \mathbf{a}_*^1 \mid \ldots \mid \mathbf{b}_*^j + \mathbf{c}_*^j \mid \ldots \mid \mathbf{a}_*^n\ \right] &= \det\left[\ \mathbf{a}_*^1 \mid \ldots \mid \mathbf{b}_*^j \mid \ldots \mid \mathbf{a}_*^n\ \right] \\ &\quad + \det\left[\ \mathbf{a}_*^1 \mid \ldots \mid \mathbf{c}_*^j \mid \ldots \mid \mathbf{a}_*^n\ \right]\end{aligned}$$

ii) pout tout scalaire $\alpha \in \mathbb{K}$,

$$\det\left[\ \mathbf{a}_*^1 \mid \ldots \mid \alpha\, \mathbf{a}_*^j \mid \ldots \mid \mathbf{a}_*^n\ \right] = \alpha \det\left[\ \mathbf{a}_*^1 \mid \ldots \mid \mathbf{a}_*^j \mid \ldots \mid \mathbf{a}_*^n\ \right]$$

4.2.2 Proposition. — Le déterminant d'une matrice dont deux colonnes sont égales est nul.

4.2.3 Proposition. — Le déterminant d'une matrice change de signe, lorsque l'on échange deux colonnes.

4.2.4 Théorème. — Soit $\mathbf{A} = \left[\ \mathbf{a}_*^1 \mid \mathbf{a}_*^2 \mid \ldots \mid \mathbf{a}_*^n\ \right]$ une matrice de $\mathcal{M}_n(\mathbb{K})$. La famille de vecteurs $(\mathbf{a}_*^1, \mathbf{a}_*^2, \ldots, \mathbf{a}_*^n)$ forme une base de $\mathbb{K}^n$ si, et seulement si, $\det(\mathbf{A})$ est non nul.

FIGURE 4.2 – Gabriel Cramer (1704 - 1752)

Gabriel Cramer est un mathématicien suisse, il travaille notamment sur les courbes algébriques. Il publie en 1750, « Introduction à l'analyse des lignes courbes algébriques ». C'est la première publication en Europe sur les déterminants. Cramer donne un formulation basée sur les déterminants pour la solution au problème de la construction de la conique passant par cinq points donnés, problème qu'il réduit à un système d'équations linéaires.

§ 3 Les formules de Cramer

Soit $\mathbf{A} = \left[\ \mathbf{a}_*^1 \mid \mathbf{a}_*^2 \mid \ldots \mid \mathbf{a}_*^n\ \right]$ une matrice de $\mathcal{M}_n(\mathbb{K})$. Si son déterminant $\det(\mathbf{A})$ est non nul, nous allons montrer qu'il existe une formule explicite basée sur le déterminant de $\mathbf{A}$ pour les solutions de l'équation

$$\mathbf{A}\mathbf{x} = \mathbf{B}.$$

Posons

$$\mathbf{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

Le produit $\mathbf{A}\mathbf{x}$ est une combinaison linéaire de colonnes de $\mathbf{A}$, à coefficients les coefficients du vecteur $\mathbf{x}$:

$$\mathbf{A}\mathbf{x} = x_1\mathbf{a}_*^1 + x_2\mathbf{a}_*^2 + \ldots + x_n\mathbf{a}_*^n.$$

Ainsi, l'équation $\mathbf{A}\mathbf{x} = \mathbf{b}$ s'écrit sous la forme

$$x_1 \begin{bmatrix} a_1^1 \\ \vdots \\ a_n^1 \end{bmatrix} + x_2 \begin{bmatrix} a_1^2 \\ \vdots \\ a_n^2 \end{bmatrix} + \ldots + x_n \begin{bmatrix} a_1^n \\ \vdots \\ a_n^n \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

Nous souhaitons déterminer les inconnues $x_1, \ldots, x_n$. Soit x_i l'une d'entre elles. Dans l'équation précédente, on soustrait le vecteur $\mathbf{b}$ au i-ème vecteur colonne, on obtient

$$x_1 \begin{bmatrix} a_1^1 \\ \vdots \\ a_n^1 \end{bmatrix} + x_2 \begin{bmatrix} a_1^2 \\ \vdots \\ a_n^2 \end{bmatrix} + \ldots + x_i \begin{bmatrix} a_1^i - b_1 \\ \vdots \\ a_n^i - b_n \end{bmatrix} + \ldots + x_n \begin{bmatrix} a_1^n \\ \vdots \\ a_n^n \end{bmatrix} = \mathbf{0}.$$

Par suite, les colonnes de la matrice suivante sont linéairement dépendantes :

$$\begin{bmatrix} a_1^1 & \cdots & (x_i a_1^i - b_1) & \cdots & a_1^n \\ \vdots & & & & \\ a_n^1 & \cdots & (x_i a_n^i - b_n) & \cdots & a_n^n \end{bmatrix}$$

Du théorème 4.2.4, on déduit alors que le déterminant de cette matrice est nul, soit

$$x_i \det \begin{bmatrix} a_1^1 & \cdots & a_1^i & \cdots & a_1^n \\ \vdots & & & & \\ a_n^1 & \cdots & a_n^i & \cdots & a_n^n \end{bmatrix} - \det \begin{bmatrix} a_1^1 & \cdots & b_1 & \cdots & a_1^n \\ \vdots & & & & \\ a_n^1 & \cdots & b_n & \cdots & a_n^n \end{bmatrix} = 0.$$

La première matrice est la matrice $\mathbf{a}$, la seconde est la matrice $\mathbf{a}$ dans laquelle on a remplacé la i-ème colonne par le vecteur colonne $\mathbf{b}$. On a ainsi montré

4.3.1 Théorème (Formules de Cramer).— Si $\det(\mathbf{A})$ est non nul, alors l'équation

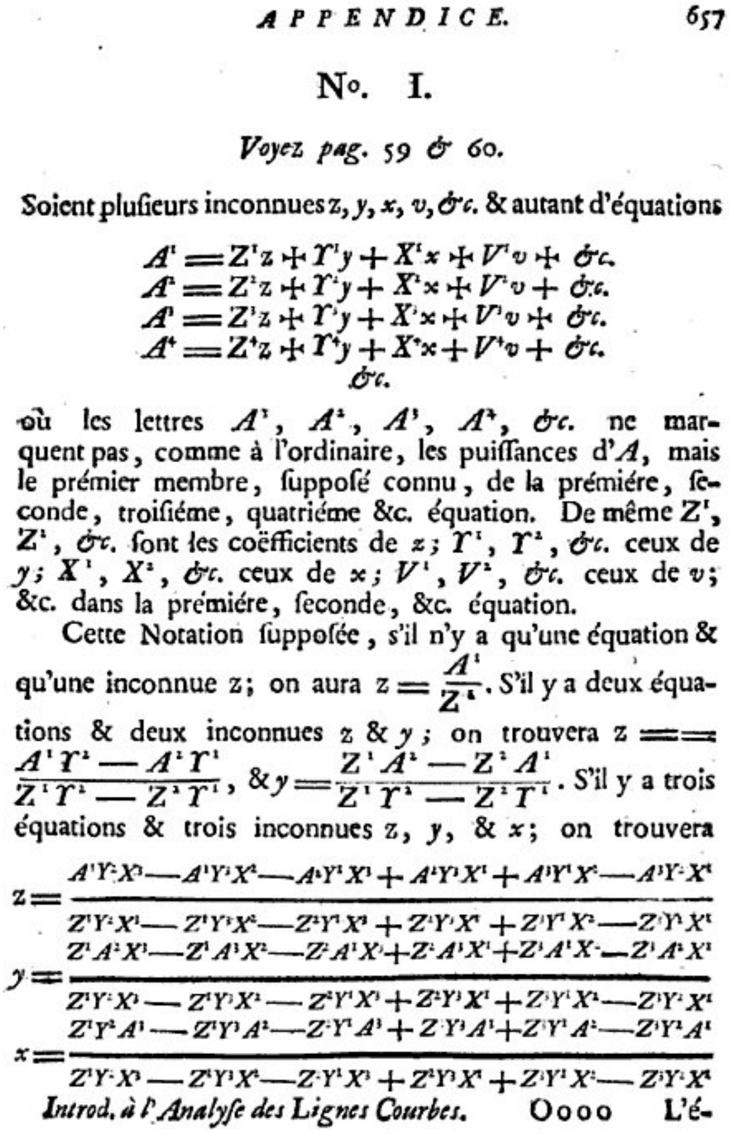
$$\mathbf{A} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

admet pour solutions

$$x_i = \frac{1}{\det(\mathbf{A})} \det \begin{bmatrix} a_1^1 & \cdots & b_1 & \cdots & a_1^n \\ \vdots & & & & \\ a_n^1 & \cdots & b_n & \cdots & a_n^n \end{bmatrix},$$

pour tout $i \in [\![1, n]\!]$.

Cette formule n'est pas toujours très utilisable en pratique, les méthodes de résolution de systèmes linéaires par élimination gaussienne sont plus efficaces. Les formules de Cramer gardent un intérêt théorique qui sera exploité plus loin.



APPENDICE. 657

No. I.

Voyez pag. 59 *&* 60.

Soient pluſieurs inconnues $z, y, x, v,$ *&c.* & autant d'équations

$$A^1 = Z^1z + Y^1y + X^1x + V^1v + \&c.$$
$$A^2 = Z^2z + Y^2y + X^2x + V^2v + \&c.$$
$$A^3 = Z^3z + Y^3y + X^3x + V^3v + \&c.$$
$$A^4 = Z^4z + Y^4y + X^4x + V^4v + \&c.$$
&c.

où les lettres A^1, A^2, A^3, A^4, *&c.* ne marquent pas, comme à l'ordinaire, les puiſſances d'A, mais le prémier membre, ſuppoſé connu, de la prémiére, ſeconde, troiſiéme, quatriéme &c. équation. De même Z^1, Z^2, *&c.* ſont les coëfficients de z; Y^1, Y^2, *&c.* ceux de y; X^1, X^2, *&c.* ceux de x; V^1, V^2, *&c.* ceux de v; &c. dans la prémiére, ſeconde, &c. équation.

Cette Notation ſuppoſée, s'il n'y a qu'une équation & qu'une inconnue z; on aura $z = \frac{A^1}{Z^1}$. S'il y a deux équations & deux inconnues z & y; on trouvera $z = \frac{A^1Y^2 - A^2Y^1}{Z^1Y^2 - Z^2Y^1}$, & $y = \frac{Z^1A^2 - Z^2A^1}{Z^1Y^2 - Z^2Y^1}$. S'il y a trois équations & trois inconnues z, y, & x; on trouvera

$$z = \frac{A^1Y^2X^3 - A^1Y^3X^2 - A^2Y^1X^3 + A^2Y^3X^1 + A^3Y^1X^2 - A^3Y^2X^1}{Z^1Y^2X^3 - Z^1Y^3X^2 - Z^2Y^1X^3 + Z^2Y^3X^1 + Z^3Y^1X^2 - Z^3Y^2X^1}$$

$$y = \frac{Z^1A^2X^3 - Z^1A^3X^2 - Z^2A^1X^3 + Z^2A^3X^1 + Z^3A^1X^2 - Z^3A^2X^1}{Z^1Y^2X^3 - Z^1Y^3X^2 - Z^2Y^1X^3 + Z^2Y^3X^1 + Z^3Y^1X^2 - Z^3Y^2X^1}$$

$$x = \frac{Z^1Y^2A^3 - Z^1Y^3A^2 - Z^2Y^1A^3 + Z^2Y^3A^1 + Z^3Y^1A^2 - Z^3Y^2A^1}{Z^1Y^2X^3 - Z^1Y^3X^2 - Z^2Y^1X^3 + Z^2Y^3X^1 + Z^3Y^1X^2 - Z^3Y^2X^1}$$

Introd. à l'Analyſe des Lignes Courbes. Oooo L'é-

FIGURE 4.3 – « *Introduction à l'analyse des lignes courbes algébriques* » de Gabriel Cramer 1750.

§ 4 Formulation explicite du déterminant

Nous avons vu dans le paragraphe 1, une définition récursive du déterminant. Dans cette section, nous établissons une formulation explicite qui sera utile dans la suite pour établir certaines propriétés des déterminants.

Considérons le cas $n = 2$. Soit

$$\mathbf{A} = \begin{bmatrix} a_1^1 & a_1^2 \\ a_2^1 & a_2^2 \end{bmatrix}$$

une matrice de $\mathcal{M}_2(\mathbb{K})$. La matrice $\mathbf{A}$ s'exprime par colonne sous la forme $\mathbf{A} = \left[\ \mathbf{a}_*^1 \mid \mathbf{a}_*^2\ \right]$. Notons $\mathcal{C}an = (\mathbf{c}_1, \mathbf{c}_2)$ la base canonique de $\mathbb{K}^2$. Les colonnes $\mathbf{a}_*^1$ et $\mathbf{a}_*^2$ qui s'identifient à des vecteurs de $\mathbb{K}^2$ se décomposent dans la base canonique en

$$\begin{aligned}\mathbf{a}_*^1 &= a_1^1\mathbf{c}_1 + a_2^1\mathbf{c}_2\\ \mathbf{a}_*^2 &= a_1^2\mathbf{c}_1 + a_2^2\mathbf{c}_2\end{aligned}$$

Avec ces notations, on a

$$\begin{aligned}\det(\mathbf{A}) &= \det\left[\ \mathbf{a}_*^1 \mid \mathbf{a}_*^2\ \right]\\ &= \det\left[\ a_1^1\mathbf{c}_1 + a_2^1\mathbf{c}_2 \mid a_1^2\mathbf{c}_1 + a_2^2\mathbf{c}_2\ \right]\\ &= (a_1^1a_2^2 - a_2^1a_1^2)\ \det\left[\ \mathbf{c}_1 \mid \mathbf{c}_2\ \right]\end{aligned}$$

Or $\det\left[\ \mathbf{c}_1 \mid \mathbf{c}_2\ \right] = 1$, on retrouve ainsi la formule donnée précédemment : $\det(\mathbf{A}) = a_1^1a_2^2 - a_2^1a_1^2$. Ce qui s'écrit aussi sous la forme

$$\det(\mathbf{A}) = \operatorname{sgn}(\mathrm{Id})a^1_{\mathrm{Id}(1)}a^2_{\mathrm{Id}(2)} + \operatorname{sgn}(\tau)a^1_{\tau(1)}a^2_{\tau(2)},$$

avec $\tau = (1, 2)$. Plus généralement, montrons la formulation suivante

4.4.1 Théorème (Formule de Leibniz).— Soit $\mathbf{A} = [a_i^j]$ une matrice de $\mathcal{M}_n(\mathbb{K})$. On a

$$\det(\mathbf{A}) = \sum_{\sigma\in\mathcal{S}_n} \operatorname{sgn}(\sigma)a^1_{\sigma(1)}\,a^2_{\sigma(2)}\ldots a^n_{\sigma(n)}.$$

§ 5 Calcul des déterminants

Les résultats suivants sont utiles dans la pratique pour le calcul de déterminants.

4.5.1 Proposition.— Pour toute matrice $\mathbf{A}$ de $\mathcal{M}_n(\mathbb{K})$, on a

$$\det(\mathbf{A}^\top) = \det(\mathbf{A}).$$

Comme conséquence de la proposition précédente, on a

4.5.2 Proposition.—

i) le déterminant d'une matrice est une application linéaire par rapport à chaque ligne,

ii) le déterminant d'une matrice dont deux lignes sont égales est nul,

iii) le déterminant d'une matrice change de signe, lorsque l'on échange deux lignes,

iv) le déterminant d'une matrice est non nul si, et seulement si, les vecteurs lignes de la matrice sont linéairement indépendants.

4.5.3. Déterminant d'un produit.— La propriété suivante exprime que le déterminant est compatible au produit de matrices.

4.5.4 Théorème.— Pour toutes matrices $\mathbf{A}$ et $\mathbf{B}$ de $\mathcal{M}_n(\mathbb{K})$, on a

$$\det(\mathbf{AB}) = \det(\mathbf{A})\det(\mathbf{B}).$$

On en déduit la caractérisation importante suivante des matrices inversibles

4.5.5 Proposition.— Une matrice $\mathbf{A}$ de $\mathcal{M}_n(\mathbb{K})$ est inversible si, et seulement si, $\det(\mathbf{A})$ est non nul. On a alors

$$\det(\mathbf{A}^{-1}) = \frac{1}{\det(\mathbf{A})}.$$

§ 6 Calcul de l'inverse d'une matrice

4.6.1. Matrice des cofacteurs.— Soit $\mathbf{A} = [a_i^j]$ une matrice de $\mathcal{M}_n(\mathbb{K})$. On appelle *cofacteur* du coefficient a_i^j le scalaire

$$\mathrm{cof}(a_i^j) = (-1)^{i+j}\det(\mathbf{A}_{\check{i}\check{j}}),$$

où $\mathbf{A}_{\check{i}\check{j}}$ est la matrice obtenue en supprimant la i-ème ligne et la j-ème colonne de $\mathbf{A}$.

On appelle *comatrice de* $\mathbf{A}$, la matrice notée $\mathbf{Com}(\mathbf{A}) = (c_i^j)$, définie par

$$c_i^j = \mathrm{cof}(a_i^j).$$

4.6.2 Proposition.— Pour tout $i \in [\![1, n]\!]$, on a la relation du *développement du déterminant selon la i-ème ligne*

$$\det(\mathbf{A}) = \sum_{j=1}^{n} a_i^j\,\mathrm{cof}(a_i^j). \tag{4.1}$$

De la même façon, pour tout $j \in [\![1, n]\!]$, on a le *développement du déterminant selon la j-ème colonne*

$$\det(\mathbf{A}) = \sum_{i=1}^{n} a_i^j\,\mathrm{cof}(a_i^j). \tag{4.2}$$

De la proposition précédente, on déduit une formule utile pour le calcul de l'inverse d'une matrice.

4.6.3 Théorème.— Pour toute matrice $\mathbf{A}$ de $\mathcal{M}_n(\mathbb{K})$, on a :

$$\mathbf{A}\mathbf{Com}(\mathbf{A})^\top = \mathbf{Com}(\mathbf{A})^\top\mathbf{A} = \det(\mathbf{A})\mathbf{1}_n.$$

Si la matrice $\mathbf{A}$ est inversible, on a la formule d'inversion

$$\mathbf{A}^{-1} = \frac{1}{\det(\mathbf{A})}\mathbf{Com}(\mathbf{A})^\top.$$

Cette formule d'inversion est aussi connue sous le nom de *règle de Cramer*.

4.6.4 Exercice.— Calculer l'inverse des matrices inversibles suivantes

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad \mathbf{C} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \quad \mathbf{D} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$\mathbf{E} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 2 & 1 \end{bmatrix} \quad \mathbf{F} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \quad \mathbf{G} = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix}$$

4.6.5 Exercice.— Trouver la matrice $\mathbf{X}$, telle que $\mathbf{X} = \mathbf{A}\mathbf{X} + \mathbf{b}$, avec

$$\mathbf{A} = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 0 & 0 & 0 \end{bmatrix} \quad \text{et} \quad \mathbf{B} = \begin{bmatrix} 1 & 2 \\ 2 & 1 \\ 3 & 3 \end{bmatrix}.$$

4.6.6 Exercice.— Soit $\mathbf{A}$ une matrice inversible symétrique de $\mathcal{M}_n(\mathbb{K})$. Montrer que la matrice $\mathbf{A}^{-1}$ est symétrique.

§ 7 Déterminant d'un endomorphisme

4.7.1 Proposition.— Deux matrices semblables ont le même déterminant.

Preuve. Soient $\mathbf{A}$ et $\mathbf{B}$ deux matrices semblables de $\mathcal{M}_n(\mathbb{K})$. Il existe donc une matrice inversible $\mathbf{P}$ de $\mathcal{M}_n(\mathbb{K})$ telle que

$$\mathbf{A} = \mathbf{P}\mathbf{B}\mathbf{P}^{-1}.$$

Du théorème 4.5.4, on déduit que

$$\det(\mathbf{A}) = \det(\mathbf{P}\mathbf{B}\mathbf{P}^{-1}) = \det(\mathbf{P})\det(\mathbf{B})\det(\mathbf{P}^{-1}).$$

D'après la proposition 4.5.5, on a $\det(\mathbf{P})\det(\mathbf{P}^{-1}) = 1$. Ainsi, $\det\mathbf{A} = \det\mathbf{B}$. □

Deux matrices semblables, représentent le même endomorphisme exprimé dans des bases différentes. La proposition 4.7.1 permet de définir le déterminant d'un endomorphisme de la façon suivante.

4.7.2. Définition. — Soit E un $\mathbb{K}$-espace vecetoriel de dimension finie n et soit u un endomorphisme de E. On appelle *déterminant de* u le déterminant de la matrice $[u]_{\mathcal{B}}$ qui représente u dans une base quelconque $\mathcal{B}$ de E :

$$\det(u) = \det([u]_{\mathcal{B}}).$$

On peut compléter la caractérisation des applications linéaires inversibles en dimension finie donnée dans la proposition 2.4.16 :

4.7.3 Proposition. — Soit $u : E \longrightarrow E'$ une application linéaire entre deux $\mathbb{K}$-espaces vectoriel de même dimension finie. Les assertions suivantes sont équivalentes :

- **i)** $\det(u)$ est non nul,
- **ii)** u est injective,
- **iii)** u est surjective,
- **iv)** u est bijective
- **v)** $\mathrm{Ker}(u) = \{\mathbf{0}\}$,
- **vi)** $\mathrm{Im}(u) = E'$,
- **vii)** $\mathrm{rg}(u) = \dim(E')$.