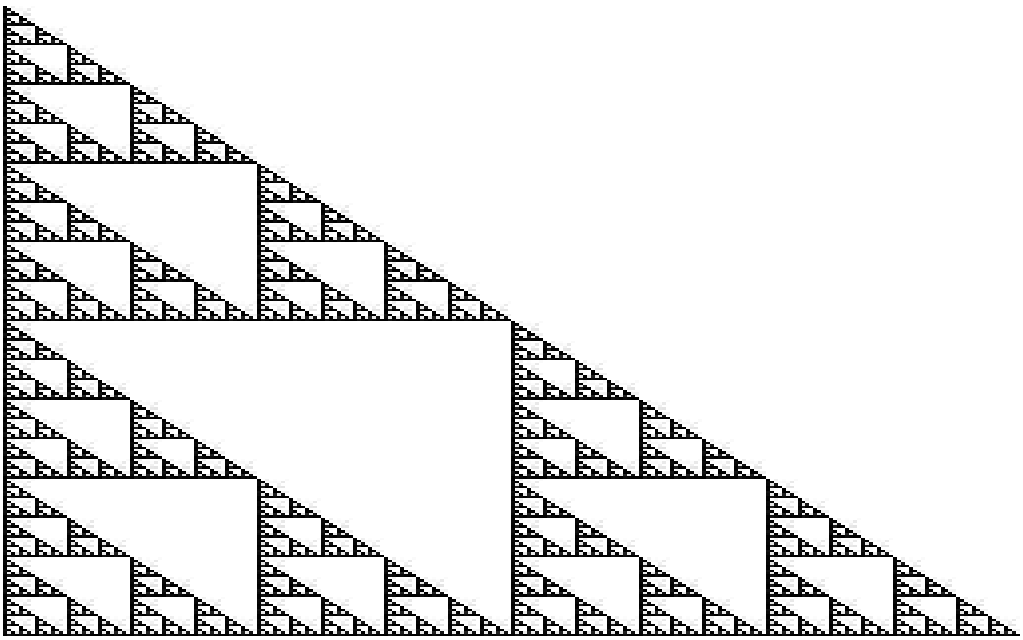
Université de Liège

Faculté des sciences
Département de Mahtématiques

Algèbre linéaire



1ers Bacheliers en sciences mathématiques
2èmes Bacheliers en sciences physiques
Année académique 2009–2010

Michel Rigo

Préambule

Ce texte contient l'ensemble des notes du cours d'*algèbre linéaire* destiné aux premiers bacheliers en sciences mathématiques et deuxièmes bacheliers en sciences physiques.

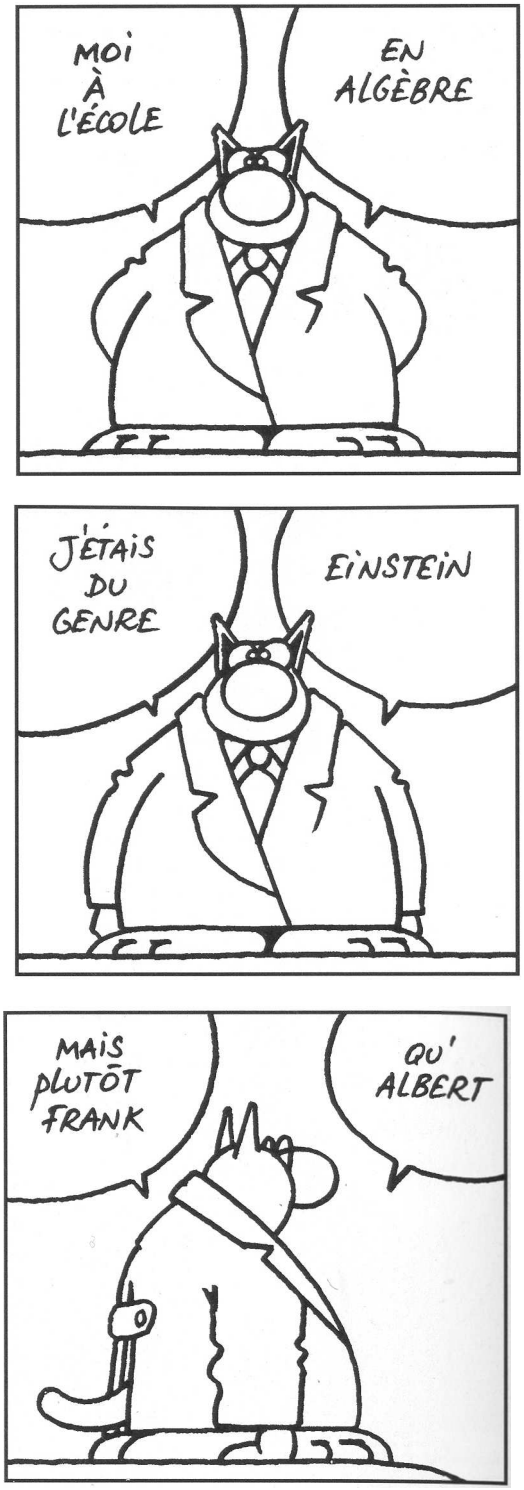
On y présente tout d'abord les nombres complexes pour ensuite aborder les structures algébriques classiques (groupes, anneaux et corps) illustrées principalement par l'intermédiaire des "entiers modulo n". Cela permettra en particulier de définir la notion d'espace vectoriel sur un corps quelconque. Ensuite, on développe les bases du calcul matriciel comprenant une étude complète des déterminants. On étudie également les systèmes d'équations linéaires en insistant, en particulier, sur leur discussion, utile entre autres dans l'étude des lieux géométriques. Les six premiers chapitres dispensés en début d'année académique sont uniquement destinés aux étudiants mathématiciens. Les étudiants physiciens ont reçu une formation analogue dans leurs cours de mathématiques générales, hormis peut-être les structures algébriques classiques qui ne se seront que peu employées dans la suite de ces notes.

Ensuite, on présente les polynômes à coefficients réels ou complexes et le théorème fondamental de l'algèbre ainsi que les fractions rationnelles et les théorèmes de décomposition en fractions simples. On introduit aussi les polynômes à coefficients dans un champ quelconque et ceci débouche sur la notion d'idéal d'un anneau.

Ces notes contiennent des chapitres détaillés portant sur les espaces vectoriels abstraits et les applications linéaires. Enfin, on étudie le problème – capital à de nombreux égards – de la diagonalisation des endomorphismes (i.e., les applications linéaires d'un espace vectoriel dans lui-même), avec comme cas particulier, la diagonalisation des matrices à coefficients réels ou complexes en insistant en particulier sur le cas des matrices hermitiennes, unitaires et normales. La réduction à la forme canonique de Jordan des endomorphismes est également détaillée.

De nombreux chapitres de ce texte se terminent par des applications directes de la théorie, comme par exemple : des problèmes de dénombrement dans un graphe fini, l'analyse input-output ou encore la modélisation de processus stochastiques. Des compléments théoriques sur la matière enseignée concluent les autres chapitres. On y présente par exemple la méthode de résolution de Cardan des équations polynomiales de degrés trois et quatre, l'algorithme de Gauss-Jordan de résolution de systèmes linéaires ou encore des résultats sur le dual d'un espace vectoriel. Ces compléments ont pour modeste ambition de servir de référence au lecteur désirant élargir ses connaissances. L'exposé oral fixe les limites du cours proprement dit.

Enfin, on trouvera tout au long de ce texte, de nombreuses notes en bas de page. Elles ont pour but de fournir des compléments d'information. Le détail de ces notes pourra être passé en revue lors d'une seconde lecture.



Avec l'aimable autorisation de Philippe Geluck.

Table des matières

CHAPITRE I

Nombres complexes

Soyez sûr que je travaille et que je continuerai à le faire jusqu'à la limite de mes forces. Mais un bon travail mathématique ne se fait pas rapidement.

Sonia Kovalevskaia (1850–1891).

Une équation comme $x^2 + 2 = 0$ ne possède pas de solution réelle. Dans ce chapitre, nous introduisons la notion de nombre complexe qui permet de pallier cet inconvient en fournissant des solutions à une équation comme $x^2+2 = 0$. Ce chapitre sera aussi l'occasion de passer en revue quelques constructions mathématiques classiques comme les démonstrations par "récurrence" ou les symboles sommatoires.

1. Quelques notations

Tout au long de ce texte, nous utiliserons la théorie *naïve* des ensembles. Cela signifie que l'on ne définira pas de manière rigoureuse la notion d'ensemble mais qu'on la supposera connue implicitement[1]. En effet, définir un *ensemble* comme une "*collection* d'objets de même nature" poserait le problème de définir ce que l'on entend par collection[2] !

Si A est un ensemble et si a est un élément de A, on écrit $a \in A$ (et cela se lit : "*a appartient à A*") ou encore $A \ni a$. Si A et B sont des ensembles et si tout élément de A est un élément de B, on écrit $A \subset B$ ("*A est inclus dans B*", "*A est une partie de B*"). On trouve aussi l'écriture $B \supset A$. Si deux ensembles A et B ont exactement les mêmes éléments, alors $A = B$. En particulier, $A = B$ si et seulement si $A \subset B$ et $B \subset A$ (ainsi, pour démontrer que deux ensembles sont égaux, il sera souvent commode de vérifier ces deux inclusions). On trouve parfois la notation $A \subseteq B$ pour signaler que A est inclus ou est égal à B (il y a donc une certaine redondance avec la notation $A \subset B$ qui a, somme toute, la même signification). Si par contre, on désire indiquer que A est inclus dans B et est différent de B, on écrira $A \subsetneq B$ ("*A est inclus strictement dans B*"). L'*union* (resp. l'*intersection*) des ensembles A et B est l'ensemble $A \cup B$ (resp. $A \cap B$) des éléments appartenant à A ou

[1] Définir de manière rigoureuse la notion d'ensemble est une question délicate qui n'a pas sa place ici.

[2] Imaginez alors définir une collection comme un ensemble d'objets...

à B (resp. à A et à B). Enfin, l'*ensemble vide*, noté $\emptyset$, est l'unique ensemble ne contenant aucun élément.

Soient A et B deux ensembles, $A \setminus B = \{x \mid x \in A, x \notin B\}$.

Nous allons par la suite manipuler de nombreux ensembles de nombres et nous adopterons les conventions d'écriture suivantes. On note $\mathbb{N}$ l'ensemble des *entiers naturels* : $0, 1, 2, 3, \ldots$ et $\mathbb{N}_0$ l'ensemble des *entiers positifs* : $1, 2, 3, \ldots$ (en d'autres termes, $\mathbb{N}_0 = \mathbb{N} \setminus \{0\}$). On écrit $\mathbb{Z}$ (comme "Zahlen") pour l'ensemble des *entiers relatifs* ou simplement *entiers* : $0, 1, -1, 2, -2, \ldots$ et $\mathbb{Q}$ (comme "quotient") pour l'ensemble des *nombres rationnels*, c'est-à-dire les nombres de la forme $\frac{a}{b}$ où $a \in \mathbb{Z}$ et $b \in \mathbb{N}_0$. Enfin, $\mathbb{R}$ représente l'ensemble des *nombres réels*. Dans ce cours élémentaire, nous ne préciserons pas comment ces ensembles peuvent être construits[3]. Pour rappel, on dispose des inclusions (strictes)

$$\mathbb{N}_0 \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Soient a et b deux nombres réels et $\leq$ la relation d'ordre usuelle sur $\mathbb{R}$, $a \leq b$ se lit "*a est inférieur ou égal à b*". Si de plus, a et b sont distincts, alors on écrit $a < b$ qui se lit *"a est inférieur à b"* (pour insister sur le caractère distinct de a et de b, on peut aussi dire que *"a est strictement inférieur à b"*). On emploie une terminologie analogue si $a \geq b$. Enfin, si a est un nombre réel, $a \geq 0$ (resp. $a > 0$, $a \leq 0$, $a < 0$) se lit "*a est positif ou nul*" (resp. "*a est positif*", "*a est négatif ou nul*", "*a est négatif*").

Définition I.1.1. Soient A et B deux ensembles. Le *produit cartésien* de A et de B est l'ensemble des couples d'éléments de A et de B, i.e.,

$$A \times B = \{(a, b) \mid a \in A,\, b \in B\}.$$

En particulier, il est bien évidemment licite de considérer le produit cartésien de A avec lui-même, $A \times A = \{(a_1, a_2) \mid a_1, a_2 \in A\}$. Notons que pour tout entier $n \geq 2$, si $A_1, \ldots, A_n$ sont des ensembles, on définit le produit cartésien de $A_1, \ldots, A_n$ comme l'ensemble des n-uples dont la j-ième composante appartient à A_j,

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, \ldots, a_n) \mid \forall j \in \{1, \ldots, n\} : a_j \in A_j\}.$$

2. Notion de champ

Les ensembles $\mathbb{Q}$ et $\mathbb{R}$ (ou encore l'ensemble des nombres complexes que nous introduirons bientôt) jouissent des mêmes propriétés structurelles par rapport aux opérations d'addition et de multiplication. Ainsi, plutôt que d'étudier séparément et à plusieurs reprises des objets possédant certaines propriétés communes, il est commode d'introduire un unique concept

[3] On peut, comme Zermelo (1908) ou von Neumann, se ramener à la théorie des ensembles pour définir les entiers naturels. Une fois $\mathbb{Q}$ construit, les nombres réels sont en général obtenus en utilisant la notion de coupure de Dedekind, voir par exemple Roger Godement, *Analyse Mathématique I, Convergence, fonctions élémentaires*, 2ème édition, Springer (2001).

générique regroupant ces propriétés. C'est dans cette optique qu'est introduite la notion de champ.

Définition I.2.1. Un *champ* $\mathbb{K}$ est un ensemble muni de deux opérations binaires internes et partout définies[4]

$$+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$$

et

$$\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$$

qui jouissent des propriétés suivantes.

(1) L'opération $+$ est *associative*

$$\forall a, b, c \in \mathbb{K} : (a + b) + c = a + (b + c).$$

Remarquons dès à présent que cette propriété permet de donner un sens à une expression comme $a + b + c$ puisque les opérations peuvent être réalisées dans n'importe quel ordre.

(2) *Existence d'un neutre* pour $+$

$$\exists e \in \mathbb{K}, \forall a \in \mathbb{K} : a + e = a = e + a.$$

De là, on peut facilement montrer l'unicité[5] du neutre que l'on note dès lors 0.

(3) *Existence d'un opposé* — (1)–(3) : $(\mathbb{K}, +)$ est un groupe

$$\forall a \in \mathbb{K}, \exists b \in \mathbb{K} : a + b = 0 = b + a.$$

On peut montrer que tout élément $a \in \mathbb{K}$ possède un unique opposé noté $-a$.

(4) *Commutativité* de $+$ — (1)–(4) : $(\mathbb{K}, +)$ est un groupe commutatif

$$\forall a, b \in \mathbb{K} : a + b = b + a.$$

(5) L'opération $\cdot$ est *associative*

$$\forall a, b, c \in \mathbb{K} : (a \cdot b) \cdot c = a \cdot (b \cdot c).$$

(6) *Existence d'un neutre* (unique) noté 1 pour l'opération $\cdot$

$$\forall a \in \mathbb{K} : a \cdot 1 = a = 1 \cdot a.$$

(7) L'opération $\cdot$ est *distributive* par rapport à $+$; pour tous a, b, c appartenant à $\mathbb{K}$, on a — (1)–(7) : $(\mathbb{K}, +, \cdot)$ est un anneau

$$(a + b) \cdot c = a \cdot c + b \cdot c \quad \text{et} \quad a \cdot (b + c) = a \cdot b + a \cdot c.$$

[4] L'adjectif "*binaire*" signifie que l'opération requiert deux arguments; l'adjectif "*interne*" stipule que l'opération est à valeurs dans l'ensemble $\mathbb{K}$ et enfin, l'expression "*partout défini*" signifie que l'opération est définie pour chaque couple d'éléments de $\mathbb{K}$.

[5] La démonstration de l'unicité du neutre est laissée au lecteur. Remarquons que c'est précisément parce que le neutre est unique que l'on peut utiliser une notation particulière pour le représenter. Cette remarque s'adapte aisément aux points (3), (6) et (8).

(1)–(8) : $(\mathbb{K}, +, \cdot)$ est un corps

(8) $\mathbb{K} \neq \{0\}$ et tout élément non nul possède un inverse pour l'opération $\cdot$

$$\forall a \in \mathbb{K} \setminus \{0\}, \exists b \in \mathbb{K} : a \cdot b = 1 = b \cdot a.$$

On peut montrer que tout $a \in \mathbb{K} \setminus \{0\}$ possède un unique inverse noté a^{-1}.

(1)–(9) : $(\mathbb{K}, +, \cdot)$ est un champ

(9) Enfin, l'opération $\cdot$ est *commutative*

$$\forall a, b \in \mathbb{K} : a \cdot b = b \cdot a.$$

Remarque I.2.2. Au vu de la propriété (9) dont jouissent les champs, pour tous $a, b \in \mathbb{K}$, $b \neq 0$, on a $a \cdot b^{-1} = b^{-1} \cdot a$. Ceci permet de donner un sens aux notations

$$a/b \quad \text{ou} \quad \frac{a}{b}.$$

En effet, si l'opération $\cdot$ n'était pas commutative, la valeur de $a \cdot b^{-1}$ pourrait différer de celle de $b^{-1} \cdot a$ et dans une écriture comme $\frac{a}{b}$, on ne saurait pas décider si l'on doit mulitplier à gauche ou à droite par b^{-1}.

Exemple I.2.3. Il est laissé au lecteur le soin de vérifier que $\mathbb{Q}$ (resp. $\mathbb{R}$) muni des opérations habituelles d'addition et de multiplication des nombres rationnels (resp. de nombres réels) est un champ. Par contre, $\mathbb{Z}$ n'est pas un champ car la propriété (8) est mise en défaut.

3. Définition de $\mathbb{C}$

L'équation $3x + 2 = 0$ possède une unique solution $x = -2/3$ qui est un nombre rationnel. Par contre, l'équation $x^2 - 2 = 0$ ne possède pas de solution dans $\mathbb{Q}$. Pour trouver les solutions de cette dernière équation, il faut passer à l'ensemble $\mathbb{R}$ et on trouve alors comme solutions $-\sqrt{2}$ et $\sqrt{2}$ qui ne sont pas des nombres rationnels[6]. Si on regarde à présent l'équation $x^2 + 2 = 0$, on s'aperçoit qu'elle ne possède aucune solution réelle (en effet, le carré d'un nombre réel est toujours positif ou nul). Pour pallier cet inconvénient, nous allons introduire le champ $\mathbb{C}$ des nombres complexes[7]. En effet, nous verrons que dans $\mathbb{C}$, toute équation polynomiale de la forme

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = 0$$

[6] Montrer que $\sqrt{2}$ est irrationnel.

[7] Roger Godement, *Analyse Mathématique I*, p. 53 : "On croit souvent que les nombres complexes ont été inventés pour donner des racines aux équations du second degré $ax^2 + bx + c = 0$ lorsque $b^2 - 4ac < 0$. Tel n'est pas le cas : les Italiens du XVIème siècle les ont inventés parce qu'ayant trouvé de miraculeuses formules de résolution des équations du troisième degré, ils ont découvert que ces formules, tout en faisant parfois apparaître des racines carrées de nombres négatifs — donc apparemment "impossibles" — fournissaient néanmoins une racine réelle lorsque l'on portait la formule dans l'équation en calculant sans savoir ce dont on parle. Ils ont ainsi été conduits à introduire des "nombres" nouveaux de la forme $a + b\sqrt{-1}$, où a et b sont des nombres usuels, et à calculer mécaniquement sur ceux-ci en tenant compte du "fait" que le carré de $\sqrt{-1}$ est égal à -1. Plus tard, Euler a introduit la convention consistant à désigner cet étrange nombre par la lettre i."

avec $a_n,\ a_{n-1}, \ldots,\ a_1,\ a_0 \in \mathbb{C}$, possède toujours une solution[8].

Définition I.3.1. On pose

$$\mathbb{C} = \mathbb{R} \times \mathbb{R} = \{(a, b) \mid a, b \in \mathbb{R}\}.$$

$\mathbb{R} \times \mathbb{R}$ est le produit cartésien de deux copies de $\mathbb{R}$. Un nombre complexe n'est autre qu'un couple de réels.

Les éléments de $\mathbb{C}$ sont les *nombres complexes*. On définit la *somme de deux nombres complexes* par

$$+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$$

et

$$(a, b) + (c, d) = (a + c, b + d).$$

Le *produit de deux nombres complexes* est défini par

$$\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$$

et

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Proposition I.3.2. *L'ensemble $\mathbb{C}$ muni des opérations d'addition et de multiplication de nombres complexes est un champ. De plus,*

i) *le neutre pour $+$ est $(0, 0)$;*
ii) *l'opposé de (a, b) est $(-a, -b)$;*
iii) *le neutre pour $\cdot$ est $(1, 0)$;*
iv) *l'inverse de $(a, b) \neq (0, 0)$ est*

$$\left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right).$$

Démonstration. Il s'agit de simples vérifications. A titre d'exemple, vérifions que $\cdot$ est commutatif. Soient (a, b) et (c, d) deux nombres complexes, on a

$$(c, d) \cdot (a, b) = (ca - db, da + cb) = (ac - bd, ad + bc) = (a, b) \cdot (c, d)$$

car la multiplication de nombres réels est commutative. Vérifions à présent le point iv). Soit $(a, b) \neq (0, 0)$, on a par définition de la multiplication de deux nombres complexes

$$(a, b) \cdot \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) = \left(\frac{a^2 - b(-b)}{a^2 + b^2}, \frac{a(-b) + ba}{a^2 + b^2}\right) = (1, 0).$$

■

Définition I.3.3. On identifie un nombre réel a au nombre complexe $(a, 0)$. Cette identification est compatible[9] avec les propriétés de champ dont jouissent $\mathbb{R}$ et $\mathbb{C}$. En effet,

$$(a, 0) + (c, 0) = (a + c, 0),$$

[8] Nous verrons même qu'elle possède exactement n racines si on tient compte des multiplicités. (cf. le théorème fondamental de l'algèbre VIII.3.4.)

[9] Au vu de cette compatibilité par rapport à $+$ et $\cdot$, on dit que cette identification est un homomorphisme (d'anneaux). En fait, par cette identification, $\mathbb{R}$ est en bijection avec le sous-ensemble $\mathbb{R}^* = \{(a, 0) \mid a \in \mathbb{R}\}$ de $\mathbb{C}$. Cette identification entre $\mathbb{R}$ et $\mathbb{R}^*$ étant un homomorphisme bijectif, on dit que $\mathbb{R}$ et $\mathbb{R}^*$ sont isomorphes.

$$(a,0)\cdot(c,0)=(ac,0),$$

le neutre de $\mathbb{C}$ pour l'addition étant $(0,0)$ et celui pour la multiplication $(1,0)$. Le nombre complexe $(0,1)$ se note i et est appelé *unité imaginaire*. Tout nombre complexe de la forme $(0,b)$ est dit *imaginaire pur*. On emploie parfois la notation $\mathbb{R}i$ pour désigner l'ensemble des imaginaires purs.

Proposition I.3.4. *Tout nombre complexe $z\in\mathbb{C}$ s'écrit de manière unique sous la forme*

$$z=a+i\,b$$

avec $a,b\in\mathbb{R}$.

Démonstration. On a $z=a+i\,b$ si et seulement si

$$z=(a,0)+(0,1)\cdot(b,0)=(a,b).$$

■

Proposition I.3.5. *On a $i^2=-1$ et cette relation suffit pour retrouver la structure de champ de $\mathbb{C}$.*

Démonstration. On a

$$i^2=(0,1)\cdot(0,1)=(-1,0)=-1.$$

Utilisons à présent les propriétés de champ de $\mathbb{C}$. Puisque $+$ est associatif et commutatif (cf. les propriétés (1) et (4) de la définition I.2.1), on a

$$(a+i\,b)+(c+id)=(a+c)+i\,(b+d).$$

On retrouve donc bien la définition de l'opération d'addition de deux nombres complexes. En utilisant encore la structure de champ de $\mathbb{C}$, on obtient

$$(a+i\,b)(c+id)=ac+iad+ibc+i^2bd=(ac-bd)+i\,(ad+bc),$$

ce qui suffit.

■

4. Nombres associés à un nombre complexe

Définition I.4.1. Soit $z=a+i\,b$ un nombre complexe avec $a,b\in\mathbb{R}$. On associe à z les nombres suivants

- la *partie réelle* de z est $\mathfrak{Re}\,z=a$,
- la *partie imaginaire* de z est $\mathfrak{Im}\,z=b$,
- le *module* de z est $|z|=\sqrt{a^2+b^2}$,
- le *conjugué* de z est $\overline{z}=a-i\,b$.

Exemple I.4.2. Soit $z=2+3\,i$. On a $\mathfrak{Re}\,z=2$, $\mathfrak{Im}\,z=3$, $|z|=\sqrt{13}$ et $\overline{z}=2-3\,i$.

Proposition I.4.3. *Soient z,z_1,z_2 des nombres complexes. On a*

i) $\overline{\overline{z}}=z$, $\overline{z_1+z_2}=\overline{z_1}+\overline{z_2}$, $\overline{z_1z_2}=\overline{z_1}\,\overline{z_2}$, $\overline{z_1/z_2}=\overline{z_1}/\overline{z_2}$ *si* $z_2\neq 0$,

ii)
$$\mathfrak{Re}\, z = \frac{1}{2}\,(z+\overline{z}),\ \ \mathfrak{Im}\, z = \frac{1}{2\,i}\,(z-\overline{z}),$$
iii) $z \in \mathbb{R} \Leftrightarrow \mathfrak{Im}\, z = 0 \Leftrightarrow z = \overline{z}$,
iv) z *est imaginaire pur* $\Leftrightarrow \mathfrak{Re}\, z = 0 \Leftrightarrow z = -\overline{z}$,
v) *si* $z \neq 0$ *alors*
$$\frac{1}{z} = \frac{\overline{z}}{|z|^2},$$
vi) $|z|^2 = z\overline{z}$, $|\overline{z}| = |z|$, $|z_1 z_2| = |z_1|\,|z_2|$, $|z_1/z_2| = |z_1|/|z_2|$ *si* $z_2 \neq 0$,
vii) $|z_1 + z_2|^2 = |z_1|^2 + 2\,\mathfrak{Re}\,(z_1\overline{z_2}) + |z_2|^2$.

Démonstration. Nous nous contentons de démontrer certaines de ces formules. Les autres sont laissées à titre d'exercice. Le point v) découle de la formule d'inversion donnée dans la proposition I.3.2. Pour le point vii), il vient

$$|z_1 + z_2|^2 = (z_1 + z_2)(\overline{z_1} + \overline{z_2}) = |z_1|^2 + z_1\overline{z_2} + \overline{z_1} z_2 + |z_2|^2$$

On conclut en remarquant que $\overline{z_1} z_2 = \overline{z_1 \overline{z_2}}$ et en appliquant le point ii).

■

Remarque I.4.4. On peut observer que si z_1 et z_2 sont des nombres complexes, alors

$$z_1 = z_2 \Leftrightarrow (\mathfrak{Re}\, z_1 = \mathfrak{Re}\, z_2 \text{ et } \mathfrak{Im}\, z_1 = \mathfrak{Im}\, z_2).$$

Proposition I.4.5. *Soient* z, z_1, z_2 *des nombres complexes. On a*
i) $|\mathfrak{Re}\, z| \leq |z|$, $|\mathfrak{Im}\, z| \leq |z|$,
ii) $|z_1 + z_2| \leq |z_1| + |z_2|$,
iii) $|z_1 - z_2| \geq \big|\,|z_1| - |z_2|\,\big|$.

Démonstration.
i) Soit z un nombre complexe de la forme $a + ib$ avec $a, b \in \mathbb{R}$. Puisque $a^2 \leq a^2 + b^2$ et $b^2 \leq a^2 + b^2$, on trouve
$$|a| \leq \sqrt{a^2 + b^2} \quad \text{et} \quad |b| \leq \sqrt{a^2 + b^2}$$
en d'autres termes $|\mathfrak{Re}\, z| \leq |z|$ et $|\mathfrak{Im}\, z| \leq |z|$.
ii) En utilisant la proposition précédente et le point i) de cette proposition, il vient
$$\begin{aligned} |z_1 + z_2|^2 &= |z_1|^2 + 2\,\mathfrak{Re}\,(z_1\overline{z_2}) + |z_2|^2 \\ &\leq |z_1|^2 + 2\,|z_1|\,|z_2| + |z_2|^2 \\ &\leq (|z_1| + |z_2|)^2, \end{aligned}$$
ce qui suffit.
iii) Par le point précédent, $|z_1| \leq |z_1 - z_2| + |z_2|$ d'où
$$|z_1| - |z_2| \leq |z_1 - z_2|.$$

Par un raisonement analogue, on a aussi

$$|z_2| - |z_1| \leq |z_1 - z_2|,$$

ce qui permet de conclure.

■

5. Forme trigonométrique

Définition I.5.1. Soit $z = a + ib$ un nombre complexe avec $a, b \in \mathbb{R}$. L'*exponentielle* de z, notée e^z, est donnée[10] par

$$e^z = e^a(\cos b + i \sin b).$$

On s'aperçoit que cette définition est compatible avec la définition de l'exponentielle des réels.

Proposition I.5.2. *Soient z, z_1, z_2 des nombres complexes. On a*

i) $e^{z_1} e^{z_2} = e^{z_1+z_2}$,
ii) $(e^z)^{-1} = e^{-z}$,
iii) *pour tout $n \in \mathbb{Z}$,* $(e^z)^n = e^{nz}$.

Démonstration.
i) Soient $z_j = a_j + i\, b_j$ avec $a_j, b_j \in \mathbb{R}$, $j = 1, 2$. Par définition de l'exponentielle complexe, pour $j = 1, 2$, on a

$$e^{z_j} = e^{a_j}(\cos b_j + i \sin b_j).$$

Ainsi,

$$e^{z_1} e^{z_2} = e^{a_1} e^{a_2}[(\cos b_1 \cos b_2 - \sin b_1 \sin b_2) + i(\sin b_1 \cos b_2 + \cos b_1 \sin b_2)]$$

Vu les propriétés de l'exponentielle réelle, on a $e^{a_1} e^{a_2} = e^{a_1+a_2}$ et en utilisant les formules d'addition de la trigonométrie, on obtient

$$e^{z_1} e^{z_2} = e^{a_1+a_2}[\cos(b_1 + b_2) + i \sin(b_1 + b_2)] = e^{z_1+z_2}.$$

ii) En utilisant le point précédent, $e^z e^{-z} = e^0 = 1$, ce qui permet de conclure. Enfin, le point iii) est une conséquence de i) et ii) que l'on applique itérativement.

■

Proposition I.5.3. *Si x est un nombre réel, on a*

$$\cos x = \frac{e^{ix} + e^{-ix}}{2} \quad \text{et} \quad \sin x = \frac{e^{ix} - e^{-ix}}{2i}.$$

Démonstration. C'est une conséquence directe de la définition I.5.1.

■

Si on munit le plan $\mathbb{R}^2$ d'un repère orthonormé ayant O comme origine, alors le nombre complexe $z = a+ib$ est représenté par le point de coordonnées (a, b).

[10] On notera que pour définir l'exponentielle complexe, on utilise des fonctions définies sur $\mathbb{R}$: l'exponentielle réelle $e^{\cdot} : a \in \mathbb{R} \mapsto e^a \in \mathbb{R}$, $\sin : \mathbb{R} \to \mathbb{R}$ et $\cos : \mathbb{R} \to \mathbb{R}$.

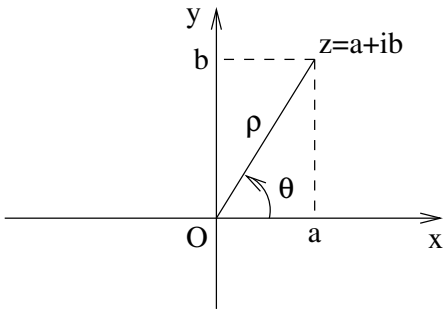


FIGURE I.1. Représentation d'un nombre complexe.

La distance ρ de l'origine du repère O au point z de coordonnées (a, b) est exactement $\sqrt{a^2+b^2} = |z|$. Notons θ la mesure de l'angle orienté entre Ox et Oz. Nous choisissons de prendre θ dans l'intervalle $[0, 2\pi[$. Ce nombre réel est l'*argument* du nombre complexe z. Il est alors immédiat que

$$z = \rho(\cos\theta + i\sin\theta) = \rho\, e^{i\theta}.$$

On dit qu'un nombre complexe écrit de cette façon est mis sous *forme trigonométrique*. On remarquera qu'à tout nombre complexe $z \neq 0$ correspond un unique couple $(\rho, \theta) \in]0, +\infty[\times[0, 2\pi[$ et réciproquement.

On a une bijection entre $\mathbb{C}\setminus\{0\}$ et $]0, +\infty[\times[0, 2\pi[$.

Remarque I.5.4. On dispose ainsi de deux systèmes de coordonnées pour repérer les points du plan complexe : en termes de coordonnées cartésiennes d'une part $(\mathfrak{Re}\, z, \mathfrak{Im}\, z)$ et en termes de coordonnées polaires d'autre part (ρ, θ).

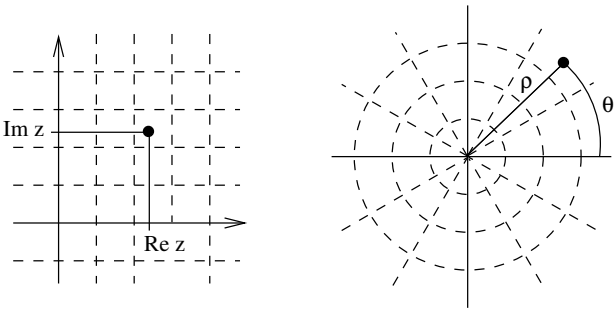


FIGURE I.2. Système de coordonnées cartésiennes et polaires.

Exemple I.5.5. Voici quelques exemples de nombres complexes mis sous forme trigonométrique. Si $z = 1 + i$, on a $|z| = \sqrt{2}$ donc

$$1 + i = \sqrt{2}\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = \sqrt{2}\,(\cos\frac{\pi}{4} + \sin\frac{\pi}{4}) = \sqrt{2}\, e^{i\pi/4}.$$

Si $z = 2 + 3\,i$, on a

$$2 + 3\,i = \sqrt{13}\left(\frac{2}{\sqrt{13}} + i\frac{3}{\sqrt{13}}\right) = \sqrt{13}\,(\cos\theta + i\sin\theta)$$

Pour rappel, arcos : $[-1,1] \to [0,\pi]$ et arcsin est à valeurs dans $[-\frac{\pi}{2}, \frac{\pi}{2}]$.

où $\theta = \arccos(\frac{2}{\sqrt{13}}) = \arcsin(\frac{3}{\sqrt{13}})$ (car $\mathfrak{Re}\, z > 0$ et $\mathfrak{Im}\, z > 0$ donc θ appartient au premier quadrant). Pour terminer, considérons le nombre complexe $z = -2 - 3\,i$. Dans cet exemple, il faut être plus prudent dans la détermination de l'argument car nous recherchons un angle du troisème quadrant. Ainsi,

$$-2 - 3\,i = \sqrt{13}\left(-\frac{2}{\sqrt{13}} - i\frac{3}{\sqrt{13}}\right) = \sqrt{13}\,(\cos\phi + i\sin\phi)$$

Quelques manipulations élémentaires.

où $\phi = 2\pi - \arccos(-\frac{2}{\sqrt{13}}) = \pi - \arcsin(-\frac{3}{\sqrt{13}}) = \pi + \arccos(\frac{2}{\sqrt{13}})$.

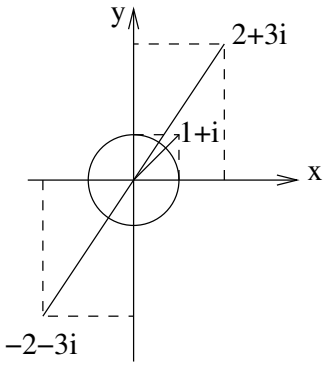


FIGURE I.3. Trois nombres complexes.

Un des avantages de la mise sous forme trigonométrique est de rendre certains calculs plus simples à effectuer, en particulier les multiplications de nombres complexes. En effet, si z_1 et z_2 sont des nombres complexes mis sous forme trigonométrique, $z_j = \rho_j\, e^{i\theta_j}$, $j = 1, 2$, alors

$$z_1 z_2 = (\rho_1\, e^{i\theta_1})\,(\rho_2\, e^{i\theta_2}) = \rho_1\rho_2\, e^{i(\theta_1+\theta_2)}. \tag{1}$$

De plus, si $\rho \neq 0$ alors

$$(\rho\, e^{i\theta})^{-1} = \frac{1}{\rho}\, e^{-i\theta}$$

et pour tout $n \in \mathbb{Z}$,

$$(\rho\, e^{i\theta})^n = \rho^n\, e^{in\theta}.$$

Dans le cas où $\rho = 1$, on retrouve la formule de A. de Moivre qui peut se réécrire

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta.$$

Exemple I.5.6. Voici une application à la trigonométrie. Il est facile de développer

$$(\cos\theta + i\sin\theta)^3 = \cos^3\theta + 3\,i\cos^2\theta\sin\theta - 3\cos\theta\sin^2\theta - i\sin^3\theta.$$

D'autre part, la formule de A. de Moivre donne

$$(\cos\theta + i\sin\theta)^3 = \cos(3\theta) + i\sin(3\theta).$$

En égalant les parties réelles (resp. imaginaires) des deux expressions, on trouve

$$\begin{cases} \cos 3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta \\ \sin 3\theta = 3\cos^2\theta\sin\theta - \sin^3\theta. \end{cases}$$

En se rappelant que $\cos^2\theta + \sin^2\theta = 1$, on retrouve les formules classiques

$$\begin{cases} \cos 3\theta = 4\cos^3\theta - 3\cos\theta \\ \sin 3\theta = 3\sin\theta - 4\sin^3\theta. \end{cases}$$

Exemple I.5.7. Nous présentons ici quelques ensembles de nombres complexes. Soit la partie A de $\mathbb{C}$ définie par $A = \{z \in \mathbb{C} : |z| < 1\}$. Il s'agit de la boule ouverte de rayon un et centrée à l'origine. Soit B défini par $B = \{z \in \mathbb{C} : |z| < 1 \text{ et } |z-1| < 1\}$. Il s'agit de l'intersection de l'ensemble A avec la boule ouverte de rayon 1 et de centre $(1, 0)$. Enfin, considérons $C = \{z \in \mathbb{C} : -1 \leq \mathfrak{Re}\, z \leq 1 \text{ et } -1 \leq \mathfrak{Im}\, z \leq 1\}$.

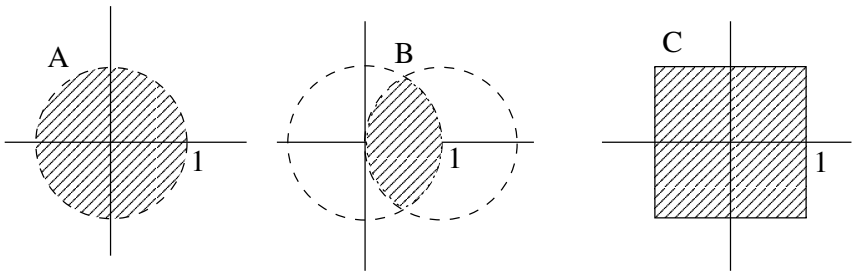


FIGURE I.4. Des parties de $\mathbb{C}$.

6. Interprétation géométrique

Nous avons vu dans la section précédente que tout nombre complexe correspond à un unique point du plan $\mathbb{R}^2$ et réciproquement. Nous allons à présent interpréter géométriquement les opérations d'addition et de multiplication de nombres complexes.

Soit $z_0 = a + i\,b$ un nombre complexe où $a, b \in \mathbb{R}$. Considérons l'application

$$s : \mathbb{C} \to \mathbb{C} : z \mapsto z + z_0.$$

Si $z = c + i\,d$ est un nombre complexe où $c, d \in \mathbb{R}$, alors z est représenté par le point de coordonnées (c, d). Il est clair que $z + z_0 = a + c + i\,(b + d)$ est représenté par le point de coordonnées $(a + c, b + d)$. Dès lors, l'application s correspond à une translation du vecteur $\overrightarrow{Oz_0}$ de composantes (a, b). Une illustration est donnée à la figure I.5.

Considérons à présent l'application

$$p : \mathbb{C} \to \mathbb{C} : z \mapsto z\,z_0.$$

En utilisant la forme trigonométrique introduite précédemment, les nombres z et z_0 peuvent s'écrire respectivement $\rho\,e^{i\theta}$ et $\rho_0\,e^{i\theta_0}$. La formule (1) à la

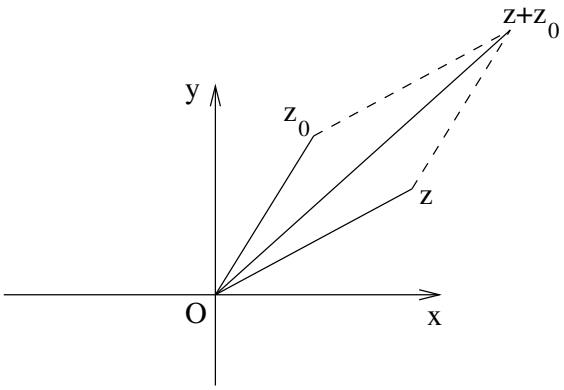


FIGURE I.5. Interprétation de l'addition de deux complexes.

page 10 montre que $z\,z_0$ est un nombre complexe ayant comme argument la somme des arguments de z et z_0 et comme module le produit des modules ρ et ρ_0. De là, l'application p correspond à une rotation d'angle θ_0 suivie d'une homothétie de centre O et de rapport ρ_0. Une illustration est donnée à la figure I.6.

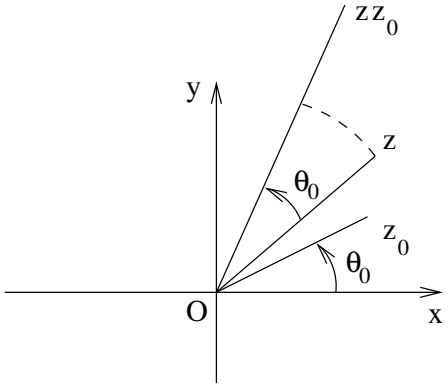


FIGURE I.6. Interprétation du produit de deux complexes.

Exemple I.6.1. Voici un exemple où l'on considère les nombres complexes

$$z_0 = 0,9\,e^{i\pi/9} \quad \text{et } z = e^{i\pi/4}.$$

On représente sur la figure I.7 qui suit les points $z, z\,z_0, z\,z_0^2, \ldots, z\,z_0^n, \ldots$. Observez l'effet des multiplications successives par z_0. On passe de $z\,z_0^n$ à $z\,z_0^{n+1}$ grâce à une rotation d'angle 20° suivie d'une homothétie de rapport 9/10.

Exemple I.6.2. Considérons les trois nombres complexes 3, $-1+i$ et $\frac{1}{2}+2i$ formant le triangle représenté en trait discontinu. La figure I.8 reprend les actions respectives de la multiplication par $e^{i\pi/6}$, $2e^{i\pi/6}$ et $\frac{1}{2}e^{i\pi/6}$.

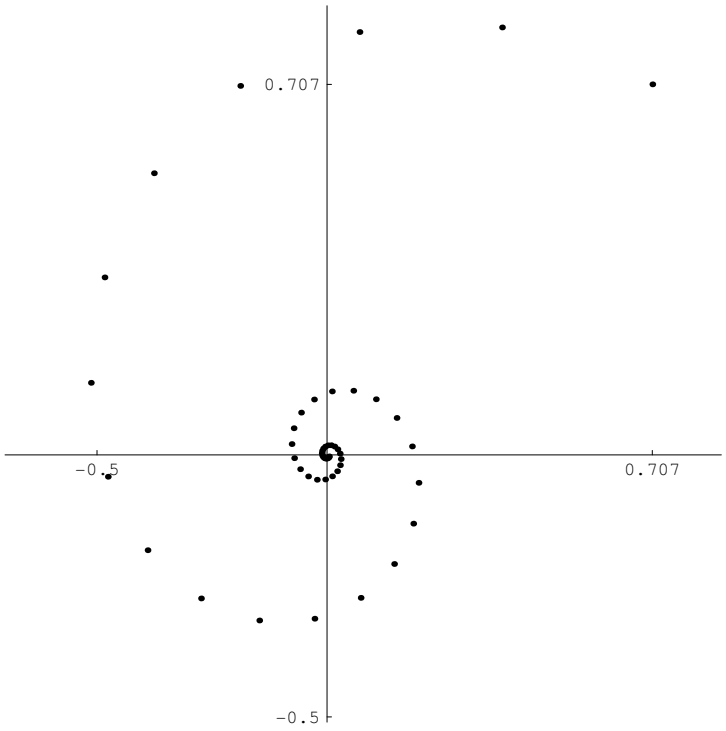


FIGURE I.7. Les nombres $z, z\,z_0, z\,z_0^2, \ldots, z\,z_0^n, \ldots$.

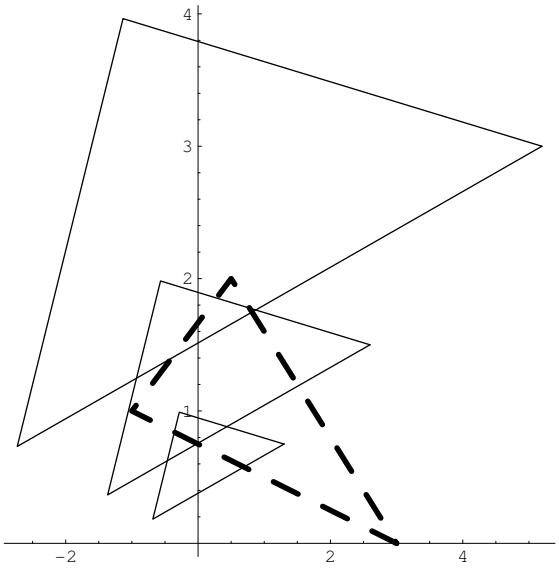


FIGURE I.8. Action de la multiplication par $e^{i\pi/6}$, $2e^{i\pi/6}$ et $\frac{1}{2}e^{i\pi/6}$.

7. Racines carrées

Dans cette section, étant donné un nombre complexe z, notre but est de déterminer les nombres complexes w satisfaisant $w^2 = z$. Nous allons

procéder de deux façons : tout d'abord en utilisant la forme cartésienne puis, en tirant parti de la forme trigonométrique.

Soient a et b deux nombres réels et $z = a + i\,b$. On recherche les nombres réels x et y qui satisfont

$$(x + i\,y)^2 = a + i\,b.$$

En développant le carré et en égalant respectivement les parties réelles et imaginaires des deux membres, cette dernière relation est équivalente à

$$\left\{ \begin{array}{rcl} x^2 - y^2 & = & a \\ 2xy & = & b. \end{array} \right.$$

En élevant les deux égalités au carré et en additionnant membre à membre, on obtient

$$(x^2 + y^2)^2 = a^2 + b^2 \quad \text{et donc} \quad x^2 + y^2 = \sqrt{a^2 + b^2}.$$

En faisant la somme et la différence de la première équation et de la dernière égalité que nous venons d'obtenir, il vient

$$x^2 = \frac{\sqrt{a^2 + b^2} + a}{2} \quad \text{et} \quad y^2 = \frac{\sqrt{a^2 + b^2} - a}{2}.$$

Dès lors,

$$x = \sigma_x \sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}} \quad \text{et} \quad y = \sigma_y \sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}}$$

avec $\sigma_x = \pm 1$ et $\sigma_y = \pm 1$. Quelles que soient les valeurs choisies pour σ_x et σ_y, l'équation $x^2 - y^2 = a$ est toujours satisfaite. Par contre,

$$2xy = 2\sigma_x \sigma_y \sqrt{\frac{a^2 + b^2 - a^2}{4}} = \sigma_x \sigma_y |b|$$

et donc, l'équation $2xy = b$ n'est satisfaite que si

$$\sigma_x \sigma_y |b| = b.$$

$\mathrm{sgn}(b) = 1$, si $b > 0$
$\mathrm{sgn}(b) = -1$, si $b < 0$

Si $b \neq 0$, cette dernière condition signifie que $\sigma_x \sigma_y = \mathrm{sgn}(b)$. Si $b = 0$, la condition est vide. Ainsi,

- pour $b = 0$ et $a \geq 0$, on a
$$x = \pm\sqrt{a} \quad \text{et} \quad y = 0;$$
- pour $b = 0$ et $a < 0$, on a
$$x = 0 \quad \text{et} \quad y = \pm\sqrt{-a};$$
- pour $b \neq 0$, on a
$$(x, y) = \pm \left(\sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}},\ \mathrm{sgn}(b) \sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}} \right).$$

Exemple I.7.1. Les racines carrées de $3-4\,i$ sont

$$2-i \quad \text{et} \quad -2+i.$$

De même, les racines carrées de $3+4\,i$ sont

$$2+i \quad \text{et} \quad -2-i.$$

En utilisant la mise sous forme trigonométrique, les calculs à effectuer pour rechercher les racines carrées d'un nombre complexe sont plus simples. Si $z=\rho\,e^{i\theta}$ où $\rho>0$ et $\theta\in[0,2\pi[$, on cherche $\alpha>0$ et $\beta\in[0,2\pi[$ tels que

$$(\alpha\,e^{i\beta})^2=\rho\,e^{i\theta}.$$

Cette relation est équivalente à

$$\left\{\begin{array}{rcl}\alpha^2 &=& \rho\\ 2\beta &=& \theta+2k\pi, \quad k\in\mathbb{Z}.\end{array}\right.$$

Ou encore à

$$\left\{\begin{array}{rcl}\alpha &=& \sqrt{\rho}\\ \beta &=& \frac{\theta}{2}+k\pi, \quad k\in\mathbb{Z}.\end{array}\right.$$

Or, puisque $\theta\in[0,2\pi[$,

$$\{\frac{\theta}{2}+k\pi \mid k\in\mathbb{Z}\}\cap[0,2\pi[=\{\frac{\theta}{2},\frac{\theta}{2}+\pi\}$$

et les racines carrées de z sont donc

$$\pm\sqrt{\rho}\,e^{i\theta/2}.$$

8. Equations du deuxième degré

Le but de cette section est de résoudre l'équation polynomiale générale du deuxième degré dans $\mathbb{C}$, à savoir

$$az^2+bz+c=0 \tag{2}$$

où $a,b,c\in\mathbb{C}$ et $a\neq 0$. Tout d'abord, remarquons que le premier membre de l'équation (2) se réécrit

$$az^2+bz+c=a\left(z^2+\frac{b}{a}z+\frac{c}{a}\right)=a\left[\left(z+\frac{b}{2a}\right)^2-\frac{b^2-4ac}{4a^2}\right].$$

Ainsi, si on pose $\Delta=b^2-4ac$, z est solution de (2) si et seulement si

$$\left(z+\frac{b}{2a}\right)^2=\frac{\Delta}{4a^2}.$$

En général, Δ est un nombre complexe. Soit δ une de ses racines carrées. On a donc

$$z+\frac{b}{2a}=\pm\frac{\delta}{2a}$$

et les solutions de (2) s'écrivent donc

$$z_1=\frac{-b+\delta}{2a} \quad \text{et} \quad z_2=\frac{-b-\delta}{2a}.$$

Les deux solutions sont distinctes si $\Delta \neq 0$ et confondues sinon. Dans le cas particulier où a, b, c sont réels, Δ est lui aussi un nombre réel. Si $\Delta \geq 0$, les solutions s'écrivent

$$z_1 = \frac{-b + \sqrt{\Delta}}{2a} \quad \text{et} \quad z_2 = \frac{-b - \sqrt{\Delta}}{2a}$$

et sont donc réelles (les solutions sont distinctes si $\Delta > 0$, confondues si $\Delta = 0$). Enfin, si $\Delta < 0$, les solutions sont données par

$$z_1 = \frac{-b + i\sqrt{-\Delta}}{2a} \quad \text{et} \quad z_2 = \frac{-b - i\sqrt{-\Delta}}{2a}$$

qui sont deux nombres complexes conjugués l'un de l'autre.

Remarque I.8.1. Somme et produit des racines de (2). Une conséquence directe de nos développements est que

$$\boxed{z_1 + z_2 = -\frac{b}{a} \quad \text{et} \quad z_1 z_2 = \frac{c}{a}.}$$

Comme nous le verrons plus loin (cf. Proposition VIII.3.7), ces formules se généralisent aux équations polynomiales de degré arbitraire.

9. Puissances n-ièmes

Pour rappel, si $0 \leq k \leq n$, le *coefficient binomial* C_n^k est défini par

$$\mathrm{C}_n^k = \frac{n!}{k!\,(n-k)!}$$

et compte le nombre de choix possibles de k éléments distincts pris parmi n éléments sans tenir compte de l'ordre[11].

Lemme I.9.1 (Triangle de Pascal). *Si* $1 \leq k \leq n$, *alors*

$$\mathrm{C}_n^{k-1} + \mathrm{C}_n^k = \mathrm{C}_{n+1}^k.$$

Démonstration. On a

$$\begin{aligned} \mathrm{C}_n^{k-1} + \mathrm{C}_n^k &= \frac{n!}{(k-1)!\,(n-k+1)!} + \frac{n!}{k!\,(n-k)!} \\ &= \frac{n!\,k}{k!\,(n-k+1)!} + \frac{n!\,(n-k+1)}{k!\,(n-k+1)!} \\ &= \frac{n!\,(n+1)}{k!\,(n-k+1)!} = \mathrm{C}_{n+1}^k. \end{aligned}$$

■

[11] On emploie aussi parfois la notation anglo-saxonne $\binom{n}{k}$, on remarquera que l'ordre des arguments n et k est inversé dans les deux notations.

Remarque I.9.2. A titre indicatif, voici les premières lignes du triangle de Pascal.

C_0^0													1								
C_1^0	C_1^1												1	1							
C_2^0	C_2^1	C_2^2											1	2	1						
C_3^0	C_3^1	C_3^2	C_3^3										1	3	3	1					
C_4^0	C_4^1	C_4^2	C_4^3	C_4^4									1	4	6	4	1				
$\vdots$					$\ddots$								$\vdots$					$\ddots$			
C_n^0	$\dots$	C_n^{k-1}	C_n^k	$\dots$		C_n^n															
		$\searrow$	$\downarrow$																		
C_{n+1}^0		$\dots$	C_{n+1}^k		$\dots$		C_{n+1}^{n+1}														

Avant d'introduire la formule du binôme de Newton, il est grand temps de présenter le *symbole sommatoire* (noté "sigma" majuscule)

$$\sum$$

La manipulation en est primordiale ! Entrainez-vous autant que nécessaire.

qui permet une écriture simplifiée de sommes dont les termes dépendent d'un même indice. Ainsi,

$$\sum_{i=1}^{8} x_i$$

est une écriture abrégée de

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8.$$

On appelle i l'*indice de sommation*. Il s'agit d'une *variable liée* ou "muette" (semblable, dans son rôle, à la variable d'intégration que l'on rencontre sous le signe d'intégration). Ainsi, on peut remplacer cet indice par un autre sans altérer la somme représentée à condition d'effectuer cette substitution partout,

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 = \sum_{\mathbf{k}=1}^{8} x_{\mathbf{k}}.$$

Cette dernière somme se lit "somme pour k allant de 1 à 8 des x_k".

Exemple I.9.3. La somme des n premiers entiers se note

$$1 + 2 + 3 + \cdots + n = \sum_{i=1}^{n} i.$$

Le polynôme $1 + 2x + 3x^2 + 4x^3 + 5x^4 + \cdots + 21x^{20}$ se notera

$$\sum_{i=0}^{20} (i+1)\, x^i.$$

Les propriétés suivantes sont immédiates. Soient $n \in \mathbb{N}_0$ et $a, b, x_1, \dots, x_n$ des nombres complexes :

- $\sum_{i=1}^{n} a x_i = a \sum_{i=1}^{n} x_i$,
- $\sum_{i=1}^{n} (x_i + y_i) = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i$,

- $\sum_{i=1}^{n}(ax_i + by_i) = a\sum_{i=1}^{n} x_i + b\sum_{i=1}^{n} y_i$,
- $\sum_{i=1}^{n} a = n\,a$.

Soit $j \in \mathbb{Z}$, on a

$$\sum_{i=1}^{n} x_i = \sum_{i=1+j}^{n+j} x_{i-j}.$$

Remarque I.9.4. Soient I un ensemble fini de la forme $\{i_1, \ldots, i_k\}$ et des éléments $x_{i_1}, \ldots, x_{i_k}$ indicés par les éléments de I. On dispose alors de la notation

$$\sum_{i\in I} x_i = x_{i_1} + \cdots + x_{i_k}$$

qui généralise le cas précédent. En particulier, si $I = \emptyset$, alors on pose $\sum_{i\in I} x_i = 0$.

On dispose aussi d'une notation analogue pour le produit de n facteurs,

$$x_1 \cdots x_n = \prod_{i=1}^{n} x_i.$$

Cette notation s'étend naturellement à un ensemble fini I d'indices. On a aussi

- $\prod_{i=1}^{n} ax_i = a^n \sum_{i=1}^{n} x_i$,
- $\prod_{i=1}^{n} x_i y_i = (\prod_{i=1}^{n} x_i)\,(\prod_{i=1}^{n} y_i)$,
- $\prod_{i=1}^{n} a = a^n$,
- $\prod_{i\in\emptyset} x_i = 1$.

Remarque I.9.5. La démonstration de la formule du binôme de Newton se fait par *récurrence* sur la valeur de l'exposant. Rappelons le principe d'une telle démonstration. Soit une propriété $P(n)$ où $n \in \mathbb{N}$ est une "variable indéterminée". Pour prouver que la propriété P est vraie pour toute valeur de $n \geq a$, ce que l'on notera : $\forall n \geq a, P(n)$, il suffit de montrer que

- $P(a)$ est vrai,
- si $P(n)$ est vrai, avec $n \geq a$, alors $P(n+1)$ l'est aussi.

Ces étapes sont toutes deux indispensables. La première est appelée le *cas de base* et la seconde est parfois appelée *étape d'induction*. Le fait de supposer $P(n)$ vrai est ce qu'on appelle l'*hypothèse de récurrence*.

C'est même vrai si $n = 0$.

Exemple I.9.6. Démontrer que pour tout $n \in \mathbb{N}_0$, la somme des n premiers entiers vaut $n(n+1)/2$, i.e.,

$$P(n) := \sum_{i=1}^{n} i = \frac{n(n+1)}{2}. \tag{3}$$

Tout d'abord, si $n = 1$, le membre de gauche vaut 1 et celui de droite aussi. Ainsi le cas de base est vérifié (i.e., $P(1)$ est vrai). Supposons à présent la propriété vraie pour n et vérifions-la pour $n+1$. Il vient

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + n + 1 = \frac{n(n+1)}{2} + n + 1 = \frac{n^2+3n+2}{2} = \frac{(n+1)(n+2)}{2}.$$

Ceci prouve que la propriété est encore vérifiée pour $n+1$ (i.e., nous venons donc de montrer que $P(n)$ vrai implique $P(n+1)$ vrai). De là, on en conclut que cette propriété (3) est vraie pour tout $n \in \mathbb{N}_0$.

Proposition I.9.7 (Binôme de Newton). *Soient w et z deux nombres complexes. On a*

$$(w+z)^n = \sum_{k=0}^{n} \mathrm{C}_n^k \, w^k \, z^{n-k}.$$

Démonstration. On procède par récurrence. La formule est vraie si $n = 0$. Supposons-la satisfaite pour $n \geq 0$. Dès lors,

$$\begin{aligned}
(w+z)^{n+1} &= (w+z)\,(w+z)^n \\
&= (w+z) \sum_{k=0}^{n} \mathrm{C}_n^k \, w^k \, z^{n-k} \\
&= \sum_{k=0}^{n} \mathrm{C}_n^k \, w^{k+1} \, z^{n-k} + \sum_{k=0}^{n} \mathrm{C}_n^k \, w^k \, z^{n-k+1} \\
&= \sum_{\ell=1}^{n+1} \mathrm{C}_n^{\ell-1} \, w^{\ell} \, z^{n-\ell+1} + \sum_{\ell=0}^{n} \mathrm{C}_n^{\ell} \, w^{\ell} \, z^{n-\ell+1} \\
&= w^{n+1} + \sum_{\ell=1}^{n} (\mathrm{C}_n^{\ell-1} + \mathrm{C}_n^{\ell}) \, w^{\ell} \, z^{n-\ell+1} + z^{n+1}.
\end{aligned}$$

En utilisant à présent la formule du triangle de Pascal, on trouve

$$\begin{aligned}
(w+z)^{n+1} &= \mathrm{C}_{n+1}^{n+1} \, w^{n+1} + \sum_{\ell=1}^{n} \mathrm{C}_{n+1}^{\ell} \, w^{\ell} \, z^{n-\ell+1} + \mathrm{C}_{n+1}^{0} \, z^{n+1} \\
&= \sum_{k=0}^{n+1} \mathrm{C}_{n+1}^{k} \, w^{k} \, z^{n+1-k}.
\end{aligned}$$

On retrouve bien la formule annoncée quand l'exposant est $n+1$. Par conséquent, la formule du binôme de Newton est satisfaite pour tout entier naturel n.

■

Démonstration. Voici une preuve alternative et bien plus directe! Le terme en $w^i z^{n-i}$, $0 \leq i \leq n$, s'obtient par distributivité en sélectionnant dans l'expression

$$(w+z)^n = (w+z)\,(w+z)\,\cdots(w+z)$$

i fois un terme w dans les n facteurs $(w+z)$ et les $n-i$ autres fois, un terme z. Pour conclure, rappelons que choisir i facteurs parmi n peut se faire de C_n^i façons distinctes.

■

Remarque I.9.8. Un moyen commode pour retenir la formule du binôme de Newton est d'introduire les *puissances divisées* notées $x^{[n]}$ et définies comme suit. Soit $n \in \mathbb{N}$,

$$x^{[n]} = \frac{x^n}{n!}.$$

Avec cette notation, la formule du binôme de Newton se réécrit simplement

$$(w+z)^{[n]} = \sum_{k=0}^{n} w^{[k]}\, z^{[n-k]}.$$

Remarque I.9.9. On peut généraliser aisément la formule du binôme de Newton au cas multinomial. Soient $z_1, \ldots, z_p$ des nombres complexes[12]. On a

$$(z_1 + \cdots + z_p)^n = \sum_{\substack{k_1,\ldots,k_p \in \mathbb{N} \\ k_1+\cdots+k_p=n}} \frac{n!}{k_1! \cdots k_p!}\; z_1^{k_1} \cdots z_p^{k_p}.$$

En recourant aux puissances divisées, cette identité se réécrit

$$(z_1 + \cdots + z_p)^{[n]} = \sum_{\substack{k_1,\ldots,k_p \in \mathbb{N} \\ k_1+\cdots+k_p=n}} z_1^{[k_1]} \cdots z_p^{[k_p]}.$$

Le principe de démonstration est simple mais peu élégant. Il suffit de procéder une fois encore par récurrence. Par exemple, pour ne pas surcharger l'écriture, prenons le cas $p = 3$,

$$\begin{aligned}(z_1+z_2+z_3)^{[n]} &= \sum_{k=0}^{n} (z_1+z_2)^{[k]} z_3^{[n-k]} \\ &= \sum_{k=0}^{n}\sum_{\ell=0}^{k} z_1^{[\ell]} z_2^{[k-\ell]} z_3^{[n-k]} = \sum_{\substack{k_1,k_2,k_3 \in \mathbb{N} \\ k_1+k_2+k_3=n}} z_1^{[k_1]} z_2^{[k_2]} z_3^{[k_3]}.\end{aligned}$$

Une autre méthode consiste (une fois connue la notion de dérivée) à développer les produits se trouvant dans $(z_1+\cdots+z_p)^{[n]}$ pour obtenir une expression de la forme

$$(z_1 + \cdots + z_p)^{[n]} = \sum_{\substack{k_1,\ldots,k_p \in \mathbb{N} \\ k_1+\cdots+k_p=n}} \alpha_{k_1,\ldots,k_p}\, z_1^{k_1} \cdots z_p^{k_p}$$

puis d'appliquer l'opérateur de dérivation $D_{z_1}^{k_1} \cdots D_{z_p}^{k_p}$ aux deux membres (où $k_1 + \cdots + k_p = n$) pour déterminer la valeur de ces coefficients $\alpha_{k_1,\ldots,k_p}$.

[12] On trouve parfois la notation anglo-saxonne $\binom{n}{k_1 \ldots k_p}$ pour le coefficient multinomial $\frac{n!}{k_1! \cdots k_p!}$.

Exemple I.9.10. Soit n un entier naturel, on a

$$\begin{aligned}(x+i\,y)^n &= \sum_{k=0}^{n} \mathrm{C}_n^k\, x^{n-k} i^k y^k \\ &= \left(\sum_{\ell=0}^{\lfloor n/2\rfloor} (-1)^\ell \mathrm{C}_n^{2\ell}\, x^{n-2\ell} y^{2\ell}\right) \\ &\quad + i\left(\sum_{\ell=0}^{\lfloor (n-1)/2\rfloor} (-1)^\ell \mathrm{C}_n^{2\ell+1}\, x^{n-2\ell-1} y^{2\ell+1}\right).\end{aligned}$$

La notation $\lfloor x\rfloor$ désigne la partie entière (par défaut) de x, $\sup\{y\in\mathbb{Z}\mid y\le x\}$. Par exemple, $\lfloor 1,2\rfloor = 1$, $\lfloor \pi\rfloor = 3$, $\lfloor -2,5\rfloor = -3$ et $\lfloor 7\rfloor = 7$.

De là, on a directement une expression pour $\mathfrak{Re}\,(x+i\,y)^n$ et $\mathfrak{Im}\,(x+i\,y)^n$ sous forme de polynômes en x et en y. Dans le cas particulier où $x=\cos\theta$ et $y=\sin\theta$, ces formules permettent d'exprimer $\cos n\theta$ et $\sin n\theta$ comme des polynômes en $\cos\theta$ et $\sin\theta$. (Pour $n=3$, on réobtient les formules données dans l'exemple I.5.6.)

10. Racines n-ièmes

La section précédente nous a montré que l'écriture sous forme cartésienne des nombres complexes pouvait conduire à des expressions délicates pour la recherche des racines n-ièmes d'un nombre complexe lorsque $n>2$. Nous allons donc considérer ici un nombre complexe $z\neq 0$ sous la forme

$$z=\rho\,e^{i\theta} \quad \text{avec } \rho>0 \text{ et } \theta\in[0,2\pi[.$$

Le problème posé est de déterminer les nombres complexes w tels que

$$w^n = z$$

où

$$w=\alpha\,e^{i\beta} \quad \text{avec } \alpha>0 \text{ et } \beta\in[0,2\pi[.$$

L'équation $w^n=z$ est équivalente à

$$\alpha^n\, e^{in\beta} = \rho\, e^{i\theta}$$

c'est-à-dire à

$$\left\{\begin{array}{rcl} \alpha^n &=& \rho \\ n\beta &=& \theta + 2k\pi,\ k\in\mathbb{Z}.\end{array}\right.$$

Ces relations ayant lieu si et seulement si

$$\alpha = \sqrt[n]{\rho}$$

et

$$\beta\in\left\{\frac{\theta}{n}+2k\frac{\pi}{n} : k\in\mathbb{Z}\right\}\cap[0,2\pi[=\left\{\frac{\theta}{n}+2k\frac{\pi}{n} : k=0,\dots,n-1\right\}.$$

Par conséquent, le nombre complexe $z\neq 0$ possède n racines n-ièmes à savoir

$$\boxed{\sqrt[n]{\rho}\,e^{i\,\frac{\theta+2k\pi}{n}} \quad \text{avec } k=0,\dots,n-1.}$$

Remarque I.10.1. Considérons les racines n-ièmes de l'unité. Soit

$$\omega_n = e^{2i\pi/n}.$$

Les racines n-ièmes de l'unité sont

$$U_n = \{1, \omega_n, \omega_n^2, \ldots, \omega_n^{n-1}\}.$$

On remarquera que ces racines sont toutes des nombres complexes de module 1 et que le produit de deux racines est encore une racine de l'unité[13]. Si on représente les éléments de U_n, on obtient un polygone régulier à n côtés inscrit dans le cercle unité et ayant 1 pour sommet. Deux exemples sont donnés à la figure I.9.

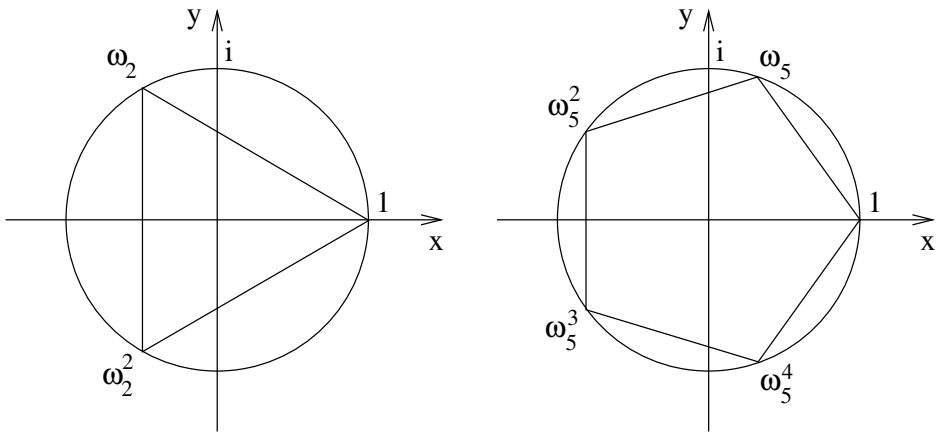


FIGURE I.9. Racines n-ièmes de l'unité pour $n = 3$ et $n = 5$.

Proposition I.10.2. *Soit $n \geq 2$. La somme des racines n-ièmes de l'unité est nulle.*

Démonstration. Pour tout nombre complexe $z \neq 1$, on a

$$1 + z + \cdots + z^{n-1} = \frac{1 - z^n}{1 - z}.$$

Dans cette formule, si $z = \omega_n$, on obtient

$$1 + \omega_n + \cdots + \omega_n^{n-1} = \frac{1 - \omega_n^n}{1 - \omega_n} = 0.$$

■

Proposition I.10.3. *Soit w une racine n-ième du nombre complexe non nul z. Les $n-1$ autres racines n-ièmes de z sont*

$$w\,\omega_n,\ w\,\omega_n^2,\ \ldots,\ w\,\omega_n^{n-1}.$$

Démonstration. Il est immédiat de vérifier que $(w\,\omega_n^j)^n = z$ pour tout $j = 1, \ldots, n-1$.

■

[13]Les racines n-ièmes de l'unité forment un sous-groupe de $(\mathbb{C}, \cdot)$.

Une illustration est donnée à la figure I.10.

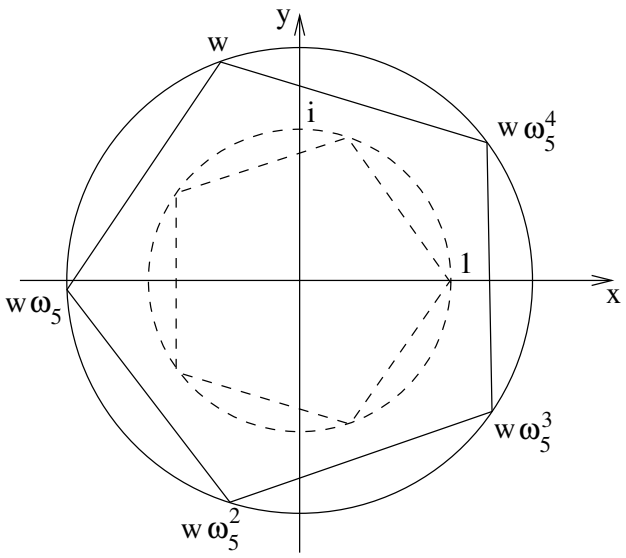


FIGURE I.10. Racines n-ièmes d'un complexe z.

Définition I.10.4. Soit ω une racine n-ième de l'unité. On dit que ω est une racine n-ième *primitive* de l'unité si n est le plus petit entier positif t tel que $\omega^t = 1$.

Exemple I.10.5. Par exemple, i et $-i$ sont les deux seules racines quatrièmes primitives de l'unité. Il s'agit d'une simple vérification.

Proposition I.10.6. *Si ω une racine n-ième primitive de l'unité, alors*

$$\{\omega, \omega^2, \ldots, \omega^{n-1}, \omega^n = 1\}$$

décrit exactement l'ensemble des racines n-ièmes de l'unité.

Démonstration. Nous savons qu'il y a exactement n racines n-ièmes distinctes de l'unité. Pour $j = 1, \ldots, n$, le nombre complexe ω^j est toujours une racine n-ième de l'unité. Il nous suffit dès lors de montrer que si $j, k \in \{1, \ldots, n\}$ avec $j \neq k$, alors $\omega^j \neq \omega^k$. Procédons par l'absurde et supposons de plus que $j < k$. Dans ce cas, $\omega^{k-j} = 1$ et ceci contredit le fait que ω soit une racine primitive.

■

Remarque I.10.7. On peut montrer que $\omega_n^k = e^{2ik\pi/n}$, $k \in \{1, \ldots, n-1\}$, est une racine primitive de l'unité si et seulement si k est premier[14] avec n. On définit une fonction φ qui à tout entier $n \geq 2$, associe le nombre d'entiers strictement inférieurs à n et premiers avec n. On pose $\varphi(1) = 1$. Cette fonction est appelée la *fonction indicatrice d'Euler*. Autrement dit,

[14]Deux entiers sont *premiers entre eux* si leur seul diviseur commun est 1.

le nombre de racines n-ièmes primitives de l'unité vaut $\varphi(n)$. Voici à titre indicatif les premières valeurs de cette fonction,

n	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	2	2	4	2	6	4	6	4	10	4

Exemple I.10.8. Il est clair que 1 et 3 sont premiers avec 4. Ainsi, $\varphi(4) = 2$ et on retrouve donc bien les deux seules racines quatrièmes primitives de l'unité: $\omega_4 = i$ et $\omega_4^3 = -i$.

11. Complément : Equations de degré 3 et 4

Nous avons vu précédemment comment résoudre explicitement une équation de degré 2. Une théorie profonde dûe à E. Galois montre qu'il n'existe pas de méthode explicite pour résoudre une équation polynomiale de degré supérieur à 4. En d'autres termes, il n'est pas possible d'exprimer les solutions de l'équation générale

$$a_n z^n + a_{n-1} z^{n-1} + a_1 z + a_0 = 0$$

où $a_n,\ a_{n-1},\ \ldots, a_1,\ a_0 \in \mathbb{C}$, $a_n \neq 0$ et $n \geq 5$, par des formules ne faisant intervenir que des fonctions rationnelles et l'extraction de racines. Dans ce cas, on utilise des méthodes numériques[15] pour rechercher des approximations des zéros.

Néanmoins, nous allons voir dans cette section que les solutions des équations polynomiales de degré 3 et 4 peuvent être décrites explicitement.

Considérons l'équation générale du troisième degré[16]

$$az^3 + bz^2 + cz + d = 0$$

où $a, b, c, d \in \mathbb{C}$, $a \neq 0$. Pour se débarrasser des termes du second degré, effectuons d'abord la substitution

$$z = w - \frac{b}{3a}.$$

Il est donc équivalent de connaître z ou w.

On se ramène alors à résoudre

$$w^3 + \underbrace{\left(\frac{c}{a} - \frac{b^2}{3a^2}\right)}_{:=p} w + \underbrace{\frac{d}{a} - \frac{bc}{3a^2} + \frac{2b^3}{27a^3}}_{:=q} = 0.$$

Si $p = 0$, la résolution de l'équation revient à chercher les racines cubiques d'un nombre complexe.

Il est donc équivalent de connaître w ou α.

Si $p \neq 0$, on recherche alors w sous la forme

$$w = \alpha - \frac{p}{3\alpha}, \quad \alpha \neq 0.$$

[15] Voir plus tard, le cours d'analyse numérique.

[16] La méthode que nous reprenons ici est dûe à H. Cardan (de son vrai nom, Geronimo Cardano). Elle lui aurait été transmise par N. Tartaglia mais on réfère généralement à la méthode de Cardan.

(On vérifie aisément que tout nombre complexe peut toujours s'écrire sous cette forme.) Il vient ainsi

$$w^3 + pw + q = \left(\alpha - \frac{p}{3\alpha}\right)^3 + p\left(\alpha - \frac{p}{3\alpha}\right) + q = \alpha^3 - \frac{p^3}{27\alpha^3} + q.$$

En réduisant au même dénominateur, on est dès lors amené à résoudre l'équation du second degré en α^3

$$(\alpha^3)^2 + q\alpha^3 - \frac{p^3}{27} = 0. \tag{4}$$

Soit[17] $\Delta = \frac{q^2}{4} + \frac{p^3}{27}$ et δ une de ses racines carrées. On a donc

$$\alpha^3 = -\frac{q}{2} \pm \delta.$$

On obtient de cette manière jusqu'à <u>six</u> valeurs pour α (les trois racines cubiques de $-\frac{q}{2} + \delta$ et aussi celles de $-\frac{q}{2} - \delta$).

Il est remarquable que l'on trouve tous les zéros de l'équation de départ en attribuant à α les valeurs des <u>trois</u> racines cubiques de $-\frac{q}{2}+\delta$ (ou bien, de manière équivalente, en attribuant à α les valeurs des trois racines cubiques de $-\frac{q}{2} - \delta$). En effet, nous allons prouver que pour tout α satisfaisant $\alpha^3 = -\frac{q}{2} + \delta$, on peut trouver β satisfaisant $\beta^3 = -\frac{q}{2} - \delta$ tel que

$$\alpha - \frac{p}{3\alpha} = \beta - \frac{p}{3\beta}$$

et inversement.

En fait, il suffit de <u>choisir</u> α et β tels que $\alpha\beta = -p/3$ ce qui est toujours possible car, si on applique la remarque I.8.1 concernant le produit des racines d'une équation du deuxième degré à l'équation (4), on a

$$(\underbrace{-\frac{q}{2} + \delta}_{\alpha^3})(\underbrace{-\frac{q}{2} - \delta}_{\beta^3}) = (-\frac{p}{3})^3.$$

En toute généralité, si $(\rho\, e^{i\theta})^3 = (\rho'\, e^{i\theta'})^3$ cela n'implique pas $\theta = \theta'$ mais bien $\theta = \theta' + 2k\frac{\pi}{3}$. C'est pour cette raison, qu'un "choix" doit être fait pour assurer $\alpha\beta = -p/3$. Dans ce cas,

$$\beta - \alpha = -\frac{p}{3\alpha\beta}(\beta - \alpha) = -\frac{p}{3\alpha} + \frac{p}{3\beta}$$

et on a bien

$$\alpha - \frac{p}{3\alpha} = \beta - \frac{p}{3\beta}.$$

En résumé, connaissant les 3 valeurs possibles pour α, on trouve les valeurs de w et enfin celles de z.

[17] Pour simplifier les expressions qui suivent, nous pouvons de manière équivalente considérer l'équation $\frac{1}{2}(\alpha^3)^2 + \frac{q}{2}\alpha^3 - \frac{p^3}{2.27} = 0$. Il s'agit d'un artifice permettant d'alléger certaines écritures. On pourrait très bien s'en passer.

Remarque I.11.1. Considérons à présent le cas particulier où $a, b, c, d \in \mathbb{R}$, $a \neq 0$. Plusieurs cas sont à envisager.

i) Si $\Delta > 0$ et $p \neq 0$, alors on a[18]

$$\alpha^3 = -\frac{q}{2} + \sqrt{\Delta}$$

Au vu de la proposition I.10.3, on a pour zéros de $w^3 + pw + q$

$$\alpha - \frac{p}{3\alpha}, \quad \alpha\,\omega - \frac{p}{3\alpha}\omega^2 \quad \text{et} \quad \alpha\,\omega^2 - \frac{p}{3\alpha}\omega$$

avec

$$\alpha = \sqrt[3]{-\frac{q}{2} + \sqrt{\Delta}} \ \text{ et } \ \omega = e^{2i\pi/3}.$$

Le premier zéro est réel. Montrons que les deux autres sont des zéros complexes conjugués. Puisque $\overline{\omega} = \omega^2$, on a

$$\begin{aligned} \mathfrak{Re}\left(\alpha\,\omega - \frac{p}{3\alpha}\omega^2\right) &= \alpha\,\mathfrak{Re}\,\omega - \frac{p}{3\alpha}\,\mathfrak{Re}\,\omega^2 = \left(\alpha - \frac{p}{3\alpha}\right)\,\mathfrak{Re}\,\omega \\ &= \mathfrak{Re}\left(\alpha\,\omega^2 - \frac{p}{3\alpha}\omega\right) \end{aligned}$$

et

$$\mathfrak{Im}\left(\alpha\,\omega - \frac{p}{3\alpha}\omega^2\right) = \alpha\,\mathfrak{Im}\,\omega - \frac{p}{3\alpha}\,\mathfrak{Im}\,\omega^2 = \left(\alpha + \frac{p}{3\alpha}\right)\,\mathfrak{Im}\,\omega.$$

De la même manière,

$$\mathfrak{Im}\left(\alpha\,\omega^2 - \frac{p}{3\alpha}\omega\right) = \alpha\,\mathfrak{Im}\,\omega^2 - \frac{p}{3\alpha}\,\mathfrak{Im}\,\omega = -\left(\alpha + \frac{p}{3\alpha}\right)\,\mathfrak{Im}\,\omega.$$

Il suffit donc de montrer que $\alpha + \frac{p}{3\alpha}$ est non nul. Une fois encore, on a

$$(-\frac{q}{2} + \sqrt{\Delta})(-\frac{q}{2} - \sqrt{\Delta}) = (-\frac{p}{3})^3$$

et dès lors, par définition de α, on a

$$-\frac{p}{3\alpha} = \sqrt[3]{-\frac{q}{2} - \sqrt{\Delta}}.$$

Puisque $\Delta > 0$, on a bien $\alpha \neq -\frac{p}{3\alpha}$. On vérifie facilement qu'on obtient également un zéro réel et deux zéros complexes conjugués lorsque $p = 0$.

ii) Si $\Delta = \frac{q^2}{4} + \frac{p^3}{27} = 0$ et $p \neq 0$, on a

$$\left(w + \frac{3q}{2p}\right)^2 \left(w - \frac{3q}{p}\right) = w^3 - \frac{27q^2}{4p^2}w - \frac{27q^3}{4p^3} = w^3 + pw + q.$$

On est donc en présence d'un zéro réel double et d'un zéro réel simple.

iii) Si $p = q = 0$, l'équation possède un zéro réel triple.

iv) Si $\Delta < 0$, alors nécessairement $p < 0$. Choisissons α tel que

$$\alpha^3 = -\frac{q}{2} + i\sqrt{-\Delta}.$$

Comme en i), les zéros de $w^3 + pw + q$ sont

$$\alpha - \frac{p}{3\alpha}, \quad \alpha\,\omega - \frac{p}{3\alpha}\omega^2 \quad \text{et} \quad \alpha\,\omega^2 - \frac{p}{3\alpha}\omega$$

[18] On a aussi le cas $\alpha^3 = -\frac{q}{2} - \sqrt{\Delta}$ mais nous avons déjà montré précédemment que cette situation fournit les mêmes zéros.

Ces trois zéros sont réels. En effet,

$$(-\frac{q}{2}+i\sqrt{\Delta})(-\frac{q}{2}-i\sqrt{\Delta})=(-\frac{p}{3})^3$$

d'où l'on tire, $|\alpha|^2=-\frac{p}{3}$ et donc $\overline{\alpha}=-\frac{p}{3\alpha}$. Ainsi, puisque $\overline{\omega}=\omega^2$

$$\alpha-\frac{p}{3\alpha}=2\,\mathfrak{Re}\,\alpha,\quad \alpha\,\omega-\frac{p}{3\alpha}\omega^2=2\mathfrak{Re}\,(\alpha\,\omega)\quad\text{et}\ \alpha\,\omega^2-\frac{p}{3\alpha}\omega=2\,\mathfrak{Re}\,(\alpha\,\omega^2).$$

On peut vérifier que ces nombres sont distincts deux à deux. Montrons à titre d'exemple que $\mathfrak{Re}\,\alpha\neq\mathfrak{Re}\,(\alpha\,\omega)$. Procédons par l'absurde et supposons que $\mathfrak{Re}\,\alpha=\mathfrak{Re}\,(\alpha\,\omega)$. Ainsi, $\alpha(1-\omega)$ est un imaginaire pur de la forme it pour un t réel. En élevant au cube, on a

$$\alpha^3(1-3\omega+3\omega^2-\omega^3)=-it^3.$$

Il vient

$$3\,\alpha^3\,[\underbrace{-\cos\frac{2\pi}{3}+\cos\frac{4\pi}{3}}_{=0}+i(\underbrace{-\sin\frac{2\pi}{3}+\sin\frac{4\pi}{3}}_{=-\sqrt{3}})]=-it^3$$

d'où $3\sqrt{3}\alpha^3=t^3\in\mathbb{R}$ alors que α^3 n'est pas réel. D'où l'absurdité.

Considérons pour terminer ce chapitre, l'équation générale[19]

$$az^4+bz^3+cz^2+dz+e=0$$

avec $a,b,c,d,e\in\mathbb{C}$, $a\neq 0$. On peut se ramener à la résolution d'une équation de degré trois de la façon suivante. Quitte à diviser par a, on peut supposer $a=1$. Pour tout nombre complexe ζ, si z est un zéro de l'équation de départ on a

$$\begin{aligned}\left(z^2+\frac{b}{2}z+\zeta\right)^2 &= z^4+bz^3+\left(2\zeta+\frac{b^2}{4}\right)z^2+b\zeta z+\zeta^2\\ &= \left(2\zeta+\frac{b^2}{4}-c\right)z^2+(b\zeta-d)z+\zeta^2-e\end{aligned}$$

On cherche ζ pour que le dernier membre soit de la forme $(pz+q)^2$. Il suffit pour cela que ζ soit un zéro de

$$(b\zeta-d)^2-4\left(2\zeta+\frac{b^2}{4}-c\right)(\zeta^2-e)$$

qui est un polynôme de degré 3 en ζ. Il suffit donc de trouver un zéro de ce dernier polynôme, le calcul des zéros de l'équation de départ se ramenant alors au calcul des zéros de deux polynômes de degré 2.

[19] C'est un élève de Cardan, L. Ferrari, qui a énoncé le premier la règle permettant de résoudre l'équation générale du quatrième degré.

CHAPITRE II

Structures algébriques

1. Relation d'équivalence

Définition II.1.1. Soit A un ensemble. Une *relation d'équivalence* sur A est une partie $\mathfrak{R}$ de $A \times A$ qui est

- *réflexive* : $\forall x \in A,\ (x,x) \in \mathfrak{R}$,
- *symétrique* : $\forall x, y \in A,\ (x,y) \in \mathfrak{R} \Rightarrow (y,x) \in \mathfrak{R}$,
- *transitive* : $[\forall x, y, z \in A,\ (x,y) \in \mathfrak{R} \text{ et } (y,z) \in \mathfrak{R}] \Rightarrow (x,z) \in \mathfrak{R}$.

Remarque II.1.2. Si aucune confusion n'est possible, on s'autorisera souvent à écrire $x\,\mathfrak{R}\,y$ au lieu de $(x,y) \in \mathfrak{R}$. Dans ce cas, on dit que "x est en relation avec y pour $\mathfrak{R}$". Ainsi, exprimer que $\mathfrak{R}$ est symétrique, s'écrira simplement : $\forall x, y \in A,\ x\,\mathfrak{R}\,y \Rightarrow y\,\mathfrak{R}\,x$.

Exemple II.1.3. Définissons une relation $\mathfrak{S}$ sur $\mathbb{R}$ de manière telle que $x\,\mathfrak{S}\,y$ si et seulement si $\sin x = \sin y$. Ainsi, il est évident que pour tout nombre réel θ et tout entier relatif k, on a

$$\theta\,\mathfrak{S}\,(\theta + 2k\pi) \quad \text{et} \quad \theta\,\mathfrak{S}\,(\pi - \theta + 2k\pi).$$

Exemple II.1.4. Deux entiers p et q supérieurs à un sont dits "*multiplicativement indépendants*" si[1] les seuls naturels k et ℓ satisfaisant

$$p^k = q^\ell$$

sont $k = \ell = 0$. Sinon, p et q sont "*multiplicativement dépendants*". Par exemple, 2 et 3 sont multiplicativement indépendants. Par contre, 2 et 4 sont multiplicativement dépendants puisque $2^2 = 4^1$. On vérifie facilement que la relation $p\,\mathfrak{M}\,q$: "p et q sont multiplicativement dépendants" est une relation d'équivalence sur $\mathbb{N}_{\geq 2} = \mathbb{N} \setminus \{0,1\}$.

- Elle est réflexive. Soit $p \geq 2$. On a $p\,\mathfrak{M}\,p$ car $p^1 = p^1$.
- Elle est symétrique. Soient $p, q \geq 2$ tels que $p\,\mathfrak{M}\,q$. Ainsi, il existe des entiers naturels non nuls k et ℓ tels que $p^k = q^\ell$. Cela signifie aussi trivialement que $q\,\mathfrak{M}\,p$.
- Enfin, elle est transitive. Si $p\,\mathfrak{M}\,q$ et $q\,\mathfrak{M}\,r$, alors il existe $k, \ell, m, n \in \mathbb{N}_0$ tels que $p^k = q^\ell$ et $q^m = r^n$. Ainsi, $p^{k.m} = q^{\ell.m} = r^{\ell.n}$ et donc $p\,\mathfrak{M}\,r$.

[1] Montrer que $p, q \geq 2$ sont multiplicativement indépendants si et seulement si $\log p / \log q$ est irrationnel.

Exemple II.1.5. Soient E et F des ensembles non vides et $f : E \to F$ une application. La relation $\mathfrak{R}$ définie sur E par

$$x \,\mathfrak{R}\, y \Leftrightarrow f(x) = f(y)$$

est clairement une relation d'équivalence. L'exemple II.1.3 n'est qu'un cas particulier de la situation décrite ici.

Exemple II.1.6. On considère l'ensemble A des droites du plan affin euclidien $\mathbb{R}^2$. Il est clair que la relation "être parallèle" (que nous noterons $\|$) est une relation d'équivalence sur A. Par exemple, cette relation est transitive : si $\mathcal{D}_1, \mathcal{D}_2$ et $\mathcal{D}_3$ sont trois droites telles que $\mathcal{D}_1 \parallel \mathcal{D}_2$ et $\mathcal{D}_2 \parallel \mathcal{D}_3$, alors $\mathcal{D}_1 \parallel \mathcal{D}_3$.

Définition II.1.7. Soient A un ensemble et $\mathfrak{R}$ une relation d'équivalence sur A. La *classe d'équivalence* de $x \in A$ (pour la relation $\mathfrak{R}$) est l'ensemble des éléments en relation avec x pour $\mathfrak{R}$,

$$[x]_{\mathfrak{R}} = \{y \in A \mid x \,\mathfrak{R}\, y\}.$$

Si $y \in [x]_{\mathfrak{R}}$, on dit que y est un *représentant* de $[x]_{\mathfrak{R}}$.

Exemple II.1.8. Considérons une fois encore la relation "être multiplicativement dépendant". Les premiers éléments de quelques classes d'équivalence pour cette relation sont repris ci-dessous[2] :

$$\begin{array}{rclrcl} [2]_{\mathfrak{M}} &=& \{2,4,8,16,32,64,\ldots\} & [3]_{\mathfrak{M}} &=& \{3,9,27,81,243,\ldots\} \\ [5]_{\mathfrak{M}} &=& \{5,25,125,625,3125,\ldots\} & [6]_{\mathfrak{M}} &=& \{6,36,216,1296,\ldots\} \\ [7]_{\mathfrak{M}} &=& \{7,49,343,2401,16807\} & [10]_{\mathfrak{M}} &=& \{10,100,1000,\ldots\} \\ [11]_{\mathfrak{M}} &=& \{11,121,1331,14641\ldots\} & [12]_{\mathfrak{M}} &=& \{12,144,1728,\ldots\} \end{array}$$

Exemple II.1.9. Si on reprend l'exemple II.1.6, une classe d'équivalence pour la relation $\|$ est constituée de l'ensemble des droites ayant une direction donnée. Si le plan est muni d'un repère, une classe d'équivalence est donc de la forme

Une classe d'équivalence est complètement caractérisée par une direction.

$$\{\mathcal{D} \equiv ax + by = c \mid c \in \mathbb{R}\}$$

où a et b sont des nombres réels fixés.

Proposition II.1.10. *Soient A un ensemble et $\mathfrak{R}$ une relation d'équivalence sur A.*

i) *Pour tout $x \in A$, $[x]_{\mathfrak{R}}$ est un sous-ensemble non vide de A.*

ii) *Pour tous $x, y \in A$, on a*

$$x \,\mathfrak{R}\, y \Leftrightarrow [x]_{\mathfrak{R}} = [y]_{\mathfrak{R}}.$$

iii) *Si x et y ne sont pas en relation, alors $[x]_{\mathfrak{R}} \cap [y]_{\mathfrak{R}} = \emptyset$.*

iv) *L'ensemble des classes d'équivalence pour la relation $\mathfrak{R}$ est une partition[3] de A.*

[2] Le plus petit entier d'une classe pour la relation "être multiplicativement dépendant" est dit *simple*.

[3] Pour rappel, une partition de l'ensemble E est un ensemble de parties $E_i \subset E$ ($i \in I$) toutes non vides, telles que si $i \neq j$ alors $E_i \cap E_j = \emptyset$ et telles que $\cup_{i \in I} E_i = E$.

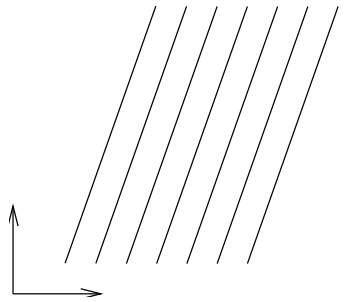


FIGURE II.1. Droites appartenant à la même classe d'équivalence.

Démonstration. Pour i), il est immédiat que $x \in [x]_{\mathfrak{R}}$.

Pour ii), supposons tout d'abord que $x \,\mathfrak{R}\, y$. Soit $t \in A$. Si $t \in [x]_{\mathfrak{R}}$, alors $t \,\mathfrak{R}\, x$. Par transitivité de $\mathfrak{R}$, puisque $x \,\mathfrak{R}\, y$, il vient $t \,\mathfrak{R}\, y$ et donc $t \in [y]_{\mathfrak{R}}$. Nous avons donc montré que $[x]_{\mathfrak{R}} \subset [y]_{\mathfrak{R}}$. Par un raisonnement analogue, on a $[y]_{\mathfrak{R}} \subset [x]_{\mathfrak{R}}$ et donc $[x]_{\mathfrak{R}} = [y]_{\mathfrak{R}}$.

Supposons à présent que $[x]_{\mathfrak{R}} = [y]_{\mathfrak{R}}$. Vu i), y appartient à $[x]_{\mathfrak{R}}$ et donc $x \,\mathfrak{R}\, y$.

Pour démontrer iii), procédons par l'absurde et supposons que x et y ne sont pas en relation et que $[x]_{\mathfrak{R}} \cap [y]_{\mathfrak{R}} \neq \emptyset$. Il existe donc $z \in [x]_{\mathfrak{R}} \cap [y]_{\mathfrak{R}}$. En d'autres termes, $x \,\mathfrak{R}\, z$ et $z \,\mathfrak{R}\, y$. Par transitivité, on conclut que $x \,\mathfrak{R}\, y$ ce qui est absurde.

Au vu de i), chaque classe d'équivalence est non vide et l'union de ces classes est A tout entier. Enfin, si $[x]_{\mathfrak{R}} \neq [y]_{\mathfrak{R}}$, alors par ii), x et y ne sont pas en relation et donc par iii), $[x]_{\mathfrak{R}} \cap [y]_{\mathfrak{R}} = \emptyset$. Le point iv) est ainsi démontré.

■

L'énoncé suivant est une conséquence directe de la proposition II.1.10.

Corollaire II.1.11. *Soient A un ensemble et $\mathfrak{R}$ une relation d'équivalence sur A.*

i) *Tout $x \in \mathfrak{R}$ appartient à une et une seule classe, à savoir $[x]_{\mathfrak{R}}$. En particulier, $x, y \in A$, $x \in [y]_{\mathfrak{R}} \Rightarrow [x]_{\mathfrak{R}} = [y]_{\mathfrak{R}}$,*

ii) *x et y appartiennent à la même classe d'équivalence si et seulement si $x \,\mathfrak{R}\, y$.*

Démonstration. Le premier point est une conséquence directe du point iv) de la proposition II.1.10. Le second point découle du point ii) de la même proposition.

■

Définition II.1.12. Soient A un ensemble et $\mathfrak{R}$ une relation d'équivalence sur A. On pose

$$A/\mathfrak{R} = \{[x]_{\mathfrak{R}} \mid x \in A\}.$$

Cet ensemble formé des classes d'équivalence de A pour $\mathfrak{R}$ est appelé l'*ensemble quotient* de A par $\mathfrak{R}$. L'application

$$\pi_{\mathfrak{R}} : A \to A/\mathfrak{R} : x \mapsto [x]_{\mathfrak{R}}$$

qui à x associe sa classe d'équivalence est appelée *projection canonique*.

Exemple II.1.13. Si on reprend la relation $\mathfrak{M}$ "être multiplicativement dépendant", l'ensemble quotient de $\mathbb{N}_{\geq 2} = \mathbb{N} \setminus \{0, 1\}$ par $\mathfrak{M}$ est[4]

$$\mathbb{N}_{\geq 2}/\mathfrak{M} = \{[2]_{\mathfrak{M}}, [3]_{\mathfrak{M}}, [5]_{\mathfrak{M}}, [6]_{\mathfrak{M}}, [7]_{\mathfrak{M}}, \ldots\}.$$

Remarque II.1.14. Rappelons que $\mathbb{Z}$ est muni de la *division euclidienne*. Ainsi, pour tous entiers $n, k \in \mathbb{Z}$, $k > 0$, il existe deux entiers uniques q et r tels que

$$n = qk + r, \quad 0 \leq r < k.$$

On a supposé ci-dessus $k > 0$. Si $k < 0$ alors $-k > 0$ et on peut appliquer la division euclidienne à n et $-k$. Ainsi, il existe des entiers uniques q et r tels que

$$n = q(-k) + r, \quad 0 \leq r < |k|.$$

Cette relation peut se réécrire $n = (-q)k + r$ où $-q$ est encore un entier et donc, on a l'énoncé général suivant. Si $n, k \in \mathbb{Z}$, $k \neq 0$, il existe deux entiers uniques q et r tels que

$$\boxed{n = qk + r, \quad 0 \leq r < |k|.}$$

L'entier r est le *reste* de la division de n par k et q en est le *quotient*. Si $n \neq 0$, quand le reste est nul, on dit que k divise n, ce que l'on note $k|n$.

Voici des exemples de divisions euclidiennes,

$$\begin{array}{llll} n = 17, & k = 5, & 17 = 3.5 + 2, & 0 \leq 2 < 5 \\ n = -17, & k = 5, & -17 = (-4).5 + 3, & 0 \leq 3 < 5 \\ n = 17, & k = -5, & 17 = (-3).(-5) + 2, & 0 \leq 2 < |-5| \\ n = -17, & k = -5, & -17 = 4.(-5) + 3, & 0 \leq 3 < |-5|. \end{array}$$

Exemple II.1.15. Nous présentons maintenant un exemple fondamental. Soit $m > 1$ un entier positif. Définissons une relation $\mathfrak{R}$ sur $\mathbb{Z}$ par

Le cas $m = 1$ est trivial.

$$x \,\mathfrak{R}\, y \Leftrightarrow x - y \text{ est divisible par } m.$$

Il est facile de vérifier que $\mathfrak{R}$ est une relation d'équivalence. Si $x \,\mathfrak{R}\, y$, on dit que x *est congru à* y *modulo* m ce que l'on note $x \equiv_m y$ ou $x \equiv y \pmod{m}$. En particulier, $x \equiv_m y$ si x et y ont même reste après division euclidienne par m. On note $[x]_m$ la classe d'équivalence de $x \in \mathbb{Z}$ pour la relation $\equiv_m$. Par exemple, si $m = 3$, on a les trois classes d'équivalence

$$\begin{array}{lll} [0]_3 & = & \{0, 3, -3, 6, -6, 9, -9, \ldots\} = \{3n \mid n \in \mathbb{Z}\}, \\ [1]_3 & = & \{1, -2, 4, -5, 7, -8, 10, \ldots\} = \{3n + 1 \mid n \in \mathbb{Z}\}, \\ [2]_3 & = & \{2, -1, 5, -4, 8, -7, 11, \ldots\} = \{3n + 2 \mid n \in \mathbb{Z}\}. \end{array}$$

[4]Il est licite d'écrire par exemple, $4 \in [2]_{\mathfrak{M}} \in \mathbb{N}_{\geq 2}/\mathfrak{M}$ car 4 est un élément de la classe d'équivalence $[2]_{\mathfrak{M}}$ et la classe elle-même est un élément de l'ensemble quotient.

Proposition II.1.16. *Soit m un entier positif. Si $x \in \mathbb{Z}$, alors il existe un unique élément $r \in \{0, \ldots, m-1\}$ tel que*

$$x \equiv_m r.$$

On dit que r est le reste de x modulo m.

Démonstration. Si on effectue la division euclidienne de x par m, on obtient un quotient q et un reste r tels que

$$x = qm + r, \quad 0 \leq r \leq m-1.$$

Ainsi, $x - r$ est divisible par m et par définition, $x \equiv_m r$.

Il reste à démontrer l'unicité. Soient $r, r' \in \{0, \ldots, m-1\}$ tels que $r \equiv_m x \equiv_m r'$. Par transitivité, $r \equiv_m r'$ et il existe donc $k \in \mathbb{Z}$ tel que

$$r' = km + r.$$

Mais $r' = 0.m + r'$. L'unicité de la division euclidienne entraîne que $k = 0$ et $r = r'$.

■

Définition II.1.17. Soit m un entier positif. L'*ensemble $\mathbb{Z}_m$ des entiers modulo m* est l'ensemble quotient[5] de $\mathbb{Z}$ par $\equiv_m$,

$$\mathbb{Z}_m = \mathbb{Z}/\equiv_m .$$

Proposition II.1.18. *Soit m un entier positif. L'application qui à $r \in \{0, \ldots, m-1\}$ associe $[r]_m \in \mathbb{Z}_m$ est une bijection entre $\{0, \ldots, m-1\}$ et $\mathbb{Z}_m$.*

Démonstration. Trivial.

■

Remarque II.1.19. Cette dernière proposition nous montre que l'on peut identifier les ensembles $\{0, \ldots, m-1\}$ et $\mathbb{Z}_m$. Ainsi, si $x \in \{0, \ldots, m-1\}$, on s'autorise souvent à écrire simplement x au lieu de $[x]_m$ si le contexte clarifie la situation.

Exemple II.1.20. La figure II.2 reprend les restes modulo 2 des entrées du triangle de Pascal (0 et 1 sont représentés en blanc et noir respectivement). Ainsi, on peut considérer l'ensemble

$$A = \{(p, q) \in \mathbb{N} \times \mathbb{N} \mid p \geq q\}$$

et la relation d'équivalence $\mathfrak{R}$ sur A définie par

$$(p, q)\, \mathfrak{R}\, (p', q') \Leftrightarrow \mathrm{C}_p^q \equiv \mathrm{C}_{p'}^{q'} \pmod 2.$$

La figure II.2 donne donc une représentation graphique des éléments appartenant aux deux classes d'équivalence.

[5] Cet ensemble est aussi souvent noté $\mathbb{Z}/m\mathbb{Z}$.

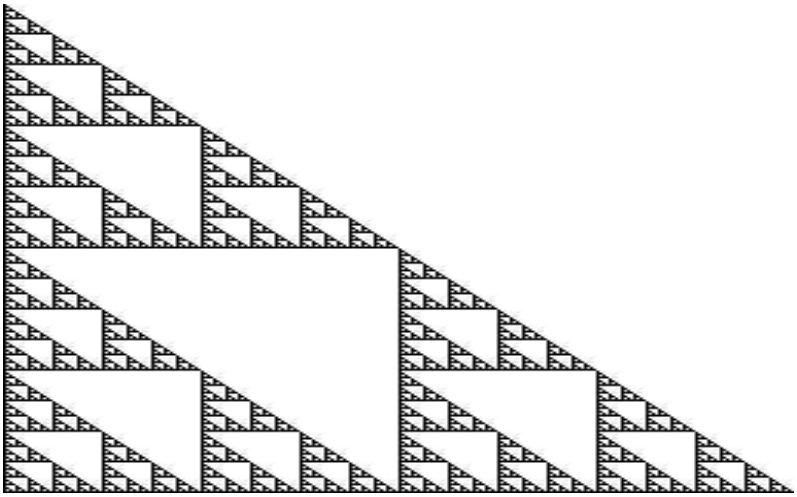


FIGURE II.2. Les 256 premières lignes du triangle de Pascal (mod 2).

2. Groupes

Définition II.2.1. Un *groupe* G est un ensemble muni d'une opération binaire interne et partout définie

$$\circ : G \times G \to G$$

qui jouit des propriétés suivantes :

(1) *associativité*, $\forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c)$
(2) *existence d'un neutre*, $\exists e \in G, \forall a \in G : a \circ e = e \circ a = a$. Il est facile de vérifier que ce neutre est unique (on pourra dès lors utiliser une notation spécifique pour le représenter).
(3) *existence d'un inverse*, $\forall a \in G, \exists b \in G : a \circ b = b \circ a = e$. Une fois encore, l'inverse de a est nécessairement unique.

Si le groupe G possède la propriété supplémentaire suivante,

(4) *commutativité*, $\forall a, b \in G : a \circ b = b \circ a$

on dit alors que G est un *groupe commutatif* ou *groupe abélien*. Dans cette dernière situation, on utilise souvent la notation $+$ au lieu de $\circ$. En particulier, le neutre se note 0 et l'inverse d'un élément a s'appelle alors l'opposé de a et est noté $-a$.

Pour rappeler l'opération dont est muni le groupe, on notera souvent ce dernier par le couple $(G, \circ)$.

Exemple II.2.2. Les ensembles suivants sont des groupes :

$$(\mathbb{Z}, +),\ (\mathbb{Q}, +),\ (\mathbb{R}, +),\ (\mathbb{Q}_0, \cdot),\ (\mathbb{R}_0, \cdot),\ (\mathbb{K}_n^m, +),\ (\mathrm{GL}_n(\mathbb{R}), \cdot).$$

Ici, $\mathbb{K}_n^m$ (resp. $\mathrm{GL}_n(\mathbb{R})$) représente l'ensemble des matrices à coefficients dans $\mathbb{K}$ de forme $m \times n$ (resp. inversibles réelles de forme $n \times n$). Puisque ces nombreux ensembles (et il en existe bien d'autres) jouissent d'une même

L'importance de l'abstraction.

structure de groupe, il est plus commode d'étudier les propriétés générales des groupes plutôt que d'étudier séparément et à plusieurs reprises les propriétés de ces différents ensembles. Nous ne ferons qu'effleurer ces notions par la présentation des entiers modulo.

Exemple II.2.3. Voici un exemple de groupe fini non commutatif. Soit Q un ensemble fini de $\mathbb{C}_2^2$ dont les éléments sont $\{I, -I, J, -J, K, -K, L, -L\}$ où

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, L = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Muni du produit de matrices, l'ensemble Q est un groupe ayant I pour neutre. Ce groupe est appelé le groupe des *quaternions* et on vérifie facilement que

$$JK = -KJ = L,\ KL = -LK = J,\ LJ = -JL = K$$

et

$$J^2 = K^2 = L^2 = -I.$$

Exemple II.2.4. Voici un exemple de groupe utilisant des opérations ensemblistes. Soit X un ensemble. On désigne par $\mathcal{P}(X)$, l'*ensemble des parties*[6] de X, i.e.,

$$\mathcal{P}(X) = \{Y \mid Y \subseteq X\}.$$

Par exemple,

$$\mathcal{P}(\{0,1,2\}) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{1,2,3\}\}.$$

Il est facile de vérifier que $(\mathcal{P}(X), \Delta)$ est un groupe commutatif. Rappelons que si Y et Z sont des parties de X, la *différence symétrique* de Y et Z est

$$Y \Delta Z = (Y \cup Z) \setminus (Y \cap Z) = \{x \in X \mid x \in Y \cup Z \text{ et } x \notin Y \cap Z\}.$$

Le neutre du groupe est $\emptyset$. En effet, pour tout $Y \subseteq X$, $Y \Delta \emptyset = Y = \emptyset \Delta Y$.

Définition II.2.5. Soient $(G, \circ)$ un groupe et H un sous-ensemble de G. Si la restriction de l'opération $\circ$ à H définit un groupe sur H, alors on dit que H est un *sous-groupe* de G.

Nous allons à présent munir l'ensemble $\mathbb{Z}_m$ d'une structure de groupe.

Définition II.2.6. Soit m un entier positif. On définit l'opération

$$+ : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$$

par

$$[x]_m + [y]_m = [x + y]_m.$$

[6] On trouve aussi la notation 2^X au lieu de $\mathcal{P}(X)$. Si X est fini, il est facile de se convaincre que $\#\mathcal{P}(X) = 2^{\#X}$. Ceci explique certainement cette autre notation.

Cette définition a un sens[7]. En effet, si $x \equiv_m x'$ et si $y \equiv_m y'$, alors il existe des entiers relatifs k et ℓ tels que

$$x' = x + km$$
$$y' = y + \ell m.$$

Dès lors,

$$x' + y' = x + y + (k + \ell)m.$$

Par conséquent, $x' + y' \equiv_m x + y$ et en d'autres termes,

$$[x + y]_m = [x' + y']_m.$$

Proposition II.2.7. *L'ensemble $\mathbb{Z}_m$ des entiers modulo m muni de l'opération $+$ définie ci-dessus est un groupe commutatif ayant $[0]_m$ pour neutre. De plus, l'opposé de $[x]_m$ est $[-x]_m$.*

Démonstration. Il s'agit de simples vérifications. Nous montrons uniquement l'associativité de $+$. Soient $x, y, z \in \mathbb{Z}$. Il vient[8]

$$\begin{array}{lll} & ([x]_m + [y]_m) + [z]_m & \\ = & [x + y]_m + [z]_m & \text{, par définition de } + \text{ dans } \mathbb{Z}_m \\ = & [(x + y) + z]_m & \text{, par définition de } + \text{ dans } \mathbb{Z}_m \\ = & [x + (y + z)]_m & \text{, par associativité de } + \text{ dans } \mathbb{Z} \\ = & [x]_m + [y + z]_m & \text{, par définition de } + \text{ dans } \mathbb{Z}_m \\ = & [x]_m + ([y]_m + [z]_m) & \text{, par définition de } + \text{ dans } \mathbb{Z}_m \end{array}$$

■

Exemple II.2.8. Voici les tables des groupes $(\mathbb{Z}_3, +)$ et $(\mathbb{Z}_4, +)$. Pour rappel, si $x \in \{0, \ldots, m-1\}$, nous nous autorisons à écrire x au lieu de $[x]_m$ (cf. remarque II.1.19).

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

On voit par exemple que pour $(\mathbb{Z}_4, +)$, 2 est son propre opposé.

[7] Il faut vérifier que cette définition ne dépend pas du représentant choisi pour les classes $[x]_m$ et $[y]_m$.

[8] Il faut être conscient que nous sommes en présence de deux symboles "+" distincts; d'une part, l'addition de classes d'équivalence définie en II.2.6 et d'autre part, l'addition usuelle d'entiers.

3. Anneaux

En mathématiques, il est fréquent de rencontrer des structures possédant non pas une seule opération mais deux opérations. Nous introduisons donc la notion d'anneau.

Définition II.3.1. Un *anneau* est un ensemble A muni de deux opérations binaires internes et partout définies

$$+ : A \times A \to A$$

et

$$\cdot : A \times A \to A$$

qui jouit des propriétés suivantes

(1) $(A, +)$ est un groupe commutatif (nous conviendrons donc de noter le neutre pour $+$ par 0 et l'opposé de $a \in A$ par $-a$).
(2) L'opération $\cdot$ est associative,
(3) $\cdot$ possède un neutre (nécessairement unique) noté 1,
(4) $\cdot$ est distributif à gauche et à droite par rapport à $+$, i.e., pour tous $a, b, c \in A$,

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c$$

On dit que 0 (resp. 1) est le *zéro* (resp. l'*unité*) de l'anneau.

Si de plus, l'opération $\cdot$ est commutative, alors l'anneau est dit *commutatif*.

Proposition II.3.2. *Si A est un anneau, on a*

$$0 \cdot a = 0,$$
$$(-1) \cdot a = -a.$$

Démonstration. Tout d'abord, on a

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$$

donc $0 \cdot a$ est un neutre pour $+$. D'où la conclusion, vu l'unicité du neutre. Ensuite,

$$\underbrace{0 \cdot a}_{0} = (1 + (-1)) \cdot a = 1 \cdot a + (-1) \cdot a = a + (-1) \cdot a.$$

Ainsi, $(-1) \cdot a$ est bien l'opposé de a.

■

Exemple II.3.3. Les ensembles

$$\mathbb{Z},\ \mathbb{Q},\ \mathbb{R},\ \mathbb{C},\ \mathbb{K}_n^n$$

muni des opérations usuelles d'addition et de multiplication ont une structure d'anneau.

Exemple II.3.4. Nous avons vu dans l'exemple II.2.4 que $(\mathcal{P}(X), \Delta)$ possède une structure de groupe commutatif. Munissons cette structure d'une seconde opération pour en faire un anneau. Il est facile de vérifier que

$$(\mathcal{P}(X), \Delta, \cap)$$

possède une structure d'anneau, le neutre pour $\cap$ étant X. L'opération "d'addition" (resp. de "multiplication") est ici Δ (resp. $\cap$). Le zéro (resp. l'unité) de cet anneau est $\emptyset$ (resp. X). En particulier, dans cet anneau, tout élément est égal à son carré[9]. En effet, $Y \cap Y = Y$.

Définition II.3.5. Soient A est un anneau et B un sous-ensemble de A contenant l'unité de A. Si la restriction des opérations $+$ et $\cdot$ à B définissent un anneau sur B, alors B est qualifié de *sous-anneau* de A.

Dans la section précédente, nous avions muni $\mathbb{Z}_m$ d'une structure de groupe. Nous allons à présent le munir d'une structure d'anneau.

Définition II.3.6. Soit m un entier positif. On définit l'opération

$$\cdot : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$$

par

$$[x]_m \cdot [y]_m = [xy]_m.$$

Vérifions que cette définition a un sens[10]. Si $x' \equiv_m x$ et $y' \equiv_m y$, alors il existe des entiers relatifs k et ℓ tels que

$$x' = x + km$$
$$y' = y + \ell m.$$

Dès lors,

$$x'y' = (x + km)(y + \ell m) = xy + (x\ell + yk + k\ell m)m.$$

Par conséquent, $x'y' \equiv_m xy$ et en d'autres termes,

$$[xy]_m = [x'y']_m.$$

Proposition II.3.7. *L'ensemble $\mathbb{Z}_m$ des entiers modulo m muni de l'opération $+$ donnée dans la définition II.2.6 et de l'opération $\cdot$ définie ci-dessus est un anneau commutatif d'unité $[1]_m$.*

[9] Un anneau ayant cette propriété est qualifié d'*anneau de Boole*.

[10] Pour rappel, nous devons montrer que cette définition ne dépend pas des représentants choisis.

Démonstration. Il s'agit une fois encore de simples vérifications. Montrons la distributivité à gauche de $\cdot$ par rapport à $+$. Soient $x, y, z \in \mathbb{Z}$,

$$\begin{array}{lll} & [x]_m \cdot ([y]_m + [z]_m) & \\ = & [x]_m \cdot [y+z]_m & \text{, par définition de } + \text{ dans } \mathbb{Z}_m \\ = & [x(y+z)]_m & \text{, par définition de } \cdot \text{ dans } \mathbb{Z}_m \\ = & [xy+xz]_m & \text{, par distributivité dans } \mathbb{Z} \\ = & [xy]_m + [xz]_m & \text{, par définition de } + \text{ dans } \mathbb{Z}_m \\ = & [x]_m \cdot [y]_m + [x]_m \cdot [z]_m & \text{, par définition de } \cdot \text{ dans } \mathbb{Z}_m \end{array}$$

Remarquons que l'on utilise le fait que $\mathbb{Z}$ est un anneau. Les vérifications des autres axiomes sont laissées au lecteur.

■

Exemple II.3.8. Poursuivons l'exemple II.2.8 en donnant à présent la table de multiplication de $\mathbb{Z}_3$ et $\mathbb{Z}_4$,

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Définition II.3.9. Soit A un anneau. Un élément $x \in A$ est *inversible* s'il existe un élément $x' \in A$, appelé *inverse* de x, tel que $xx' = x'x = 1$.

Exemple II.3.10. Au vu de l'exemple II.3.8, on remarque que, dans l'anneau $\mathbb{Z}_3$, 2 est inversible et est son propre inverse puisque $2 \cdot 2 = 1$. Par contre, dans $\mathbb{Z}_4$, 2 n'est pas inversible mais 1 et 3 le sont.

Définition II.3.11. Un anneau non trivial A dans lequel tout élément non nul possède un inverse est appelé *corps*. Un corps commutatif[11] est un *champ*.

Exemple II.3.12. Au vu de l'exemple II.3.8, $\mathbb{Z}_3$ est un champ mais $\mathbb{Z}_4$ est un anneau commutatif qui n'est pas un corps.

Pour étudier de manière précise la division dans $\mathbb{Z}_m$, il est nécessaire de revoir en détail certains résultats sur les entiers.

Définition II.3.13. Soit $a, b \in \mathbb{Z}$ tels que $ab \neq 0$. Le *plus grand commun diviseur* (ou *p.g.c.d.*) de a et de b est l'entier positif d qui satisfait aux deux conditions suivantes :

i) $d|a$ et $d|b$,
ii) si $c|a$ et $c|b$, alors $c \leq d$.

L'algorithme d'Euclide permet de rechercher le p.g.c.d. de deux entiers.

Proposition II.3.14. *Soient $a, b \in \mathbb{Z}$ avec $ab \neq 0$. En appliquant succes-*

On pourrait même se restreindre à $a, b \in \mathbb{N}$ car $\text{pgcd}(a,b) = \text{pgcd}(-a,b) = \text{pgcd}(a,-b)$.

[11] Cela signifie que $\cdot$ est commutatif. En effet, par définition d'un anneau, $+$ est toujours commutatif.

sivement la division euclidienne, on obtient la suite d'équations

$$\begin{array}{rcll} b & = & a\,q_1 + r_1, & 0 < r_1 < a \\ a & = & r_1\,q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 & = & r_2\,q_3 + r_3, & 0 < r_3 < r_2 \\ & \vdots & & \\ r_{j-2} & = & r_{j-1}\,q_j + r_j, & 0 < r_j < r_{j-1} \\ r_{j-1} & = & r_j\,q_{j+1}, & r_j \neq 0. \end{array}$$

Le p.g.c.d. de a et de b est le dernier reste non nul r_j.

Lemme II.3.15. *Soient $a, b, m \in \mathbb{Z}$, $ab \neq 0$. On a*

$$\mathrm{pgcd}(a, b + ma) = \mathrm{pgcd}(a, b).$$

Démonstration. Soient d le p.g.c.d de a et de b et g celui de a et de $b + ma$. Puisque $d|a$ et $d|b$, alors $d|b + ma$. Donc d est un diviseur commun de a et de $b + ma$. Pour conclure, il suffit de montrer que $g \leq d$. On sait que $g|a$ et $g|b + ma$; de là on tire que $g|b$. Ainsi, g est un diviseur commun de a et de b donc $g \leq d$.

■

Démontrons à présent l'algorithme d'Euclide.

Démonstration. Par le lemme précédent, il vient immédiatement

$$\mathrm{pgcd}(a, b) = \mathrm{pgcd}(a, r_1) = \mathrm{pgcd}(r_1, r_2) = \ldots = \mathrm{pgcd}(r_{j-1}, r_j) = r_j$$

■

Exemple II.3.16. Calculons le p.g.c.d. de 966 et 429 par l'algorithme d'Euclide,

$$\begin{array}{rcl} 966 & = & 429.2 + 108 \\ 429 & = & 108.3 + 105 \\ 108 & = & 105.1 + 3 \\ 105 & = & 3.35. \end{array}$$

Ainsi, le p.g.c.d. recherché est 3.

Théorème II.3.17 (Théorème de Bezout). *Soient $a, b \in \mathbb{Z}$ tels que $ab \neq 0$ et d le p.g.c.d. de a et de b. Il existe des entiers relatifs x_0 et y_0 tels que*

$$d = ax_0 + by_0.$$

Démonstration. Considérons l'ensemble

$$S = \{ax + by \mid x, y \in \mathbb{Z} \text{ et } ax + by > 0\}.$$

Cet ensemble est une partie non vide de $\mathbb{N}$, elle contient donc un plus petit élément[12] $d = ax_0 + by_0$. Montrons que d est le p.g.c.d. de a et de b en vérifiant qu'il satisfait aux conditions de la définition II.3.13. Supposons

[12] On dit que $\mathbb{N}$ est bien ordonné.

que d ne divise pas a. Dès lors, si on effectue la division euclidienne de a par d, il existe $q, r \in \mathbb{Z}$ tels que

$$a = qd + r, \quad 0 < r < d.$$

Par conséquent,

$$r = a - qd = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0)$$

ce qui signifie que $r \in S$ et $r < d$. Ceci contredit le fait que d est le plus petit élément de S. Par conséquent, $d|a$. De manière analogue, on montre que $d|b$. Soit c un diviseur commun de a et b. Dès lors, $c|ax + by$ pour tous $x, y \in \mathbb{Z}$. Donc $c|d$ et comme $d > 0$, on conclut que $c \leq d$. Ce qui suffit.

■

Remarque II.3.18. Soient $a, b \in \mathbb{Z}$ tels que $ab \neq 0$ et d le p.g.c.d. de a et de b. Les entiers x_0 et y_0 donnés dans le théorème de Bezout peuvent être obtenus par élimination de $r_1, r_2, \ldots, r_{j-1}$ dans le système d'équations fourni par l'algorithme d'Euclide. En effet, on a

$$r_j = r_{j-2} - q_j r_{j-1}$$

et en utilisant l'équation précédente, on trouve

$$r_j = r_{j-2} - q_j(r_{j-3} - q_{j-1} r_{j-2})$$

En continuant de proche en proche, on exprime r_j comme combinaison de a et de b. En particulier, on aurait pu reproduire ici la preuve du théorème VIII.5.14.

Exemple II.3.19. Poursuivons l'exemple II.3.16. En remontant de proche en proche, on a

$$\begin{aligned} 3 &= 108 - 105 \\ &= 108 - (429 - 108.3) = 108.4 - 429 \\ &= (966 - 429.2).4 - 429 = 966.4 + 429.(-9) \end{aligned}$$

Définition II.3.20. Deux entiers non nuls a et b sont *premiers entre eux* ou *relativement premiers* si leur p.g.c.d. vaut 1.

Un entier $p > 1$ est un *nombre premier* si ses seuls diviseurs sont 1 et p. Un entier plus grand que 1 qui n'est pas premier est dit *composé*. Les premiers nombres premiers sont

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, \ldots$$

Proposition II.3.21. *Soient $a, b \in \mathbb{Z}$ tels que $ab \neq 0$; a et b sont premiers entre eux si et seulement si il existe $x, y \in \mathbb{Z}$ tels que $ax + by = 1$.*

Démonstration. La condition est nécessaire par le théorème de Bezout. Supposons à présent qu'il existe $x, y \in \mathbb{Z}$ tels que $ax + by = 1$. Soit d le p.g.c.d. de a et de b. Puisque d divise a et b, il divise $ax + by$ quels que soient $x, y \in \mathbb{Z}$. Comme $d \geq 1$, alors $d = 1$.

■

Proposition II.3.22. *Soient m et a deux entiers positifs. L'élément $x = [a]_m$ de $\mathbb{Z}_m$ est inversible si et seulement si a est premier avec m.*

Démonstration. Soit $a \in \{0, \ldots, m-1\}$ tel que $x = [a]_m$. Supposons que x est inversible dans $\mathbb{Z}_m$. Il existe donc $b \in \{0, \ldots, m-1\}$ tel que

$$[a]_m \cdot [b]_m = [1]_m.$$

Par conséquent, il existe $k \in \mathbb{Z}$ tel que $ab + km = 1$. Par la proposition II.3.21, a et m sont premiers entre eux.

Réciproquement, si a est premier avec m, par la proposition II.3.21, il existe $\alpha, \beta \in \mathbb{Z}$ tels que $a\alpha + m\beta = 1$. De là, on trouve

$$[a]_m \cdot [\alpha]_m = [1]_m,$$

ce qui signifie que $x = [a]_m$ est inversible.

■

Exemple II.3.23. Plaçons-nous dans $\mathbb{Z}_{21}$ et recherchons l'inverse de 8. L'algorithme d'Euclide nous donne

$$\begin{aligned} 21 &= 8.2 + 5 \\ 8 &= 5.1 + 3 \\ 5 &= 3.1 + 2 \\ 3 &= 2.1 + 1 \\ 2 &= 1.1. \end{aligned}$$

On s'aperçoit que 8 et 21 sont premiers entre deux. Ainsi, 8 est bien inversible dans $\mathbb{Z}_{21}$. De ces relations, on tire

$$\begin{aligned} 1 &= 3 - 2 = 3 - (5 - 3.1) = 3.2 - 5 \\ &= (8 - 5).2 - 5 = 8.2 - 5.3 \\ &= 8.2 - (21 - 8.2).3 = 8.8 - 21.3. \end{aligned}$$

Donc $8.8 \equiv_{21} 1$ et l'inverse de $[8]_{21}$ est $[8]_{21}$. A titre d'exercice, on peut vérifier que $[10]_{21}^{-1} = [19]_{21}$.

Par contre, $3.7 = 21 \equiv_{21} 0$, c'est-à-dire que

$$[3]_{21}.[7]_{21} = [0]_{21}.$$

Les nombres 3 et 21 ne sont pas premiers entre eux. Si nous supposons que $[3]_{21}$ est inversible dans $\mathbb{Z}_{21}$, on pourrait multiplier la dernière relation par l'inverse de $[3]_{21}$ et obtenir la contradiction $[7]_{21} = [0]_{21}$ (en effet, $7 \not\equiv_{21} 0$ et donc les classes d'équivalence $[7]_{21}$ et $[0]_{21}$ sont distinctes).

Remarque II.3.24. Dans l'exemple précédent, $\mathbb{Z}_{21}$ n'est pas un corps et on a trouvé deux éléments non nuls dont le produit est nul[13]. Si a et b sont

[13] On dit que $[3]_{21}$ et $[7]_{21}$ sont des diviseurs de zéro.

des éléments d'un corps $\mathbb{K}$ et si $a \cdot b = 0$, alors $a = 0$ ou $b = 0$. En effet, si $a \neq 0$, alors il possède un inverse a^{-1} et en multipliant par cet inverse, on a

$$0 = a^{-1} \cdot a \cdot b = b.$$

Proposition II.3.25. *Soit m un entier supérieur ou égal à 2. L'anneau $\mathbb{Z}_m$ est un champ si et seulement si m est un nombre premier.*

Démonstration. Si $\mathbb{Z}_m$ est un corps, tout élément non nul est inversible. Au vu de la proposition II.3.22, $1, \ldots, m-1$ sont premiers avec m. Par conséquent, m a comme seuls diviseurs 1 et m et est donc premier.

Supposons à présent que $m \geq 2$ est premier. Dans $\mathbb{Z}_m$, $0 \neq 1$ et $1, \ldots, m-1$ sont tous premiers avec m. Par la proposition II.3.22, tous les éléments non nuls de $\mathbb{Z}_m$

$$[1]_m, \ldots, [m-1]_m$$

sont inversibles et donc $\mathbb{Z}_m$ est un corps[14].

■

[14] C'est même un champ.

CHAPITRE III

Matrices

Dans ce chapitre, on considère un champ $\mathbb{K}$ fixé une fois pour toutes[1]. Les éléments de $\mathbb{K}$ sont appelés *scalaires*.

1. Premières définitions

Définition III.1.1. Pour tous entiers positifs m et n, une *matrice* $m \times n$ à coefficients dans $\mathbb{K}$ est un tableau rectangulaire d'éléments de $\mathbb{K}$ formé de m lignes et de n colonnes. On note une matrice par

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}.$$

L'élément de la matrice A se trouvant à la i-ième ligne et à la j-ième colonne se note simplement a_{ij}, $1 \leq i \leq m$, $1 \leq j \leq n$. Pour désigner la matrice A, on écrit aussi parfois

$$A = (a_{ij})_{\substack{1 \leq i \leq m, \\ 1 \leq j \leq n}}$$

et même simplement $A = (a_{ij})$ si les valeurs de m et n sont clairement déterminées par le contexte. L'ensemble des matrices $m \times n$ à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}_n^m$.

Soit $A \in \mathbb{K}_n^m$, m est la *hauteur* de A et n sa *largeur*. La matrice A est

- *horizontale* si $m < n$,
- *verticale* si $m > n$,
- *carrée* si $m = n$,
- *rectangulaire* si $m \neq n$.

Si A est une matrice carrée, on appelle la valeur commune des entiers m et n, la *dimension* de A.

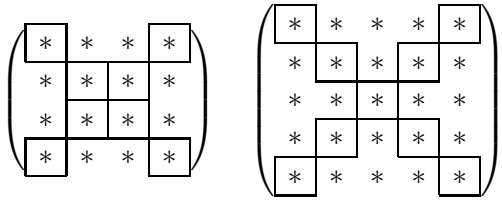
Enfin, deux matrices $A = (a_{ij})$ et $B = (b_{ij})$ de forme $m \times n$ sont *égales* si $a_{ij} = b_{ij}$ pour tous $i \in \{1, \ldots, m\}$ et $j \in \{1, \ldots, n\}$.

[1] On pourra par exemple considérer que $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$. Néanmoins, toutes les notions introduites dans ce chapitre peuvent s'adapter à un champ arbitraire. Rappelons que l'on note 0 (resp. 1) le neutre pour l'opération $+$ (resp. $\cdot$) de $\mathbb{K}$.

Exemple III.1.2. Voici quelques exemples de matrices.

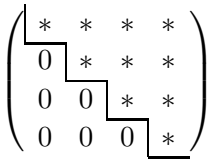
- La matrice horizontale A de $\mathbb{Q}_3^2$ définie par $a_{11} = 1$, $a_{12} = 2$, $a_{13} = 3/4$, $a_{21} = 0$, $a_{22} = -1$ et $a_{23} = 5$ est la matrice
$$A = \begin{pmatrix} 1 & 2 & 3/4 \\ 0 & -1 & 5 \end{pmatrix}.$$
- La matrice verticale B de $\mathbb{R}_2^3$ définie par $a_{ij} = i - j$ est la matrice
$$B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \\ 2 & 1 \end{pmatrix}.$$
- La matrice carrée $\mathfrak{H} = (h_{ij})$ de $\mathbb{R}_n^n$ définie par
$$h_{ij} = \frac{1}{i+j-1}$$
est appelée *matrice de Hilbert*. Si $n = 4$, alors
$$\mathfrak{H} = \begin{pmatrix} 1 & 1/2 & 1/3 & 1/4 \\ 1/2 & 1/3 & 1/4 & 1/5 \\ 1/3 & 1/4 & 1/5 & 1/6 \\ 1/4 & 1/5 & 1/6 & 1/7 \end{pmatrix}.$$

Définition III.1.3. Si $A = (a_{ij})$ est une matrice carrée, les nombres a_{ii} sont les *coefficients diagonaux* de A. La diagonale formée par ces nombres et qui part du coin supérieur gauche est la *diagonale principale* de A. L'autre diagonale de la matrice A qui part du coin supérieur droit est la *diagonale secondaire*. Si n est la dimension de A, cette dernière diagonale est formée des nombres $a_{i,n-i+1}$. Ces deux diagonales sont représentées ci-dessous pour des matrices de dimension 4 et 5 :



On dit que A est *diagonale* si $a_{ij} = 0$ dès que $i \neq j$. Une matrice diagonale étant complètement déterminée par ses coefficients diagonaux $\lambda_1, \ldots, \lambda_n$, on note
$$A = \operatorname{diag}(\lambda_1, \ldots, \lambda_n).$$

La matrice A est *triangulaire supérieure* (resp. *triangulaire inférieure*) si $a_{ij} = 0$ dès que $i > j$ (resp. $i < j$). Voici un exemple de matrice triangulaire supérieure :



Il est souvent commode d'introduire le *symbole de Kronecker* défini par

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

Exemple III.1.4. Considérons la matrice carrée $A \in \mathbb{R}_n^n$ définie par

$$a_{ij} = i\,\delta_{ij}.$$

C'est une matrice diagonale de la forme

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & n \end{pmatrix} = \operatorname{diag}(1, 2, \ldots, n).$$

Définition III.1.5. La *matrice nulle* $m \times n$ est la matrice dont tous les éléments sont nuls. On la note $0_{m,n}$ ou même 0 si m et n sont sous-entendus.

La *matrice unité* (aussi appelée *matrice identité*) de dimension n est la matrice diagonale

$$I_n = \operatorname{diag}(1, \ldots, 1) = (\delta_{ij})_{1 \leq i,j \leq n}.$$

Une matrice $m \times 1$ est appelée *vecteur colonne*. L'ensemble de ces vecteurs se note $\mathbb{K}^m$. De même, une matrice $1 \times n$ est appelée *vecteur ligne*. L'ensemble de ces vecteurs se note $\mathbb{K}_n$.

2. Opérations sur les matrices

2.1. Multiplication scalaire. Soient $\lambda \in \mathbb{K}$ et $A \in \mathbb{K}_n^m$. On note λA la matrice $m \times n$ dont les coefficients sont obtenus en multipliant les coefficients de A par le scalaire λ,

$$\lambda A = (\lambda\, a_{ij})_{\substack{1 \leq i \leq m, \\ 1 \leq j \leq n}}.$$

On vérifie aisément que si $\lambda, \mu \in \mathbb{K}$ et si $A \in \mathbb{K}_n^m$, alors

$$1A = A,$$

$$\lambda(\mu A) = (\lambda\mu)A.$$

Exemple III.2.1. Par exemple,

$$3 \begin{pmatrix} 1 & 0 & 3 \\ 2 & \pi & 0 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 9 \\ 6 & 3\pi & 0 \\ 0 & 0 & -3 \end{pmatrix}.$$

2.2. Addition. La somme de deux matrices n'est définie que si elles ont même forme. Soient $A, B \in \mathbb{K}_n^m$, on note $A+B$ la matrice dont les coefficients s'obtiennent en additionnant les coefficients correspondants de A et de B,

$$A + B = (a_{ij} + b_{ij})_{\substack{1\le i\le m,\\ 1\le j\le n}}.$$

On vérifie aisément que si $\lambda, \mu \in \mathbb{K}$ et si $A, B, C \in \mathbb{K}_n^m$, alors

$$(\lambda+\mu)A = \lambda A + \mu A,$$
$$\lambda(A+B) = \lambda A + \lambda B$$

et aussi[2]

$$(A+B)+C = A+(B+C)$$
$$A+B = B+A$$
$$A+0 = 0+A = A.$$

L'opposé de la matrice A se note $-A = (-1)A$.

Exemple III.2.2. Par exemple,

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} -1 & 3 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 5 \\ 3 & 6 \end{pmatrix}.$$

Définition III.2.3. Soient $A_1, \ldots, A_r \in \mathbb{K}_n^m$ et $\lambda_1, \ldots, \lambda_r \in \mathbb{K}$. Une expression de la forme

$$\sum_{j=1}^{r} \lambda_i \, A_i = \lambda_1 A_1 + \cdots + \lambda_r A_r$$

est appelée une *combinaison linéaire* des matrices $A_1, \ldots, A_r$. Les scalaires $\lambda_1, \ldots, \lambda_r$ sont les *coefficients* de cette combinaison.

2.3. Multiplication. Le produit de deux matrices A et B n'est défini que si le nombre de colonnes de A est égal au nombre de lignes de B. Soient $A \in \mathbb{K}_n^m$ et $B \in \mathbb{K}_\ell^n$. On note AB la matrice $m \times \ell$ définie par

$$AB = \left(\sum_{k=1}^{n} a_{ik} b_{kj} \right)_{\substack{1\le i\le m,\\ 1\le j\le \ell}}.$$

On voit donc que l'élément d'indices i, j du produit de A et de B est la somme des produits des éléments de la i-ième ligne de A par ceux correspondants de la j-ième colonne de B. On dit que le produit s'effectue lignes par colonnes.

Exemple III.2.4. On a

$$\begin{pmatrix} 1 & 0 & -1 \\ 2 & 2 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 1 \\ -1 & 3 & 0 & 0 \\ 0 & 2 & 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -2 & -1 & 2 \\ 0 & 6 & 0 & 2 \end{pmatrix}$$

[2] $(\mathbb{K}_n^m, +)$ est un groupe commutatif. En outre, muni de la multiplication scalaire, $\mathbb{K}_n^m$ possède même une structure d'espace vectoriel.

Proposition III.2.5. *On a les propositions suivantes.*

i) *Si λ est un scalaire et si $A \in \mathbb{K}_n^m$, $B \in \mathbb{K}_\ell^n$, alors*

$$(\lambda A)B = A(\lambda B) = \lambda(AB).$$

ii) *Le produit matriciel est bilinéaire, i.e., si A, B et C sont des matrices et λ, μ des scalaires, alors*

$$(\lambda A + \mu B).C = \lambda AC + \mu BC$$

$$A.(\lambda B + \mu C) = \lambda AB + \mu AC$$

où l'on suppose que les produits matriciels ont un sens.

iii) *Le produit matriciel est associatif :*

$$A(BC) = (AB)C$$

où $A \in \mathbb{K}_q^m$, $B \in \mathbb{K}_p^q$, $C \in \mathbb{K}_n^p$.

iv) *Si $A \in \mathbb{K}_n^m$, alors*

$$0_{\ell,m}A = 0, \quad A0_{n,\ell} = 0$$

et

$$I_m A = A, \quad AI_n = A.$$

Démonstration. Nous démontrons l'associativité du produit matriciel. On a tout d'abord

$$\begin{aligned}[(AB)C]_{ij} &= \sum_{k=1}^{p}(AB)_{ik}C_{kj} \\ &= \sum_{k=1}^{p}\left(\sum_{\ell=1}^{q}A_{i\ell}B_{\ell k}\right)C_{kj} = \sum_{k=1}^{p}\sum_{\ell=1}^{q}A_{i\ell}B_{\ell k}C_{kj}.\end{aligned}$$

De plus,

$$\begin{aligned}[A(BC)]_{ij} &= \sum_{\ell=1}^{q}A_{i\ell}(BC)_{\ell j} \\ &= \sum_{\ell=1}^{q}A_{i\ell}\sum_{k=1}^{p}B_{\ell k}C_{kj} = \sum_{\ell=1}^{q}\sum_{k=1}^{p}A_{i\ell}B_{\ell k}C_{kj}.\end{aligned}$$

On conclut en permutant les sommes.

A présent, montrons que $AI_n = A$. Les autres résultats sont laissés en exercice. Rappelons que $(I_n)_{ij} = \delta_{ij}$. Dès lors, on a

$$(AI_n)_{ij} = \sum_{k=1}^{n}a_{ik}\delta_{kj} = a_{ij},$$

ce qui suffit.

■

Exemple III.2.6. Vérifier que le produit de deux matrices carrées de même dimension et diagonales (resp. triangulaires supérieures, triangulaires inférieures) est encore une matrice diagonale (resp. triangulaire supérieure, triangulaire inférieure).

Définition III.2.7. Puisque le produit matriciel est associatif, on peut définir la *puissance* n-ième d'une matrice carrée A de dimension k, $n > 0$, par

$$A^n = \underbrace{A \dots A}_{n \text{ fois}}.$$

Si $n = 0$, on pose $A^0 = I_k$.

Remarque III.2.8. Le produit de matrices carrées n'est en général pas commutatif. En effet, on a

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

et

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

Définition III.2.9. Deux matrices carrées A et B *commutent* si[3]

$$AB = BA.$$

Remarque III.2.10. Si les matrices A et B sont carrées de même dimension et commutent alors, la formule du binôme de Newton subsiste

$$(A+B)^n = \sum_{k=0}^{n} \mathrm{C}_n^k \, A^k \, B^{n-k}.$$

Par contre, si A et B ne commutent pas[4], alors

$$\begin{aligned} (A+B)^n &= A^n + A^{n-1}B + A^{n-2}BA + \cdots + ABA^{n-2} + BA^{n-1} \\ &\quad + A^{n-2}B^2 + \cdots + B^n. \end{aligned}$$

Par exemple, si A et B ne commutent pas, alors

$$(A+B)^3 = A^3 + A^2B + ABA + BA^2 + B^2A + BAB + AB^2 + B^3$$

et

$$\begin{aligned} (A+B)^4 &= A^4 + A^3B + A^2BA + ABA^2 + BA^3 \\ &\quad + A^2B^2 + ABAB + BA^2B + AB^2A + BABA + B^2A^2 + B^4. \end{aligned}$$

[3] On définit le *commutateur* de A et B par $[A, B] = AB - BA$. Ainsi, A et B commutent si et seulement si leur commutateur est nul.

[4] On peut faire l'analogie avec les mots de longueur n que l'on peut écrire (sans se préoccuper du sens) sur un alphabet de deux lettres $\{a, b\}$. Il est clair que le mot *aba* est différent du mot *baa* (on ne peut donc en général pas commuter les lettres d'un mot sans le modifier). Ainsi, tous les mots de longueurs 3 sur $\{a, b\}$ sont *aaa*, *aab*, *aba*, *baa*, *bba*, *bab*, *abb* et *bbb*. On pourra comparer cette liste avec développement de $(A+B)^3$ ci-dessus.

Exemple III.2.11. Voici quelques exemples de matrices qui commutent.

- Toute matrice carrée A commute avec 0 et I. En effet, $A0 = 0A = 0$ et $AI = IA = A$.
- Les puissances d'une même matrice carrée A commutent. Soient $p, q \in \mathbb{N}$. Il vient
$$A^p A^q = A^q A^p.$$
Par conséquent, si $\lambda_0, \lambda_1, \ldots, \lambda_r$ et $\mu_0, \mu_1, \ldots, \mu_s$ sont des scalaires et si A et une matrice carrée, alors[5]
$$\lambda_0 I + \lambda_1 A + \cdots + \lambda_r A^r \quad \text{et} \quad \mu_0 I + \mu_1 A + \cdots + \mu_s A^s$$
commutent.
- Deux matrices diagonales (de même dimension) commutent et
$$\operatorname{diag}(\lambda_1, \ldots, \lambda_r) \operatorname{diag}(\mu_1, \ldots, \mu_r) = \operatorname{diag}(\lambda_1\mu_1, \ldots, \lambda_r\mu_r).$$

Remarque III.2.12. Quelques remarques concernant le produit matriciel.

- Il existe des matrices A, B telles que $BA = -AB$ (dans ce cas, on dit que les matrices sont *anticommutatives*). Par exemple,
$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = - \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$
- Le produit de deux matrices peut être nul sans qu'aucun des facteurs ne soit nul. Par exemple,
$$\begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix}^2 = 0, \quad \begin{pmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = 0.$$

2.4. Transposition. La *transposée* de la matrice $A = (a_{ij}) \in \mathbb{K}_n^m$ est la matrice $\widetilde{A} \in \mathbb{K}_m^n$ dont les lignes sont les colonnes de A,
$$(\widetilde{A})_{ij} = a_{ji}.$$
On vérifie facilement que
$$\begin{aligned} \widetilde{\widetilde{A}} &= A, \\ (\lambda A + \mu B)\widetilde{\ } &= \lambda \widetilde{A} + \mu \widetilde{B}, \\ (AB)\widetilde{\ } &= \widetilde{B}\widetilde{A}. \end{aligned}$$

[5] On dit que $\lambda_0 I + \lambda_1 A + \cdots + \lambda_r A^r$ est un *polynôme de matrices*. On peut également définir l'exponentielle d'une matrice carrée A de la manière suivante. Si A est une matrice carrée, alors la série
$$e^A = \sum_{n=0}^{\infty} \frac{A^n}{n!}$$
converge vers une matrice carrée de même dimension appelée l'*exponentielle* de A (dans ce cours d'algèbre linéaire, nous ne voulons pas nous étendre sur la notion de convergence). On a $e^0 = I$, $e^A e^{-A} = e^0 = I$. Cependant, la formule $e^A e^B = e^{A+B}$ n'est valable que si les matrices A et B commutent (cf. la remarque III.2.10).

Définition III.2.13. Si A est une matrice carrée telle que $\widetilde{A} = A$, alors on dit que A est *symétrique*. En d'autres termes, A est symétrique si $a_{ij} = a_{ji}$ pour tous i, j. Si $\widetilde{A} = -A$, alors A est dite *antisymétrique*. Dans ce cas, $a_{ij} = -a_{ji}$ pour tous i, j.

2.5. Opérations spécifiques aux matrices complexes. Dans ce paragraphe, le corps $\mathbb{K}$ est $\mathbb{C}$.

Définition III.2.14. On peut associer à la matrice complexe $A = (a_{ij})$, les matrices suivantes

- la partie réelle de A : $(\mathfrak{Re}\, A)_{ij} = \mathfrak{Re}\, a_{ij}$,
- la partie imaginaire de A : $(\mathfrak{Im}\, A)_{ij} = \mathfrak{Im}\, a_{ij}$,
- la *matrice conjuguée* de A : $(\overline{A})_{ij} = \overline{a_{ij}}$,
- la *matrice adjointe* de A :

$$A^* = \widetilde{\overline{A}} = \overline{\widetilde{A}},$$

autrement dit, $(A^*)_{ij} = \overline{a_{ji}}$.

Exemple III.2.15. Soit la matrice

$$A = \begin{pmatrix} 1+i & 2 & 1-i \\ 0 & \pi & 3+2i \end{pmatrix},$$

on a

$$\mathfrak{Re}\, A = \begin{pmatrix} 1 & 2 & 1 \\ 0 & \pi & 3 \end{pmatrix},\ \mathfrak{Im}\, A = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 2 \end{pmatrix},\ \overline{A} = \begin{pmatrix} 1-i & 2 & 1+i \\ 0 & \pi & 3-2i \end{pmatrix}$$

et

$$A^* = \begin{pmatrix} 1-i & 0 \\ 2 & \pi \\ 1+i & 3-2i \end{pmatrix}.$$

Pour autant que les opérations soient définies, il est immédiat de vérifier que

$$\begin{array}{cc} A = \mathfrak{Re}\, A + i\, \mathfrak{Im}\, A & \overline{A} = \mathfrak{Re}\, A - i\, \mathfrak{Im}\, A \\ \mathfrak{Re}\, A = \frac{1}{2}(A + \overline{A}) & \mathfrak{Im}\, A = \frac{1}{2i}(A - \overline{A}) \\ \overline{\overline{A}} = A & (A^*)^* = A \\ \overline{\lambda A + \mu B} = \overline{\lambda}\, \overline{A} + \overline{\mu}\, \overline{B} & (\lambda A + \mu B)^* = \overline{\lambda}\, A^* + \overline{\mu}\, B^* \\ (AB)^* = B^* A^* & \end{array}$$

Définition III.2.16. Une matrice carrée A est *hermitienne* si $A^* = A$. Elle est *antihermitienne* si $A^* = -A$. En particulier, si A est hermitienne (resp. antihermitienne), alors ses éléments diagonaux sont réels (resp. imaginaires purs).

3. Sous-matrices

Soit A une matrice $m \times n$. La construction d'une sous-matrice revient à extraire les éléments se trouvant sur certaines lignes et certaines colonnes afin d'obtenir une nouvelle matrice. Considérons les entiers $i_1, \ldots, i_r$ et $j_1, \ldots, j_s$ tels que

$$1 \leq i_1 < \cdots < i_r \leq m,$$
$$1 \leq j_1 < \cdots < j_s \leq n.$$

On pose

$$A_{(i_1,\ldots,i_r;j_1,\ldots,j_s)} = (a_{i_k j_\ell})_{\substack{1\leq k\leq r\\ 1\leq \ell\leq s}}.$$

On dit que cette matrice est une *sous-matrice* de A.

Exemple III.3.1. Soit la matrice

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix}.$$

On a par exemple,

$$A_{(1,2;1,3)} = \begin{pmatrix} 1 & 3 \\ 5 & 7 \end{pmatrix}, \quad A_{(1;1,2,3,4)} = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}, \quad A_{(1,2,3;3)} = \begin{pmatrix} 3 \\ 7 \\ 11 \end{pmatrix}.$$

Comme nous l'a montré l'exemple précédent, les lignes $L_1, \ldots, L_m$ et les colonnes $C_1, \ldots, C_n$ de A sont des sous-matrices particulières de A.

Notons enfin que, par abus de langage, on appelle *sous-matrice diagonale* de A, une sous-matrice de A pour laquelle on a sélectionné des lignes et des colonnes de même indice dans A. Ainsi, une sous-matrice diagonale est de la forme

Cette notion réapparaîtra notamment dans la proposition XI.3.6.

$$A_{(i_1,\ldots,i_k;i_1,\ldots,i_k)}.$$

On remarque que les éléments de la diagonale principale de $A_{(i_1,\ldots,i_k;i_1,\ldots,i_k)}$ sont des éléments de la diagonale principale de A. Par exemple,

$$\begin{pmatrix} 1 & 3 \\ 9 & 11 \end{pmatrix}$$

est une sous-matrice diagonale de la matrice A donnée ci-dessus. En général, une sous-matrice diagonale n'est pas une matrice diagonale !

4. Matrices composées

La section précédente nous a montré qu'une matrice pouvait se décomposer suivant ses lignes ou ses colonnes. Dit autrement, si $L_1, \ldots, L_m \in \mathbb{K}_n$ (resp. $C_1, \ldots, C_n \in \mathbb{K}^m$) sont les lignes (resp. colonnes) de $A \in \mathbb{K}_n^m$ alors

$$A = \begin{pmatrix} L_1 \\ \vdots \\ L_m \end{pmatrix} = \begin{pmatrix} C_1 & \cdots & C_n \end{pmatrix}.$$

Inversement, si on se donne m vecteurs lignes ou n vecteurs colonnes, on peut construire une matrice A.

Ce phénomène de construction d'une matrice à partir de certaines de ses sous-matrices se généralise de la manière suivante. Considérons les matrices A_{ij}, $1 \leq i \leq r$, $1 \leq j \leq s$, où A_{ij} est une matrice $m_i \times n_j$ (pour tous i, j, m_i et n_j sont des entiers positifs). On considère alors la matrice

$$\begin{pmatrix} A_{11} & \cdots & A_{1s} \\ \vdots & & \vdots \\ A_{r1} & \cdots & A_{rs} \end{pmatrix} = (A_{ij})_{\substack{1 \leq i \leq r, \\ 1 \leq j \leq s}}$$

obtenue en juxtaposant les matrices A_{ij} dans l'ordre. Les matrices A_{ij} sont bien sûr des sous-matrices particulières de A, on les appelle les *matrices partielles* de la matrice composée.

Exemple III.4.1. Considérons les vecteurs colonnes

$$C_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}, \quad C_3 = \begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix}.$$

La matrice composée $(C_1\ C_2\ C_3)$ est

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

Considérons à présent les matrices

$$A_{11} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad A_{12} = \begin{pmatrix} 5 \\ 6 \end{pmatrix}, \quad A_{21} = \begin{pmatrix} 7 & 8 \end{pmatrix}, \quad A_{22} = \begin{pmatrix} 9 \end{pmatrix}.$$

La matrice composée $(A_{ij})_{1 \leq i,j \leq 2}$ est la matrice

$$\left(\begin{array}{cc|c} 1 & 2 & 5 \\ 3 & 4 & 6 \\ \hline 7 & 8 & 9 \end{array}\right)$$

Définition III.4.2. Soient $A_1, \ldots, A_r$ des matrices carrées de dimensions respectives $n_1, \ldots, n_r$. On peut construire la *matrice composée diagonale*

$$\operatorname{diag}(A_1, \ldots, A_r) = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_r \end{pmatrix} = (A_i \delta_{ij})_{1 \leq i,j \leq r}.$$

Cette matrice est une matrice carrée de dimension $\sum_{j=1}^{r} n_j$ dont les seules matrices partielles non nulles sont celles se trouvant sur la diagonale.

Exemple III.4.3. Soient les matrices

$$A_1 = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix}.$$

La matrice composée diagonale $\mathrm{diag}(A_1, A_2)$ est la matrice

$$\left(\begin{array}{cc|cc} 1 & 2 & 0 & 0 \\ 3 & 4 & 0 & 0 \\ \hline 0 & 0 & 5 & 6 \\ 0 & 0 & 7 & 8 \end{array}\right).$$

Un des intérêts des matrices composées est que les opérations sur les matrices composées peuvent s'exprimer en termes de leurs matrices partielles.

Si A et B sont des matrices composées

$$A = (A_{ij})_{\substack{1\leq i\leq r,\\ 1\leq j\leq s}}, \quad B = (B_{ij})_{\substack{1\leq i\leq t,\\ 1\leq j\leq u}}$$

telles que $r = t$, $s = u$ et pour tous i, j, A_{ij} et B_{ij} ont même forme, alors

$$\lambda A + \mu B = (\lambda A_{ij} + \mu B_{ij})_{\substack{1\leq i\leq r,\\ 1\leq j\leq s}}.$$

Intéressons-nous à présent au produit de deux matrices composées. Le produit de deux matrices composées peut s'effectuer lignes de matrices partielles par colonnes de matrices partielles à condition que la division des lignes de la première soit identique à la division des colonnes de la seconde. En d'autres termes, si

$$A = (A_{ij})_{\substack{1\leq i\leq r,\\ 1\leq j\leq s}}, \quad B = (B_{ij})_{\substack{1\leq i\leq t,\\ 1\leq j\leq u}}$$

sont telles que $s = t$ et que les produits $A_{ik}B_{kj}$ ont un sens, alors

$$AB = \left(\sum_{k=1}^{s} A_{ik}B_{kj}\right)_{\substack{1\leq i\leq r,\\ 1\leq j\leq u}}.$$

On dit parfois qu'on effectue le produit "grosse ligne par grosse colonne".

Exemple III.4.4. Le résultat précédent est immédiat si on remarque qu'il ne s'agit finalement que d'une manière évoluée de faire le produit. Traitons un exemple,

$$\left(\begin{array}{cc|c} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ \hline a_{31} & a_{32} & a_{33} \end{array}\right)\left(\begin{array}{cc} b_{11} & b_{12} \\ b_{21} & b_{22} \\ \hline b_{31} & b_{32} \end{array}\right)$$

$$= \begin{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} + \begin{pmatrix} a_{13} \\ a_{23} \end{pmatrix}\begin{pmatrix} b_{31} & b_{32} \end{pmatrix} \\ \begin{pmatrix} a_{31} & a_{32} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} + \begin{pmatrix} a_{33} \end{pmatrix}\begin{pmatrix} b_{31} & b_{32} \end{pmatrix} \end{pmatrix}$$

$$= \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} + a_{13}b_{31} & a_{11}b_{12} + a_{12}b_{22} + a_{13}b_{32} \\ a_{21}b_{11} + a_{22}b_{21} + a_{23}b_{31} & a_{21}b_{12} + a_{22}b_{22} + a_{23}b_{32} \\ a_{31}b_{11} + a_{32}b_{21} + a_{33}b_{31} & a_{31}b_{12} + a_{32}b_{22} + a_{33}b_{32} \end{pmatrix}.$$

Remarque III.4.5. Dans le cas particulier où $L_1, \ldots, L_m$ sont les lignes de $A \in \mathbb{K}_n^m$ et $C_1, \ldots, C_r$ les colonnes de $B \in \mathbb{K}_r^n$, alors

$$AB = (L_i C_j)_{\substack{1 \le i \le m, \\ 1 \le j \le r}}.$$

Enfin, si

$$A = (A_{ij})_{\substack{1 \le i \le r, \\ 1 \le j \le s}}, \quad \text{alors } \widetilde{A} = (\widetilde{A_{ji}})_{\substack{1 \le i \le s, \\ 1 \le j \le r}}.$$

5. Vecteurs

Rappelons qu'un vecteur colonne (resp. ligne) est une matrice particulière de forme $n \times 1$ (resp. $1 \times m$). Le nombre n (resp. m) est la *dimension* du vecteur. On notera un vecteur colonne x par

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

et un vecteur ligne y par

$$y = \begin{pmatrix} y_1 & \cdots & y_m \end{pmatrix}.$$

Ici, un seul indice est nécessaire. Les scalaires x_i (resp. y_j) sont appelés *composantes* du vecteur x (resp. y).

Le nom de *vecteur*[6] sans autre précision est en général réservé aux vecteurs colonnes. Les vecteurs étant des matrices de formes particulières, toutes les opérations définies précédemment sont applicables aux vecteurs colonne et ligne. En particulier, on peut considérer des combinaisons linéaires de vecteurs de même dimension.

Définition III.5.1. Les *vecteurs unitaires* à n dimensions sont donnés par

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ \ldots, \ e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Quel que soit le vecteur $x \in \mathbb{K}^n$, on a

$$x = \sum_{j=1}^{n} x_j \, e_j.$$

Remarque III.5.2. Si $A \in \mathbb{K}_m^n$, alors il est aisé de vérifier que

$$A \, e_j = C_j \text{ et } \widetilde{e_k} \, A = L_k$$

[6] Dans le chapitre VII, on étudie les espaces vectoriels en général. Un vecteur est alors simplement un élément d'un espace vectoriel. Il est facile de vérifier que $\mathbb{K}^n$ est un espace vectoriel particulier.

où C_j (resp. L_k) est la j-ième colonne (resp. k-ième ligne) de A, $1 \leq j \leq m$, $1 \leq k \leq n$. En particulier,

$$\widetilde{e_k}\, A\, e_j = A_{kj}.$$

Dans ce qui suit, on va s'intéresser principalement à des vecteurs complexes.

Définition III.5.3. Le[7] *produit scalaire (canonique)* de deux vecteurs $x, y \in \mathbb{C}^n$ est le nombre complexe[8]

$$\langle x, y\rangle = y^* x = \sum_{j=1}^{n} x_j \overline{y_j}.$$

Dans ce cours, c'est le seul produit scalaire que nous utiliserons. Sachez qu'on pourrait cependant en définir d'autres...

Exemple III.5.4. Soient deux vecteurs de $\mathbb{C}^3$

$$x = \begin{pmatrix} 2 \\ 2i \\ 3 \end{pmatrix} \text{ et } y = \begin{pmatrix} 2+i \\ 1 \\ 1+i \end{pmatrix}.$$

On a $\langle x, y\rangle = 2.(2-i) + 2i.1 + 3.(1-i) = 7 - 3i$.

Le produit scalaire jouit des propriétés suivantes (les démonstrations sont immédiates et sont laissées au lecteur) :

- $\langle y, x\rangle = \overline{\langle x, y\rangle}$;
- le produit scalaire est linéaire par rapport au premier facteur et antilinéaire par rapport au second, i.e., pour tous $\lambda, \mu \in \mathbb{C}$, $x, y, z \in \mathbb{C}^n$, on a

$$\langle \lambda x + \mu y, z\rangle = \lambda\langle x, z\rangle + \mu\langle y, z\rangle,$$
$$\langle x, \lambda y + \mu z\rangle = \overline{\lambda}\langle x, y\rangle + \overline{\mu}\langle x, z\rangle;$$

- $\langle x, x\rangle \geq 0$, l'annulation ayant lieu si et seulement si $x = 0$;
- pour tout $j \in \{1, \ldots, n\}$, $\langle x, e_j\rangle = x_j$;
- pour tous $i, j \in \{1, \ldots, n\}$, $\langle e_i, e_j\rangle = \delta_{ij}$.

[7] D'une manière générale, **un** produit scalaire sur un espace vectoriel complexe est une forme bilinéaire gauche hermitienne définie positive (les définitions sont précisées ci-dessous). Ici, l'application de $\mathbb{C}^n \times \mathbb{C}^n$ dans $\mathbb{C}$ que nous venons de définir n'est qu'un cas particulier de produit scalaire.

De manière analogue, dans le cas d'un espace vectoriel réel, **un** produit scalaire est une forme bilinéaire symétrique définie positive. Par exemple, si on considère le $\mathbb{R}$-vectoriel E des fonctions à valeurs réelles continues sur $[0, 1]$, l'application $\langle \cdot, \cdot\rangle : E \times E \to \mathbb{R}$ définie par

$$\langle f, g\rangle = \int_0^1 f(x)g(x)\, dx$$

est un produit scalaire sur E.

[8] On peut aussi de manière analogue définir le produit scalaire (canonique) de deux matrices $A, B \in \mathbb{C}_n^m$ par $\langle A, B\rangle = \sum_{i=1}^m \sum_{j=1}^n a_{ij}\overline{b_{ij}}$.

On peut résumer les trois premières propriétés en disant que $\langle \cdot, \cdot \rangle$ est une forme bilinéaire gauche hermitienne définie positive[9].

Définition III.5.5. Le produit scalaire d'un vecteur x par lui-même, parfois appelé *carré scalaire*, est le nombre positif ou nul,

$$\langle x, x \rangle = x^* x = \sum_{j=1}^{n} |x_j|^2.$$

On peut dès lors considérer la racine carrée de $\langle x, x \rangle$ qui est appelée *module* ou *norme*[10] du vecteur x,

$$|x| = \sqrt{\langle x, x \rangle} = \sqrt{\sum_{j=1}^{n} |x_j|^2}.$$

Un vecteur est *normé* si sa norme vaut 1.

On a immédiatement

$$|x|^2 = \sum_{j=1}^{n} |x_j|^2 = \sum_{j=1}^{n} (\mathfrak{Re}\, x_j)^2 + \sum_{j=1}^{n} (\mathfrak{Im}\, x_j)^2 = |\mathfrak{Re}\, x|^2 + |\mathfrak{Im}\, x|^2.$$

Remarque III.5.6. Soit $x \in \mathbb{C}^n$,

$$x = 0 \Leftrightarrow |x| = 0.$$

Remarque III.5.7. Soit $x \in \mathbb{C}^n$. Pour tout $\lambda \in \mathbb{C}$, on a

$$|\lambda x| = |\lambda|\, |x|.$$

Démonstration. Il vient

$$|\lambda x|^2 = \langle \lambda x, \lambda x \rangle = \lambda \overline{\lambda} \langle x, x \rangle = |\lambda|^2\, |x|^2.$$

■

[9] Une *forme bilinéaire gauche* sur un espace vectoriel complexe E est une application $B : E \times E \to \mathbb{C}$ qui est linéaire par rapport au premier facteur et antilinéaire par rapport au second. Si elle satisfait $B(y, x) = \overline{B(x, y)}$, on dit qu'elle est *hermitienne*. Si elle satisfait $B(x, x) > 0$ pour tout $x \in E \setminus \{0\}$, on dit qu'elle est *définie positive*. Enfin, une forme bilinéaire est *symétrique* si $B(y, x) = B(x, y)$.

[10] D'une manière générale, une *norme* sur un espace vectoriel E (réel ou complexe) est une application $|| \cdot || : E \to \mathbb{R}$ satisfaisant les trois propriétés suivantes

- pour tout $v \in E$ et pour tout $\alpha \in \mathbb{R}$ (ou $\mathbb{C}$), $||\alpha v|| = |\alpha|\, ||v||$,
- pour tous $u, v \in E$, $||u + v|| \leq ||u|| + ||v||$,
- pour tous $u \in E$, $||u|| = 0$ si et seulement si $u = 0$.

Une application jouissant de ces deux premières propriétés est qualifiée de *semi-norme*. En particulier, en procédant comme dans la définition III.5.5, tout produit scalaire sur E induit une norme sur ce même espace. De plus, tout norme induit une distance. Par définition, une *distance* sur un ensemble M est une application $d : M \times M \to \mathbb{R}$ vérifiant

- pour tous $x, y \in M$, $d(x, y) \geq 0$ et $d(x, y) = 0$ si et seulement si $x = y$,
- pour tous $x, y \in M$, $d(x, y) = d(y, x)$,
- pour tous $x, y, z \in M$, $d(x, y) \leq d(x, y) + d(y, z)$. (Inégalité triangulaire).

La distance sur un espace vectoriel E induite par la norme $|| \cdot ||$ est définie par $d(x, y) = ||x - y||$, pour tous $x, y \in E$. On vérifiera qu'ainsi défini, il s'agit bien d'une distance.

Proposition III.5.8 (Inégalité de Cauchy-Schwarz). *Pour tous vecteurs $x, y \in \mathbb{C}^n$, on a*

$$|\langle x, y\rangle| \leq |x|\,|y|,$$

l'égalité ayant lieu si et seulement si il existe $\alpha, \beta \in \mathbb{C}$, $(\alpha, \beta) \neq (0, 0)$, tels que[11]

$$\alpha x + \beta y = 0.$$

Démonstration. Si y est nul, l'inégalité est immédiate. On a même l'égalité et $0.x + 1.y = 0$. Nous pouvons donc supposer $y \neq 0$.

Pour tout $\lambda \in \mathbb{C}$, on a

$$\begin{aligned} |x + \lambda y|^2 &= \langle x + \lambda y, x + \lambda y\rangle \\ &= |x|^2 + \lambda\langle y, x\rangle + \overline{\lambda}\langle x, y\rangle + |\lambda|^2|y|^2 \\ &= |x|^2 + 2\,\mathfrak{Re}\,(\overline{\lambda}\langle x, y\rangle) + |\lambda|^2|y|^2 \geq 0. \end{aligned}$$

Si on considère en particulier $\lambda = -\frac{\langle x,y\rangle}{|y|^2}$, on obtient alors

$$|x|^2 - \frac{|\langle x, y\rangle|^2}{|y|^2} \geq 0.$$

et donc

$$|\langle x, y\rangle|^2 \leq |x|^2|y|^2.$$

On obtient l'inégalité proposée en passant aux racines carrées.

Attention! En général, si $a, b \in \mathbb{R}$, alors $a^2 \leq b^2 \not\Rightarrow a \leq b$. Pourquoi, ici, peut-on le faire ?

Au vu de la remarque III.5.6, l'égalité a lieu si et seulement si $x+\lambda y = 0$. Si $\alpha \neq 0$, la relation $\alpha x + \beta y = 0$ annoncée se réécrit $x + (\beta/\alpha)y = 0$ et est donc bien de la forme $x + \lambda y = 0$. Si $\beta \neq 0$, on obtient une relation de la forme $\lambda' x + y = 0$ et on aurait pu, par symétrie, raisonner dans la preuve ci-dessus sur $x \neq 0$ et $|\lambda' x + y|$.

■

Corollaire III.5.9 (Inégalité de Minkowski). *Pour tous vecteurs $x, y \in \mathbb{C}^n$, on a*

$$|x + y| \leq |x| + |y|,$$

l'égalité ayant lieu si et seulement si il existe des nombres **réels positifs ou nuls** *λ, μ, $(\lambda, \mu) \neq (0, 0)$, tels que $\lambda x = \mu y$.*

Démonstration. Puisque la partie réelle d'un nombre complexe est majorée par son module, on a

$$\begin{aligned} |x + y|^2 = \langle x + y, x + y\rangle &= |x|^2 + 2\,\mathfrak{Re}\,\langle x, y\rangle + |y|^2 \\ &\leq |x|^2 + 2\,|\langle x, y\rangle| + |y|^2. \end{aligned}$$

En utilisant l'inégalité de Cauchy-Schwarz, il vient

$$|x + y|^2 \leq |x|^2 + 2\,|x|\,|y| + |y|^2 = (|x| + |y|)^2.$$

[11] En d'autres termes, cela signifie que x et y sont des vecteurs linéairement dépendants du $\mathbb{C}$-vectoriel $\mathbb{C}^n$.

D'où la conclusion. Le cas de l'égalité est trivial si $x = 0$ ou $y = 0$. Supposons donc x et y non nuls. L'égalité a lieu si et seulement si $\mathfrak{Re}\,\langle x, y\rangle = |\langle x, y\rangle|$ et $|\langle x, y\rangle| = |x|\,|y|$. Au vu de l'inégalité de Cauchy-Schwarz, la dernière égalité a lieu si et seulement si il existe $\alpha \in \mathbb{C}$ tel que $y = \alpha\, x$. Dans ce cas, $\langle x, y\rangle = \overline{\alpha}|x|^2$ et $|\langle x, y\rangle| = |\alpha|\,|x|^2$. Ainsi, la première égalité a lieu si et seulement si $\mathfrak{Re}\,\overline{\alpha} = |\alpha|$, c'est-à-dire si et seulement si α est un nombre réel positif ou nul. Encore une fois, par symétrie et comme dans la preuve de la propriété précédente, on se ramène aux conditions de l'énoncé.

■

Terminons cette section sur les vecteurs en introduisant la notion de dépendance linéaire.

Considérons un exemple de logique rudimentaire mais au combien crucial. Quelle est la négation de l'affirmation : "tous les élèves de la classe ont des lunettes" ? Vous répondrez certainement : "au moins un élève de la classe ne porte pas de lunettes". Ces deux phrases sont la négation l'une de l'autre. De la même façon, la négation de "tous les coefficients de la relation sont nuls" est "au moins un coefficient de cette relation est non nul".

Nous considérons ici des vecteurs colonnes de $\mathbb{K}^n$ pour un champ $\mathbb{K}$ quelconque. Les développements qui suivent s'adaptent aisément au cas de vecteurs lignes.

Définition III.5.10. Des vecteurs $x_1, \ldots, x_p \in \mathbb{K}^n$ sont *linéairement dépendants* si il existe $\lambda_1, \ldots, \lambda_p \in \mathbb{K}$ non tous nuls tels que

$$\lambda_1 x_1 + \cdots + \lambda_p x_p = 0.$$

Dans le cas contraire, $x_1, \ldots, x_p \in \mathbb{K}^n$ sont dit *linéairement indépendants*, c'est-à-dire que toute combinaison linéaire de la forme

$$\lambda_1 x_1 + \cdots + \lambda_p x_p = 0$$

entraîne

$$\lambda_1 = \cdots = \lambda_p = 0.$$

L'indépendance linéaire signifie que la **seule** façon d'obtenir 0 est que tous les coefficients soient nuls.

Proposition III.5.11. *Des vecteurs $x_1, \ldots, x_p$ sont linéairement dépendants si et seulement si l'un d'eux s'exprime comme combinaison linéaire des autres.*

Démonstration. Si $x_1, \ldots, x_p$ sont linéairement dépendants, il existe des scalaires $\lambda_1, \ldots, \lambda_p$ non tous nuls tels que $\lambda_1 x_1 + \cdots + \lambda_p x_p = 0$. Sans perte de généralité, nous pouvons supposer que $\lambda_1 \neq 0$. Ainsi,

$$x_1 = -\frac{\lambda_2}{\lambda_1} x_2 - \cdots - \frac{\lambda_p}{\lambda_1} x_p$$

et x_1 est combinaison linéaire des autres vecteurs.

Réciproquement, supposons que

$$x_1 = \lambda_2 x_2 + \cdots + \lambda_p x_p.$$

Dans ce cas,

$$x_1 - \lambda_2 x_2 - \cdots - \lambda_p x_p = 0$$

ce qui signifie que les p vecteurs sont linéairement dépendants (on ne sait rien sur la valeur de $\lambda_2, \ldots, \lambda_p$ mais le coefficient de x_1 vaut 1 et est bien non nul).

■

Exemple III.5.12. Voici des exemples de vecteurs linéairement dépendants ou indépendants.

- Les vecteurs unitaires $e_1, \ldots, e_n$ de $\mathbb{K}^n$ sont linéairement indépendants.
- Les vecteurs,

$$x_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad x_2 = \begin{pmatrix} 2 \\ 9 \\ 0 \end{pmatrix}, \quad x_3 = \begin{pmatrix} -4 \\ 6 \\ 2 \end{pmatrix}$$

  sont linéairement indépendants. En effet, quels que soient $\lambda_1, \lambda_2, \lambda_3$, on a

$$\lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3 = 0 \Leftrightarrow \begin{cases} \lambda_1 + 2\lambda_2 - 4\lambda_3 &= 0 \\ 9\lambda_2 + 6\lambda_3 &= 0 \\ 2\lambda_3 &= 0 \end{cases}.$$

  Ce système possède l'unique solution $\lambda_1 = \lambda_2 = \lambda_3 = 0$.
- Par contre, les vecteurs

$$x_1 = \begin{pmatrix} 0 \\ 12 \\ 1 \end{pmatrix}, \quad x_2 = \begin{pmatrix} 2 \\ 9 \\ 0 \end{pmatrix}, \quad x_3 = \begin{pmatrix} -4 \\ 6 \\ 2 \end{pmatrix}$$

  sont linéairement indépendants. En effet, il est facile de voir que

$$2x_1 - 2x_2 - x_3 = 0.$$

- Soient les vecteurs de $\mathbb{R}^3$

$$\begin{pmatrix} 1 \\ -1 \\ 2-m \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ m-2 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ m \end{pmatrix}.$$

  Pour quelle(s) valeur(s) du paramètre $m \in \mathbb{R}$ ces trois vecteurs sont-ils linéairement indépendants ? Il est facile[12] de vérifier que les trois vecteurs sont linéairement dépendants si et seulement si $m = 0$.

Remarque III.5.13. Les quelques résultats suivants découlent immédiatement de la définition[13].

[12] Les calculs peuvent s'avérer parfois fastidieux. Nous aurons dans les chapitres suivants d'autres outils à notre disposition, comme par exemple le calcul de déterminants.

[13] C'est un bon exercice que de les démontrer.

- Pour qu'un seul vecteur soit linéairement indépendant, il faut et il suffit que ce vecteur soit non nul.
- Si $x_1, \ldots, x_p$ sont linéairement indépendants, alors $x_1, \ldots, x_{p-1}$ sont encore linéairement indépendants. De manière générale, parmi des vecteurs linéairement indépendants, on ne peut trouver que des vecteurs linéairement indépendants.
- Si $x_1, \ldots, x_p$ sont linéairement dépendants, alors quel que soit y, $x_1, \ldots, x_p, y$ sont encore linéairement dépendants. En particulier, les vecteurs $0, x_1, \ldots, x_p$ sont toujours linéairement dépendants.
- Si $x_1, \ldots, x_p$ sont linéairement indépendants et si $x_1, \ldots, x_p, x_{p+1}$ sont linéairement dépendants, alors x_{p+1} est combinaison linéaire des autres.

Théorème III.5.14 (Théorème de Steinitz). *Soit p un entier positif, $p+1$ combinaisons de p vecteurs sont toujours linéairement dépendantes.*

cf. théorème VII.2.3.

Corollaire III.5.15. *Dans $\mathbb{K}^n$, on ne peut trouver plus de n vecteurs linéairement indépendants.*

Démonstration. De fait, tout vecteur de $\mathbb{K}^n$ est combinaison linéaire des vecteurs unitaires $e_1, \ldots, e_n$. Par conséquent, des vecteurs quelconques $x_1, \ldots, x_{n+1}$ de $\mathbb{K}^n$ sont $n+1$ combinaisons linéaires des n vecteurs $e_1, \ldots, e_n$ et sont donc toujours linéairement dépendants.

■

6. Quelques applications

Dans cette courte section, nous illustrons brièvement quelques applications immédiates et élémentaires du calcul matriciel.

Exemple III.6.1. Considérons quatre ordinateurs placés en réseau suivant le schéma repris à la figure III.1. Nous supposons que les communications sont à sens unique (par exemple, l'ordinateur 1 peut envoyer des données à l'ordinateur 4 mais l'inverse n'est pas vrai). Considérons la matrice $A = (a_{ij})$ où $a_{ij} = 1$ si l'ordinateur i est relié à l'ordinateur j et $a_{ij} = 0$ sinon :

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

La question est la suivante. Peut-on, au moyen de la matrice A, déterminer quels ordinateurs peuvent communiquer avec quels autres ordinateurs (en

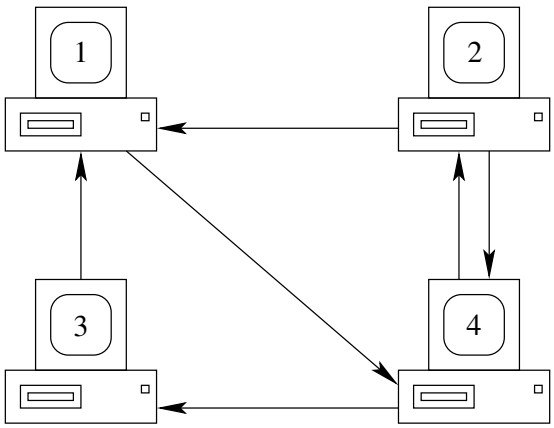


FIGURE III.1. Un mini réseau informatique.

passant par de possibles intermédiaires) ? Examinons le carré de A,

$$B = A^2 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 1 \end{pmatrix}.$$

On a

$$b_{ij} = \sum_{k=1}^{4} a_{ik}\, a_{kj}.$$

De là, on s'aperçoit que b_{ij} compte les connexions de longueur exactement 2 allant de l'ordinateur i à l'ordinateur j. Par exemple,

$$b_{41} = \underbrace{a_{41}a_{11}}_{=0} + \underbrace{a_{42}a_{21}}_{=1} + \underbrace{a_{43}a_{31}}_{=1} + \underbrace{a_{44}a_{41}}_{=0} = 2.$$

Ainsi, le réseau dispose des connexions $4 \to 2 \to 1$ et $4 \to 3 \to 1$. Il y a donc deux chemins possibles pour acheminer des données de 4 à 1.

En examinant A et A^2, on s'aperçoit qu'il n'y a aucune connexion de longueur 1 ou 2 allant de l'ordinateur 3 à l'ordinateur 2. Si on regarde la matrice A^3, on s'aperçoit que l'élément à la troisième ligne et à la deuxième colonne est non nul. Ainsi, le calcul de A^2 et A^3 montre que tout ordinateur est relié à tout autre par une connexion de longueur au plus 3.

Bien évidemment, le problème posé ici est particulièrement simple et peut être résolu directement sans recourir à l'algèbre. Par contre, les techniques algébriques deviennent indispensables lorsque la taille des réseaux grandit.

D'une manière générale, on peut compter le nombre de chemins de longueur n dans un graphe en calculant la n-ième puissance de la matrice associée au graphe. Dans notre exemple, remarquons qu'il n'est pas interdit pour un chemin de repasser deux fois par le même noeud. Ainsi, $1 \to 4 \to$

$2 \to 1 \to 4$ est un chemin de longueur 4 entre les ordinateurs 1 et 4 qui est pris en compte dans la matrice A^4.

Exemple III.6.2 (Matrices de Pauli). En physique quantique, lors de l'étude du moment angulaire intrinsèque ou spin de l'électron, apparaissent les équations suivantes

$$\begin{array}{rclcl} \sigma_x\sigma_y & = & -\sigma_y\sigma_x & = & i\sigma_z, \\ \sigma_y\sigma_z & = & -\sigma_z\sigma_y & = & i\sigma_x, \\ \sigma_z\sigma_x & = & -\sigma_x\sigma_z & = & i\sigma_y. \end{array}$$

Une représentation est donnée par les matrices reprises ci-dessous,

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Exemple III.6.3. Un *vecteur de probabilité* est un vecteur (ligne ou colonne) dont les composantes sont des nombres réels positifs ou nuls et dont la somme vaut 1. Une matrice dont les lignes sont toutes des vecteurs de probabilité est dite *stochastique*.

Considérons un pays imaginaire dans lequel trois partis politiques R, S et T s'opposent. Les analystes politiques locaux ont décrit un modèle de prédiction de répartition des votes d'une élection à l'élection suivante. Ce modèle est repris schématiquement à la figure III.2. Les informations du

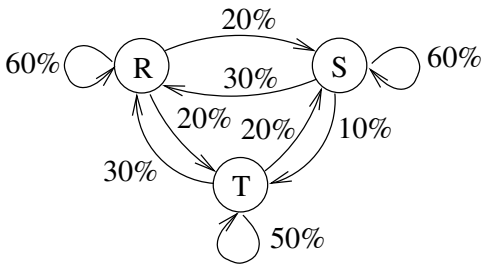


FIGURE III.2. Modèle d'élections

modèle peuvent être enregistrées dans la matrice stochastique

$$P = \begin{pmatrix} 0,6 & 0,2 & 0,2 \\ 0,3 & 0,6 & 0,1 \\ 0,3 & 0,2 & 0,5 \end{pmatrix}.$$

Supposons qu'à l'instant t_0, les proportions dans la population des personnes votant respectivement pour R, S et T sont de 30%, 50% et 20%. Le modèle permet d'estimer ces mêmes proportions au temps t_i situé après i élections.

$$\text{En } t_1 : \begin{pmatrix} 0,3 & 0,5 & 0,2 \end{pmatrix} \begin{pmatrix} 0,6 & 0,2 & 0,2 \\ 0,3 & 0,6 & 0,1 \\ 0,3 & 0,2 & 0,5 \end{pmatrix} = \begin{pmatrix} 0,39 & 0,4 & 0,21 \end{pmatrix}.$$

En t_2, on calcule P^2 et

$$\begin{pmatrix}0,3 & 0,5 & 0,2\end{pmatrix}\begin{pmatrix}0,48 & 0,28 & 0,24\\ 0,39 & 0,44 & 0,17\\ 0,39 & 0,28 & 0,33\end{pmatrix} = \begin{pmatrix}0,417 & 0,36 & 0,223\end{pmatrix}.$$

On remarquera que le carré d'une matrice stochastique est encore stochastique[14]. Ainsi, en calculant la puissance n-ième de P, on peut rechercher, suivant le modèle choisi, le pourcentage de la population ayant voté pour un parti donné à partir d'une répartition initiale. La question naturelle que l'on peut se poser est de savoir si ces pourcentages se stabilisent lorsque n grandit. Nous verrons plus loin comment répondre à cette question et comment étudier le comportement asymptotique de la répartition de la population suivant les trois partis R, S et T.

Remarque III.6.4. On pourra encore noter que l'infographie, la conception assistée par ordinateur et en particulier le rendu d'images tridimensionnelles font un usage intensif du calcul matriciel[15].

Exemple III.6.5. Revenons un instant sur la notion de produit scalaire. Soient les matrices

$$A = \begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix} \text{ et } B = \begin{pmatrix}1 & 2\\ 1 & 4\end{pmatrix}.$$

Pour illustrer notre propos, plaçons-nous dans $\mathbb{R}^2$ et considérons les produits scalaires[16] suivants et les normes associées, pour tous $x, y \in \mathbb{R}^2$,

$$\langle x, y\rangle = \widetilde{y}x = x_1y_1 + x_2y_2,\ |x| = \sqrt{x_1^2 + x_2^2}$$

$$\langle x, y\rangle_A = \widetilde{y}Ax = x_1y_1 + 2x_2y_2,\ |x|_A = \sqrt{x_1^2 + 2x_2^2}$$

$$\langle x, y\rangle_B = \widetilde{y}Bx = x_1y_1 + x_1y_2 + 2x_2y_1 + 4x_2y_2,\ |x|_B = \sqrt{x_1^2 + 3x_1x_2 + 4x_2^2}$$

A la figure III.3, sont représentés, dans le plan euclidien, les vecteurs unitaires (i.e., de norme 1) de $\mathbb{R}^2$ pour les trois normes envisagées.

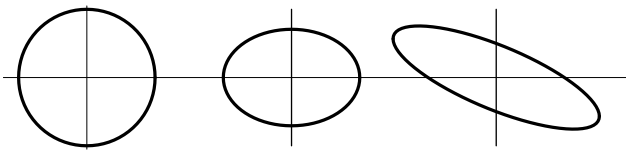


FIGURE III.3. $\{x \in \mathbb{R}^2 : |x| = 1\}$, $\{x \in \mathbb{R}^2 : |x|_A = 1\}$ et $\{x \in \mathbb{R}^2 : |x|_B = 1\}$.

[14]Essayer de le démontrer.

[15]Le lecteur intéressé pourra par exemple consulter un ouvrage introductif comme: R. Malgouyres, *algorithmes pour la synthèse d'images et l'animation 3D*, Dunod (Paris), 2002.

[16]Le lecteur vérifiera qu'il s'agit de formes bilinéaires symétriques définies positives.

CHAPITRE IV

Permutations

La définition du déterminant d'une matrice carrée fait intervenir les notions de permutation et de signature d'une permutation. Dès lors, avant d'introduire le déterminant, nous allons présenter de manière détaillée le concept de permutation d'un ensemble fini X.

1. Définition et premières propriétés

Définition IV.1.1. Une *permutation* de l'ensemble X est une bijection de X dans lui-même. On s'intéressera ici au cas d'un ensemble fini X. Dès lors, si X contient n éléments, on pourra considérer en toute généralité[1] que $X = \{1, \dots, n\}$.

La permutation $\nu : X \to X$

$$\nu : 1 \mapsto \nu(1), \dots, n \mapsto \nu(n)$$

est notée par le symbole

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \nu(1) & \nu(2) & \cdots & \nu(n) \end{pmatrix}.$$

Tout réarrangement des colonnes du symbole donne lieu à un symbole représentant la même permutation.

Nous dénotons par $\mathcal{S}_n$, l'ensemble des permutations de $\{1, \dots, n\}$. Soient $\mu, \nu \in \mathcal{S}_n$. Le *produit*[2] de μ et ν est la permutation composée $\mu \circ \nu$ définie par

$$i \mapsto \mu(\nu(i)), \quad i \in \{1, \dots, n\}$$

et notée simplement $\mu\nu$. Cette fonction est injective et surjective, il s'agit donc bien d'une nouvelle permutation. La *permutation identique* ou *identité* est la permutation

$$id = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Remarque IV.1.2. Des arguments élémentaires d'analyse combinatoire montrent que

$$\#\mathcal{S}_n = n!.$$

[1] Si un ensemble X contient n éléments, il est en bijection avec $\{1, \dots, n\}$.

[2] On vérifie que l'ensemble $\mathcal{S}_n$ muni du produit de permutations est un groupe, appelé le *groupe symétrique*. Le neutre en est la permutation identique.

Exemple IV.1.3. Soit la permutation μ de $\{1,2,3\}$ définie par $\mu(1)=3$, $\mu(2)=1$ et $\mu(3)=2$. On peut la noter indifféremment

$$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&3&2\\3&2&1\end{pmatrix}, \begin{pmatrix}2&3&1\\1&2&3\end{pmatrix}, \begin{pmatrix}2&1&3\\1&3&2\end{pmatrix}, \begin{pmatrix}3&2&1\\2&1&3\end{pmatrix}$$

ou encore

$$\begin{pmatrix}3&1&2\\2&3&1\end{pmatrix}.$$

Soient les permutations

$$\mu=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix} \quad \text{et} \quad \nu=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}.$$

Le produit $\mu\nu$ est la permutation

$$\begin{pmatrix}1&2&3&4\\&&\downarrow&\\3&2&1&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\&&&\downarrow\\4&1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\&&&\downarrow\\4&3&2&1\end{pmatrix}$$

Il est aisé de vérifier que le produit de permutations jouit des propriétés suivantes[3].

- Le produit de permutations est associatif,
- la permutation identique est un neutre à gauche et à droite,

$$\nu\, id = id\, \nu = \nu,$$

- toute permutation ν possède un inverse noté ν^{-1} qui est tel que

$$\nu\,\nu^{-1} = \nu^{-1}\,\nu = id.$$

  Le symbole de ν^{-1} est obtenu en intervertissant les lignes du symbole de ν.

Remarque IV.1.4. Le produit de permutations n'est en général pas commutatif; en effet

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

mais

$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

Définition IV.1.5. Deux permutations μ et ν de X sont *disjointes* si l'une laisse invariants les nombres modifiés par l'autre. Ainsi,

$$\mu(i)\neq i \text{ implique } \nu(i)=i.$$

Auquel cas, on a aussi[4]

$$\nu(i)\neq i \text{ implique } \mu(i)=i.$$

[3]Comme annoncé à la page précédente, cela signifie que $\mathcal{S}_n$ muni du produit de permutations est un groupe.

[4]Penser à la contraposition, $A \Rightarrow B$ est équivalent à $\neg B \Rightarrow \neg A$ (la négation de B implique la négation de A).

Proposition IV.1.6. *Deux permutations disjointes μ et ν de X commutent, i.e.,*

$$\mu\nu = \nu\mu.$$

Démonstration. Trois cas sont à envisager.

- Si $i \in X$ est tel que $\mu(i) \neq i$ alors, les permutations étant disjointes, $\nu(i) = i$ et ainsi $\mu(\nu(i)) = \mu(i)$. Puisque μ est injectif, $\mu(\mu(i)) \neq \mu(i)$ (sinon, i et $\mu(i)$ auraient même image par μ). En utilisant une fois encore le fait que les permutations sont disjointes, on a $\nu(\mu(i)) = \mu(i)$ et donc
$$\mu(\nu(i)) = \mu(i) = \nu(\mu(i)).$$
- Si $i \in X$ est tel que $\nu(i) \neq i$, alors en appliquant le même raisonnement, on a $\nu(\mu(i)) = \mu(\nu(i))$.
- Enfin, si $i \in X$ est tel que $\mu(i) = i$ et $\nu(i) = i$, alors $\mu(\nu(i)) = \nu(\mu(i))$.

■

Exemple IV.1.7. On vérifiera que les permutations suivantes sont disjointes et commutent

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}.$$

2. Cycles

Définition IV.2.1. Soit $X = \{1, \ldots, n\}$. Considérons $t_1, \ldots, t_p$ des éléments de X, $p \geq 1$, et $t_{p+1}, \ldots, t_n$, les $n - p$ autres éléments de X. Le *cycle* associé à $t_1, \ldots, t_p$ est

On parle aussi de *permutation circulaire.*

$$\begin{pmatrix} t_1 & t_2 & \cdots & t_{p-1} & t_p & t_{p+1} & \cdots & t_n \\ t_2 & t_3 & \cdots & t_p & t_1 & t_{p+1} & \cdots & t_n \end{pmatrix}.$$

Ainsi, cette permutation remplace $t_1, \ldots, t_{p-1}$ par l'élément suivant, t_p par t_1 et laisse inchangés les autres éléments.

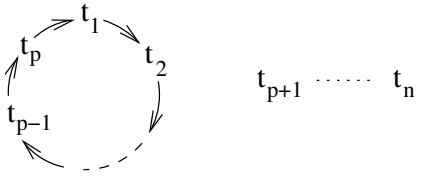


FIGURE IV.1. Un cycle.

On note ce cycle

$$(t_1 \quad t_2 \quad \cdots \quad t_{p-1} \quad t_p),$$

on dit que $t_1, \ldots, t_p$ sont les *éléments* du cycle et que p est sa *longueur.*

Exemple IV.2.2. La permutation

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

est en fait un cycle que l'on pourra alors noter plus simplement $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$. On peut aussi considérer le produit deux cycles. On a

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

car

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}.$$

Remarque IV.2.3. Les remarques suivantes sont immédiates.

- On peut permuter circulairement les éléments d'un cycle. Cela équivaut à un réarrangement de son symbole. Par exemple,

$$\begin{pmatrix} 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 1 \end{pmatrix}.$$

- Dans la définition précédente, un cycle $\begin{pmatrix} t_1 & t_2 & \cdots & t_{p-1} & t_p \end{pmatrix}$ laisse invariants les éléments de $X \setminus \{t_1, \ldots, t_p\}$. Donc en particulier, tout cycle de longueur 1 est égal à la permutation identique.

Proposition IV.2.4. *Toute permutation distincte de id est un produit de cycles disjoints. Si on omet les cycles de longueur* 1*, cette décomposition est unique à l'ordre des facteurs près.*

Avant de donner la preuve de ce résultat, considérons un exemple.

Exemple IV.2.5. On a

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 2 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 6 & 2 & 4 & 5 \\ 3 & 6 & 1 & 4 & 2 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 6 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}.$$

Pour obtenir cette décomposition, on regarde les images itérées d'un élément de X par la permutation μ. Puisque X est un ensemble fini, on réobtient l'élément de départ après un nombre fini d'itérations (les justifications précises sont données dans la preuve qui suit) et de cette manière, on détecte un cycle. Par exemple,

$$1 \xrightarrow{\mu} 3 \xrightarrow{\mu} 6 \xrightarrow{\mu} 1 \text{ donne le cycle } \begin{pmatrix} 1 & 3 & 6 \end{pmatrix}.$$

En répétant cette procédure, on épuise les éléments de X et on met en évidence les cycles de la permutation. Autrement dit, l'ensemble des orbites pour μ partitionne X et chaque orbite non triviale définit un cycle.

Démonstration. Soit μ une permutation distincte de id. Fixons $i \in X$ et considérons la suite

$$i,\ \mu(i),\ \mu^2(i), \ldots, \mu^k(i), \ldots.$$

Comme X est un ensemble fini, il existe des nombres naturels p et q distincts tels que

$$\mu^p(i) = \mu^q(i).$$

On peut supposer que $p < q$. Dès lors, $q - p$ est un entier positif tel que

Se rappeler que μ est une bijection d'inverse μ^{-1}.

$$\mu^{q-p}(i) = i.$$

Soit m_i, le plus petit entier positif ayant la propriété $\mu^{m_i}(i) = i$. De cette définition, il résulte que

$$i, \mu(i), \ldots, \mu^{m_i-1}(i)$$

sont distincts deux à deux. De plus,

$$C_i = \{i, \mu(i), \ldots, \mu^{m_i-1}(i)\} = \{\mu^k(i) \mid k \in \mathbb{Z}\}.$$

En effet, si on effectue la division euclidienne de $k \in \mathbb{Z}$ par m_i, alors il existe $q \in \mathbb{Z}$ tel que

$$k = q\, m_i + r \quad \text{avec } 0 \leq r < m_i.$$

Or, puisque $\mu^{m_i}(i) = i = \mu^{-m_i}(i)$, on a

$$\mu^k(i) = \mu^r(i) \quad \text{avec } 0 \leq r < m_i.$$

Montrons à présent que les ensembles C_i forment une partition[5] de X. On sait déjà que $i \in C_i$, il suffit donc de montrer que si $C_i \cap C_j \neq \emptyset$, alors $C_i = C_j$. Supposons qu'il existe $v \in C_i \cap C_j$. Il existe donc $k, \ell \in \mathbb{Z}$ tels que

$$v = \mu^k(i) = \mu^\ell(j).$$

Dès lors, $j = \mu^{k-\ell}(i)$. Par conséquent, pour tout $t \in \mathbb{Z}$, on a

$$\mu^t(j) = \mu^{t+k-\ell}(i) \quad \text{et} \quad \mu^t(i) = \mu^{t-k+\ell}(j),$$

ce qui signifie que $C_i = C_j$.

Choisissons à présent $i_1, \ldots, i_p \in X$ tels que $C_{i_1}, \ldots, C_{i_p}$ soient deux à deux distincts et forment une partition de X. Vu ce qui précède, on vérifie aisément que

$$\begin{aligned} \gamma_1 &= \big(i_1 \quad \mu(i_1) \quad \cdots \quad \mu^{m_i-1}(i_1)\big) \\ &\vdots \\ \gamma_p &= \big(i_p \quad \mu(i_p) \quad \cdots \quad \mu^{m_p-1}(i_p)\big) \end{aligned}$$

sont des cycles disjoints tels que $\mu = \gamma_1 \cdots \gamma_p$. Comme les cycles de longueur 1 sont égaux à l'identité, on peut les omettre sans changer la valeur du produit.

Pour conclure, il nous faut encore montrer l'unicité de la décomposition. Supposons que $\mu = \gamma'_1 \cdots \gamma'_q$ où $\gamma'_1, \ldots, \gamma'_q$ sont des cycles disjoints de longueur au moins égale à 2. Soient $k \in \{1, \ldots, q\}$ et x un élément du cycle γ'_k. Puisque γ'_k est un cycle, l'ensemble $\{\mu^i(x) \mid i \in \mathbb{Z}\}$ est exactement l'ensemble des éléments apparaissant dans γ'_k et coïncide avec un des $C_{i_1}, \ldots, C_{i_p}$. Réciproquement, pour tout $j \in \{1, \ldots, p\}$, C_{i_j} coïncide avec l'ensemble des éléments d'un des cycles γ'_k.

■

[5]Des ensembles P_j, $j \in J$, forment une *partition* de X si $\cup_{j\in J} P_j = X$ et si ces ensembles sont non vides et deux à deux disjoints.

Remarque IV.2.6. Certaines opérations sont faciles à effectuer dans le cas des cycles et par le résultat précédent, se transposent aisément à toute permutation décomposée en produit de cycles.

- On obtient la puissance k-ième d'un cycle en écrivant le (ou les) cycle(s) formé(s) par ses éléments pris de k en k.

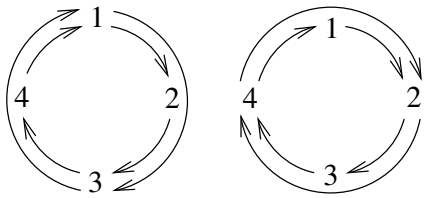


FIGURE IV.2. Un cycle et son carré.

$$\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}^2 = \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix},$$
$$\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}^3 = \begin{pmatrix}1 & 4 & 3 & 2\end{pmatrix}.$$

En particulier, la puissance ℓ-ième d'un cycle de longueur ℓ est la permutation identique.

- Voici une conséquence de la remarque précédente et de la proposition IV.2.4. Si m est le plus petit commun multiple des longueurs des cycles $\sigma_1, \ldots, \sigma_r$ apparaissant dans la décomposition de la permutation μ, alors
$$\mu^m = id.$$
En effet,
$$\mu^m = \sigma_1^m \cdots \sigma_r^m$$
et pour tout $i \in \{1, \ldots, r\}$, m est un multiple de la longueur de σ_i. Donc, vu la première remarque, $\sigma_i^m = id$.
- L'inverse d'un cycle s'obtient en renversant l'ordre de ses éléments. Par exemple,
$$\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}^{-1} = \begin{pmatrix}4 & 3 & 2 & 1\end{pmatrix}.$$

3. Transpositions

Définition IV.3.1. Une *transposition* est un cycle de longueur 2. La transposition $\begin{pmatrix}i & j\end{pmatrix}$, $i \neq j$, permute i et j et laisse les autres éléments de X inchangés.

On dispose des formules suivantes :

$$\begin{pmatrix}i & j\end{pmatrix} = \begin{pmatrix}j & i\end{pmatrix},$$
$$\begin{pmatrix}i & j\end{pmatrix}^2 = id.$$

Si k diffère de i et de j, alors

$$(i \quad j) = (k \quad i)\,(k \quad j)\,(k \quad i) = (k \quad j)\,(k \quad i)\,(k \quad j)\,.$$

Exemple IV.3.2. On a

$$(1 \quad 3) = (2 \quad 1)\,(2 \quad 3)\,(2 \quad 1)$$

car

$$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}.$$

Proposition IV.3.3. *Tout cycle de longueur p est un produit de $p-1$ transpositions.*

Démonstration. On a

$$\begin{aligned}(i_1 \quad i_2 \quad \cdots \quad i_p) &= (i_1 \quad i_p)\,(i_1 \quad i_{p-1})\cdots(i_1 \quad i_2)\\ &= (i_1 \quad i_2)\,(i_2 \quad i_3)\cdots(i_{p-1} \quad i_p)\,.\end{aligned}$$

Pour le voir, il suffit de vérifier que l'action des deux membres sur les éléments qui y figurent est la même puisque les autres restent inchangés.

■

Corollaire IV.3.4. *Toute permutation est un produit de transpositions.*

Démonstration. Cela résulte de la proposition IV.2.4 et de la proposition précédente.

■

Exemple IV.3.5. On a par exemple,

$$\begin{aligned}\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&1&2&7&8&6&5&9&4\end{pmatrix} &= (1 \quad 3 \quad 2)\,(4 \quad 7 \quad 5 \quad 8 \quad 9)\\ &= (1 \quad 3)\,(3 \quad 2)\,(4 \quad 7)\,(7 \quad 5)\,(5 \quad 8)\,(8 \quad 9)\\ &= (1 \quad 2)\,(1 \quad 3)\,(4 \quad 9)\,(4 \quad 8)\,(4 \quad 5)\,(4 \quad 7)\,.\end{aligned}$$

4. Signature d'une permutation

Définition IV.4.1. Soit μ une permutation de $X = \{1, \ldots, n\}$. Une paire[6] $\{i, j\}$, $i, j \in X$, est une *inversion* de μ si

$$i < j \quad \text{et} \quad \mu(i) > \mu(j)$$

ou

$$i > j \quad \text{et} \quad \mu(i) < \mu(j)$$

c'est-à-dire si μ inverse l'ordre des éléments i et j. La signature de la permutation μ est le nombre

$$\operatorname{sign}\mu = (-1)^N$$

[6]Ne pas confondre les notions de paire et de couple. Pour une paire, l'ordre des éléments n'est pas important (d'où la notation ensembliste). Pour un couple, si $i \neq j$, $(i, j) \neq (j, i)$.

où N est le nombre d'inversions de μ. Si $\operatorname{sign}\mu = 1$, la permutation est dite *paire*. Si $\operatorname{sign}\mu = -1$, la permutation est dite *impaire*.

Exemple IV.4.2. Soit la permutation

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}.$$

Les paires $\{1,2\}$, $\{1,4\}$ et $\{3,4\}$ sont les seules inversions de μ. Cette permutation est donc impaire.

Remarque IV.4.3. La permutation identité est paire car elle ne présente aucune inversion,

$$\operatorname{sign} id = (-1)^0 = 1.$$

Toute transposition est une permutation impaire. En effet, considérons la transposition $\tau = \begin{pmatrix} i & j \end{pmatrix}$ avec $i < j$. Cette transposition possède comme inversions la paire $\{i,j\}$ et toutes les paires $\{i,k\}$ et $\{k,j\}$ telles que $i < k < j$. Il y a donc un nombre impair d'inversions.

La propriété fondamentale de la signature est la suivante.

Proposition IV.4.4. *Soient μ, ν deux permutations de $\mathcal{S}_n$. On a*

$$\operatorname{sign}(\mu\nu) = \operatorname{sign}\mu \operatorname{sign}\nu.$$

Démonstration. Soit $\{i,j\}$ une paire telle que $1 \leq i < j \leq n$. Quatre possibilités sont à envisager :

cas	ν inverse $\{i,j\}$	μ inverse $\{\nu(i),\nu(j)\}$	$\mu\nu$ inverse $\{i,j\}$
a	oui	oui	non
b	oui	non	oui
c	non	oui	oui
d	non	non	non

Notons N_x le nombre de paires correspondant au cas x ($x = a,b,c,d$). Le nombre d'inversions de ν est égal à $N_a + N_b$ et celui de $\mu\nu$ est égal à $N_b + N_c$. Il nous faut à présent calculer le nombre d'inversions de μ. Or, ν est une permutation, les ensembles $\{\nu(i),\nu(j)\}$ décrivent donc exactement les paires d'éléments de $\{1,\ldots,n\}$. Il s'ensuit que le nombre d'inversions de μ est $N_a + N_c$. Par conséquent,

$$\begin{aligned} \operatorname{sign}\mu \operatorname{sign}\nu &= (-1)^{(N_a+N_b)}\,(-1)^{(N_a+N_c)} \\ &= (-1)^{(N_a+N_b)+(N_a+N_c)-2N_a} = (-1)^{N_b+N_c} = \operatorname{sign}(\mu\nu). \end{aligned}$$

■

Corollaire IV.4.5. *Dans une décomposition d'une permutation en transpositions, le nombre de facteurs est pair (resp. impair) si la permutation est paire (resp. impaire)*

Démonstration. Si $\mu \in \mathcal{S}_n$ est égal à $\tau_1 \cdots \tau_p$ où les τ_i sont des transpositions, on a

$$\operatorname{sign} \mu = \operatorname{sign} \tau_1 \ \cdots \ \operatorname{sign} \tau_p.$$

D'où la conclusion car toute transposition est impaire.

■

Corollaire IV.4.6. *Tout cycle de longueur paire (resp. impaire) est une permutation impaire (resp. paire). De plus, la parité d'une permutation est la parité du nombre de ses cycles de longueur paire.*

Démonstration. Cela résulte de la proposition IV.3.3.

■

Remarque IV.4.7. Pour toute permutation $\mu \in \mathcal{S}_n$, on a

$$\operatorname{sign} \mu = \operatorname{sign} \mu^{-1}.$$

En effet, $\mu^{-1}\mu = id$ et id est une permutation paire.

Proposition IV.4.8. *Soit $n > 1$. Le nombre de permutations paires*[7] *de $\{1, \ldots, n\}$ est égal au nombre de permutations impaires de $\{1, \ldots, n\}$ et vaut $n!/2$.*

Démonstration. Soient $\mu_1, \ldots, \mu_k$ les permutations paires de $\{1, \ldots, n\}$. Puisque $n > 1$, il existe au moins une permutation impaire[8] τ. Au vu de la proposition IV.4.4, les permutations $\tau\mu_1, \ldots, \tau\mu_k$ sont impaires. De plus, ces dernières permutations sont deux à deux distinctes. En effet, supposons que $\tau\mu_i = \tau\mu_j$ avec $i \neq j$. En multipliant à gauche par τ^{-1}, on trouve $\mu_i = \mu_j$. Enfin, il n'y a pas d'autre permutation impaire que $\tau\mu_1, \ldots, \tau\mu_k$. En effet, supposons que ν soit une permutation impaire distincte de $\tau\mu_i$ pour tout $i \in \{1, \ldots, k\}$. Dès lors, $\tau^{-1}\nu$ est une permutation paire. Donc il existe $j \in \{1, \ldots, k\}$ tel que $\tau^{-1}\nu = \mu_j$ et

$$\nu = \tau\tau^{-1}\nu = \tau\mu_j.$$

■

On note $\mathcal{A}_n$, l'ensemble des permutations paires de $\{1, \ldots, n\}$.

[7] Un sous-groupe H d'un groupe G est un sous-ensemble de G qui possède lui-même une structure de groupe pour la loi de G. Nous avons vu précédemment que $\mathcal{S}_n$ était un groupe. On peut facilement vérifier que l'ensemble $\mathcal{A}_n$ formé des permutations paires est un sous-groupe de $\mathcal{S}_n$, appelé le *groupe alterné* de $\{1, \ldots, n\}$. Pour vérifier que $\mathcal{A}_n$ est un sous-groupe, il suffit de vérifier que $id \in \mathcal{A}_n$ et que pour tout $\mu, \nu \in \mathcal{A}_n$, $\mu\nu \in \mathcal{A}_n$ et $\mu^{-1} \in \mathcal{A}_n$. Remarquons encore que l'ensemble des permutations impaires n'est pas un sous-groupe de $\mathcal{A}_n$.

[8] Par exemple, la transposition $\begin{pmatrix} 1 & 2 \end{pmatrix}$.

CHAPITRE V

Déterminants

Dans ce chapitre, pour faciliter l'écriture, si $\nu \in \mathcal{S}_n$, alors on s'autorise à dénoter l'élément $\nu(i)$ simplement par ν_i, $i \in \{1, \ldots, n\}$.

1. Déterminant d'une matrice carrée

Définition V.1.1. Soit $A = (a_{ij})_{1 \leq i,j \leq n}$ une matrice carrée de dimension n à coefficients dans $\mathbb{K}$. Le *déterminant* de A est le scalaire

$$\det(A) = \sum_{\nu \in \mathcal{S}_n} \operatorname{sign}(\nu)\ a_{1\nu_1} \cdots a_{n\nu_n}.$$

La somme portant sur toutes les permutations de $\{1, \ldots, n\}$, elle comporte donc $n!$ termes. Si $n > 1$, la moitié des termes sont affectés du signe $+1$, l'autre moitié de -1. Un terme de la somme est construit en sélectionnant exactement un élément sur chaque ligne et sur chaque colonne de A.

On note souvent le déterminant d'une matrice carrée en plaçant les éléments de celle-ci entre deux barres verticales.

Exemple V.1.2. Si $n = 1$, alors $A = (a)$ et $\det A = a$.
Si $n = 2$, alors $\mathcal{S}_n = \{id, \begin{pmatrix} 1 & 2 \end{pmatrix}\}$ et

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

On retrouve la règle des produits diagonaux.

Si $n = 3$, alors l'ensemble $\mathcal{S}_n$ contient trois permutations paires id, $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$ et trois permutations impaires $\begin{pmatrix} 1 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 3 \end{pmatrix}$ et $\begin{pmatrix} 2 & 3 \end{pmatrix}$. Ainsi,

$$\begin{aligned} \det(A) &= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ &\quad - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32}. \end{aligned}$$

On résume ce développement par la règle des produits triangulaires représentée schématiquement sur la figure V.1. Cette règle peut encore se réénoncer

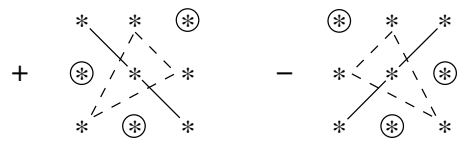


FIGURE V.1. La règle des produits triangulaires.

sous la forme de la règle de Sarrus. On recopie à droite de la matrice A les deux premières colonnes de celle-ci pour obtenir le tableau

$$\begin{array}{ccc|cc} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{array} .$$

Le déterminant de A s'obtient en sommant les produits des éléments des trois diagonales descendantes et les produits de -1 et des éléments des trois diagonales ascendantes. Ceci est résumé par la figure suivante. On notera

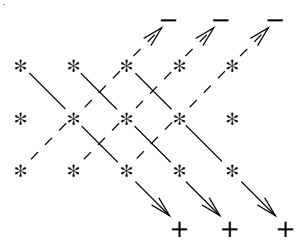


FIGURE V.2. La règle de Sarrus.

si $n = 4$, $2n = 8$ et $n! = 24$.

que cette règle ne se généralise pas au cas $n > 3$. En effet, elle ne fait intervenir que $2n$ termes alors qu'il en faut $n!$ pour calculer $\det A$. Ainsi, pour $n > 3$, le calcul d'un déterminant par application de la définition peut s'avérer fastidieux et on a dès lors généralement recours à des moyens détournés.

La définition du déterminant semble privilégier l'indice de la ligne par rapport à celui de la colonne. Le résultat suivant montre qu'il n'en est rien.

Proposition V.1.3. *Si $A = (a_{ij})_{1\leq i,j\leq n}$ est une matrice carrée de dimension n alors*

$$\det(A) = \sum_{\nu\in\mathcal{S}_n} \operatorname{sign}(\nu)\ a_{\nu_1 1}\cdots a_{\nu_n n}.$$

En particulier, $\det A = \det \widetilde{A}$.

Démonstration. Il suffit de remarquer que la somme porte encore sur toutes les permutations de $\{1,\ldots,n\}$. Par définition,

$$\det(A) = \sum_{\nu\in\mathcal{S}_n} \operatorname{sign}(\nu)\ a_{1\nu_1}\cdots a_{n\nu_n}.$$

Pour toute permutation ν, on a

$$\operatorname{sign}(\nu)\ a_{1\nu_1}\cdots a_{n\nu_n} = \operatorname{sign}(\nu^{-1})\ a_{\nu^{-1}(1)1}\cdots a_{\nu^{-1}(n)n}$$

car d'une part, $\operatorname{sign}(\nu) = \operatorname{sign}(\nu^{-1})$ et d'autre part, si la permutation ν est telle que

$$\nu : i \mapsto \nu_i = j$$

alors la permutation ν^{-1}

$$\nu^{-1} : j \mapsto \nu^{-1}(j) = \nu^{-1}\nu_i = i.$$

Ainsi, le facteur $a_{i\nu_i}$ du premier membre est égal au facteur $a_{\nu^{-1}(j)j}$ du second membre et par conséquent, les deux membres sont les produits des mêmes éléments. Comme l'application

$$\mathcal{S}_n \to \mathcal{S}_n : \nu \mapsto \nu^{-1}$$

est une bijection de $\mathcal{S}_n$, on a

$$\begin{aligned}\det(A) &= \sum_{\nu\in\mathcal{S}_n} \operatorname{sign}(\nu^{-1})\ a_{\nu^{-1}(1)1}\cdots a_{\nu^{-1}(n)n} \\ &= \sum_{\mu\in\mathcal{S}_n} \operatorname{sign}(\mu)\ a_{\mu(1)1}\cdots a_{\mu(n)n}.\end{aligned}$$

■

Remarque V.1.4. La proposition précédente permet de traduire les propriétés du déterminant par rapport aux lignes de A en termes de propriétés par rapport aux colonnes de A et inversement.

Remarque V.1.5. Dans le cas de matrices complexes (i.e., $\mathbb{K} = \mathbb{C}$), il est clair que

$$\det \overline{A} = \overline{\det A}.$$

Et donc, en vertu de la proposition précédente, il vient

$$\det A^* = \overline{\det A}.$$

2. Premières propriétés

Proposition V.2.1. *L'application* $\det : \mathbb{K}_n^n \to \mathbb{K} : A \mapsto \det(A)$ *jouit des propriétés suivantes. (On note* $C_1, \ldots, C_n$ *les colonnes de* A*.)*

i) $\det I = 1$,

ii) $\det A$ *est multilinéaire*[1] *par rapport aux colonnes de* A*, i.e., pour tous* $X_1, \ldots, X_\ell \in \mathbb{K}^n$ *et* $\lambda_1, \ldots, \lambda_\ell \in \mathbb{K}$,

Cette notation signifie qu'une colonne de A est combinaison linéaire des X_i.

$$\begin{aligned}&\det\begin{pmatrix} C_1 & \cdots & \sum_{i=1}^{\ell}\lambda_i X_i & \cdots & C_n\end{pmatrix} \\ &= \sum_{i=1}^{\ell}\lambda_i \det\begin{pmatrix} C_1 & \cdots & X_i & \cdots & C_n\end{pmatrix};\end{aligned}$$

iii) $\det A$ *est alterné par rapport aux colonnes de* A*, i.e., si* $i \neq j$ *et si* $C_i = C_j$ *alors*

$$\det\begin{pmatrix} C_1 & \cdots & C_i & \cdots & C_j & \cdots & C_n\end{pmatrix} = 0.$$

[1] Soit E un espace vectoriel. Une application $f : \overbrace{E \times E \times \cdots \times E}^{r \text{ fois}} \to E$ est *r-linéaire* ou *multilinéaire* si pour tout $i \in \{1, \ldots, r\}$ et tous $r-1$ éléments $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_r \in E$, l'application $\xi \in E \mapsto f(x_1, \ldots, x_{i-1}, \xi, x_{i+1}, \ldots, x_r)$ est linéaire.

En particulier, $\det A$ *est antisymétrique par rapport aux colonnes de* A*, i.e., pour toute permutation* $\mu \in \mathcal{S}_n$ *on a*

$$\det\begin{pmatrix} C_{\mu_1} & \cdots & C_{\mu_n}\end{pmatrix} = \operatorname{sign}(\mu)\det\begin{pmatrix} C_1 & \cdots & C_n\end{pmatrix}.$$

Remarque V.2.2. Cette proposition peut évidemment se réexprimer en termes des lignes de A.

Exemple V.2.3. Nous voudrions, avant de passer à la preuve proprement dite, illustrer les notations employées dans l'énoncé. Avec les notations du point ii), considérons le cas où $\ell = 2$, $n = 3$, $\lambda_1 = 2$, $\lambda_2 = 3$,

$$X_1 = \begin{pmatrix}1\\0\\1\end{pmatrix},\ X_2 = \begin{pmatrix}3\\2\\1\end{pmatrix},\ C_1 = \begin{pmatrix}1\\2\\3\end{pmatrix} \text{ et } C_2 = \begin{pmatrix}4\\5\\6\end{pmatrix}.$$

Ainsi, l'expression

$$\det\begin{pmatrix} C_1 & \lambda_1 X_1 + \lambda_2 X_2 & C_3\end{pmatrix} = \lambda_1 \det\begin{pmatrix} C_1 & X_1 & C_3\end{pmatrix} + \lambda_2 \det\begin{pmatrix} C_1 & X_2 & C_3\end{pmatrix}$$

revient à

$$\det\begin{pmatrix}1 & 11 & 4\\ 2 & 6 & 5\\ 3 & 5 & 6\end{pmatrix} = 2\det\begin{pmatrix}1 & 1 & 4\\ 2 & 0 & 5\\ 3 & 1 & 6\end{pmatrix} + 3\det\begin{pmatrix}1 & 3 & 4\\ 2 & 2 & 5\\ 3 & 1 & 6\end{pmatrix}.$$

Démonstration. Le point i) est immédiat.

Il est commode d'utiliser la définition du déterminant privilégiant l'indice des colonnes. Pour démontrer ii), il vient

$$\det\begin{pmatrix} C_1 & \cdots & \overbrace{\sum_{i=1}^{\ell}\lambda_i X_i}^{j\text{-ième colonne}} & \cdots & C_n\end{pmatrix}$$

$\sum_{i=1}^{\ell}\lambda_i X_i \in \mathbb{K}^n$ est un vecteur colonne et $\left(\sum_{i=1}^{\ell}\lambda_i X_i\right)_{\nu_j}$ représente une de ses composantes.

$$= \sum_{\nu\in\mathcal{S}_n} \operatorname{sign}(\nu)\ a_{\nu_1 1}\cdots\left(\sum_{i=1}^{\ell}\lambda_i X_i\right)_{\nu_j}\cdots a_{\nu_n n}$$

$$= \sum_{i=1}^{\ell}\lambda_i \sum_{\nu\in\mathcal{S}_n} \operatorname{sign}(\nu)\ a_{\nu_1 1}\cdots (X_i)_{\nu_j}\cdots a_{\nu_n n}$$

$$= \sum_{i=1}^{\ell}\lambda_i \det\begin{pmatrix} C_1 & \cdots & X_i & \cdots & C_n\end{pmatrix}$$

iii) Soient $i \neq j$. Considérons la transposition $\tau = \begin{pmatrix} i & j\end{pmatrix}$ et rappelons que $\mathcal{A}_n$ dénote l'ensemble des permutations paires. Par un raisonnement analogue à celui de la preuve de la proposition IV.4.8, on a

$$\begin{aligned}\det A &= \sum_{\nu\in\mathcal{S}_n} \operatorname{sign}(\nu)\ a_{\nu_1 1}\cdots a_{\nu_n n}\\ &= \sum_{\nu\in\mathcal{A}_n} \operatorname{sign}(\nu)\ a_{\nu_1 1}\cdots a_{\nu_n n} + \sum_{\nu\in\mathcal{A}_n} \operatorname{sign}(\nu\tau)\ a_{(\nu\tau)_1 1}\cdots a_{(\nu\tau)_n n}.\end{aligned}$$

Or, si $\nu \in \mathcal{A}_n$, alors $\text{sign}\,(\nu\tau) = -\text{sign}\,(\nu) = -1$ et

$$(\nu\tau)_i = \nu_j, \quad (\nu\tau)_j = \nu_i$$

et pour tout $k \neq i, j$,

$$(\nu\tau)_k = \nu_k.$$

Donc

$$\begin{aligned} \det A &= \sum_{\nu\in\mathcal{A}_n} a_{\nu_1 1}\cdots a_{\nu_i i}\cdots a_{\nu_j j}\cdots a_{\nu_n n} \\ &\quad - \sum_{\nu\in\mathcal{A}_n} a_{\nu_1 1}\cdots a_{\nu_j i}\cdots a_{\nu_i j}\cdots a_{\nu_n n}. \end{aligned}$$

Si les colonnes C_i et C_j sont égales, alors $a_{ki} = a_{kj}$ pour tout $k \in \{1, \ldots, n\}$. Dans ce cas, $a_{\nu_i i} = a_{\nu_i j}$, $a_{\nu_j i} = a_{\nu_j j}$ et donc $\det A$ est alterné sur les colonnes.

Considérons à présent le cas particulier. Par multilinéarité du déterminant, on trouve

$$\begin{aligned} &\det\begin{pmatrix} C_1 & \cdots & C_i + C_j & \cdots & C_i + C_j & \cdots & C_n \end{pmatrix} \\ = \;& \det\begin{pmatrix} C_1 & \cdots & C_i & \cdots & C_i & \cdots & C_n \end{pmatrix} \\ + \;& \det\begin{pmatrix} C_1 & \cdots & C_i & \cdots & C_j & \cdots & C_n \end{pmatrix} \\ + \;& \det\begin{pmatrix} C_1 & \cdots & C_j & \cdots & C_i & \cdots & C_n \end{pmatrix} \\ + \;& \det\begin{pmatrix} C_1 & \cdots & C_j & \cdots & C_j & \cdots & C_n \end{pmatrix}. \end{aligned}$$

Vu le caractère alterné du déterminant, il vient

$$\begin{aligned} &\det\begin{pmatrix} C_1 & \cdots & C_i & \cdots & C_j & \cdots & C_n \end{pmatrix} \\ = -\;& \det\begin{pmatrix} C_1 & \cdots & C_j & \cdots & C_i & \cdots & C_n \end{pmatrix}. \end{aligned}$$

Le résultat annoncé résulte du fait que toute permutation est un produit de transpositions.

■

Remarque V.2.4. Dans la preuve précédente, on a en fait montré que si une application $D : \mathbb{K}_n^n \to \mathbb{K}$ est multilinéaire et alternée sur les colonnes, alors elle est antisymétrique. En effet, dans la dernière partie de cette preuve, on n'a utilisé aucune autre propriété pour montrer le caractère antisymétrique du déterminant (qui est un cas particulier d'application définie sur $\mathbb{K}_n^n$ et à valeurs dans $\mathbb{K}$).

Corollaire V.2.5. *Si on ajoute à une colonne d'une matrice A, une combinaison linéaire des autres colonnes de A, alors on ne modifie pas la valeur du déterminant.*

Démonstration. Soient $A \in \mathbb{K}_n^n$ et $j \in \{1, \ldots, n\}$. Dans cette preuve, la colonne centrale représente toujours la colonne en j-ième position. Par multilinéarité du déterminant, on a

$$\det\begin{pmatrix} C_1 & \cdots & C_j + \sum_{i\neq j} \lambda_i C_i & \cdots & C_n \end{pmatrix}$$

$$= \det\begin{pmatrix} C_1 & \cdots & C_j & \cdots & C_n \end{pmatrix} + \sum_{i \neq j} \lambda_i \underbrace{\det\begin{pmatrix} C_1 & \cdots & C_i & \cdots & C_n \end{pmatrix}}_{=0}$$

et pour $i \neq j$, les déterminants dans la dernière somme s'annulent tous car on trouve la colonne C_i aux positions i et j.

■

Les propriétés énoncées dans la proposition V.2.1 caractérisent complètement l'application $\det : \mathbb{K}_n^n \to \mathbb{K}$. En d'autres termes, si $D : \mathbb{K}_n^n \to \mathbb{K}$ est une application satisfaisant aux propriétés i), ii) et iii) de la proposition V.2.1, alors $D = \det$. Cela est explicité par la proposition suivante.

Proposition V.2.6. [2] *Si $D : \mathbb{K}_n^n \to \mathbb{K}$ est une application multilinéaire et alternée sur les colonnes, alors, pour tout $A \in \mathbb{K}_n^n$,*

$$D(A) = D(I)\ \det(A).$$

Démonstration. Soit $A \in \mathbb{K}_n^n$. Pour tout $j \in \{1, \ldots, n\}$, il existe des a_{kj} dans $\mathbb{K}$ tels que la j-ième colonne C_j de A se décompose suivant les vecteurs unitaires de $\mathbb{K}^n$

$$C_j = \sum_{k=1}^{n} a_{kj} e_k.$$

Puisque D est multilinéaire, il vient

$$D\begin{pmatrix} C_1 & \cdots & C_n \end{pmatrix} = \sum_{k_1=1}^{n} \cdots \sum_{k_n=1}^{n} a_{k_1 1} \cdots a_{k_n n}\ D\begin{pmatrix} e_{k_1} & \cdots & e_{k_n} \end{pmatrix}$$

Puisque D est alterné, $D\begin{pmatrix} e_{k_1} & \cdots & e_{k_n} \end{pmatrix} = 0$ si $k_r = k_s$ pour $r \neq s$. Il s'en suit que

$$D(A) = \sum_{\mu \in \mathcal{S}_n} a_{\mu_1 1} \cdots a_{\mu_n n}\ D\begin{pmatrix} e_{\mu_1} & \cdots & e_{\mu_n} \end{pmatrix}.$$

En procédant comme dans la preuve de la proposition V.2.1, puisque D est alterné sur les colonnes (cf. remarque V.2.4), on trouve

$$D\begin{pmatrix} e_{\mu_1} & \cdots & e_{\mu_n} \end{pmatrix} = \operatorname{sign}(\mu)\ D\begin{pmatrix} e_1 & \cdots & e_n \end{pmatrix} = \operatorname{sign}(\mu)\ D(I)$$

d'où la conclusion.

■

Proposition V.2.7. *Soient $A_1, \ldots, A_t$ des matrices carrées et A une matrice triangulaire composée de la forme*

$$A = \begin{pmatrix} A_1 & * & \cdots & * \\ 0 & A_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & A_t \end{pmatrix}.$$

[2] Certains auteurs définissent l'application déterminant comme étant l'unique application multilinéaire et alternée qui envoie la matrice identité sur 1. Cette manière de procéder aurait l'avantage de ne pas devoir recourir aux permutations. Avec l'approche choisie ici, il s'agit d'une propriété découlant de notre définition.

Alors

$$\det A = \det A_1 \cdots \det A_t.$$

Démonstration. On procède de proche en proche. Il suffit donc de considérer le cas où la matrice n'est composée que de deux matrices partielles diagonales,

$$A = \begin{pmatrix} A_1 & * \\ 0 & A_2 \end{pmatrix}$$

Supposons A_1 de dimension r et A_2 de dimension $n-r$. Par définition du déterminant (si on privilégie ici les indices des colonnes), on a

$$\det A = \sum_{\nu \in \mathcal{S}_n} \operatorname{sign} \begin{pmatrix} 1 & \cdots & r & r+1 & \cdots & n \\ \nu_1 & \cdots & \nu_r & \nu_{r+1} & \cdots & \nu_n \end{pmatrix} a_{\nu_1 1} \cdots a_{\nu_r r}\, a_{\nu_{r+1} r+1} \cdots a_{\nu_n n}.$$

Dans chaque terme, les facteurs choisis dans les r premières colonnes sont nuls s'ils ne sont pas dans les r premières lignes. Autrement dit, le terme correspondant à une permutation ν est nul sauf si $\nu_1, \ldots, \nu_r$ définissent une permutation ϕ de $\{1, \ldots, r\}$. Auquel cas, $\nu_{r+1}, \ldots, \nu_n$ définissent eux une permutation ψ de $\{r+1, \ldots, n\}$ et dès lors,

$$\nu = \begin{pmatrix} 1 & \cdots & r & r+1 & \cdots & n \\ \nu_1 & \cdots & \nu_r & r+1 & \cdots & n \end{pmatrix} \begin{pmatrix} 1 & \cdots & r & r+1 & \cdots & n \\ 1 & \cdots & r & \nu_{r+1} & \cdots & \nu_n \end{pmatrix}$$

et

$$\operatorname{sign}(\nu) = \operatorname{sign}(\phi)\, \operatorname{sign}(\psi).$$

De là,

$$\begin{aligned} \det A &= \sum_{\phi} \sum_{\psi} \operatorname{sign}(\phi)\operatorname{sign}(\psi)\; a_{\phi_1 1} \cdots a_{\phi_r r}\, a_{\psi_{r+1} r+1} \cdots a_{\psi_n n} \\ &= \sum_{\phi} \operatorname{sign}(\phi)\; a_{\phi_1 1} \cdots a_{\phi_r r} \sum_{\psi} \operatorname{sign}(\psi)\; a_{\psi_{r+1} r+1} \cdots a_{\psi_n n} \\ &= \det A_1 \det A_2. \end{aligned}$$

■

Remarque V.2.8. La proposition précédente s'applique bien évidemment à une matrice triangulaire composée de la forme

$$A = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ * & A_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ * & \cdots & * & A_t \end{pmatrix}$$

où les A_i sont des matrices carrées.

En particulier, le déterminant d'une matrice diagonale est égal au produit des éléments diagonaux,

$$\det(\operatorname{diag}(\lambda_1, \ldots, \lambda_n)) = \lambda_1 \cdots \lambda_n.$$

Définition V.2.9. Soit $A = (a_{ij})$ une matrice carrée de dimension n. On appelle *mineur* d'ordre p de A le déterminant d'une sous-matrice carrée de A de dimension p. On a le plus souvent recours aux mineurs d'ordre $n-1$, simplement appelés *mineurs*. Le mineur $M_{ij}(A)$ de l'élément a_{ij}, $1 \leq i, j \leq n$, est le déterminant de la sous-matrice de A obtenue en effaçant la i-ième ligne et la j-ième colonne de A.

Le *cofacteur* ou *mineur algébrique* de l'élément a_{ij}, $1 \leq i, j \leq n$, est le scalaire

$$\mathrm{cof}_{ij}(A) = (-1)^{i+j} M_{ij}(A).$$

La *matrice des cofacteurs* de A est la matrice

$$\mathrm{cof}(A) = (\mathrm{cof}_{ij}(A))_{1 \leq i,j \leq n}.$$

Exemple V.2.10. Soit la matrice

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & -1 \\ 3 & -2 & 0 \end{pmatrix}.$$

Les mineurs de A sont

$$M_{11} = \begin{vmatrix} 1 & -1 \\ -2 & 0 \end{vmatrix} = -2,\ M_{12} = \begin{vmatrix} 0 & -1 \\ 3 & 0 \end{vmatrix} = 3,\ M_{13} = \begin{vmatrix} 0 & 1 \\ 3 & -2 \end{vmatrix} = -3$$

$$M_{21} = \begin{vmatrix} 2 & 1 \\ -2 & 0 \end{vmatrix} = 2,\ M_{22} = \begin{vmatrix} 1 & 1 \\ 3 & 0 \end{vmatrix} = -3,\ M_{23} = \begin{vmatrix} 1 & 2 \\ 3 & -2 \end{vmatrix} = -8$$

$$M_{31} = \begin{vmatrix} 2 & 1 \\ 1 & -1 \end{vmatrix} = -3,\ M_{32} = \begin{vmatrix} 1 & 1 \\ 0 & -1 \end{vmatrix} = -1,\ M_{33} = \begin{vmatrix} 1 & 2 \\ 0 & 1 \end{vmatrix} = 1.$$

La matrice des cofacteurs est

$$\mathrm{cof}(A) = \begin{pmatrix} -2 & -3 & -3 \\ -2 & -3 & 8 \\ -3 & 1 & 1 \end{pmatrix}.$$

Lemme V.2.11. *Soit $A = (a_{ij})_{1 \leq i,j \leq n}$ une matrice carrée. Le cofacteur $\mathrm{cof}_{ij}(A)$ de a_{ij} est le déterminant de la matrice obtenue en remplaçant la j-ième de colonne de A par le vecteur unitaire e_i, ou en remplaçant la i-ème ligne de A par $\widetilde{e_j}$.*

Démonstration. Soit $A = \begin{pmatrix} C_1 & \cdots & C_j & \cdots & C_n \end{pmatrix}$. Considérons la matrice où C_j est remplacé par e_i, il vient

$$\det \begin{pmatrix} C_1 & \cdots & e_i & \cdots & C_n \end{pmatrix} = (-1)^{j-1} \det \begin{pmatrix} e_i & C_1 & \cdots & \widehat{C_j} & \cdots & C_n \end{pmatrix}$$

car on a effectué $j-1$ transpositions pour ramener la j-ième colonne e_i en première position (la notation $\widehat{C_j}$ signifie que la colonne C_j est omise). Le vecteur e_i contient 1 en i-ième position; il nous faut à présent ramener cet élément dans le coin supérieur gauche en effectuant $i-1$ transpositions de lignes. On a

$$\det \begin{pmatrix} e_i & C_1 & \cdots & \widehat{C_j} & \cdots & C_n \end{pmatrix}$$

$$= (-1)^{i-1} \det \begin{pmatrix} 1 & a_{i1} & \cdots & \widehat{a_{ij}} & \cdots & a_{in} \\ 0 & a_{11} & \cdots & \widehat{a_{1j}} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots & & \vdots \\ \widehat{0} & \widehat{a_{i1}} & & \widehat{a_{ij}} & & \widehat{a_{in}} \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & a_{n1} & \cdots & \widehat{a_{nj}} & \cdots & a_{nn} \end{pmatrix}.$$

On est maintenant ramené à calculer le déterminant d'une matrice triangulaire composée dont la première sous-matrice diagonale est 1 et la seconde est exactement la matrice A privée de sa i-ième ligne et j-ième colonne. Ainsi, par définition du mineur, il vient

$$\det \begin{pmatrix} C_1 & \cdots & e_i & \cdots & C_n \end{pmatrix} = (-1)^{i+j-2} M_{ij}(A) = (-1)^{i+j} M_{ij}(A) = \operatorname{cof}_{ij}(A).$$

■

Proposition V.2.12 (Loi des mineurs). *Pour toute matrice carrée $A = (a_{ij})_{1 \leq i,j \leq n}$, on a*

$$\boxed{\sum_{k=1}^{n} a_{ik} \operatorname{cof}_{jk}(A) = \sum_{k=1}^{n} a_{ki} \operatorname{cof}_{kj}(A) = \delta_{ij} \det A.}$$

Autrement dit, la somme des produits des éléments d'une ligne (resp. d'une colonne) par leurs cofacteurs respectifs est égale au déterminant (première loi des mineurs); la somme des produits des éléments d'une ligne (resp. d'une colonne) par les cofacteurs des éléments correspondants d'une ligne (resp. d'une colonne) parallèle est nulle (seconde loi des mineurs). Sous forme matricielle,

$$A \widetilde{\operatorname{cof}(A)} = \widetilde{\operatorname{cof}(A)}\, A = \det(A)\, I.$$

Démonstration. Raisonnons sur les colonnes de la matrice A. On peut refaire une démonstration analogue en raisonnant sur les lignes de A ou en passant à la transposée de A. Soit $A = \begin{pmatrix} C_1 & \cdots & C_n \end{pmatrix}$. Pour tout $i \in \{1, \ldots, n\}$, il existe des scalaires a_{ki} tels que

$$C_i = \sum_{k=1}^{n} a_{ki}\, e_k.$$

Par multilinéarité du déterminant, il vient

$$\det \begin{pmatrix} C_1 & \cdots & C_i & \cdots & C_n \end{pmatrix} = \sum_{k=1}^{n} a_{ki} \det \begin{pmatrix} C_1 & \cdots & e_k & \cdots & C_n \end{pmatrix}$$

et par le lemme précédent,

$$\det A = \sum_{k=1}^{n} a_{ki}\, \operatorname{cof}_{ki}(A).$$

Considérons à présent la seconde loi des mineurs. Supposons $i < j$. Si on remplace la j-ième colonne de A par un vecteur arbitraire $x = \sum_{k=1}^{n} x_k\, e_k$ de $\mathbb{K}^n$, de la première loi des mineurs, il découle que

$$\det\begin{pmatrix} C_1 & \cdots & C_i & \cdots & x & \cdots & C_n \end{pmatrix} = \sum_{k=1}^{n} x_k \operatorname{cof}_{kj}(A).$$

Si maintenant, $x = C_i$, il vient

$$0 = \det\begin{pmatrix} C_1 & \cdots & C_i & \cdots & C_i & \cdots & C_n \end{pmatrix} = \sum_{k=1}^{n} a_{ki} \operatorname{cof}_{kj}(A).$$

■

Proposition V.2.13 (Loi du produit). *Soient A et B, deux matrices carrées de dimension n. On a*

$$\det(AB) = \det A \det B.$$

Démonstration. Soit l'application

$$D : \mathbb{K}_n^n \to \mathbb{K} : A \mapsto \det(BA).$$

Si la matrice $A = \begin{pmatrix} C_1 & \cdots & C_n \end{pmatrix}$, alors $BA = \begin{pmatrix} BC_1 & \cdots & BC_n \end{pmatrix}$ et

$$D(A) = \det\begin{pmatrix} BC_1 & \cdots & BC_n \end{pmatrix}.$$

Dès lors, $D(A)$ est multilinéaire et alterné[3] sur les colonnes de A. Au vu de la proposition V.2.6, on a

$$D(A) = D(I)\det(A) = \det B \det A.$$

■

Remarque V.2.14. Notons qu'on peut démontrer un résultat plus général à propos du produit de matrices rectangulaires (et non pas seulement carrées). Le *théorème de Binet-Cauchy* s'énonce comme suit. Soient deux matrices rectangulaires

$$A = \begin{pmatrix} C_1 & \cdots & C_m \end{pmatrix} \in \mathbb{K}_m^n \text{ et } B = \begin{pmatrix} L'_1 \\ \vdots \\ L'_m \end{pmatrix} \in \mathbb{K}_n^m.$$

Alors,

$$\det(AB) = \begin{cases} 0 & \text{, si } n > m \\ \displaystyle\sum_{1 \le i_1 < \cdots < i_n \le m} \det\begin{pmatrix} C_{i_1} & \cdots & C_{i_n} \end{pmatrix} \det\begin{pmatrix} L'_{i_1} \\ \vdots \\ L'_{i_m} \end{pmatrix} & \text{, si } n \le m. \end{cases}$$

[3] C'est un bon exercice que de s'en convaincre.

3. Déterminant et indépendance linéaire

La vérification de la dépendance ou de l'indépendance linéaire de vecteurs de $\mathbb{K}^n$ peut se ramener à des calculs de déterminants. Plus précisément, nous avons les deux propositions suivantes[4].

Proposition V.3.1. *Soit $A = (a_{ij})$ une matrice carrée de dimension n. Les propositions suivantes sont équivalentes*

i) $\det A = 0$,
ii) *les colonnes de A sont linéairement dépendantes,*
iii) *les lignes de A sont linéairement dépendantes.*

Démonstration. En se rappelant que $\det \widetilde{A} = \det A$, il suffit de montrer que les propositions i) et ii) sont équivalentes.

Si les colonnes $C_1, \ldots, C_n$ de A sont linéairement dépendantes, l'une d'elles est combinaison linéaire des autres[5]. Vu la multilinéarité du déterminant, $\det A$ s'exprime comme une combinaison linéaire de déterminants dont deux colonnes sont identiques. Par conséquent, $\det A = 0$.

Supposons à présent que $\det A = 0$. Nous devons montrer que les colonnes $C_1, \ldots, C_n$ de A sont linéairement dépendantes. On procède par récurrence sur la dimension de A. Si $n = 1$, le résultat est exact. Supposons le résultat acquis pour les matrices de dimension $n-1$ et démontrons-le pour un déterminant de dimension n. Si la première colonne de A est nulle, alors le résultat est démontré. Sinon, un des éléments de cette colonne est non nul. Quitte à permuter les lignes de A, nous allons supposer que $a_{11} \neq 0$. Vu le corollaire V.2.5, on peut remplacer les colonnes C_j, $2 \leq j \leq n$, par $C_j - \frac{a_{1j}}{a_{11}} C_1$ sans modifier la valeur du déterminant. Ainsi, il vient

$$\det A = \det \left(\begin{array}{c|ccc} a_{11} & 0 & \cdots & 0 \\ \hline a_{21} & & & \\ \vdots & & \left(a_{ij} - \frac{a_{1j}}{a_{11}} a_{i1} \right)_{2 \leq i,j \leq n} & \\ a_{n1} & & & \end{array} \right).$$

[4]Voici un exemple d'application de la première proposition dans le cas où $\mathbb{K} = \mathbb{Z}_3$. Considérons les vecteurs

$$v_1 = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}, \; v_2 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}, \; v_3 = \begin{pmatrix} 2 \\ 2 \\ 2 \end{pmatrix}.$$

Ils sont linéairement dépendants car

$$\begin{vmatrix} 0 & 1 & 2 \\ 1 & 2 & 2 \\ 2 & 0 & 2 \end{vmatrix} \equiv 0 \pmod 3.$$

On aurait pu également le voir en remarquant $v_1 + 2v_2 - v_3 = 0$.

[5]En effet, il existe des scalaires $\lambda_1, \ldots, \lambda_n$ non tous nuls tels que $\lambda_1 C_1 + \cdots + \lambda_n C_n = 0$. Pour fixer les idées, supposons $\lambda_1 \neq 0$. Dès lors, $C_1 = -\frac{\lambda_2}{\lambda_1} C_2 - \cdots - \frac{\lambda_n}{\lambda_1} C_n$.

Puisque nous sommes en présence d'une matrice triangulaire composée, on a

$$0 = a_{11} \det \left(a_{ij} - \frac{a_{1j}}{a_{11}} a_{i1} \right)_{2 \leq i,j \leq n}.$$

Or, $a_{11} \neq 0$. En conséquence, c'est le déterminant de dimension $n-1$ qui est nul. Par hypothèse de récurrence, ses colonnes sont donc linéairement dépendantes. Il existe des scalaires $\lambda_2, \ldots, \lambda_n$ non tous nuls tels que

$$\sum_{j=2}^{n} \lambda_j \left(a_{ij} - \frac{a_{1j}}{a_{11}} a_{i1} \right) = 0, \quad \text{pour i} = 2, \ldots, n.$$

Cette relation est également valable si $i = 1$. Cela signifie que

$$\sum_{j=2}^{n} \lambda_j \left(C_j - \frac{a_{1j}}{a_{11}} C_1 \right) = 0.$$

Si on pose $\lambda_1 = -\sum_{j=2}^{n} \lambda_j \frac{a_{1j}}{a_{11}}$, alors on a

$$\sum_{j=1}^{n} \lambda_j C_j = 0$$

avec des λ_j non tous nuls et donc les colonnes de A sont linéairement dépendantes.

■

Proposition V.3.2. *Soient $x_1, \ldots, x_p$ des vecteurs de $\mathbb{K}^n$, $p \leq n$. Ces vecteurs sont linéairement dépendants si et seulement si tous les mineurs d'ordre p de la matrice $A = \begin{pmatrix} x_1 & \cdots & x_p \end{pmatrix}$ sont nuls. Auquel cas, si*

$$A = \begin{pmatrix} L_1 \\ \vdots \\ L_n \end{pmatrix}$$

alors, quels que soient $i_1, \ldots, i_p$ pris parmi $1, \ldots, n$, on a

$$\det \begin{pmatrix} L_{i_1} \\ \vdots \\ L_{i_p} \end{pmatrix} = 0.$$

Remarque V.3.3. En vertu du théorème de Steinitz, il est inutile dans la proposition précédente de considérer le cas $p > n$. De plus, si $p > n$, alors la matrice $A = \begin{pmatrix} x_1 & \cdots & x_p \end{pmatrix}$ est de dimension $n \times p$ et ne contient aucun mineur d'ordre p.

La preuve de ce résultat utilise des raisonnements de base concernant les systèmes d'équations linéaires. Plus précisément, elle fait appel aux propositions VI.2.1 et VI.2.4.

Démonstration. Si $x_1, \ldots, x_p$ sont linéairement dépendants, il existe $\lambda_1, \ldots, \lambda_p \in \mathbb{K}$ non tous nuls tels que

$$\sum_{i=1}^{p} \lambda_i x_i = 0.$$

Donc, pour tout $j \in \{1, \ldots, n\}$, on a

$(x_i)_j$ est la j-ième composante du vecteur $x_i \in \mathbb{K}^n$.

$$\sum_{i=1}^{p} \lambda_i (x_i)_j = 0. \tag{5}$$

Soit A' une sous-matrice de A de la forme

$$A' = A_{(i_1,\ldots,i_p;1,\ldots,p)}$$

avec $i_1, \ldots, i_p$ pris parmi $1, \ldots, n$. Vu la relation (5), une colonne de A' est combinaison linéaire des autres donc $\det A' = 0$. Ceci prouve que tous les mineurs d'ordre p de la matrice A sont nuls[6].

Pour la réciproque, procédons par l'absurde. Supposons que tous les mineurs d'ordre p de la matrice A sont nuls et que $x_1, \ldots, x_p$ sont linéairement indépendants . Le système homogène de n équations à p inconnues

Pour tout $i \in \{1, \ldots, p\}$, $x_i = \begin{pmatrix} x_{1i} \\ \vdots \\ x_{ni} \end{pmatrix}$

$$\begin{pmatrix} x_{11} & \cdots & x_{1p} \\ \vdots & & \vdots \\ x_{n1} & \cdots & x_{np} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_p \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

possède l'unique solution $\lambda_1 = \cdots = \lambda_p = 0$. Puisque les lignes de la matrice sont des éléments de $\mathbb{K}_p$, au plus p lignes de ce système sont linéairement indépendantes (c'est encore une conséquence du théorème de Steinitz). Pour simplifier l'écriture, supposons que ces lignes se trouvent parmi les p premières. Le système est donc équivalent[7] au système

$$\begin{pmatrix} x_{11} & \cdots & x_{1p} \\ \vdots & & \vdots \\ x_{p1} & \cdots & x_{pp} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_p \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Puisque ce système possède l'unique solution $\lambda_1 = \cdots = \lambda_p = 0$, la matrice du système possède un déterminant non nul[8]. Ceci contredit l'hypothèse que tous les mineurs d'ordre p sont nuls.

■

[6] Plus simplement, il suffit de remarquer que toute relation linéaire entre les colonnes de A a aussi lieu entre les colonnes correspondantes de toute sous-matrice A' obtenue en privilégiant certaines lignes de A.

[7] On utilise ici la proposition VI.2.1 adaptée au cas d'un système homogène.

[8] Ceci résulte de la proposition VI.2.4.

4. Rang d'une matrice

Proposition V.4.1. *Dans toute matrice $A \in \mathbb{K}_m^n$, le nombre de vecteurs lignes linéairement indépendants est égal au nombre de vecteurs colonnes linéairement indépendants. Ce nombre est encore égal au plus grand ordre des mineurs non nuls de cette matrice.*

Démonstration. Soient ℓ, le nombre de vecteurs lignes linéairement indépendants et c, le nombre de vecteurs colonnes linéairement indépendants. Soit r le plus grand entier tel qu'il existe des indices

$$1 \leq i_1 < \cdots < i_r \leq n \text{ et } 1 \leq j_1 < \cdots < j_r \leq m$$

tels que la sous-matrice carrée

$$A_{(i_1,\ldots,i_r;j_1,\ldots,j_r)}$$

soit de déterminant non nul. Au vu de la proposition V.3.1, les vecteurs

$$\begin{pmatrix} a_{i_1 j_1} \\ \vdots \\ a_{i_r j_1} \end{pmatrix}, \ldots, \begin{pmatrix} a_{i_1 j_r} \\ \vdots \\ a_{i_r j_r} \end{pmatrix}$$

sont linéairement indépendants. Par conséquent, les colonnes $C_{j_1}, \ldots, C_{j_r}$ de A sont aussi linéairement indépendantes. On procède de manière analogue pour trouver r lignes de A linéairement indépendantes. Ceci prouve que $r \leq c$ et $r \leq \ell$.

Pour conclure, il nous reste à montrer que si $C_{i_1}, \ldots, C_{i_k}$ sont k colonnes linéairement indépendantes, alors on peut trouver un mineur de A d'ordre k non nul. Cela résulte directement de la proposition V.3.2. Dès lors, $c \leq r$. Et de manière analogue, $\ell \leq r$. Donc $c = r = \ell$.

■

Définition V.4.2. Le nombre dont il est question dans la propriété précédente s'appelle le *rang* de la matrice A. On le note $\mathrm{rg}(A)$.

Exemple V.4.3. Par exemple,

$$\mathrm{rg}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = 1, \quad \mathrm{rg}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} = 2, \quad \mathrm{rg}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 3.$$

Voici les premières propriétés du rang d'une matrice

- $\mathrm{rg}(A) = \mathrm{rg}(\widetilde{A})$,
- si A est une matrice complexe, $\mathrm{rg}(A) = \mathrm{rg}(\overline{A}) = \mathrm{rg}(A^*)$,
- $\mathrm{rg}(0) = 0$, $\mathrm{rg}(I) = n$ si I est la matrice identité de dimension n,
- pour tout scalaire λ non nul, $\mathrm{rg}(\lambda A) = \mathrm{rg}(A)$,
- si $A \in \mathbb{K}_n^m$, alors $\mathrm{rg}(A) \leq \inf(m, n)$,
- si $A \in \mathbb{K}_n^n$, alors $\mathrm{rg}(A) = n$ si et seulement si $\det A \neq 0$,
- si $A, B \in \mathbb{K}_n^m$, alors $\mathrm{rg}(A + B) \leq \mathrm{rg}(A) + \mathrm{rg}(B)$,
- si $A \in \mathbb{K}_n^m$ et $B \in \mathbb{K}_\ell^n$, alors $\mathrm{rg}(AB) \leq \inf(\mathrm{rg}(A), \mathrm{rg}(B))$.

Ces propriétés sont pour la plupart évidentes. Intéressons-nous aux deux dernières.

Exemple V.4.4. Soient les matrices

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \text{ et } C = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Il est facile de voir que ces trois matrices sont toutes de rang 1 et que

$$\operatorname{rg}(A+B) = 2 = \operatorname{rg}(A) + \operatorname{rg}(B) \text{ mais } \operatorname{rg}(A+C) = 1 < \operatorname{rg}(A) + \operatorname{rg}(C).$$

Démontrons la dernière propriété. Si $B = \begin{pmatrix} C_1 & \cdots & C_n \end{pmatrix}$, alors $AB = \begin{pmatrix} AC_1 & \cdots & AC_n \end{pmatrix}$. De plus, toute relation linéaire ayant lieu entre des colonnes de B, a aussi lieu entre les colonnes de AB. En effet, si $\sum_i \lambda_i C_i = 0$, alors $\sum_i \lambda_i AC_i = 0$. Par conséquent, $\operatorname{rg}(AB) \leq \operatorname{rg}(B)$. Pour montrer que $\operatorname{rg}(AB) \leq \operatorname{rg}(A)$, il suffit de refaire le même raisonnement sur les lignes de A.

Exemple V.4.5. Soit A une matrice $m \times n$ réelle où $m \geq n$ telle que $\operatorname{rg}(A) = n$. Montrons que le rang de $\widetilde{A}A$ vaut encore n. C'est une application du théorème de Binet-Cauchy (cf. remarque V.2.14). Puisque $\widetilde{A} \in \mathbb{R}^n_m$ et $A \in \mathbb{R}^m_n$, alors

$$\det(\widetilde{A}A) = \sum_{1 \leq i_1 < \cdots < i_n \leq m} (\det \begin{pmatrix} L_{i_1} \\ \vdots \\ L_{i_n} \end{pmatrix})^2.$$

Puisque $\operatorname{rg}(A) = n$, au moins un des termes de la somme est strictement positif et $\det(\widetilde{A}A) > 0$.

Définition V.4.6. Soient A une matrice $m \times n$, S une sous-matrice $k \times k$ de A et T une sous-matrice $(k+1) \times (k+1)$ de A. On dit que T *borde* S si S est une sous-matrice de T.

Exemple V.4.7. Soient les matrices

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 4 \\ 9 & 12 \end{pmatrix} \text{ et } T = \begin{pmatrix} 1 & 3 & 4 \\ 9 & 11 & 12 \\ 13 & 15 & 16 \end{pmatrix}.$$

Ici, T borde S.

Proposition V.4.8 (Calcul du rang par matrices bordées). *Une matrice A est de rang r si et seulement si les deux assertions suivantes sont satisfaites*

i) *il existe une sous-matrice carrée S de A de dimension r telle que* $\det S \neq 0$,

ii) *toutes les sous-matrices carrées qui bordent S possèdent un déterminant nul.*

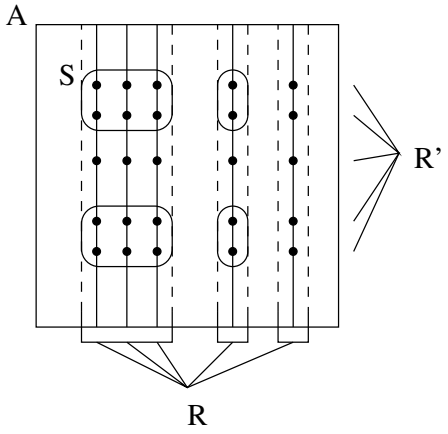


FIGURE V.3. Rang et matrices bordées.

Démonstration. Par définition même du rang, si $\mathrm{rg}(A) = r$, alors les conditions i) et ii) sont satisfaites.

Montrons la réciproque. Par la proposition V.3.1 et vu i), on obtient que $\mathrm{rg}(A) \geq r$ car les colonnes de A qui traversent S sont linéairement indépendantes. Il nous faut montrer que $\mathrm{rg}(A) = r$.

Supposons que $\mathrm{rg}(A) > r$. Dès lors, par la proposition V.4.1, il existe une colonne de A qui n'est pas combinaison linéaire des colonnes qui traversent S (en effet, si tel n'était pas le cas, on aurait dans A pas plus de r colonnes linéairement indépendantes[9]).

La matrice R constituée de ces $r+1$ colonnes de A est de rang $r+1$. Dans R, on peut donc trouver une ligne qui n'est pas combinaison linéaire des lignes de R qui traversent S (exactement le même raisonnement que précédemment, si ce n'était pas le cas, R serait de rang r). La sous-matrice R' de R formée par ces $r+1$ lignes est une matrice $(r+1) \times (r+1)$ qui borde S et de rang $r+1$. Ceci contredit ii) et donc $\mathrm{rg}(A) = r$.

■

Remarque V.4.9. Cette propriété permet d'éviter certains calculs. Par exemple, si on veut vérifier que la matrice

$$\begin{pmatrix} 1 & 2 & 3 & 1 \\ 2 & 1 & 3 & -1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 \end{pmatrix}$$

[9]On a déjà r colonnes linéairement indépendantes (celles qui traversent S), si quand on en ajoute une, les $r+1$ colonnes considérées sont linéairement dépendantes, c'est que la colonne ajoutée est combinaison linéaire des colonnes traversant S. Si c'est le cas pour toute colonne de A, alors A n'a pas plus de r colonnes linéairement indépendantes

est de rang 2, il suffit de voir que

$$\begin{vmatrix} 1 & 2 \\ 2 & 1 \end{vmatrix} \neq 0$$

et de calculer le déterminant des quatre matrices qui bordent cette sous-matrice :

$$\begin{vmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 0 & 1 & 1 \end{vmatrix} = 0, \quad \begin{vmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 1 & 0 & 1 \end{vmatrix} = 0, \quad \begin{vmatrix} 1 & 2 & 1 \\ 2 & 1 & -1 \\ 0 & 1 & 1 \end{vmatrix} = 0, \quad \begin{vmatrix} 1 & 2 & 1 \\ 2 & 1 & -1 \\ 1 & 0 & -1 \end{vmatrix} = 0.$$

Sans cette propriété, il aurait fallu calculer les 16 déterminants de dimension 3 et s'assurer qu'ils étaient tous nuls. Plus précisément, si A est une matrice $m \times n$ et si on a trouvé dans A un mineur d'ordre r non nul, il suffit pour que A soit de rang r de vérifier l'annulation de

$$(m-r)(n-r)$$

mineurs d'ordre $r+1$. Sans la proposition précédente, il aurait été nécessaire de vérifier l'annulation des

$$\mathrm{C}_m^{r+1}\,\mathrm{C}_n^{r+1}$$

mineurs d'ordre $r+1$ de A.

Par exemple, si $m = n = 25$, voici quelques valeurs

r	$(m-r)(n-r)$	$\mathrm{C}_m^{r+1}\,\mathrm{C}_n^{r+1}$
10	225	19868414760000
11	196	27043120090000
12	169	27043120090000
13	144	19868414760000
14	121	10684791937600
15	100	4173746850625
16	81	1169804480625
17	64	231072490000
18	49	31364410000
19	36	2822796900
20	25	160022500

5. Inversion de matrices

On voudrait pouvoir donner un sens à une notation comme A^{-1}.

Définition V.5.1. On appelle *inverse à gauche* (resp. *à droite*) de $A \in \mathbb{K}_n^m$ toute matrice $B \in \mathbb{K}_m^n$ telle que $BA = I$ (resp. $AB = I$). Dans ce cas, on dit que A est *inversible à gauche* (resp. *à droite*).

Par exemple, $\begin{pmatrix} 1 & 2 \end{pmatrix}$ et $\begin{pmatrix} 2 & 3 \end{pmatrix}$ sont deux inverses à gauche de $\begin{pmatrix} -1 \\ 1 \end{pmatrix}$ car

$$\begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} -1 \\ 1 \end{pmatrix} = (1) \quad \text{et} \quad \begin{pmatrix} 2 & 3 \end{pmatrix} \begin{pmatrix} -1 \\ 1 \end{pmatrix} = (1).$$

Cet exemple nous montre donc qu'une matrice peut avoir plus d'un inverse à gauche. Bien que les inverses à gauche et à droite puissent être étudiés en détail et possèdent de nombreuses applications, nous allons nous restreindre à un cas plus proche de la notion d'inverse rencontrée dans l'étude des champs.

Définition V.5.2. Si A est une matrice carrée et si il existe une matrice carrée B de même dimension telle que $AB = BA = I$, alors B est un *inverse bilatère* ou simplement *inverse* de A.

Remarque V.5.3. Soit A une matrice carrée. Si A possède B comme inverse à gauche et C comme inverse à droite alors $B = C$. En effet,

$$B = BI = B(AC) = (BA)C = IC = C.$$

Ainsi, si une matrice carrée possède un inverse à gauche et à droite, elle possède un inverse bilatère. De plus, tous ces inverses (à gauche, à droite et bilatère) sont égaux. Dans ce cas, on peut donc donner un sens à la notation A^{-1}.

Remarque V.5.4. Soit A une matrice carrée. Si A possède B comme inverse à gauche, on a

$$BA = I \quad \text{donc} \ \det(BA) = \det B \det A = \det I = 1$$

et par conséquent, $\det A$ ne peut s'annuler. De façon analogue, si A possède un inverse à droite, alors $\det A \neq 0$.

Remarque V.5.5. Réciproquement, si $\det A \neq 0$, il résulte de la forme matricielle de la loi des mineurs que A possède un inverse bilatère

$$A \left(\frac{1}{\det(A)} \widetilde{\operatorname{cof}(A)} \right) = \left(\frac{1}{\det(A)} \widetilde{\operatorname{cof}(A)} \right) A = I$$

et

$$\boxed{A^{-1} = \frac{1}{\det A} \widetilde{\operatorname{cof}(A)}.} \tag{6}$$

La proposition suivante résulte immédiatement des trois remarques précédentes.

Proposition V.5.6. *Soit A une matrice carrée. Les propositions suivantes sont équivalentes*

- $\det A \neq 0$,
- *A possède un inverse à gauche,*
- *A possède un inverse à droite,*
- *A possède un inverse bilatère.*

Lorsque ces conditions sont réalisées, tous les inverses de A sont égaux à l'inverse donné en (6).

Définition V.5.7. Si A est une matrice carrée telle que $\det A \neq 0$, alors on dit que A est *inversible*[10]. Sinon, A est *non-inversible* ou *singulière*. L'ensemble des matrices inversibles de dimension n à coefficients dans $\mathbb{K}$ se note $\mathrm{GL}_n(\mathbb{K})$.

Remarque V.5.8. Il résulte de la loi du produit (cf. proposition V.2.13) que si A est inversible, alors

$$\det A^{-1} = \frac{1}{\det A}.$$

Par conséquent, l'inverse d'une matrice inversible est toujours inversible[11] et

$$(A^{-1})^{-1} = A$$

car $(A^{-1})^{-1}A^{-1} = I = AA^{-1}$ et l'inverse est unique.

- Les matrices A et $\widetilde{A}$ sont simultanément inversibles et
$$(\tilde{A})^{-1} = \widetilde{A^{-1}}.$$
En effet, $\det(A) = \det(\tilde{A})$ et donc ces déterminants sont simultanément nuls ou non nuls. De plus, on a
$$(\tilde{A})^{-1}\tilde{A} = I = \widetilde{AA^{-1}} = \widetilde{A^{-1}}\tilde{A}.$$
- Si A est une matrice complexe, A, $\overline{A}$ et A^* sont simultanément inversibles et
$$(\overline{A})^{-1} = \overline{A^{-1}}, \quad (A^*)^{-1} = (A^{-1})^*.$$
Les justifications sont analogues aux précédentes.
- Si λ est un scalaire non nul et si A est inversible, alors λA est inversible et
$$(\lambda A)^{-1} = \frac{1}{\lambda}A^{-1}.$$
- Si A et B sont des matrices carrées et inversibles de même dimension, alors AB est inversible et
$$(AB)^{-1} = B^{-1}A^{-1}.$$
En effet,
$$(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}B = I.$$
- Une matrice diagonale est inversible si et seulement si ses éléments diagonaux sont non nuls et
$$\mathrm{diag}\,(\lambda_1, \ldots, \lambda_n)^{-1} = \mathrm{diag}\,(1/\lambda_1, \ldots, 1/\lambda_n).$$

[10] Certains auteurs emploient parfois le terme *invertible*.

[11] On note $GL_n(\mathbb{K})$ l'ensemble des matrices carrées inversibles de dimension n. Il s'agit d'un groupe pour l'opération de multiplication.

Plus généralement, si $A_1, \ldots, A_p$ sont des matrices carrées, la matrice composée diagonale $\operatorname{diag}(A_1, \ldots, A_p)$ est inversible si et seulement si les matrices A_i sont inversibles et

$$\operatorname{diag}(A_1, \ldots, A_p)^{-1} = \operatorname{diag}(A_1^{-1}, \ldots, A_p^{-1}).$$

Proposition V.5.9. *Soit A une matrice inversible de dimension n. Des vecteurs $x_1, \ldots, x_p$ de $\mathbb{K}^n$ sont linéairement indépendants si et seulement si les vecteurs $Ax_1, \ldots, Ax_p$ le sont.*

Démonstration. Si $x_1, \ldots, x_p$ sont linéairement dépendants, alors il existe des scalaires $\lambda_1, \ldots, \lambda_p$ non tous nuls tels que

$$\sum_{i=1}^{p} \lambda_i x_i = 0.$$

En multipliant par la matrice A, on trouve

$$\sum_{i=1}^{p} \lambda_i A x_i = 0$$

et les vecteurs $Ax_1, \ldots, Ax_p$ sont donc linéairement dépendants.

Réciproquement, si $Ax_1, \ldots, Ax_p$ sont linéairement dépendants, en multipliant par A^{-1}, on voit que $x_1, \ldots, x_p$ sont aussi linéairement dépendants.

■

Proposition V.5.10. *Si $B \in \mathbb{K}_n^n$ et $C \in \mathbb{K}_m^m$ sont des matrices inversibles et si $A \in \mathbb{K}_m^n$, alors*

$$\operatorname{rg}(BA) = \operatorname{rg}(A) = \operatorname{rg}(AC).$$

Démonstration. Pour rappel, si le produit matriciel XY est défini, alors $\operatorname{rg}(XY) \leq \inf(\operatorname{rg}(X), \operatorname{rg}(Y))$. Ainsi, il vient

$$\operatorname{rg}(BA) \leq \operatorname{rg}(A) = \operatorname{rg}(B^{-1}BA) \leq \operatorname{rg}(BA)$$

et de la même manière, $\operatorname{rg}(AC) \leq \operatorname{rg}(A) = \operatorname{rg}(ACC^{-1}) \leq \operatorname{rg}(AC)$.

■

Voici une preuve alternative basée sur le résultat précédent.

Démonstration. Si $A = \begin{pmatrix} C_1 & \cdots & C_m \end{pmatrix}$, alors $BA = \begin{pmatrix} BC_1 & \cdots & BC_m \end{pmatrix}$. Dès lors, les nombres de colonnes linéairement indépendantes dans A et dans BA coïncident car B est inversible.

■

Le calcul du déterminant et de l'inverse d'une matrice est souvent facilité par une décomposition préalable de la matrice en quatre blocs.

Proposition V.5.11 (Formules de Frobenius-Schur). *Soit*

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

une matrice composée dont les blocs diagonaux A et D sont carrés. On a

$$\boxed{\det(M) = \begin{cases} \det A \det(D - CA^{-1}B) & \textit{si } \det(A) \neq 0 \\ \det(A - BD^{-1}C) \det D & \textit{si } \det(D) \neq 0 \end{cases}}$$

Démonstration. Ces formules découlent immédiatement des identités matricielles suivantes,

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & 0 \\ C & I \end{pmatrix} \begin{pmatrix} I & A^{-1}B \\ 0 & D - CA^{-1}B \end{pmatrix} = \begin{pmatrix} I & B \\ 0 & D \end{pmatrix} \begin{pmatrix} A - BD^{-1}C & 0 \\ D^{-1}C & I \end{pmatrix}.$$

■

Corollaire V.5.12. *Soit*

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

une matrice composée dont les blocs diagonaux A et D sont carrés et de même dimension. On a

$$\det(M) = \begin{cases} \det(AD - CB) & \textit{si } A \textit{ et } C \textit{ commutent}, \\ \det(DA - CB) & \textit{si } A \textit{ et } B \textit{ commutent}, \\ \det(AD - BC) & \textit{si } D \textit{ et } C \textit{ commutent}, \\ \det(DA - BC) & \textit{si } D \textit{ et } B \textit{ commutent}. \end{cases}$$

Démonstration. Démontrons la première formule. Les autres se démontrent de manière analogue. Si $\det A \neq 0$, on a

$$\det M = \det A \det(D - CA^{-1}B).$$

Par conséquent, si A et C commutent,

$$\det M = \det(AD - ACA^{-1}B) = \det(AD - CAA^{-1}B) = \det(AD - CB).$$

Considérons à présent le cas général. Soit le polynôme

$$P : \lambda \mapsto \det(A - \lambda I).$$

Par définition du déterminant, c'est un polynôme de degré n en λ. Par conséquent, $P(\lambda)$ possède un nombre fini de racines $\lambda_1, \ldots, \lambda_p$, $p \leq n$. Ainsi, $A - \lambda I$ est inversible pour tout $\lambda \neq \lambda_j$. En appliquant la propriété précédente, il vient

$$\det \begin{pmatrix} A - \lambda I & B \\ C & D \end{pmatrix} = \det \big((A - \lambda I)D - CB \big),$$

pour une infinité[12] de valeurs de λ. Les deux membres sont des polynômes de degré n en λ qui prennent la même valeur en une infinité de points donc en particulier en $n + 1$ points. De là, les deux polynômes prennent la même valeur pour tout $\lambda \in \mathbb{K}$ donc en particulier pour $\lambda = 0$. Ce qui conclut la preuve.

Nous utilisons déjà un résultat sur les polynômes, cf. corollaire VIII.3.6...

[12]Nous supposons implicitement que $\mathbb{K}$ est un champ infini. En effet, si $\mathbb{K}$ ne contient que k éléments et que l'égalité entre les polynômes de degré n en λ a lieu en $k - p$ points (à savoir en $\mathbb{K} \setminus \{\lambda_1, \ldots, \lambda_p\}$), rien n'assure que $k - p \geq n + 1$. De là, on ne pourrait donc pas conclure que les polynômes sont égaux.

■

Exemple V.5.13. Soient A et B deux matrices carrées complexes de même dimension. Il vient

$$\det\begin{pmatrix} A & -B \\ B & A \end{pmatrix} = \det\begin{pmatrix} A+iB & -B \\ -i(A+iB) & A \end{pmatrix}$$

car on a ajouté à la première grosse colonne, la seconde grosse colonne multipliée par $-i$. Les blocs $A+iB$ et $-i(A+iB)$ commutent. Par le corollaire précédent, il s'ensuit que

$$\begin{aligned} \det\begin{pmatrix} A & -B \\ B & A \end{pmatrix} &= \det((A+iB)A - i(A+iB)B) \\ &= \det((A+iB)(A-iB)) = \det(A+iB)\det(A-iB). \end{aligned}$$

6. Une application

Nous présentons ici le modèle économique d'*analyse input-output* de W. Leontief. On peut noter que ce modèle sert de base à d'autres modèles plus récents et plus évolués.

Nous supposons que l'économie d'une nation est divisée en n secteurs s_i et $x \in \mathbb{R}^n$ est un vecteur dénotant la *production* des différents secteurs en un an. L'économie du pays contient aussi un secteur supplémentaire ne produisant aucun bien ni service (par exemple, la demande du consommateur). Ce secteur ne fait que consommer une partie de la production des différents secteurs s_i. On note $d \in \mathbb{R}^n$ le vecteur représentant la *demande finale* du consommateur.

Les différents secteurs produisent des biens pour assurer la demande finale du consommateur mais, pour assurer cette production, ils ont eux-même besoin de biens produits par les autres secteurs ou par leur propre secteur. L'hypothèse de base du modèle de Leontief est que pour chaque secteur s_i, on dispose d'un vecteur $S_i \in \mathbb{R}^n$ tel que la j-ième composante $(S_i)_j$ de ce vecteur colonne représente la production du secteur s_j nécessaire au secteur s_i pour produire une unité. On notera $(S_i)_j$ simplement s_{ji}.

Exemple V.6.1. Supposons que l'économie (simpliste) d'un pays se divise en trois secteurs : s_1 industrie, s_2 agriculture, s_3 services. On a les demandes suivantes

	S_1	S_2	S_3
s_1 :	0,5	0,4	0,2
s_2 :	0,2	0,3	0,1
s_3 :	0,1	0,1	0,3

Si le secteur s_1 veut produire 100 unités, il a besoin au préalable de 50 (resp. 20, 10) unités du secteur s_1 (resp. s_2, s_3). La matrice

$$S = \begin{pmatrix} S_1 & \cdots & S_n \end{pmatrix}$$

représentée ci-dessus est souvent appelée la *matrice technologique*.

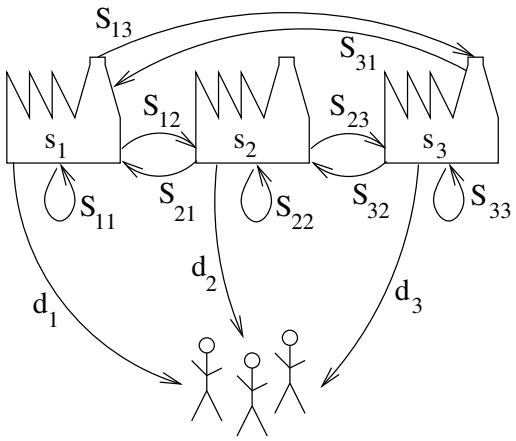


FIGURE V.4. Le modèle d'analyse input-output.

Ainsi, si le secteur s_i veut produire x_i unités, il a besoin de $s_{ji}x_i$ unités du secteur s_j.

La production totale x_i du secteur s_i doit tenir compte des demandes des différents secteurs (y compris s_i) ainsi que de la demande finale du consommateur d_i. Pour satisfaire le secteur s_j, le secteur s_i doit lui fournir $s_{ij}x_j$.

Avec nos notations, on a

$$x_i = \sum_{j=1}^{n} s_{ij}x_j + d_i$$

et sous forme matricielle,

$$x = Sx + d.$$

Il s'ensuit que

$$(I - S)x = d.$$

Si $I - S$ est inversible, alors on peut résoudre facilement le problème d'analyse input-output et trouver le vecteur x.

Exemple V.6.2. En continuant notre exemple numérique, supposons que le vecteur des demandes finales est

$$d = \begin{pmatrix} 10 \\ 20 \\ 15 \end{pmatrix}$$

alors

$$x = \begin{pmatrix} 0,5 & -0,4 & -0,2 \\ -0,2 & 0,7 & -0,1 \\ -0,1 & -0,1 & 0,7 \end{pmatrix}^{-1} \begin{pmatrix} 10 \\ 20 \\ 15 \end{pmatrix} = \left[\frac{1}{10} \begin{pmatrix} 5 & -4 & -2 \\ -2 & 7 & -1 \\ -1 & -1 & 7 \end{pmatrix} \right]^{-1} \begin{pmatrix} 10 \\ 20 \\ 15 \end{pmatrix}$$

et donc

$$x = \frac{25}{3}\begin{pmatrix}10\\7\\5\end{pmatrix}.$$

On voit que connaissant la matrice $(I-S)^{-1}$, on trouve immédiatement une nouvelle valeur pour x lorsqu'on fait varier d.

Remarque V.6.3. Cet exemple n'étant destiné qu'à illustrer le calcul d'inverses, nous nous arrêtons ici. On pourrait aller plus loin[13] en déterminant par exemple sous quelles conditions $I-S$ est inversible, ou encore donner une formule pratique du calcul de l'inverse quand la dimension de la matrice devient grande. On pourrait encore rechercher l'interprétation économique des entrées de la matrice $(I-S)^{-1}$.

[13] voir par exemple, D. C. Lay, *linear algebra and its application*, Addison-Wesley 1993.

CHAPITRE VI

Systèmes d'équations

1. Définitions

Dans ce chapitre, p est un entier supérieur ou égal à 2, n est un entier positif.

Définition VI.1.1. Un *système d'équations linéaires* à n équations et p inconnues est un système de la forme

$$(\mathbf{S}) \begin{cases} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1p}x_p & = & b_1 \\ \vdots & & & & & & \vdots & & \vdots \\ a_{n1}x_1 & + & a_{n2}x_2 & + & \cdots & + & a_{np}x_p & = & b_n \end{cases}.$$

Ce système peut encore se mettre sous forme matricielle

$$\begin{pmatrix} a_{11} & \cdots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{np} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}.$$

On dit que $A = (a_{ij}) \in \mathbb{K}_p^n$ est la *matrice du système*, $x = (x_i) \in \mathbb{K}^p$ est le vecteur des *inconnues* et $b = (b_i) \in \mathbb{K}^n$ est le *second membre* du système. Les matrices A et b sont supposées connues. Ainsi, on dénote encore le système $(\mathbf{S})$ sous la forme

$$Ax = b.$$

Tout vecteur x qui vérifie $Ax = b$ est dit *solution* du système. Cela signifie que x doit satisfaire simultanément les n équations.

Si on désigne les colonnes de A par $C_1, \ldots, C_p$, le système $(\mathbf{S})$ peut encore se mettre sous la forme vectorielle,

$$\sum_{j=1}^{n} x_j \, C_j = b.$$

Définition VI.1.2. Un système de la forme $Ax = b$ tel que $b = 0$ est dit *homogène*. Un système est *compatible* s'il possède au moins une solution. Sinon, il est dit *incompatible*. Par exemple, un système homogène est toujours compatible puisqu'il possède toujours la solution $x = 0$.

Soit $Ax = b$, un système $(\mathbf{S})$. Le système obtenu en remplaçant le second membre b par 0 est appelé le *système homogène associé* à $(\mathbf{S})$.

Si un système possède une et une seule solution, il est dit *déterminé*. S'il possède plus d'une solution, il est dit *indéterminé* .

Enfin, deux systèmes sont *équivalents* s'ils possèdent les mêmes solutions.

Si $A = (a_{ij}) \in \mathbb{K}_p^n$ et $B = (b_{ij}) \in \mathbb{K}_q^n$, alors on note $(A|B)$ la matrice $n \times (p+q)$ obtenue en juxtaposant A et B, i.e.,

$$\begin{pmatrix} a_{11} & \cdots & a_{1p} & b_{11} & \cdots & b_{1q} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{np} & b_{n1} & \cdots & b_{nq} \end{pmatrix}.$$

2. Premières propriétés

Cette première propriété[1] assez élémentaire sera revue en détail à la section suivante.

Proposition VI.2.1. *Soient $A \in \mathbb{K}_p^k$ une matrice donnée par ses lignes*

$$A = \begin{pmatrix} L_1 \\ \vdots \\ L_k \end{pmatrix} \quad \text{et} \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} \in \mathbb{K}^k$$

tels que le système **(S)** *: $Ax = b$ soit compatible.*

Si les vecteurs $(L_{k+1}|b_{k+1}), \ldots, (L_n|b_n) \in \mathbb{K}_{p+1}$ sont combinaisons linéaires de $(L_1|b_1), \ldots, (L_k|b_k)$, alors le système $Ax = b$ est équivalent au système **(S')** *:*

$$\begin{pmatrix} L_1 \\ \vdots \\ L_k \\ L_{k+1} \\ \vdots \\ L_n \end{pmatrix} x = \begin{pmatrix} b_1 \\ \vdots \\ b_k \\ b_{k+1} \\ \vdots \\ b_n \end{pmatrix}.$$

Démonstration. Il est clair que toute solution de **(S')** est aussi solution de **(S)** puisque dans **(S)**, elle doit uniquement satisfaire certaines équations de **(S')**.

Soit $x = (x_1, \ldots, x_p)^\sim$ une solution du système **(S)** : $Ax = b$. Par hypothèse, pour tout $j = k+1, \ldots, n$, il existe $\alpha_{j,1}, \ldots, \alpha_{j,k} \in \mathbb{K}$ tels que

$$L_j = \sum_{\ell=1}^{k} \alpha_{j,\ell}\, L_\ell \quad \text{et} \quad b_j = \sum_{\ell=1}^{k} \alpha_{j,\ell}\, b_\ell.$$

Par conséquent, pour tout $j = k+1, \ldots, n$, on a

$$L_j = \sum_{\ell=1}^{k} \alpha_{j,\ell}\, L_\ell\, x = \sum_{\ell=1}^{k} \alpha_{j,\ell}\, b_\ell = b_j$$

et x est encore solution du système **(S')**.

■

[1] Les propositions de cette section, relatives aux systèmes linéaires, sont les seules à être utilisées dans la preuve de la proposition V.3.2. Remarquer qu'on y fait nullement référence à la notion rang.

Exemple VI.2.2. Considérons le système

$$\begin{cases} x+y+z &= 1 \\ x-2y+3z &= 2 \end{cases}.$$

Ce système est équivalent au système suivant, où la troisième ligne est la somme des deux premières,

$$\begin{cases} x+y+z &= 1 \\ x-2y+3z &= 2 \\ 2x-y+4z &= 3 \end{cases}.$$

Proposition VI.2.3. *Si $A \in \mathbb{K}_n^n$ est inversible, le système $Ax = b$ possède l'unique solution $A^{-1}b$.*

Démonstration. Tout d'abord, $A^{-1}b$ est bien solution du système car

$$A(A^{-1}b) = (AA^{-1})b = Ib = b.$$

De plus, si x est une solution, il vérifie $Ax = b$ et alors en mutlipliant les deux membres par A^{-1}, on trouve $x = A^{-1}b$.

■

Proposition VI.2.4. *Soit $A \in \mathbb{K}_n^n$. Le système homogène $Ax = 0$ possède l'unique solution $x = 0$ si et seulement si A est inversible.*

Démonstration. Si A est inversible, par la proposition précédente, le système possède l'unique solution $A^{-1}0 = 0$.

Si A n'est pas inversible, son déterminant est nul et les colonnes de A sont linéairement dépendantes (cf. proposition V.3.1). Il existe donc des coefficients non tous nuls $x_1, \ldots, x_n$ tels que

$$\sum_{i=1}^{n} x_i \, C_i = 0.$$

Ainsi, $(x_1, \ldots, x_n)$ est une solution non nulle du système homogène.

■

3. Structure des solutions et compatibilité

La proposition suivante donne la structure des solutions d'un système d'équations. On obtient toutes les solutions[2] d'un système (**S**) en ajoutant à une solution particulière x_0 de (**S**), les solutions du système homogène associé à (**S**).

Proposition VI.3.1. *Soit $A \in \mathbb{K}_p^n$. Si x_0 vérifie $Ax_0 = b$, alors les solutions du système $Ax = b$ sont de la forme*

$$x_0 + y$$

où y vérifie $Ay = 0$.

[2]L'ensemble des solutions d'un système homogène est un sous-espace vectoriel de $\mathbb{K}^p$. Par conséquent, l'ensemble des solutions d'un système est une variété affine.

Démonstration. Si $Ax_0 = b$ et $Ay = 0$, alors il est clair que $A(x_0 + y) = b$ et donc $x_0 + y$ est solution du système.

Soit x une solution du système $Ax = b$. Vérifions qu'elle a la forme prescrite. Si x_0 est aussi solution, alors $x - x_0$ vérifie $A(x - x_0) = Ax - Ax_0 = b - b = 0$ et

$$x = x_0 + (x - x_0).$$

■

Définition VI.3.2. On appelle *rang du système* $Ax = b$, le rang de la matrice A.

La propriété suivante a un intérêt double. Elle s'avère utile dans des argumentationss théoriques mais aussi, très souvent, dans les discussions de systèmes apparaissant dans l'étude de lieux géométriques. En effet, par la méthode des génératrices, l'élimination des paramètres revient souvent à exprimer la compatibilité d'un système.

Proposition VI.3.3 (Rouché). *Soient $A \in \mathbb{K}_p^n$ et $b \in \mathbb{K}^n$. Les conditions suivantes sont équivalentes.*

i) *Le système* $(\mathbf{S})$ *: $Ax = b$ est compatible,*
ii) *tout vecteur $y \in \mathbb{K}_n$ satisfaisant $yA = 0$ est tel que $yb = 0$,*
iii) *le rang de A est égal au rang de $(A|b)$.*

Remarque VI.3.4. On appelle parfois $(A|b)$ la *matrice augmentée* de $(\mathbf{S})$. La condition ii) montre que toute relation linéaire ayant lieu entre les lignes de A doit aussi avoir lieu entre les éléments correspondants du second membre b.

Démonstration. i) implique ii). Si x_0 est une solution de $(\mathbf{S})$ et si $yA = 0$, alors en multipliant à droite par x_0, il vient

$$yAx_0 = yb = 0.$$

ii) implique iii). La condition ii) signifie que toute relation linéaire ayant lieu entre les lignes de A a aussi lieu entre les lignes de la matrice augmentée $(A|b)$. Ainsi, le nombre de lignes linéairement indépendantes dans A est égal au nombre de lignes linéairement indépendantes dans $(A|b)$. Ceci signifie que $\mathrm{rg}(A) = \mathrm{rg}(A|b)$.

iii) implique i). Soit r le rang de A. La matrice A possède donc r colonnes linéairement indépendantes : $C_{i_1}, \ldots, C_{i_r}$. Les vecteurs $C_{i_1}, \ldots, C_{i_r}, b$ sont linéairement dépendants car par hypothèse, $\mathrm{rg}(A|b) = r$. En d'autres termes, b est combinaison linéaire de $C_{i_1}, \ldots, C_{i_r}$ donc de $C_1, \ldots, C_p$. Ainsi, il existe $x_1, \ldots, x_p$ tels que

$$\sum_{j=1}^{p} x_j C_j = b$$

et le système $(\mathbf{S})$ possède une solution.

■

Exprimer les conditions nécessaire et suffisante sous lesquelles un système $Ax = b$ est compatible s'appelle l'*élimination* de x dans le système. L'expression de ces conditions revient donc à égaler le rang de A avec celui de $(A|b)$.

Exemple VI.3.5. Si on considère le système

$$\begin{cases} x + y - 2z = 1 \\ 2x + y + z = 3 \\ 3x + 2y - z = 4 \end{cases}$$

Il est clair que l'on peut par exemple supprimer la troisième équation et conserver un système équivalent car, cette dernière équation s'obtenant comme combinaison linéaire des deux précédentes, elle n'apporte aucune contrainte supplémentaire sur les solutions. On obtient ainsi le système équivalent

$$\begin{cases} x + y - 2z = 1 \\ 2x + y + z = 3 \end{cases}$$

Peut-on continuer de la sorte et supprimer, par exemple, la seconde équation ? La réponse est non car, par exemple, $x = 1$, $y = z = 0$ satisfait la première équation mais pas la seconde. Ainsi, l'ensemble des solutions du système ci-dessus est un sous-ensemble strict des solutions du système réduit à une seule équation $x + y - 2z = 1$. En fait, on conserve deux équations "indépendantes" (i.e., correspondant à des lignes linéairement indépendantes dans la matrice du système) car c'est exactement la valeur du rang du système.

Cette constatation est en fait générale et est traduite par le résultat suivant.

Corollaire VI.3.6. *Si le système* $(\mathbf{S})$ *:* $Ax = b$ *est compatible, il est équivalent à tout système* $(\mathbf{S}')$ *obtenu en ne considérant que les lignes de la matrice* A *qui sont linéairement indépendantes et en nombre égal au rang de* A*.*

Démonstration. Toute solution de $(\mathbf{S})$ est solution de $(\mathbf{S}')$ puisque dans $(\mathbf{S}')$, elle doit satisfaire uniquement certaines équations de $(\mathbf{S})$.

Montrons à présent que toute solution de $(\mathbf{S}')$ est solution de $(\mathbf{S})$. Par construction de $(\mathbf{S}')$, toute ligne L_i de A est combinaison linéaire des $r = \mathrm{rg}(A)$ lignes de la matrice de $(\mathbf{S}')$. Ces lignes sont des lignes de A et quitte à permuter les équations de $(\mathbf{S})$, on peut supposer qu'il s'agit des r premières : $L_1, \ldots, L_r$. Autrement dit, pour tout $i \in \{1, \ldots, n\}$, il existe des scalaires $\lambda_k^{(i)}$ tels que

$$L_i = \sum_{k=1}^{r} \lambda_k^{(i)} L_k.$$

Puisque le système $(\mathbf{S})$ est compatible, en vertu de la proposition précédente, ces relations ont aussi lieu entre les composantes de b,

$$b_i = \sum_{k=1}^{r} \lambda_k^{(i)} b_k.$$

Soit x, une solution de $(\mathbf{S}')$. Cela signifie que pour tout $k \in \{1, \dots, r\}$, $L_k x = b_k$. Ainsi, pour tout $i \in \{1, \dots, n\}$, on a

$$L_i x = \sum_{k=1}^{r} \lambda_k^{(i)} L_k x = \sum_{k=1}^{r} \lambda_k^{(i)} b_k = b_i.$$

Donc x est aussi solution de $(\mathbf{S})$.

■

Remarque VI.3.7. Si $A \in \mathbb{K}_p^n$, on sait que $\mathrm{rg}(A) \leq p$. Ainsi, si le système $Ax = b$ est compatible, alors il est équivalent à un système contenant un nombre n d'équations inférieur ou égal au nombre p d'inconnues.

4. Résolution

Considérons un système compatible $(\mathbf{S})$: $Ax = b$. Dans la section précédente, nous avons montré que nous pouvions uniquement considérer les lignes de A linéairement indépendantes et en nombre égal au rang. Supposons être dans une telle situation, i.e., $A \in \mathbb{K}_p^n$ et $\mathrm{rg}(A) = n \leq p$. La matrice A possède donc n colonnes linéairement indépendantes. En toute généralité, supposons que ces colonnes sont les n premières colonnes $C_1, \dots, C_n$ de A. Ainsi, vu la forme vectorielle sous laquelle peut être mis $(\mathbf{S})$, on a

$$\begin{pmatrix} C_1 & \cdots & C_n \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = b - x_{n+1} C_{n+1} - \cdots - x_p C_p$$

où on n'a conservé dans le premier membre que les inconnues correspondant aux n colonnes linéairement indépendantes. La matrice $C = \begin{pmatrix} C_1 & \cdots & C_n \end{pmatrix}$ est donc inversible. En multipliant par son inverse C^{-1}, on s'aperçoit que le système $(\mathbf{S})$ est équivalent à

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = C^{-1} b - x_{n+1} C^{-1} C_{n+1} - \cdots - x_p C^{-1} C_p.$$

On remarque qu'il n'y a aucune contrainte sur les valeurs de $x_{n+1}, \dots, x_p$. Ainsi, toute solution de $(\mathbf{S})$ peut s'écrire

$$(7) \quad \left(\begin{array}{c} x_1 \\ \vdots \\ x_n \\ \hline x_{n+1} \\ \vdots \\ \vdots \\ x_p \end{array}\right) = \left(\begin{array}{c} C^{-1}b \\ \hline 0 \\ \vdots \\ \vdots \\ 0 \end{array}\right) + \lambda_1 \left(\begin{array}{c} -C^{-1}C_{n+1} \\ \hline 1 \\ 0 \\ \vdots \\ 0 \end{array}\right) + \cdots + \lambda_{p-n} \left(\begin{array}{c} -C^{-1}C_p \\ \hline 0 \\ \vdots \\ 0 \\ 1 \end{array}\right)$$

avec $\lambda_1, \dots, \lambda_{p-n} \in \mathbb{K}$. Inversement, il est clair que tout vecteur qui s'écrit de cette façon est solution de $(\mathbf{S})$.

Remarque VI.4.1. Nous pouvons faire les observations suivantes.

- Si on pose $\lambda_1 = \cdots = \lambda_{p-n} = 0$, alors on trouve une solution particulière du système.
- Si on pose $b = 0$, c'est-à-dire si on considère le système homogène associé, on voit que les solutions de ce dernier système sont les combinaisons linéaires de $p - \mathrm{rg}(A)$ vecteurs linéairement indépendants[3].
- On retrouve (cf. proposition VI.3.1) le fait que les solutions d'un système linéaire compatible s'obtiennent en ajoutant à une solution particulière les solutions du système homogène associé.

Considérons, pour conclure, le cas des systèmes de Cramer.

Définition VI.4.2. Un système $(\mathbf{S}) : Ax = b$ d'équations linéaires est dit *de Cramer*, si A est une matrice carrée inversible.

En vertu de la proposition VI.2.3, si $(\mathbf{S})$ est de Cramer, il possède l'unique solution $x = A^{-1}b$.

Il vient,

$$x_j = (A^{-1}b)_j = \frac{1}{\det A}\left(\widetilde{\mathrm{cof}(A)}b\right)_j$$

Or, on a

$$(\widetilde{\mathrm{cof}(A)}b)_j = \sum_{k=1}^{p}\left(\widetilde{\mathrm{cof}(A)}\right)_{jk} b_k = \sum_{k=1}^{p}\mathrm{cof}_{kj}(A)b_k.$$

En se rappelant le lemme V.2.11, on obtient $\mathrm{cof}(A)_{kj}$ en remplaçant la j-ième colonne de A par e_k. Ainsi,

$$x_j = \frac{1}{\det A}\sum_{k=1}^{p} b_k \det\begin{pmatrix} C_1 & \cdots & e_k & \cdots & C_p\end{pmatrix} = \frac{\det\begin{pmatrix} C_1 & \cdots & b & \cdots & C_p\end{pmatrix}}{\det A}$$

où on a utilisé la multilinéarité du déterminant par rapport aux colonnes. En résumé, x_j est le quotient du déterminant de la matrice A du système où on a remplacé la j-ième colonne par le second membre b, par le déterminant de A. Ces formules sont appelées les *formules de G. Cramer*.

5. Quelques exemples

Exemple VI.5.1. Considérons le système homogène

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

[3]Les solutions du système homogène $Ax = 0$ à p inconnues est un sous-espace vectoriel de dimension $p - \mathrm{rg}(A)$. En effet, il s'agit de l'enveloppe linéaire de $p - \mathrm{rg}(A)$ vecteurs linéairement indépendants.

Il est facile de voir que ce système est de rang 2, on peut donc conserver deux lignes linéairement indépendantes et obtenir un système équivalent. Sous forme vectorielle, on a

$$\begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = -z \begin{pmatrix} 1 \\ 2 \end{pmatrix}.$$

Puisque

$$\begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 5/3 \\ -1/3 \end{pmatrix},$$

il vient

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \lambda \begin{pmatrix} -5/3 \\ 1/3 \\ 1 \end{pmatrix}, \quad \lambda \in \mathbb{K}.$$

Exemple VI.5.2. Reprenons le système de l'exemple VI.3.5.

$$\begin{cases} x + y - 2z = 1 \\ 2x + y + z = 3 \end{cases}$$

Il vient

$$\begin{cases} x + y = 1 + 2z \\ 2x + y = 3 - z \end{cases}$$

et

$$\begin{cases} x = 2 - 3z \\ y = -1 + 5z \end{cases}$$

Ainsi, il n'y a aucune contrainte sur z et à chaque valeur de $z = \lambda$, il correspond un unique couple $(x, y) = (2 - 3\lambda, -1 + 5\lambda)$ tel que (x, y, z) soit solution du système. Ainsi, pour obtenir une expression semblable à (7), on écrit la forme générale d'une solution du système comme

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix} + \lambda \begin{pmatrix} -3 \\ 5 \\ 1 \end{pmatrix}, \quad \lambda \in \mathbb{K}.$$

On remarque que $(x, y, z) = (2, -1, 0)$ est une solution particulière du système et que l'ensemble des solutions du système homogène associé est exactement

$$\rangle \begin{pmatrix} -3 \\ 5 \\ 1 \end{pmatrix} \langle.$$

Enfin, il est normal d'avoir la présence d'un unique paramètre λ puisque nous avons 3 inconnues et le rang du système vaut 2 (i.e., $3 - 2 = 1$).

Exemple VI.5.3. Voici un autre exemple du même type que le précédent, mais réduit cette fois à une seule équation,

$$x + y - 2z = 1.$$

Comme en (7), la forme générale d'une solution du système est directement

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \lambda_1 \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \quad \lambda_1, \lambda_2 \in \mathbb{K}.$$

Ici, une solution particulière du système est donnée par $(x, y, z) = (1, 0, 0)$ et l'ensemble des solutions du système homogène associé est exactement

$$\rangle \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} \langle .$$

Exemple VI.5.4. Voici à présent un exemple emprunté à la géométrie analytique.

On considère un espace affin euclidien muni d'un repère orthonormé d'axes Ox et Oy. Soit A, un point n'appartenant ni à Ox ni à Oy. On mène par ce point une droite variable $\mathcal{D}$ qui coupe Ox en B. On désigne par P le point de Oy dont l'ordonnée est égale à l'abscisse de B. Rechercher le lieu de la projection orthogonale de P sur la droite $\mathcal{D}$.

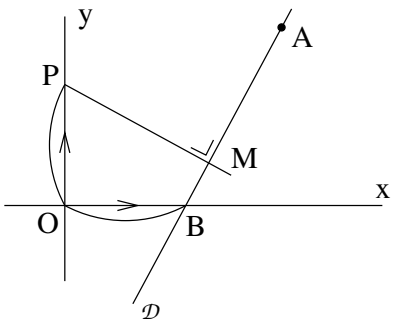


FIGURE VI.1. Un lieu géométrique.

Les points A, B et P ont pour coordonnées respectives (a_1, a_2), $(\lambda, 0)$ et $(0, \lambda)$, avec λ paramètre réel. Les génératrices du lieu ont pour équations respectives

$$-a_2(x - \lambda) - y(\lambda - a_1) = 0$$

et

$$x(\lambda - a_1) - a_2(y - \lambda) = 0.$$

Un point M de coordonnées (x, y) appartient au lieu si et seulement si il existe $\lambda \in \mathbb{R}$ tel que le système

$$\begin{cases} (a_2 - y)\lambda = a_2 x - a_1 y \\ (x + a_2)\lambda = a_1 x + a_2 y \end{cases}$$

possède une solution. L'élimination de λ revient à étudier la compatibilité du système (en l'inconnue λ). Par la proposition VI.3.3, le système est

compatible si et seulement si

$$\operatorname{rg}\begin{pmatrix} a_2 - y \\ x + a_2 \end{pmatrix} = \operatorname{rg}\begin{pmatrix} a_2 - y & a_2 x - a_1 y \\ x + a_2 & a_1 x + a_2 y \end{pmatrix}.$$

Premier cas : le rang de la matrice du système est nul. Ceci a lieu si $y = a_2$ et $x = -a_2$. Le système est donc compatible si

$$\operatorname{rg}\begin{pmatrix} 0 & -a_2^2 - a_1 a_2 \\ 0 & -a_1 a_2 + a_2^2 \end{pmatrix} = 0,$$

donc, si $a_2 = 0$, ce qui est impossible car $A \notin Ox$. On en conclut que le point $(-a_2, a_2)$ est à exclure du lieu.

Second cas : le rang de la matrice du système vaut 1. La compatibilité du système revient à ce que la matrice augmentée

$$\begin{pmatrix} a_2 - y & a_2 x - a_1 y \\ x + a_2 & a_1 x + a_2 y \end{pmatrix}$$

soit de rang 1 donc à ce que son déterminant soit nul. En annulant ce déterminant, on trouve

$$\left(x - \frac{a_1 - a_2}{2}\right)^2 + \left(y - \frac{a_1 + a_2}{2}\right)^2 = \frac{a_1^2 + a_2^2}{2}.$$

Le point $(-a_2, a_2)$ vérifie nécessairement cette équation. On en conclut que le lieu recherché est un cercle de centre $(\frac{a_1 - a_2}{2}, \frac{a_1 + a_2}{2})$ et de rayon $\frac{\sqrt{2}}{2}\sqrt{a_1^2 + a_2^2}$ privé du point $(-a_2, a_2)$.

Remarque VI.5.5. Cet exemple nous montre que la discussion sur le rang du système permet une détection facile des parties parasites du lieu.

Exemple VI.5.6. Voici à présent un système linéaire présentant une discussion complète en fonction du rang (a et b sont deux paramètres complexes)

$$\begin{cases} x + iz = 1 \\ ax + by = b \\ bx - az = b \\ ay + z = a. \end{cases}$$

Sous forme matricielle, ce système se réécrit

$$AX = B \text{ avec } A = \begin{pmatrix} 1 & 0 & i \\ a & b & 0 \\ b & 0 & -a \\ 0 & a & 1 \end{pmatrix},\ X = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \text{ et } B = \begin{pmatrix} 1 \\ b \\ b \\ a \end{pmatrix}.$$

La matrice A a 3 colonnes. Son rang est au plus 3. Le système est compatible si et seulement si $\operatorname{rg} A = \operatorname{rg}(A|B)$. En particulier, si la matrice $(A|B)$ est de rang maximal égal à 4, c'est-à-dire si $\det(A|B) \neq 0$, alors le système est incompatible. Si on calcule ce déterminant, on trouve

$$\det(A|B) = -a^2(a + ib).$$

Donc, si $a \neq 0$ et $a \neq -ib$, le système est incompatible. **(Cas I)**

Dans les autres cas, c'est-à-dire si $a = 0$ ou $a = -ib$, le rang de $(A|B)$ est inférieur ou égal à 3. **(Cas II)**

La sous-matrice constituée des quatre coins de A est de déterminant non nul. La matrice A est au moins de rang 2. Elle est exactement de rang 2 si et seulement si les deux matrices qui bordent $\begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$ dans A sont nuls. Ces deux sous-matrices ont pour déterminant

$$\begin{vmatrix} 1 & 0 & i \\ a & b & 0 \\ 0 & a & 1 \end{vmatrix} = b + ia^2 \quad \text{et} \quad \begin{vmatrix} 1 & 0 & i \\ b & 0 & -a \\ 0 & a & 1 \end{vmatrix} = a(a + ib).$$

Ainsi,

$$\begin{aligned} \operatorname{rg} A = 2 &\iff \begin{cases} b + ia^2 = 0 \\ a(a + ib) = 0 \end{cases} \\ &\iff (a = 0 \text{ et } b = 0) \text{ ou } (a = -ib \text{ et } b - ib^2 = 0) \\ &\iff (a = b = 0) \text{ ou } (b = -i \text{ et } a = -1). \end{aligned}$$

Si $a = b = 0$, alors **(Cas II.i)**

$$\operatorname{rg}(A|B) = \operatorname{rg} \begin{pmatrix} 1 & 0 & i & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = 2 = \operatorname{rg} A$$

et le système est compatible. De plus, le nombre d'inconnues moins le rang du système donne 3-2=1 paramètre dans l'expression des solutions. Le système admet une infinité simple de solutions.

Si $a = -1$ et $b = -i$, alors **(Cas II.ii)**

$$\operatorname{rg}(A|B) = \operatorname{rg} \begin{pmatrix} 1 & 0 & i & 1 \\ -1 & -i & 0 & -i \\ -i & 0 & 1 & -i \\ 0 & -1 & 1 & -1 \end{pmatrix} = 3 \text{ car } \begin{vmatrix} 1 & i & 1 \\ -1 & 0 & -i \\ 0 & 1 & -1 \end{vmatrix} = -1 \neq 0.$$

Donc $\operatorname{rg}(A|B) = 3 > 2 = \operatorname{rg}(A)$. Le système est incompatible.

Il ne reste plus que le cas où la matrice du système est de rang 3 et où le système admet une solution unique. **(Cas II.iii)**
Ce cas se présente si et seulement si $\operatorname{rg}(A|B) = \operatorname{rg}(A) = 3$, c'est-à-dire si

$$(a = 0 \text{ ou } a = -ib) \text{ et } (a, b) \neq (0, 0) \text{ et } (a, b) \neq (-1, -i)$$

ou encore si

$$(a = 0 \text{ et } b \neq 0) \text{ ou } (a = -ib \text{ et } b \neq 0 \text{ et } b \neq -i).$$

En conclusion, le système

- est incompatible si ($a \neq 0$ et $a \neq -ib$) ou ($a = -1$ et $b = -i$),
- admet une solution unique si ($a = 0$ et $b \neq 0$) ou ($a = -ib$ et $b \neq 0$ et $b \neq -i$),
- admet une infinité simple de solutions si $a = b = 0$.

6. Complément : Algorithme de Gauss-Jordan

Les méthodes de résolution de systèmes linéaires développées jusqu'à présent ont des avantages certains au point de vue de l'élimination d'éventuels paramètres et des discussions théoriques. Cependant, si l'on désire résoudre un système de manière efficace (en particulier, au moyen d'un ordinateur), on a le plus souvent recours à d'autres méthodes comme celle décrite ci-dessous.

Soit un système (**S**) de n équations à p inconnues,

$$\left\{\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1p}x_p & = & b_1 \\ \vdots & & & & & & \vdots & & \vdots \\ a_{n1}x_1 & + & a_{n2}x_2 & + & \cdots & + & a_{np}x_p & = & b_n \end{array}\right. .$$

Notons par L_i la i-ème ligne $\begin{pmatrix} a_{i1} & \cdots & a_{ip} & b_i \end{pmatrix}$ de la matrice augmentée du système. Par les résultats énoncés dans les sections précédentes, il est clair que les *opérations élémentaires* suivantes transforment le système (**S**) en un système équivalent :

- multiplier une ligne par un scalaire non nul :

$$L_i \leftarrow \lambda L_i,\ \lambda \in \mathbb{K} \setminus \{0\},$$

- ajouter à une ligne une combinaison linéaire d'autres lignes :

$$L_i \leftarrow L_i + \lambda L_j,\ \lambda \in \mathbb{K},\ i \neq j,$$

- permuter deux lignes :

$$L_i \leftrightarrow L_j,\ i \neq j.$$

Proposition VI.6.1 (Phase d'élimination). *Par des opérations élémentaires sur les lignes, le système* (**S**) *peut être transformé en un système équivalent de la forme*

$$\left\{\begin{array}{ccccccccccccc} x_{\mu_1} & + & \alpha_{1\mu_2}x_{\mu_2} & + & \cdots & + & \alpha_{1\mu_k}x_{\mu_k} & + & \cdots & + & \alpha_{1\mu_p}x_{\mu_p} & = & \beta_1 \\ & & x_{\mu_2} & + & \cdots & + & \alpha_{2\mu_k}x_{\mu_k} & + & \cdots & + & \alpha_{2\mu_p}x_{\mu_p} & = & \beta_2 \\ & & & & \ddots & & & & & & \vdots & & \\ & & & & & & x_{\mu_k} & + & \cdots & + & \alpha_{k\mu_p}x_{\mu_p} & = & \beta_k \\ & & & & & & & & & & 0 & = & \beta_{k+1} \\ & & & & & & & & & & \vdots & & \\ & & & & & & & & & & 0 & = & \beta_n \end{array}\right. .$$

où μ est une permutation de $\{1, \ldots, p\}$ et k est le rang du système.

Démonstration. On procède par récurrence sur p, le nombre d'inconnues du système. Si la matrice du système est nulle, il n'y a rien à démontrer. Sinon, choisissons une variable qui intervient avec un coefficient non nul dans une des équations du système. Quitte à permuter les lignes du système et les inconnues, on peut supposer que $a_{11} \neq 0$. On transforme le système en effectuant les transformations élémentaires

$$L_1 \leftarrow \frac{1}{a_{11}} L_1$$

et pour $i \neq 1$,

$$L_i \leftarrow L_i - \frac{a_{i1}}{a_{11}} L_1.$$

L'élément a_{11} est appelé *pivot*. On obtient alors un système équivalent ayant la forme

$$\begin{cases} x_1 + a'_{12}x_2 + \cdots + a'_{1p}x_p = b'_1 \\ \quad\; a'_{22}x_2 + \cdots + a'_{1p}x_p = b'_2 \\ \qquad\; \vdots \qquad\qquad\; \vdots \quad\; \vdots \\ \quad\; a'_{n2}x_2 + \cdots + a'_{np}x_p = b'_n \end{cases}.$$

Le système privé de la première ligne possède $n-1$ inconnues. On peut donc lui appliquer l'hypothèse de récurrence et obtenir un système équivalent du type prescrit.

■

Proposition VI.6.2 (Phase de substitution). *Par des opérations élémentaires sur les lignes, un système de la forme*

$$\begin{cases} x_1 + a_{12}x_2 + \cdots + a_{1k}x_k + \cdots + a_{1p}x_p = b_1 \\ \quad\; x_2 + \cdots + a_{2k}x_k + \cdots + a_{2p}x_p = b_2 \\ \qquad\; \ddots \qquad\qquad\qquad\qquad\qquad\; \vdots \\ \qquad\qquad\qquad\; x_k + \cdots + a_{kp}x_p = b_k \end{cases}$$

peut être transformé en un système équivalent du type

$$\begin{cases} x_1 + \alpha_{1k+1}x_{k+1} + \cdots + \alpha_{1p}x_p = \beta_1 \\ x_2 + \alpha_{2k+1}x_{k+1} + \cdots + \alpha_{2p}x_p = \beta_2 \\ \qquad\qquad\qquad\qquad\qquad\; \vdots \\ x_k + \alpha_{kk+1}x_{k+1} + \cdots + \alpha_{kp}x_p = \beta_k \end{cases}.$$

Démonstration. Pour $j = 1, \ldots, k-1$, on effectue la transformation élémentaire

$$L_j \leftarrow L_j - a_{jk}L_k$$

pour annuler le coefficient de x_k dans les $k-1$ premières équations.

Pour $j = 1, \ldots, k-2$, on effectue la transformation élémentaire

$$L_j \leftarrow L_j - a_{jk-1}L_{k-1}$$

pour annuler le coefficient de x_{k-1} dans les $k-2$ premières équations. On continue de cette manière jusqu'à obtenir la forme indiquée.

■

En effectuant la phase d'élimination, suivie de la phase de substitution, le système (**S**) de départ peut se mettre sous la forme

$$\left\{\begin{array}{lllllllll} x_{\mu_1} & + & \alpha_{1\mu_{k+1}}x_{\mu_{k+1}} & + & \cdots & + & \alpha_{1\mu_p}x_{\mu_p} & = & \beta_1 \\ x_{\mu_2} & + & \alpha_{2\mu_{k+1}}x_{\mu_{k+1}} & + & \cdots & + & \alpha_{2\mu_p}x_{\mu_p} & = & \beta_2 \\ & & & & & & \vdots & & \\ x_{\mu_k} & + & \alpha_{k\mu_{k+1}}x_{\mu_{k+1}} & + & \cdots & + & \alpha_{k\mu_p}x_{\mu_p} & = & \beta_k \\ & & & & & & 0 & = & \beta_{k+1} \\ & & & & & & \vdots & & \\ & & & & & & 0 & = & \beta_n \end{array}\right. .$$

Ainsi, (**S**) est compatible si $\beta_{k+1} = \cdots = \beta_n = 0$. De plus, si $k = p$, le système possède une unique solution $x_{\mu_i} = \beta_i$ pour $i = 1, \ldots, k$. Si $k < p$, le système possède alors une infinité de solutions[4]. Pour tout choix de valeurs pour

$$x_{\mu_{k+1}}, \ldots, x_{\mu_p}$$

les valeurs de $x_{\mu_1}, \ldots, x_{\mu_k}$ sont données par

$$\left\{\begin{array}{lll} x_{\mu_1} & = & \beta_1 - \alpha_{1\mu_{k+1}}x_{\mu_{k+1}} - \cdots - \alpha_{1\mu_p}x_{\mu_p} \\ & \vdots & \\ x_{\mu_k} & = & \beta_k - \alpha_{k\mu_{k+1}}x_{\mu_{k+1}} - \cdots - \alpha_{k\mu_p}x_{\mu_p} \end{array}\right. .$$

On retrouve les résultats donnés à la section 4 de ce chapitre concernant la structure des solutions d'un système d'équations linéaires.

Exemple VI.6.3. Voici trois exemples de systèmes résolus par la méthode de Gauss-Jordan.

$$\left\{\begin{array}{lllllll} 3x & + & 2y & - & z & = & 1 \\ x & + & y & - & z & = & 0 \\ 2x & + & 2y & + & z & = & 2 \end{array}\right. .$$

On effectue les transformations $L_1 \leftarrow \frac{1}{3}L_1$, $L_2 \leftarrow L_2 - \frac{1}{3}L_1$ et $L_3 \leftarrow L_3 - \frac{2}{3}L_1$ pour obtenir le système

$$\left\{\begin{array}{lllllll} x & + & \frac{2}{3}y & - & \frac{1}{3}z & = & \frac{1}{3} \\ & & \frac{1}{3}y & - & \frac{2}{3}z & = & -\frac{1}{3} \\ & & \frac{2}{3}y & + & \frac{5}{3}z & = & \frac{4}{3} \end{array}\right. .$$

Si $L_2 \leftarrow 3L_2$ et $L_3 \leftarrow L_3 - 2L_2$, il vient

$$\left\{\begin{array}{lllllll} x & + & \frac{2}{3}y & - & \frac{1}{3}z & = & \frac{1}{3} \\ & & y & - & 2z & = & -1 \\ & & & & 3z & = & 2 \end{array}\right. .$$

Pour terminer la phase d'élimination, $L_3 \leftarrow \frac{1}{3}L_3$ donne

$$\left\{\begin{array}{lllllll} x & + & \frac{2}{3}y & - & \frac{1}{3}z & = & \frac{1}{3} \\ & & y & - & 2z & = & -1 \\ & & & & z & = & \frac{2}{3} \end{array}\right. .$$

[4]Bien évidemment, il faut que $\mathbb{K}$ soit infini.

En substituant, on trouve

$$z = \frac{2}{3},\ y = \frac{1}{3},\ x = \frac{1}{3}.$$

Le système possède une unique solution (système déterminé).

Considérons à présent le système

$$\left\{\begin{array}{rcrcrcl} 3x & + & 2y & - & z & = & 1 \\ x & + & y & - & z & = & 0 \\ 4x & + & 3y & - & 2z & = & 1 \end{array}\right. .$$

La phase d'élimination donne d'abord

$$\left\{\begin{array}{rcrcrcl} x & + & \frac{2}{3}y & - & \frac{1}{3}z & = & \frac{1}{3} \\ & & \frac{1}{3}y & - & \frac{2}{3}z & = & -\frac{1}{3} \\ & & \frac{1}{3}y & - & \frac{2}{3}z & = & -\frac{1}{3} \end{array}\right. ,$$

puis

$$\left\{\begin{array}{rcrcrcl} x & + & \frac{2}{3}y & - & \frac{1}{3}z & = & \frac{1}{3} \\ & & y & - & 2z & = & -1 \\ & & & & 0 & = & 0 \end{array}\right. .$$

Ainsi, z peut prendre n'importe quelle valeur et pour chacune d'elles, on a

$$\left\{\begin{array}{rcl} x & = & 1 - z \\ y & = & -1 + 2z \end{array}\right. .$$

On est dans le cas d'un système indéterminé (le système est de rang 2 et on a trois inconnues).

Enfin, considérons le système

$$\left\{\begin{array}{rcrcrcl} 3x & + & 2y & - & z & = & 1 \\ x & + & y & - & z & = & 0 \\ 4x & + & 3y & - & 2z & = & 2 \end{array}\right. .$$

La seule différence avec l'exemple précédent est le second membre de la troisième équation. La phase d'élimination donne

$$\left\{\begin{array}{rcrcrcl} x & + & \frac{2}{3}y & - & \frac{1}{3}z & = & \frac{1}{3} \\ & & y & - & 2z & = & -1 \\ & & & & 0 & = & 1 \end{array}\right. .$$

On s'aperçoit donc que le système est incompatible.

Remarque VI.6.4. On peut aussi utiliser l'algorithme de Gauss-Jordan pour rechercher l'éventuel inverse d'une matrice carrée. En effet, si A est une matrice carrée inversible de dimension n et X l'inverse de A, alors

$$AX = I.$$

Si $X_1, \ldots, X_n$ sont les colonnes de X, l'équation matricielle précédente est équivalente aux n équations

$$AX_i = e_i, \quad i = 1, \ldots, n.$$

Rechercher X revient donc à résoudre n systèmes d'équations linéaires ayant même matrice A. Dans l'algorithme de Gauss-Jordan, seuls les coefficients de A jouent un rôle dans la phase d'élimination. On peut donc résoudre les n systèmes en parallèle.

Exemple VI.6.5. Soit la matrice

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 0 & 1 \\ 2 & 1 & 3 \end{pmatrix}$$

Effectuons les phases d'élimination en parallèle. On a tout d'abord

$$\left(\begin{array}{ccc|c|c|c} 1 & 2 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 2 & 1 & 3 & 0 & 0 & 1 \end{array}\right),$$

et si $L_2 \leftarrow L_2 - L_1$, $L_3 \leftarrow L_3 - 2L_1$,

$$\left(\begin{array}{ccc|c|c|c} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & -2 & 0 & -1 & 1 & 0 \\ 0 & -3 & 1 & -2 & 0 & 1 \end{array}\right).$$

Enfin, si $L_2 \leftarrow -\frac{1}{2}L_2$, $L_3 \leftarrow L_3 - \frac{3}{2}L_2$,

$$\left(\begin{array}{ccc|c|c|c} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & \frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 1 & -\frac{1}{2} & -\frac{3}{2} & 1 \end{array}\right).$$

Pour la phase de substitution, si on s'intéresse à la première colonne, on trouve $x_{31} = -\frac{1}{2}$, $x_{21} = \frac{1}{2}$ et $x_{11} = \frac{1}{2}$. Pour la deuxième colonne, $x_{32} = -\frac{3}{2}$, $x_{22} = -\frac{1}{2}$ et $x_{12} = \frac{5}{2}$ et enfin, avec la troisième colonne, $x_{33} = 1$, $x_{23} = 0$ et $x_{13} = -1$. Donc

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

7. Implémentation de l'algorithme de Gauss-Jordan

Nous donnons dans ce complément[5], deux implémentations de la méthode de Gauss. Nous avons choisi ici le langage `C` et la variable `a` est un tableau `n`×`n` représentant la matrice du système.

La première version présentée est (trop) simpliste. Elle prend comme premier pivot, le premier élément de la première ligne, puis comme deuxième pivot, le deuxième élément de la deuxième ligne et ainsi de suite...

[5]Il s'agit d'un complément car les discussions de cette section sortent du cadre de ce cours d'algèbre linéaire et s'apparentent plus à de l'analyse numérique. Cette section s'inspire des notes de cours de J. Hefferon, Saint Michael's College, Colchester, Vermont (USA). On pourra aussi consulter R. W. Hamming, *Introduction to Applied Numerical Analysis*, Hemisphere Publishing, 1971.

```
for(ligne_pivot=1;ligne_pivot<=n-1;ligne_pivot++){
  for(ligne=ligne_pivot+1;ligne<=n;ligne++){
    coefficient=a[ligne,ligne_pivot]/a[ligne_pivot,ligne_pivot];
    for(col=ligne_pivot;col<=n;col++){
      a[ligne,col]-=coefficient*a[ligne_pivot,col];
    }
  }
}
```

Pour rappel, en langage `C`, une instruction comme `x-=y` équivaut à `x=x-y` et une instruction du type `x++` incrémente d'une unité la variable `x`. Le code ci-dessus donne une idée rapide de la façon d'implémenter l'algorithme de Gauss. Cependant, il n'est pas utilisable en pratique et ce, pour diverses raisons. Tout d'abord, rien n'empêche un élément de la forme `a[i,i]` d'être nul. Cette situation n'a pas été prise en compte. En effet, lorsqu'on inspecte le code, on effectue une division par `a[ligne_pivot,ligne_pivot]`. Pour remédier à ce problème, on pourrait ajouter une condition `if ...` et alors permuter deux lignes de la matrice `a`.

Lorsqu'on utilise un ordinateur, l'arithmétique en virgule flottante peut conduire à certains désagréments. Pour éviter ces problèmes, il faut être un peu plus soigneux dans la façon d'implémenter les algorithmes.

Nous avons vu que si la matrice du système n'est pas inversible, alors ce cas doit être traité séparément (et conduit à un système incompatible ou indéterminé). Mais on peut aussi être en présence de systèmes "presque" singuliers. Par exemple, considérons le système

$$\begin{array}{rcl} x + 2\,y & = & 3 \\ 1.00000001\,x + 2\,y & = & 3.00000001 \end{array} .$$

On trouve facilement la solution $x = y = 1$. Mais un ordinateur, de par la manière dont sont représentés les nombres, peut avoir plus de difficultés. Si nous travaillons en *simple précision*, cela signifie que l'ordinateur utilise huit positions significatives pour représenter les nombres. Ainsi, pour la représentation en machine, la seconde équation sera codée par

$$1.0000000\,x + 2\,y = 3.0000000$$

perdant dans le même temps le chiffre en neuvième position. (On dispose de huits positions pour stocker le nombre 1.00000001, la première contient "1" pour le chiffre des unités, suivi de sept "0" pour les sept premières décimales.) Dès lors, au lieu de fournir la solution $x = y = 1$, l'ordinateur pensera être en présence d'un système ayant une matrice non inversible puisque les deux équations possèdent la même représentation interne.

Remarquons encore que si on remplace la deuxième équation du système par

$$1.00000001x + 2y = 3.00000003,$$

la véritable solution passe de $x = y = 1$ à $x = 3$ et $y = 0$. Par conséquent, le système peut changer de manière radicale en modifiant simplement la huitième décimale. Ceci explique les difficultés à traiter ce problème à l'aide d'un ordinateur. Un problème qui est très sensible à de telles pertubations ou imprécisions est dit *mal conditionné*. Par extension, on parle aussi de matrice *mal conditionnée*.

Il peut aussi y avoir d'autres raisons pour lesquelles les résultats fournis par un ordinateur peuvent être remis en question. Considérons par exemple le système

$$\begin{array}{rcl} 0.001x + y & = & 1 \\ x - y & = & 0 \end{array}.$$

Il est immédiat que ce système possède comme solution $x = y = 1/1.001$ qui est un nombre légèrement inférieur à un. Pour l'exposé, supposons disposer d'un ordinateur utilisant uniquement deux chiffres de mantisse[6] pour représenter les nombres de manière interne (on pourrait produire un exemple semblable en travaillant avec huit chiffres significatifs). Le système est représenté par

$$\begin{array}{rcl} (1.0 \times 10^{-3})x + (1.0 \times 10^{0})y & = & 1.0 \times 10^{0} \\ (1.0 \times 10^{0})x - (1.0 \times 10^{0})y & = & 0.0 \times 10^{0} \end{array}.$$

Si on utilise notre algorithme introduit précédemment, la phase de réduction donne $-1000\,L_1 + L_2$ et la seconde équation est donc

$$-1001y = -1000.$$

Puisque nous disposons uniquement de deux chiffres pour la mantisse, le nombre -1.001×10^3 est arrondi (tronqué) à -1.0×10^3 et la deuxième équation du système est ici représentée de manière interne par

$$(-1.0 \times 10^3)y = (-1.0 \times 10^3).$$

Dès lors, l'ordinateur trouve $y = 1$ et puis $x = 0$. Ceci est bien éloigné de la véritable solution $x = y = 1/1.001$! Cet exemple nous montre que l'arithmétique en virgule flottante et le choix de pivots petits peut conduire à des résultats bien imprécis.

Le lecteur féru de programmation pourrait objecter à ce qui précède et répondre à ces problèmes en passant en *double précision* (on utilise alors 16 positions significatives pour représenter les nombres au lieu de 8 en précision simple). Néanmoins, cela ne ferait que reporter le problème (il suffit d'adapter les exemples pour que la décimale gênante se trouve en dix-septième position...). De plus, les temps de calcul et la mémoire nécessaire au stockage en seraient certainement augmentés.

Dès lors, nous avons besoin d'une part, d'une stratégie permettant de minimiser les erreurs inhérantes au calcul en précision finie et d'autre part,

[6] Dans une écriture en virgule flottante comme 1.7231×10^{-3}, 1.7231 est la mantisse et -3 est l'exposant. Dans cet exemple, la mantisse possède cinq chiffres.

de mesures permettant d'estimer le degré de confiance que l'on peut avoir en les solutions fournies par la machine[7].

Plutôt que de considérer comme pivot, l'élément se trouvant en position `ligne_pivot`, `ligne_pivot`, il suffit de regarder toutes les entrées de la matrice se trouvant dans la colonne d'indice `ligne_pivot` et se trouvant sous la ligne `ligne_pivot`. Parmi ces éléments, on choisira comme pivot l'élément donnant les résultats les plus fiables (i.e., prendre le plus grandélément). Par exemple, dans le système introduit précédemment,

$$\begin{array}{rcl}(1.0\times 10^{-3})x+(1.0\times 10^{0})y & = & 1.0\times 10^{0}\\ (1.0\times 10^{0})x-(1.0\times 10^{0})y & = & 0.0\times 10^{0}\end{array}\ ,$$

on regarde les éléments de la première colonne et on choisit comme pivot non pas 0.001 mais 1. Ainsi, $-0.001L_2+L_1$ donne comme première équation $1.001y=1$ que l'ordinateur représente par

$$(1.0\times 10^{0})y=1.0\times 10^{0}.$$

La solution fournie par l'ordinateur est donc $x=y=1$ qui est "proche"[8] de la véritable solution du système.

Voici le code détaillé de l'algortihme de Gauss-Jordan tenant compte des choix de pivots, on appelle parfois cette méthode, le *pivotage partiel*.

```
for(ligne_pivot=1;ligne_pivot<=n-1;ligne_pivot++){
/* Recherche du pivot maximum dans cette colonne */
  max=ligne_pivot;
  for(ligne=ligne_pivot+1;ligne<=n;ligne++){
    if (abs(a[ligne,ligne_pivot]) > abs(a[max,ligne_pivot]))
      max=ligne;
  }
/* Echange de lignes, pour faire 'remonter' la ligne du pivot */
  for(col=ligne_pivot;col<=n;col++){
    temp=a[ligne_pivot,col];
    a[ligne_pivot,col]=a[max,col];
    a[max,col]=temp;
  }
/* On procede comme dans la version naive */
  for(ligne=ligne_pivot+1;ligne<=n;ligne++){
    coefficient=a[ligne,ligne_pivot]/a[ligne_pivot,ligne_pivot];
    for(col=ligne_pivot;col<=n;col++){
      a[ligne,col]-=coefficient*a[ligne_pivot,col];
    }
  }
```

[7] C'est pour cette raison qu'on introduit en analyse numérique le nombre de conditionnement d'une matrice.

[8] Il est inévitable lorsqu'on travaille avec un nombre fini de chiffres significatifs, d'avoir des erreurs d'arrondi. Une des préoccupations de l'analyse numérique est de minimiser ce type d'erreurs.

```
}
```

Pour obtenir les solutions d'un système donné, il faut bien évidemment implémenter les transformations à effectuer sur le second membre mais aussi des tests lorsqu'on est en présence d'une éventuelle matrice non inversible. Pour ne pas allourdir le texte, cette tâche est laissée au lecteur.

CHAPITRE VII

Espaces vectoriels

Soit $\mathbb{K}$ un champ fixé une fois pour toutes dans ce chapitre. Les éléments de $\mathbb{K}$ sont appelés *scalaires*. Pour rappel, tout champ possède deux éléments privilégiés notés 0 et 1.

1. Premières définitions

Définition VII.1.1. [1] Un *espace vectoriel* sur $\mathbb{K}$ ou $\mathbb{K}$-*vectoriel* est un ensemble E muni d'une addition interne

$$+ : E \times E \to E$$

et d'une multiplication interne

$$\cdot : \mathbb{K} \times E \to E$$

qui jouit des propriétés suivantes :

(1) $(E, +)$ est un groupe commutatif,
(2) pour tous $x, y \in E$ et tous scalaires $\lambda, \mu \in \mathbb{K}$
  (2.1) $\lambda \cdot (\mu \cdot x) = (\lambda\mu) \cdot x$,
  (2.2) $1 \cdot x = x$,
  (2.3) $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$,
  (2.4) $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$.

Si E est un espace vectoriel, les éléments de E sont appelés *vecteurs*.

Puisqu'en particulier, $(E, +)$ est un groupe, il existe un neutre unique pour l'addition, appelé *vecteur nul*, que l'on notera 0 tel que $x + 0 = x = 0 + x$ pour tout $x \in E$. Il faudra veiller à ne pas confondre le vecteur nul et le scalaire 0, le contexte permettant de faire la distinction[2]. Comme

[1] Bien que nous n'utiliserons pas la notion de $\mathbb{K}$-algèbre dans ce qui suit, on peut néanmoins noter qu'une $\mathbb{K}$-*algèbre* est un espace vectoriel muni d'une opération supplémentaire $* : E \times E \to E$ qui est

(3.1) associative : $\forall u, v, w \in E$, $(u * v) * w = u * (v * w)$,
(3.2) admet un neutre $1_E \in E$: $\forall u \in E$, $u * 1_E = u = 1_E * u$,
(3.3) distributive par rapport à + :
  $\forall u, v, w \in E$, $u * (v + w) = u * v + u * w$ et $(u + v) * w = u * w + v * w$,
(3.4) homogène : $\forall u, v \in E$, $\forall \lambda \in \mathbb{K}$, $(\lambda.u) * v = \lambda.(u * v) = u * (\lambda.v)$.

Une algèbre est *commutative* si $\forall u, v \in E$, $u * v = v * u$. Par exemple, $\mathbb{K}_n^n$ est une $\mathbb{K}$-algèbre non commutative.

[2] Par exemple, $\mathbb{K}^n$ est un $\mathbb{K}$-vectoriel. Le vecteur nul est le vecteur colonne de dimension n dont tous les éléments sont nuls. On ne confondra pas ce vecteur avec le scalaire $0 \in \mathbb{K}$.

d'habitude, on notera $-x$ l'opposé du vecteur x, c'est-à-dire l'unique vecteur tel que $x + (-x) = 0 = (-x) + x$.

Remarque VII.1.2. Nous voudrions à ce stade attirer l'attention du lecteur sur la différence existant entre les structures d'espace vectoriel et d'anneau. En effet, ces structures disposent toutes deux d'une même opération d'addition (on est, dans les deux cas, en présence d'un groupe commutatif pour $+$). Par contre, l'opération de multiplication est différente. Dans le cas d'un anneau A, il s'agit d'une opération *interne*, $\cdot : A \times A \to A$. Par contre pour un $\mathbb{K}$-vectoriel E, il s'agit d'une multiplication *par un scalaire*, $\cdot : \mathbb{K} \times E \to E$ (en général, $E \neq \mathbb{K}$).

Proposition VII.1.3. *Soient E un $\mathbb{K}$-vectoriel, $x, y, z \in E$ et $\lambda \in \mathbb{K}$. Alors*

$$x + z = y + z \Rightarrow x = y \quad et \quad z + x = z + y \Rightarrow x = y,$$
$$0 \cdot x = 0,$$
$$\lambda \cdot 0 = 0,$$
$$\lambda \cdot x = \lambda \cdot y \Rightarrow (\lambda = 0 \quad ou \quad x = y),$$
$$(-\lambda) \cdot x = -(\lambda \cdot x).$$

Les preuves ne sont pas difficiles mais constituent un bon moyen de se familiariser avec les axiomes des espaces vectoriels.

Démonstration. Si $x + z = y + z$, on ajoute à chaque membre l'unique vecteur $-z$, opposé de z, pour obtenir $x + 0 = y + 0$ et donc $x = y$.

Pour tout $x \in E$, $x + 0 = x = 1 \cdot x = (1 + 0) \cdot x = 1 \cdot x + 0 \cdot x = x + 0 \cdot x$. De la première propriété, il s'ensuit que $0 \cdot x = 0$.

Prouvons que $\lambda \cdot 0 = 0$. On a $\lambda \cdot 0 + \lambda \cdot 0 = \lambda \cdot (0 + 0) = \lambda \cdot 0 = \lambda \cdot 0 + 0$ et donc, par la première propriété, $\lambda \cdot 0 = 0$.

Pour l'avant-dernière propriété, si $\lambda \neq 0$, il suffit de multiplier les deux membres par le scalaire $\frac{1}{\lambda}$.

Enfin traitons la dernière propriété. On a

$$0 = 0 \cdot x = (\lambda + (-\lambda)) \cdot x = \lambda \cdot x + (-\lambda) \cdot x.$$

Ceci montre que $(-\lambda) \cdot x$ est l'opposé de $\lambda \cdot x$ que l'on note $-(\lambda \cdot x)$.

■

Remarque VII.1.4. Cette dernière propriété montre la cohérence de la notation $-x$ puisque $(-1) \cdot x = -x$. En particulier, on notera $x + (-y)$ simplement $x - y$. Nous avons alors $x - x = (1 - 1) \cdot x = 0 \cdot x = 0$, pour tout $x \in E$. Dans la suite, nous écrirons λx au lieu de $\lambda \cdot x$.

Exemple VII.1.5. Voici quelques exemples d'espaces vectoriels.

- L'ensemble $\mathbb{K}_n^m$ est un espace vectoriel sur $\mathbb{K}$. En particulier, l'ensemble $\mathbb{K}^m$ des vecteurs colonnes à m composantes et l'ensemble $\mathbb{K}_n$ des vecteurs lignes à n composantes sont aussi des espaces vectoriels sur $\mathbb{K}$.

- Soient X un ensemble et $\mathcal{F}(X;\mathbb{K})$ l'ensemble des applications de X dans $\mathbb{K}$. Muni des opérations d'addition et de multiplication définies par
$$(f+g)(x) = f(x) + g(x)$$
et
$$(\lambda f)(x) = \lambda f(x)$$
pour tous $f, g \in \mathcal{F}(X;\mathbb{K})$, $\lambda \in \mathbb{K}$, l'ensemble $\mathcal{F}(X;\mathbb{K})$ a une structure d'espace vectoriel sur $\mathbb{K}$.
- L'ensemble $C_0(\mathbb{R})$ des fonctions continues sur $\mathbb{R}$ est un espace vectoriel réel.
- L'ensemble $\mathbb{R}[x]$ (resp. $\mathbb{C}[x]$) des polynômes à coefficients dans $\mathbb{R}$ (resp. dans $\mathbb{C}$) est un espace vectoriel réel (resp. complexe).
- L'ensemble $\mathbb{R}[x]_d$ (resp. $\mathbb{C}[x]_d$) des polynômes à coefficients dans $\mathbb{R}$ (resp. dans $\mathbb{C}$) de degré au plus d est un espace vectoriel réel (resp. complexe).
- L'ensemble des solutions d'un système homogène d'équations linéaires à coefficients dans $\mathbb{K}$ est un espace vectoriel sur $\mathbb{K}$.
- L'ensemble des nombres complexes peut être vu comme un espace vectoriel sur $\mathbb{R}$. De même, $\mathbb{R}$ est aussi un $\mathbb{Q}$-vectoriel.

Définition VII.1.6. Soient E un espace vectoriel et $x_1, \ldots, x_r$ des éléments de E, $r \geq 1$. Les vecteurs $x_1, \ldots, x_r$ sont *linéairement dépendants* s'il existe des scalaires $\lambda_1, \ldots, \lambda_r$ non tous nuls tels que
$$\lambda_1 x_1 + \cdots + \lambda_r x_r = 0.$$
Dans le cas contraire, ils sont dits *linéairement indépendants*. Cela signifie que si on a une relation de la forme
$$\lambda_1 x_1 + \cdots + \lambda_r x_r = 0$$
où $\lambda_1, \ldots, \lambda_r$ sont des scalaires, alors
$$\lambda_1 = \cdots = \lambda_r = 0.$$

Des vecteurs sont linéairement dépendants si et seulement si l'un d'eux s'exprime comme combinaison linéaire des autres.

La seule façon d'obtenir le vecteur nul comme combinaison de vecteurs linéairement indépendants est que tous les coefficients de cette combinaison soient nuls.

Une expression de la forme $\lambda_1 x_1 + \cdots + \lambda_r x_r$ avec $\lambda_1, \ldots, \lambda_r \in \mathbb{K}$ est une *combinaison linéaire* des vecteurs $x_1, \ldots, x_r$. Autrement dit, $x_1, \ldots, x_r$ sont linéairement indépendants si la seule façon d'obtenir le vecteur nul comme combinaison linéaire de ces vecteurs est de considérer une combinaison linéaire dont tous les coefficients sont nuls.

Exemple VII.1.7. Voici quelques exemples de vecteurs linéairement dépendants et indépendants.

- Si on considère $\mathbb{C}$ comme un $\mathbb{R}$-vectoriel, les vecteurs 1 et i sont linéairement indépendants. En effet, si $a, b \in \mathbb{R}$ et si $a + ib = 0$, alors $a = b = 0$. (La seule combinaison linéaire à coefficients réels de 1 et i donnant 0 est la combinaison où les deux coefficients sont nuls.)

- Si on considère à présent $\mathbb{C}$ comme un $\mathbb{C}$-vectoriel, les vecteurs 1 et i sont linéairement dépendants. Il suffit de trouver deux nombres complexes a et b non simultanément nuls tels que $a + ib = 0$. On vérifie que $a = 1$ et $b = i$ conviennent. (Il suffsait de trouver une combinaison linéaire à coefficients non tous nuls, d'autres pouvaient tout aussi bien convenir.)
- Considérons le $\mathbb{R}$-vectoriel des fonctions de $\mathbb{R}$ dans $\mathbb{R}$. Les fonctions $\cos(x)$ et $\sin(x)$ sont linéairement indépendantes. En effet, si $a, b \in \mathbb{R}$ et si[3]
$$a\cos(x) + b\sin(x) = 0,\ \forall x \in \mathbb{R},$$
alors, pour $x = 0$ et $x = \pi/2$, on en déduit que $a = b = 0$. Par contre, les fonctions $\cos(x)$, $\cos(3x)$ et $\cos^3(x)$ sont linéairement dépendantes car $\cos(3x)$ est combinaison linéaire de $\cos^3(x)$ et $\cos(x)$.
- Les vecteurs du $\mathbb{R}$-vectoriel $\mathbb{R}^3$
$$\begin{pmatrix}1\\0\\0\end{pmatrix},\ \begin{pmatrix}0\\1\\0\end{pmatrix},\ \begin{pmatrix}0\\0\\1\end{pmatrix}$$
sont linéairement indépendants.
- Les vecteurs du $\mathbb{R}$-vectoriel $\mathbb{R}^3$
$$u = \begin{pmatrix}1\\2\\0\end{pmatrix},\ v = \begin{pmatrix}-1\\3\\1\end{pmatrix},\ w = \begin{pmatrix}-1\\8\\2\end{pmatrix}$$
sont linéairement dépendants. On vérifie par exemple que $u + 2v = w$. Ainsi, l'un d'eux s'expriment comme combinaison linéaire des autres. Autrement dit, on a la relation linéaire $u + 2v - w = 0$ où les coefficients sont non tous nuls.
- Les matrices suivantes de $\mathbb{C}_2^2$
$$A = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix},\ B = \begin{pmatrix}-1 & 0\\0 & i\end{pmatrix},\ C = \begin{pmatrix}i & 1\\0 & i\end{pmatrix}$$
sont linéairement indépendantes. En effet, soient a, b, c des nombres complexes tels que
$$aA + bB + cC = 0.$$
Cette égalité est équivalente à
$$\begin{cases} a - b + ic &= 0\\ c &= 0\\ a + ib + ic &= 0\end{cases}$$
et ce système possède l'unique solution $a = b = c = 0$.

[3]Remarquer que dans cet exemple, le vecteur nul est la fonction réelle zéro $0 : x \mapsto 0$. Il faut donc prendre garde de ne pas confondre l'élément 0 de $\mathbb{K}$ et le vecteur nul, aussi noté 0, du $\mathbb{K}$-vectoriel considéré.

- Les fonctions polynomiales 1, x et x^2 sont des vecteurs linéairement indépendants de l'espace $\mathbb{R}[x]$. En effet, si
$$ax^2 + bx + c = 0, \ \forall x \in \mathbb{R},$$
alors $a = b = c = 0$.

2. A propos de l'indépendance linéaire

Dans ce qui suit, E est un espace vectoriel sur $\mathbb{K}$.

Proposition VII.2.1. *Soient p un entier supérieur ou égal à 2 et $x_1, \ldots, x_p$ des vecteurs linéairement indépendants de E. Aucun des x_i n'est le vecteur nul. De plus, les vecteurs $x_1, \ldots, x_p$ sont deux à deux distincts et pour tout entier positif q tel que $q \leq p$, les vecteurs $x_1, \ldots, x_q$ sont linéairement indépendants.*

Démonstration. C'est immédiat.

■

Proposition VII.2.2. *Soient p un entier positif, $x_1, \ldots, x_p$ des vecteurs linéairement indépendants de E et y un vecteur de E. Alors y est combinaison linéaire de $x_1, \ldots, x_p$ si et seulement si les vecteurs $x_1, \ldots, x_p, y$ sont linéairement dépendants.*

Démonstration. Si y est combinaison linéaire de $x_1, \ldots, x_p$, alors il est clair que $x_1, \ldots, x_p, y$ sont linéairement dépendants. Réciproquement, supposons $x_1, \ldots, x_p, y$ linéairement dépendants. Il existe donc des scalaires non tous nuls $\lambda_1, \ldots, \lambda_p, \lambda$ tels que
$$\lambda_1 x_1 + \cdots + \lambda_p x_p + \lambda y = 0.$$
Si λ était nul alors les vecteurs $x_1, \ldots, x_p$ seraient linéairement dépendants. Par conséquent, $\lambda \neq 0$ et on trouve
$$y = -\frac{\lambda_1}{\lambda} x_1 - \cdots - \frac{\lambda_p}{\lambda} x_p.$$
Ceci conclut la preuve.

■

Théorème VII.2.3 (Théorème de Steinitz). *Soit p un entier positif, $p+1$ combinaisons linéaires de p vecteurs sont linéairement dépendantes.*

Démonstration. Soient
$$\begin{aligned} y_1 &= \lambda_{11} x_1 + \cdots + \lambda_{1p} x_p \\ &\vdots \\ y_{p+1} &= \lambda_{p+1,1} x_1 + \cdots + \lambda_{p+1,p} x_p \end{aligned}$$
$p+1$ combinaisons linéaires de p vecteurs $x_1, \ldots, x_p$. Pour démontrer que $y_1, \ldots, y_{p+1}$ sont linéairement dépendants, on procède par récurrence sur p.

Si $p = 1$, on a deux vecteurs $y_1 = \lambda_{11}x_1$ et $y_2 = \lambda_{21}x_1$. Si λ_{11} ou λ_{21} est nul, alors y_1 ou y_2 est nul et donc, y_1 et y_2 sont linéairement dépendants. Sinon, $\lambda_{21}y_1 - \lambda_{11}y_2 = 0$ est une relation linéaire liant y_1 et y_2.

Supposons la propriété satisfaite pour p combinaisons linéaires de $p-1$ vecteurs et démontrons-la pour $p+1$ combinaisons linéaires de p vecteurs. Si tous les coefficients λ_{ij} sont nuls, alors les vecteurs $y_1, \ldots, y_{p+1}$ sont nuls et donc linéairement dépendants. Sinon, au moins un des λ_{ij} est non nul et quitte à renuméroter les vecteurs, on peut supposer que $\lambda_{11} \neq 0$. Considérons les vecteurs

$$\begin{array}{rcl} z_2 & = & \lambda_{11}y_2 - \lambda_{21}y_1 \\ & \vdots & \\ z_{p+1} & = & \lambda_{11}y_{p+1} - \lambda_{p+1,1}y_1 \end{array} .$$

Nous sommes en présence de p combinaisons linéaires de $p-1$ vecteurs. Par hypothèse de récurrence, ces vecteurs sont linéairement dépendants. Dès lors, il existe des scalaires $\mu_2, \ldots, \mu_{p+1}$ non tous nuls tels que

$$\mu_2 z_2 + \cdots + \mu_{p+1}z_{p+1} = 0.$$

En posant $\mu_1 = -(\mu_2\lambda_{21} + \cdots + \mu_{p+1}\lambda_{p+1,1})$, il vient

$$\mu_1 y_1 + \mu_2\lambda_{11}y_2 + \cdots + \mu_{p+1}\lambda_{11}y_{p+1} = 0.$$

Il est clair que les coefficients de cette dernière combinaison linéaire ne sont pas tous nuls.

■

3. Base et dimension

Dans cette section, E est toujours un $\mathbb{K}$-vectoriel.

Définition VII.3.1. Une partie finie $A \subset E$ est dite *libre* si les vecteurs de A sont linéairement indépendants. Dans le cas contraire, A est dite *liée*. La partie A est dite *génératrice* si tout vecteur de E est combinaison linéaire des vecteurs de A. Si $x_1, \ldots, x_p$ est une partie génératrice de E, on dit aussi que E est *engendré* par les vecteurs $x_1, \ldots, x_p$.

Exemple VII.3.2. Dans $\mathbb{R}^3$, les vecteurs

$$\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}$$

forment une partie libre (qui n'est pas génératrice) et les vecteurs

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

forment une partie génératrice de $\mathbb{R}^3$ (mais cette partie n'est pas libre).

Remarque VII.3.3. Si A est une partie libre et si $B \subset A$, alors B est aussi libre (cf. proposition VII.2.1).

Si A est une partie liée et si $B \supset A$, alors B est aussi liée (la justification est immédiate[4]).

Enfin, si A est une partie génératrice et si $B \supset A$, alors B l'est aussi.

Définition VII.3.4. Un espace vectoriel E est dit de *dimension finie* s'il contient une partie génératrice finie.

Une *base* de E est une partie[5] libre et génératrice de E.

Théorème VII.3.5. [6] *Soit E un espace vectoriel de dimension finie. Alors,*

i) *toute partie génératrice finie de E contient une base,*

ii) *toute partie libre finie de E est incluse dans une base.*

Démonstration. Par définition, E possède une partie génératrice à p éléments. Tout vecteur de E étant combinaison linéaire de ces p éléments, le théorème de Steinitz nous assure que toute partie libre contient au plus p éléments[7]. Démontrons i). Soit A une partie génératrice de E. Parmi les parties libres de E incluses dans A, choisissons-en une dont le nombre d'éléments est maximum. Soit B cette partie. Il nous suffit de montrer que B engendre E. Tout vecteur de A est combinaison linéaire des éléments de B. Sinon, vu la proposition VII.2.2, on pourrait trouver dans A des vecteurs linéairement indépendants en nombre supérieur au nombre d'éléments de B. Puisque A engendre E, on en conclut que B aussi.

Passons au point ii). Soit A une partie libre de E. Choisissons dans E une partie B formée d'un nombre maximum d'éléments tels que les vecteurs de $A \cup B$ soient encore linéairement indépendants. Il nous suffit de montrer que $A \cup B$ engendre E. Vu la proposition VII.2.2, tout élément de E est combinaison linéaire des éléments de $A \cup B$ car sinon, le nombre d'éléments de B ne serait pas maximum. Ceci conclut la preuve.

■

[4] Si $x_1, \ldots, x_p$ sont linéairement dépendants, alors $x_1, \ldots, x_p, x_{p+1}$ le sont aussi. En effet, il existe des scalaires $\lambda_1, \ldots, \lambda_p$ non tous nuls tels que $\lambda_1 x_1 + \cdots + \lambda_p x_p = 0$. Par conséquent, on a $\lambda_1 x_1 + \cdots + \lambda_p x_p + 0 x_{p+1} = 0$ avec les λ_i non tous nuls, ce qui montre bien que $x_1, \ldots, x_p, x_{p+1}$ sont linéairement dépendants.

[5] Le vocable "partie" est très certainement mal choisi ! En effet, comme nous le verrons par la suite (lorsque nous parlerons des composantes d'un vecteur dans une base), si une base contient n éléments, on considérera cette base comme un n-uple ordonné. Par exemple, parler de la première composante d'un vecteur fait référence au premier élément de la base. Cette dernière est donc ordonnée.

[6] Le point ii) du théorème est parfois appelé *théorème de la base incomplète* car, si $x_1, \ldots, x_p$ sont linéairement indépendants et si $y_1, \ldots, y_q$ forment une partie génératice de E, alors on peut compléter $x_1, \ldots, x_p$ par certains des vecteurs y_i pour obtenir une base de E.

[7] Cette première partie de la preuve nous assure que l'on peut définir une partie libre contenant *un nombre maximum d'éléments*. En effet, sans cette information, une partie libre pourrait *a priori* être infinie et on ne pourrait donc pas parler du nombre maximum d'éléments d'un ensemble infini !

Proposition VII.3.6. *Soit E un espace vectoriel de dimension finie. Alors,*

i) *E possède une base,*

ii) *deux bases quelconques de E ont le même nombre d'éléments.*

Démonstration. Le premier point résulte de la proposition précédente. Soient B et B' deux bases de E contenant respectivement p et p' éléments. Les p éléments de B sont linéairement indépendants et sont aussi p combinaisons linéaires des p' éléments de B'. Vu le théorème de Steinitz, $p \leq p'$. De manière analogue, on a $p' \leq p$.

■

Définition VII.3.7. La théorème précédent nous montre que toutes les bases de E ont le même nombre d'éléments. Ce nombre est appelé la *dimension* de E et est noté $\dim E$. De plus, on définit la dimension de l'espace vectoriel $\{0\}$ en posant $\dim\{0\} = 0$.

Corollaire VII.3.8. *Soit E un espace vectoriel de dimension finie n. Toute partie libre (resp. génératrice) contient au plus (resp. au moins) n éléments. Si A est une partie libre (resp. génératrice) de E contenant n éléments, alors A est une base.*

Démonstration. Cela résulte immédiatement du théorème VII.3.5 et de la proposition précédente.

■

La notion de base d'un espace vectoriel permet d'introduire l'important concept de composantes d'un vecteur dans une base.

Proposition VII.3.9. *Soient E un espace vectoriel de dimension finie n et $U = (u_1, \ldots, u_n)$ une base de E. Pour tout $x \in E$, il existe des scalaires uniques $x_1, \ldots, x_n \in \mathbb{K}$ tels que*

C'est l'intérêt primordial des bases !

$$\boxed{x = x_1 u_1 + \cdots + x_n u_n.}$$

Ces scalaires $x_1, \ldots, x_n \in \mathbb{K}$ s'appellent les composantes[8] *de x dans la base $(u_1, \ldots, u_n)$.*

Démonstration. Puisque U est une base, U est en particulier une partie génératrice de E. Il existe $x_1, \ldots, x_n \in \mathbb{K}$ tels que

$$x = x_1 u_1 + \cdots + x_n u_n.$$

Supposons qu'il existe également $x'_1, \ldots, x'_n \in \mathbb{K}$ tels que

$$x = x'_1 u_1 + \cdots + x'_n u_n.$$

En soustrayant les deux relations et en utilisant les propriétés des espaces vectoriels, il vient

$$0 = (x_1 - x'_1)u_1 + \cdots + (x_n - x'_n)u_n,$$

[8] Certains auteurs utilisent aussi le terme *coordonnéees*. Nous préférons utiliser ce dernier terme lorsqu'on parle des coordonnées d'un point dans un repère (cf. le cours de géométrie).

et donc $x_i = x'_i$ pour tout $i \in \{1, \ldots, n\}$ puisque les vecteurs de U sont linéairement indépendants.

■

Proposition VII.3.10. *Soient E un espace vectoriel de dimension finie n et $U = (u_1, \ldots, u_n)$ une base de E. L'application*

$$\Phi : E \to \mathbb{K}^n : x \mapsto \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

est une bijection telle que pour tous $\lambda \in \mathbb{K}$, $x, y \in E$,

$$\Phi(\lambda x) = \lambda \Phi(x)$$

et

$$\Phi(x + y) = \Phi(x) + \Phi(y).$$

Démonstration. Le fait que Φ est une bijection résulte de la proposition précédente. Pour le reste, il s'agit de simples vérifications.

■

Le vecteur $\Phi(x)$ est le *vecteur des composantes* de x dans la base U. Si il est nécessaire de faire référence à la base, on écrira alors $\Phi_U(x)$.

Remarque VII.3.11. Cette proposition signifie que l'application Φ préserve les structures d'espace vectoriel de E et de $\mathbb{K}^n$. On dit que les deux espaces sont *isomorphes* et que Φ est un *isomorphisme*. En particulier, des vecteurs $y_1, \ldots, y_k \in E$ sont linéairement dépendants (resp. indépendants) si et seulement si $\Phi(y_1), \ldots, \Phi(y_k) \in \mathbb{K}^n$ sont linéairement dépendants (resp. indépendants). On pourra dès lors utiliser les propositions V.3.1 et V.3.2 des pages 87 et 88 lorsque, par l'intermédiaire d'une base, on considérera les composantes des vecteurs. C'est aussi pour cette raison que l'archétype du $\mathbb{K}$-vectoriel de dimension finie n est $\mathbb{K}^n$.

On retrouvera cette notion au chapitre suivant, cf. définition X.1.8

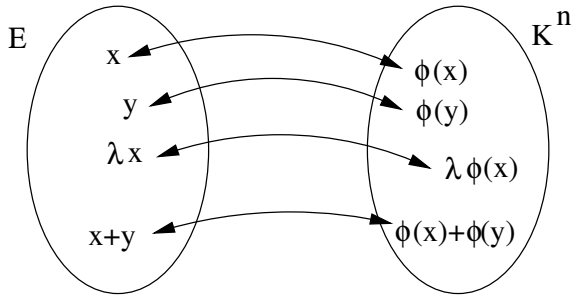


FIGURE VII.1. Isomorphisme entre E et $\mathbb{K}^n$

Remarque VII.3.12. Il résulte de la proposition précédente qu'un espace vectoriel E sur $\mathbb{Z}_p$ (p premier) est de dimension finie si et seulement si il est fini. De plus, dans ce cas,

$$\#E = p^{\dim E}$$

4. Changement de base

Le problème posé dans cette section est le suivant. Soit E un espace vectoriel ayant $U = (u_1, \ldots, u_n)$ et $U' = (u'_1, \ldots, u'_n)$ comme bases. Tout vecteur x de E se décompose de manière unique dans les bases U et U'. Connaissant les composantes $x_1, \ldots, x_n$ de x dans la base U, peut-on déterminer les composantes $x'_1, \ldots, x'_n$ de x dans la base U' ?

Exemple VII.4.1. Soit l'espace vectoriel $\mathbb{R}^2$ muni de la base canonique

$$U = (e_1 = \begin{pmatrix}1\\0\end{pmatrix}, e_2 = \begin{pmatrix}0\\1\end{pmatrix})$$

et de la base

$$U' = (u'_1 = \begin{pmatrix}3\\1\end{pmatrix}, u'_2 = \begin{pmatrix}-1\\2\end{pmatrix}).$$

Si $x = ae_1 + be_2$, peut-on calculer a' et b' tels que $x = a'u'_1 + b'u'_2$?

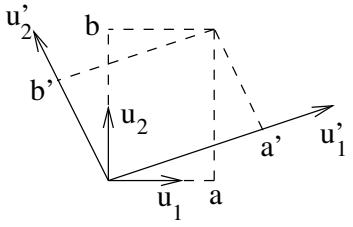


FIGURE VII.2. Changement de base.

Traitons le cas général d'un espace vectoriel de dimension n possédant deux bases U et U'. Tout vecteur de E se décompose dans la base U'; en particulier, pour $i \in \{1, \ldots, n\}$, on a

$$u_i = \sum_{j=1}^{n} a_{ji}\, u'_j.$$

Si $x \in E$ se décompose dans la base U par

$$x = \sum_{i=1}^{n} x_i\, u_i,$$

alors on trouve

$$x = \sum_{i=1}^{n} x_i \sum_{j=1}^{n} a_{ji}\, u'_j = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} a_{ji}\, x_i \right) u'_j.$$

Puisque la décomposition dans une base est unique, il vient

$$x'_j = \sum_{i=1}^{n} a_{ji}\, x_i$$

et sous forme matricielle,

$$\begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

On remarque que la i-ème colonne de cette matrice contient les composantes du i-ème vecteur de l'ancienne base U dans la nouvelle base U'. La connaissance de cette matrice permet donc de calculer les composantes de tout vecteur $x \in E$ dans la base U' connaissant les composantes de x dans la base U. On dit que cette matrice est la *matrice de changement de base* de U à U'.

On résume ce qui précède par la proposition suivante.

Proposition VII.4.2. [9] *Soit x un vecteur de E ayant X et X' pour vecteur de composantes dans les bases U et U'. Si P est la matrice de changement de base de U à U', alors*

$$X' = PX.$$

Exemple VII.4.3. Poursuivons l'exemple précédent. Les vecteurs de la base U se décomposent de la manière suivante,

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{2}{7}\begin{pmatrix} 3 \\ 1 \end{pmatrix} - \frac{1}{7}\begin{pmatrix} -1 \\ 2 \end{pmatrix}$$

et

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{7}\begin{pmatrix} 3 \\ 1 \end{pmatrix} + \frac{3}{7}\begin{pmatrix} -1 \\ 2 \end{pmatrix}.$$

La matrice de changement de base de U à U' est donnée par

$$\begin{pmatrix} \frac{2}{7} & \frac{1}{7} \\ -\frac{1}{7} & \frac{3}{7} \end{pmatrix}.$$

Ainsi, si x se décompose dans la base U sous la $x = ae_1 + be_2$ et dans la base U' sous la forme $x = a'u'_1 + b'u'_2$, alors les coefficients a' et b' peuvent être obtenus par

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} \frac{2}{7} & \frac{1}{7} \\ -\frac{1}{7} & \frac{3}{7} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \frac{2}{7}a + \frac{1}{7}b \\ -\frac{1}{7}a + \frac{3}{7}b \end{pmatrix}.$$

Exemple VII.4.4. Voici un exemple un peu moins classique. Il est aisé de voir que $U = (x^2, x, 1)$ et $U' = ((x+\alpha)^2, x+\alpha, \alpha)$ sont deux bases de $\mathbb{R}[x]_2$, $\alpha \neq 0$. Un polynôme quelconque de $\mathbb{R}[x]_2$ s'écrit

$$ax^2 + bx + c = a'(x+\alpha)^2 + b'(x+\alpha) + c'\alpha.$$

[9] Avec les notations de la section précédente, on a $X = \Phi_U(x)$ et $X' = \Phi_{U'}(x)$.

Connaissant a, b, c, nous voudrions trouver un moyen pour calculer a', b', c'. Il est facile de vérifier que

$$\begin{array}{rcl} x^2 & = & 1\ (x+\alpha)^2\ -2\alpha\ (x+\alpha)\ +\alpha\ \alpha \\ x & = & 0\ (x+\alpha)^2\ +1\ (x+\alpha)\ -1\ \alpha\ . \\ 1 & = & 0\ (x+\alpha)^2\ +0\ (x+\alpha)\ +\frac{1}{\alpha}\ \alpha \end{array}$$

Ayant à notre disposition les composantes des vecteurs de U dans la base U', il vient

$$\begin{pmatrix} a' \\ b' \\ c' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -2\alpha & 1 & 0 \\ \alpha & -1 & \frac{1}{\alpha} \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix}.$$

Proposition VII.4.5. *Soient U, U' et U'' trois bases de E telles que P est la matrice de changement de base de U à U' et Q la matrice de changement de base de U' à U''. La matrice de changement de base de U à U'' est QP.*

Démonstration. On a

$$u_i = \sum_{j=1}^{n} a_{ji}\, u'_j$$

et

$$u'_k = \sum_{\ell=1}^{n} a'_{\ell k} u''_\ell.$$

Donc

$$u_i = \sum_{j=1}^{n} a_{ji} \left(\sum_{\ell=1}^{n} a'_{\ell j} u''_\ell \right) = \sum_{\ell=1}^{n} \left(\sum_{j=1}^{n} a'_{\ell j} a_{ji} \right) u''_\ell,$$

ce qui suffit car on retrouve exactement la formule du produit matriciel.

■

Il arrive souvent que ce soit les composantes des vecteurs de la nouvelle base U' qui sont données dans la base U. On a dès lors le résultat suivant.

Corollaire VII.4.6. *Si P est la matrice de changement de base de U à U', alors $P' = P^{-1}$ est la matrice de changement de base*[10] *de U' à U. En particulier, si x est un vecteur de E ayant X et X' pour vecteur de composantes dans les bases U et U', alors*

$$X' = P'^{-1} X.$$

Démonstration. Cela résulte de la proposition précédente. Noter que U est toujours inversible car ses colonnes sont les composantes de vecteurs linéairement indépendants.

■

[10] Les colonnes de P' sont formées des composantes des vecteurs de U' dans la base U.

Exemple VII.4.7. Voici un exemple où ce sont les vecteurs de la nouvelle base U' qui sont donnés dans l'ancienne base U. Considérons l'espace $\mathbb{R}^4$ muni de la base canonique $U = (e_1, e_2, e_3, e_4)$. On considère les vecteurs f_1, f_2, f_3, f_4 ayant pour vecteur de composantes dans cette base, respectivement $(1,0,1,0)$, $(1,0,0,1)$, $(1,1,0,1)$ et $(1,1,1,1)$. Il est laissé au lecteur le soin de vérifier que $U' = (f_1, f_2, f_3, f_4)$ forme une base de $\mathbb{R}^4$. Soit x un vecteur quelconque de $\mathbb{R}^4$,

$$x = ae_1 + be_2 + ce_3 + de_4 = a'f_1 + b'f_2 + c'f_3 + d'f_4.$$

Soit la matrice P' donnée par

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

Ainsi, P' est la matrice de changement de base de la base U' à la base U. On a

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} a' \\ b' \\ c' \\ d' \end{pmatrix}$$

et enfin, pour passer des composantes dans la base canonique U à celles dans la base U', il suffit d'inverser P'

$$\begin{pmatrix} a' \\ b' \\ c' \\ d' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & -1 & 0 & 1 \\ 1 & 1 & -1 & -1 \\ -1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}.$$

En particulier, grâce à cette dernière matrice de changement de base, il est à présent facile de retrouver les composantes des vecteurs de l'ancienne base U dans la nouvelle base U'. Il suffit de regarder les colonnes de P'^{-1}.

5. Sous-espaces vectoriels

Définition VII.5.1. Soit E un espace vectoriel. Un sous-ensemble non vide $F \subset E$ est un *sous-espace vectoriel* s'il contient les combinaisons linéaires de ses éléments.

Proposition VII.5.2. *Soit E un espace vectoriel. Le sous-ensemble $F \subset E$ est un sous-espace vectoriel si et seulement si les propositions suivantes sont satisfaites :*

i) $0 \in F$,
ii) *si* $x, y \in F$ *alors* $x + y \in F$,
iii) *si* $x \in F$ *et* $\lambda \in \mathbb{K}$ *alors* $\lambda x \in F$.

Démonstration. C'est immédiat.

■

Notons que l'on peut remplacer la première condition de la proposition précédente par la condition, F non vide, et obtenir un résultat équivalent.

Proposition VII.5.3. *Si F est un sous-espace vectoriel de E, alors F muni des opérations induites par celles de E est un espace vectoriel.*

Démonstration. C'est immédiat.

■

Exemple VII.5.4. Voici quelques sous-espaces vectoriels.

- $\{0\}$ et E sont des sous-espaces vectoriels. On dit que ces sous-espaces sont *triviaux* . Tout sous-espace vectoriel distinct de E et $\{0\}$ est dit *propre*.
- Les fonctions paires définies sur $\mathbb{R}$ forment un sous-espace vectoriel de l'ensemble de fonctions définies sur $\mathbb{R}$.
- Il en va de même de l'ensemble des fonctions périodiques de période P définies sur $\mathbb{R}$.
- Les fonctions polynomiales s'annulant en 1 forment un sous-espace vectoriel de l'espace vectoriel $\mathbb{R}[x]$ des polynômes à coefficients réels.
- Les polynômes dont la somme des coefficients est nulle forment aussi un sous-espace vectoriel de $\mathbb{R}[x]$.
- L'ensemble $\mathbb{R}[x]_d$ est un sous-espace vectoriel de $\mathbb{R}[x]$.
- L'ensemble des solutions d'un système homogène de n équations à p inconnues est un sous-espace vectoriel de $\mathbb{K}^p$.
- Dans le $\mathbb{R}$-vectoriel $\mathbb{R}^n$, les vecteurs satisfaisant l'équation

$$a_1x_1 + \cdots + a_nx_n = 0$$

forment un sous-espace vectoriel[11].

Proposition VII.5.5. *Supposons E de dimension finie n. Si F est un sous-espace vectoriel de E, alors F est de dimension finie, inférieure ou égale à n. De plus, si $\dim F = n$, alors $F = E$.*

Démonstration. Si $F = \{0\}$, alors $\dim F = 0$. Supposons $F \neq \{0\}$. Il existe donc un vecteur non nul appartenant à F. Par le théorème de Steinitz, $n+1$ vecteurs de E ne sont jamais linéairement indépendants. En particulier, $n+1$ vecteurs de F ne sont jamais linéairement indépendants. Soit p le plus grand entier (compris entre 1 et n) pour lequel on peut trouver p vecteurs de F linéairement indépendants. Nommons-les $f_1, \ldots, f_p$. Soit x un vecteur quelconque de F. Par définition de p, il est clair que les vecteurs $f_1, \ldots, f_p, x$ sont linéairement dépendants. Au vu de la proposition VII.2.1, x est donc combinaison linéaire de $f_1, \ldots, f_p$. Cela signifie que F est engendré par $f_1, \ldots, f_p$. Donc $(f_1, \ldots, f_p)$ est une base de F et

$$\dim F = p \leq n.$$

[11] C'est même un hyperplan vectoriel.

Si $p = n$, $f_1, \ldots, f_p$ sont des vecteurs de E linéairement indépendants donc, vu le corollaire VII.3.8, $(f_1, \ldots, f_p)$ est une base de E. Ainsi, F contient une base de E, donc aussi toute combinaison linéaire des vecteurs de cette base, par suite $F = E$.

■

Remarque VII.5.6. En général, l'union de sous-espaces vectoriels ne contient pas les combinaisons linéaires de ses éléments. En effet, considérons le $\mathbb{R}$-vectoriel $\mathbb{R}^2$ ayant $F = \{\begin{pmatrix}\alpha\\0\end{pmatrix} : \alpha \in \mathbb{R}\}$ et $G = \{\begin{pmatrix}-\beta\\\beta\end{pmatrix} : \beta \in \mathbb{R}\}$ comme sous-espaces vectoriels. L'ensemble $F \cup G$ n'est pas un sous-espace vectoriel

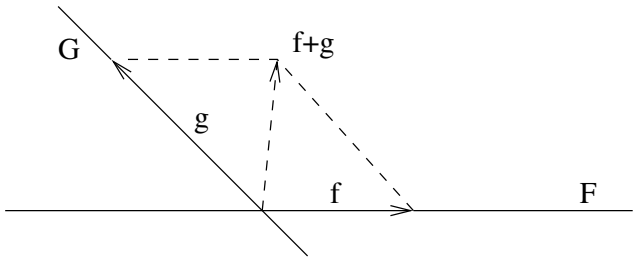


FIGURE VII.3. Union de sous-espaces vectoriels.

car il ne contient pas la somme de ses éléments. Si $f \in F$ et $g \in G$ sont non nuls, alors $f + g \notin F \cup G$.

Par contre, on introduit la somme de sous-espaces vectoriels qui est encore un sous-espace vectoriel.

Proposition VII.5.7. *Soient F et G des sous-espaces vectoriels de E et soit*

$$H = \{f + g \mid f \in F, g \in G\}.$$

Alors H est un sous-espace vectoriel de E. Ce sous-espace H est appelé la somme de F et G et se note $F + G$.

Démonstration. Il est clair que le vecteur nul appartient à H car il appartient à F et à G. Soient $z, z' \in H$. Il existe $f, f' \in F$, $g, g' \in G$ tels que $z = f + g$ et $z' = f' + g'$. Il vient

$$z + z' = (\underbrace{f + f'}_{\in F}) + (\underbrace{g + g'}_{\in G}).$$

Donc $z + z'$ appartient à H. Pour tout $\lambda \in \mathbb{K}$, on a

$$\lambda z = \underbrace{\lambda f}_{\in F} + \underbrace{\lambda g}_{\in G}$$

donc λz appartient à H. On conclut par la proposition VII.5.2.

■

Remarque VII.5.8. Si F et G sont des sous-espaces vectoriels de E, alors $F \subset F+G$ et $G \subset F+G$. En effet, si $x \in F$, alors $x = x+0$ et $0 \in G$ car G est un sous-espace vectoriel. Dès lors, $x \in F+G$ et il s'ensuit que $F \subset F+G$. On procède de la même manière avec G.

Proposition VII.5.9. *Soient F et G des sous-espaces vectoriels de E engendrés respectivement par $x_1, \ldots, x_p$ et $y_1, \ldots, y_q$. Alors $F+G$ est engendré par $x_1, \ldots, x_p, y_1, \ldots, y_q$*

Démonstration. Les vecteurs $x_1, \ldots, x_p, y_1, \ldots, y_q$ appartiennent à F ou à G donc appartiennent tous à $F+G$. Puisque $F+G$ est un sous-espace vectoriel de E, toute combinaison linéaire de ces vecteurs appartient encore à $F+G$. Réciproquement, si $z \in F+G$, alors il existe $f \in F$ et $g \in G$ tels que $z = f+g$. Puisque f (resp. g) est combinaison linéaire de $x_1, \ldots, x_p$ (resp. $y_1, \ldots, y_q$), alors z est combinaison linéaire de $x_1, \ldots, x_p, y_1, \ldots, y_q$.

■

Proposition VII.5.10. *Toute intersection de sous-espaces vectoriels est encore un sous-espace vectoriel.*

Démonstration. C'est immédiat.

■

Définition VII.5.11. Soit A, un sous-ensemble de E. En vertu de la proposition précédente, l'intersection de tous les sous-espaces vectoriels de E contenant A est un sous-espace vectoriel de E qui contient A. C'est le plus petit en ce sens qu'il est inclus dans tout sous-espace vectoriel de E contenant A. On dit que c'est l'*enveloppe linéaire* de A et on le note

$$\rangle A \langle .$$

Par abus de langage, si $x_1, \ldots, x_p$ sont des éléments de E, on appelle *enveloppe linéaire* de $x_1, \ldots, x_p$, l'enveloppe linéaire du sous-ensemble $\{x_1, \ldots, x_p\}$ et on s'autorise à ecrire $\rangle x_1, \ldots, x_p \langle$ au lieu de $\rangle \{x_1, \ldots, x_p\} \langle$.

Proposition VII.5.12. *Soient $J \geq 1$ et $A = \{a_1, \ldots, a_J\}$. Alors*

$$\rangle A \langle = \left\{ \sum_{j=1}^{J} \lambda_j a_j \mid \lambda_j \in \mathbb{K},\ \forall j = 1, \ldots, J \right\}.$$

Démonstration. On procède par double inclusion. Il est clair que si $\lambda_j \in \mathbb{K}$, alors

$$\sum_{j=1}^{J} \lambda_j a_j \in \rangle A \langle .$$

Cela résulte du fait que $\rangle A \langle$ est un sous-espace vectoriel et que, par définition de l'enveloppe linéaire, $a_j \in A \subset \rangle A \langle$.

Pour montrer l'autre inclusion, il suffit de vérifier que

$$\left\{ \sum_{j=1}^{J} \lambda_j a_j \mid \lambda_j \in \mathbb{K},\ \forall j = 1, \ldots, J \right\}$$

est un sous-espace vectoriel de E contenant A. C'est immédiat car

$$\left(\sum_{j=1}^{J} \lambda_j a_j \right) + \left(\sum_{j=1}^{J} \lambda'_j a_j \right) = \sum_{j=1}^{J} (\lambda_j + \lambda'_j) a_j$$

et

$$\lambda \left(\sum_{j=1}^{J} \lambda_j a_j \right) = \sum_{j=1}^{J} (\lambda \lambda_j) a_j.$$

■

On a introduit, à la proposition VII.5.7, la somme de deux sous-espaces vectoriels. Le résultat suivant relie la somme de deux sous-espaces et l'enveloppe linéaire d'un ensemble.

Corollaire VII.5.13. *Si F et G sont des sous-espaces vectoriels de E, alors*

$$F + G = \rangle F \cup G \langle$$

Démonstration. Cela résulte immédiatement de la proposition précédente.

■

Remarque VII.5.14. Si F est un sous-espace vectoriel engendré par les vecteurs $f_1, \ldots, f_p$, alors il est clair que

$$F = \rangle f_1, \ldots, f_p \langle.$$

Théorème VII.5.15. *Si F et G sont des sous-espaces vectoriels de dimension finie*[12]*, alors*

On parle parfois de la formule de Grassman.

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

Démonstration. Soient $x_1, \ldots, x_p$ une base de $F \cap G$. Comme $F \cap G \subset F$ et $F \cap G \subset G$, on peut appliquer le théorème VII.3.5. Il existe donc des vecteurs $y_1, \ldots, y_q$ de F et $z_1, \ldots, z_r$ de G tels que

$$x_1, \ldots, x_p, y_1, \ldots, y_q$$

forment une base de F et

$$x_1, \ldots, x_p, z_1, \ldots, z_r$$

forment une base de G. Par construction, les vecteurs

cf. proposition VII.5.9.

$$x_1, \ldots, x_p, y_1, \ldots, y_q, z_1, \ldots, z_r$$

[12] On retrouve ce genre de "formule" dans d'autres branches des mathématiques. Par exemple, si A et B sont des ensembles finis, alors $\#(A \cup B) = \#A + \#B - \#(A \cap B)$ ou en probabilité, si A et B sont des événements, alors $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$.

engendrent $F+G$. Il suffit de montrer qu'ils sont linéairement indépendants car, dans ce cas,

$$\dim(F+G) = p+q+r, \quad \dim(F\cap G) = p$$

et

$$\dim F = p+q, \quad \dim G = p+r.$$

Supposons que

$$\sum_{i=1}^{p} \lambda_i x_i + \sum_{j=1}^{q} \mu_j y_j + \sum_{k=1}^{r} \nu_k z_k = 0.$$

Le vecteur

$$\sum_{j=1}^{q} \mu_j y_j = -\sum_{i=1}^{p} \lambda_i x_i - \sum_{k=1}^{r} \nu_k z_k$$

appartient à $F\cap G$. Il est donc combinaison linéaire de $x_1,\dots,x_p$. Il existe $\alpha_1,\dots,\alpha_p$ tels que

$$\sum_{j=1}^{q} \mu_j y_j = \sum_{k=1}^{p} \alpha_k x_k.$$

Ainsi,

$$\sum_{k=1}^{p} \alpha_k x_k - \sum_{j=1}^{q} \mu_j y_j = 0.$$

Or les vecteurs $x_1,\dots,x_p,y_1,\dots,y_q$ sont linéairement indépendants ce qui entraîne que $\mu_1 = \cdots = \mu_q = 0$. De là, puisque $x_1,\dots,x_p,z_1,\dots,z_r$ sont linéairement indépendants, on en déduit que $\lambda_1 = \cdots = \lambda_p = \nu_1 = \cdots = \nu_r = 0$. Ceci conclut la preuve.

■

Définition VII.5.16. On dit que la somme $F+G$ de deux sous-espaces vectoriels de E est *directe* si $F\cap G = \{0\}$. Dans ce cas, on écrit

$$F\oplus G.$$

Si $E = F\oplus G$, on dit que G est **un** *supplémentaire* de F dans E. En vertu du théorème précédent, on a bien sûr

$$\dim(F\oplus G) = \dim F + \dim G.$$

Proposition VII.5.17. *Soient F et G, deux sous-espaces vectoriels d'un espace vectoriel E. La somme de F et G est directe si et seulement si tout vecteur x de $F+G$ se décompose de manière unique sous la forme $x = y+z$ avec $y\in F$ et $z\in G$.*

Démonstration. Si la somme de F et G est directe et si $x = y+z = y'+z'$ avec $y,y'\in F$ et $z,z'\in G$, alors, $y-y' = z'-z$ appartient à $F\cap G = \{0\}$ et donc $y = y'$ et $z = z'$.

Réciproquement, nous devons montrer que la somme de F et G est directe. Soit $x \in F \cap G$. Le vecteur

$$\underbrace{x}_{\in F} - \underbrace{x}_{\in G} = \underbrace{0}_{\in F} - \underbrace{0}_{\in G}$$

est dans $F + G$ et par hypothèse, il se décompose de manière unique. Donc $x = 0$.

■

Remarque VII.5.18. Soient F et G, deux sous-espaces vectoriels d'un espace vectoriel E. Il est aussi aisé de vérifier que la somme de F et G est directe si et seulement si toute relation du type $0 = y + z$ avec $y \in F$ et $z \in G$ entraîne $y = z = 0$. En effet, il suffit d'adapter la preuve de la proposition précédente.

Exemple VII.5.19. Soit l'espace vectoriel $\mathbb{R}^3$ muni de la base canonique (e_1, e_2, e_3). Les sous-espaces vectoriels $F = \rangle e_1, e_2 \langle = \{\alpha e_1 + \beta e_2 \mid \alpha, \beta \in \mathbb{R}\}$ et $G = \rangle e_3 \langle = \{\gamma e_3 \mid \gamma \in \mathbb{R}\}$ sont en somme directe et $\mathbb{R}^3 = F \oplus G$.

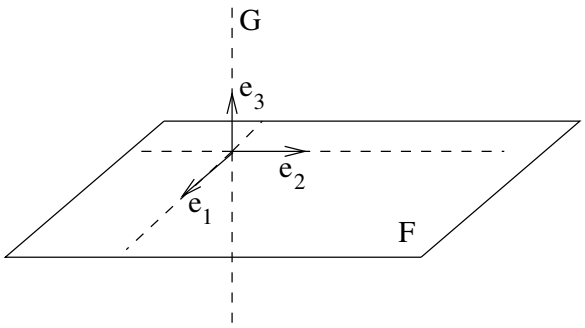


FIGURE VII.4. Sous-espaces en somme directe.

Tout sous-espace vectoriel possède un supplémentaire.

Proposition VII.5.20. *Pour tout sous-espace vectoriel F d'un espace vectoriel E de dimension finie, il existe un sous-espace vectoriel G de E tel que $E = F \oplus G$.*

Démonstration. Soit $(f_1, \ldots, f_p)$ une base de F. Au vu du théorème VII.3.5, il existe des vecteurs $e_{p+1}, \ldots, e_n$ de E tels que

$$f_1, \ldots, f_p, e_{p+1}, \ldots, e_n$$

forment une base de E. Posons $G = \rangle e_{p+1}, \ldots, e_n \langle$. La somme de F et de G est directe car tout vecteur de E possède une unique décomposition comme combinaison linéaire des vecteurs $f_1, \ldots, f_p, e_{p+1}, \ldots, e_n$ donc comme somme d'un élément de F et d'un élément de G. La somme de F et de G est égale à E car $f_1, \ldots, f_p, e_{p+1}, \ldots, e_n$ engendrent E.

■

Remarque VII.5.21. Le supplémentaire n'est en général pas unique. Reprenons l'exemple VII.5.19 où $F = \rangle e_1, e_2 \langle$ et $G = \rangle e_3 \langle$. Il est aisé de vérifier que $H = \rangle e_1 + e_3 \langle$ est aussi un supplémentaire de F dans $\mathbb{R}^3$ (i.e., $\mathbb{R}^3 = F \oplus H$).

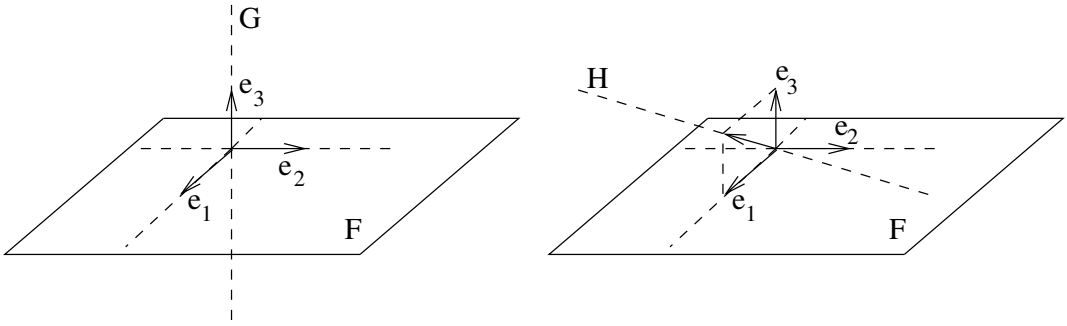


FIGURE VII.5. Deux supplémentaires.

La somme de deux sous-espaces vectoriels peut se généraliser à la somme de $p \geq 2$ sous-espaces.

Remarque VII.5.22. D'une manière générale, si $F_1, \ldots, F_p$ sont des sous-espaces vectoriels de E, on définit la somme de $F_1, \ldots, F_p$ par récurrence en posant

$$F_1 + \cdots + F_p = (F_1 + \cdots + F_{p-1}) + F_p.$$

Par des raisonnements analogues à ceux développés précédemment, il est facile de voir que la somme de $F_1, \ldots, F_p$ est l'enveloppe linéaire de l'union de ces sous-espaces,

$$F_1 + \cdots + F_p = \rangle \bigcup_{i=1}^{p} F_i \langle = \{x_1 + \cdots + x_p \mid x_i \in F_i\}.$$

Au vu de la remarque VII.5.18, on peut définir la somme directe de p sous-espaces vectoriels de la manière suivante.

Définition VII.5.23. La somme de p sous-espaces vectoriels $F_1, \ldots, F_p$ de E est *directe* si

$$(x_1 \in F_1, \ldots, x_p \in F_p \text{ et } x_1 + \cdots + x_p = 0) \Rightarrow x_1 = \cdots = x_p = 0.$$

On écrit

$$F_1 + \cdots + F_p = F_1 \oplus \cdots \oplus F_p = \bigoplus_{i=1}^{p} F_i.$$

Cette condition exprime que le vecteur nul se décompose de manière unique comme somme d'éléments de $F_1, \ldots, F_p$.

Remarque VII.5.24. Lorsque $p = 2$, la condition qui exprime que le vecteur nul se décompose de manière unique comme somme d'un élément de F_1 et d'un élément de F_2 est équivalente à $F_1 \cap F_2 = \{0\}$.

Par contre, si $p > 2$, $F_1 \cap \cdots \cap F_p = \{0\}$ n'entraîne pas que 0 se décompose de manière unique comme somme d'éléments de $F_1, \ldots, F_p$. En effet, considérons $\mathbb{R}^3$ muni de la base canonique (e_1, e_2, e_3) et les sous-espaces $F_1 = \rangle e_1 \langle$, $F_2 = \rangle e_1, e_2 \langle$ et $F_3 = \rangle e_3 \langle$. Il est clair que $F_1 \cap F_2 \cap F_3 = \{0\}$ mais le vecteur nul peut se décomposer d'une infinité de façons

$$\underbrace{\alpha\, e_1}_{\in F_1} + \underbrace{(-\alpha\, e_1 + 0\, e_2)}_{\in F_2} + \underbrace{0\, e_3}_{\in F_3},\ \alpha \in \mathbb{R}.$$

Par exemple, si les vecteurs $u_1, \ldots, u_n$ forment une base de E, alors la somme des sous-espaces $\rangle u_1 \langle, \ldots, \rangle u_n \langle$ est directe.

Proposition VII.5.25. *La somme de p sous-espaces vectoriels $F_1, \ldots, F_p$ de E est directe si et seulement si tout élément x de $F_1 + \cdots + F_p$ se décompose de manière unique sous la forme $x = x_1 + \cdots + x_p$ avec $x_i \in F_i$ pour tout $i \in \{1, \ldots, p\}$.*

La somme de p sous-espaces vectoriels $F_1, \ldots, F_p$ de E est directe si et seulement si la somme de $F_2, \ldots, F_p$ est directe ainsi que la somme de F_1 et $F_2 \oplus \cdots \oplus F_p$. En particulier,

$$\dim(F_1 \oplus \cdots \oplus F_p) = \dim F_1 + \cdots + \dim F_p.$$

Démonstration. Si $x = x_1 + \cdots + x_p = x'_1 + \cdots + x'_p$ avec $x_i, x'_i \in F_i$ pour tout $i \in \{1, \ldots, p\}$, alors

$$0 = \underbrace{(x_1 - x'_1)}_{\in F_1} + \cdots + \underbrace{(x_p - x'_p)}_{\in F_p}.$$

Par la définition de la somme directe de p sous-espaces vectoriels, il vient $x_i = x'_i$ pour tout i. Réciproquement, si tout vecteur de $F_1 + \cdots + F_p$ se décompose de manière unique, en particulier

$$0 = \underbrace{0}_{\in F_1} + \cdots + \underbrace{0}_{\in F_p}$$

et donc la somme de $F_1, \ldots, F_p$ est directe.

Passons à la deuxième partie de la proposition. Supposons que la somme de $F_1, \ldots, F_p$ soit directe. En prenant $x_1 = 0$ dans la définition VII.5.23, on voit que la somme de $F_2, \ldots, F_p$ est directe. Montrons que la somme de F_1 et de $F_2 \oplus \cdots \oplus F_p$ est directe. Au vu de la définition VII.5.16 de la somme directe de deux sous-espaces, il suffit de vérifier que

$$F_1 \cap (F_2 \oplus \cdots \oplus F_p) = \{0\}.$$

Soit x appartenant à $F_1 \cap (F_2 \oplus \cdots \oplus F_p)$. Puisque x appartient à $F_2 \oplus \cdots \oplus F_p$, il existe $x_i \in F_i$, $i \in \{2, \ldots, p\}$ tels que

$$\underbrace{x}_{\in F_1} \underbrace{-x_2}_{\in F_2} - \cdots \underbrace{-x_p}_{\in F_p} = 0.$$

Comme, par hypothèse, la somme de $F_1, \dots, F_p$ est directe, on trouve $x = 0$.

Passons à la réciproque. Soient des vecteurs $x_1, \dots, x_p$ tels que $x_i \in F_i$, $i \in \{1, \dots, p\}$ et

$$x_1 + \cdots + x_p = 0.$$

Il vient,

$$x_1 = -x_2 - \cdots - x_p \in F_1 \cap (F_2 \oplus \cdots \oplus F_p).$$

Puisque la somme de F_1 et de $F_2 \oplus \cdots \oplus F_p$ est directe, on a $x_1 = 0$ et

$$x_2 + \cdots + x_p = 0.$$

De là, puisque la somme de $F_2, \dots, F_p$ est directe, $x_2 = \cdots = x_p = 0$. Ceci prouve que la somme de $F_1, \dots, F_p$ est directe.

Enfin,

$$\begin{aligned} \dim(F_1 \oplus \cdots \oplus F_p) &= \dim(F_1) + \dim(F_2 \oplus \cdots \oplus F_p) \\ &\vdots \\ &= \dim(F_1) + \cdots + \dim(F_p). \end{aligned}$$

■

La remarque suivante sera très utile pour la suite.

Remarque VII.5.26. Soient p sous-espaces vectoriels $F_1, \dots, F_p$ de E tels que $E = F_1 \oplus \cdots \oplus F_p$. Si pour tout $i \in \{1, \dots, p\}$, $(u_{i,1}, \dots, u_{i,d_i})$ est une base de F_i, alors

$$(u_{1,1}, \dots, u_{1,d_1}, \dots, u_{p,1}, \dots, u_{p,d_p})$$

forme une base E. Il est clair que ces vecteurs forment une partie génératrice de E. S'ils n'étaient pas linéairement indépendants, alors la somme ne serait plus directe.

CHAPITRE VIII

Polynômes et fractions rationnelles

On peut bien sûr vouloir étudier les polynômes en tant que tels, simplement comme un nouvel objet mathématique à traiter. Cependant, insistons sur le fait qu'ils interviennent dans la modélisation de nombreux phénomènes (en physique, en analyse numérique, en statistique, ...). Ainsi, il n'est pas rare d'approximer une fonction, par exemple un signal, au moyen d'un développement de Taylor limité. De ce point de vue, l'étude des polynômes revêt un intérêt capital pour appréhender de nombreuses situations tant théoriques qu'appliquées[1].

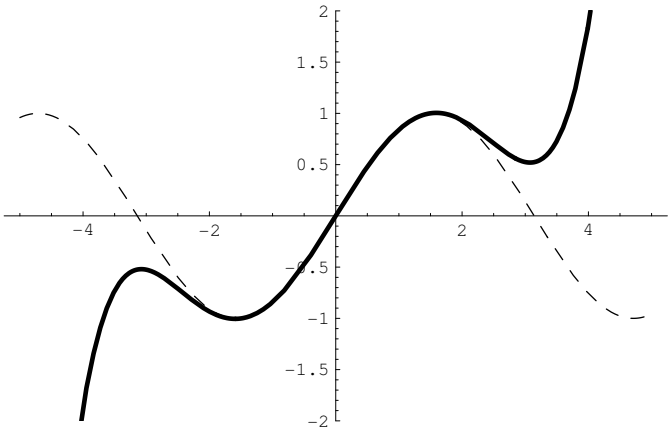


FIGURE VIII.1. Les fonctions $\sin x$ et $x - x^3/3! + x^5/5!$.

1. Polynômes à coefficients dans $\mathbb{C}$

Dans toute la première partie de ce chapitre, le champ $\mathbb{K}$ considéré est l'ensemble $\mathbb{C}$ des nombres complexes.

Définition VIII.1.1. Une fonction P définie sur $\mathbb{C}$ et à valeurs complexes est un *polynôme* (aussi appelée *fonction polynomiale*) s'il existe des nombres complexes $c_0, c_1, \ldots, c_k \in \mathbb{C}$ tels que

$$P(z) = c_0 + c_1\, z + \cdots + c_k\, z^k$$

[1]Par exemple, un théorème de Weierstrass stipule que l'ensemble des polynômes est dense dans l'ensemble $C_0([a,b])$ des fonctions continues sur $[a,b]$ pour $||\cdot||_\infty$

pour tout $z \in \mathbb{C}$. S'il est nécessaire de rappeler le contexte dans lequel on se trouve, on parlera de *polynôme à coefficients complexes*. L'ensemble des polynômes à coefficients complexes se note $\mathbb{C}[z]$.

Commençons par quelques rappels d'analyse mathématique. Soit f une fonction définie sur un ouvert Ω de $\mathbb{R}^2$. Cette fonction est *dérivable par rapport à* x (resp. y) en (x_0, y_0) si la limite

$$\lim_{h\to 0, h\neq 0} \frac{f[(x_0,y_0)+h(1,0)] - f(x_0,y_0)}{h}$$

$$(\text{resp. } \lim_{h\to 0, h\neq 0} \frac{f[(x_0,y_0)+h(0,1)] - f(x_0,y_0)}{h})$$

existe et est finie. On la note $[D_x f]_{(x_0,y_0)}$ ou encore $[\frac{\partial}{\partial x} f]_{(x_0,y_0)}$ (resp. $[D_y f]_{(x_0,y_0)}$ ou encore $[\frac{\partial}{\partial y} f]_{(x_0,y_0)}$). La fonction f est *dérivable sur* Ω si elle est dérivable par rapport à x et à y en tout point de Ω. Elle est *continûment dérivable sur* Ω (on dit aussi qu'elle est de classe C_1 sur Ω) si elle est dérivable sur Ω et si $D_x f$ et $D_y f$ sont des fonctions continues sur Ω. Enfin, f est p *fois continûment dérivable sur* Ω (ou de classe C_p) si elle admet toutes les dérivées partielles d'ordre $m \leq p$ (i.e., $D_x^i D_y^{m-i} f$, $i = 0, \ldots, m$) et si ces dernières sont continues sur Ω. De plus, f est *infiniment continûment dérivable sur* Ω (ou de classe C_∞ sur Ω) si elle est de classe C_p pour tout $p \geq 0$.

Rappelons aussi qu'une fonction f définie sur une partie A de $\mathbb{R}^2$ est continue sur A si et seulement si, pour tout $x \in A$ et toute suite $(x_n)_{n\geq 0}$ de A qui converge vers x, la suite $(f(x_n))_{n\geq 0}$ converge vers $f(x)$.

Remarque VIII.1.2. Nous pouvons appliquer les définitions ci-dessus en identifiant $z \in \mathbb{C}$ à $(\mathfrak{Re}\, z, \mathfrak{Im}\, z) \in \mathbb{R}^2$. Nous attirons cependant l'attention du lecteur sur le fait que l'on peut aussi définir, pour les fonctions $f : \mathbb{C} \to \mathbb{C}$, une notion de "dérivabilité au sens complexe" (qui est plus forte que simplement supposer l'existence des dérivées partielles $D_x f$ et $D_y f$). On introduit alors, dans ce cadre, la notion de *fonction holomorphe* qui sera développée en deuxième année.

En particulier, la fonction $f : \mathbb{C} \to \mathbb{C},\ z \mapsto z$ est trivialement continue sur $\mathbb{C}$ (en appliquant le critère par les suites rappelé ci-dessus). Puisque le produit de fonctions continues est continu, pour tout $m \geq 1$, la fonction z^m est aussi continue sur $\mathbb{C}$.

Proposition VIII.1.3. *Tout polynôme P est une fonction de classe C_∞ sur $\mathbb{C} = \mathbb{R}^2$.*

Démonstration. Soit $m \in \mathbb{N}$. Si $z = x + iy$, alors[2]

$$D_x z^m = D_x (x+iy)^m = m(x+iy)^{m-1} = m\, z^{m-1}$$

[2]Voici le détail du calcul, on a

$$D_x z^m = \lim_{h\to 0} \frac{(x+iy+h)^m - (x+iy)^m}{h}.$$

et

$$D_y z^m = D_y(x+iy)^m = i\,m(x+iy)^{m-1} = i\,m\,z^{m-1}.$$

Il est dès lors clair que la fonction $P : z \mapsto z^m$ est de classe C_∞ sur $\mathbb{C} = \mathbb{R}^2$. La conclusion résulte de la linéarité des opérateurs de dérivation D_x et D_y. Autrement dit, on a $D_x(\sum_i a_i z^i) = \sum_i a_i\, D_x z^i$.

■

Il est commode d'introduire deux opérateurs de dérivation particuliers :

$$D_z = \frac{1}{2}(D_x - iD_y) \text{ et } D_{\overline{z}} = \frac{1}{2}(D_x + iD_y)$$

il s'agit en fait d'un simple raccourci d'écriture,

$$D_z f = \frac{1}{2}(D_x f - iD_y f) \text{ et } D_{\overline{z}} f = \frac{1}{2}(D_x f + iD_y f).$$

L'opérateur $D_{\overline{z}}$ est appelé *opérateur de Cauchy-Riemann*. Il résulte des calculs effectués dans la preuve précédente que

$$D_z z^m = \frac{1}{2}(D_x z^m - iD_y z^m) = mz^{m-1}$$

et

$$D_{\overline{z}} z^m = \frac{1}{2}(D_x z^m + iD_y z^m) = 0.$$

Remarquons que, par linéarité, si $P \in \mathbb{C}[z]$, alors $D_{\overline{z}} P = 0$.

Remarque VIII.1.4. Si $f : \mathbb{C} \to \mathbb{C}$ est dérivable par rapport à x et à y en z_0 quand $\mathbb{C}$ est identifié à $\mathbb{R}^2$, alors pour que f soit une fonction holomorphe en z_0, elle doit de plus satisfaire $(D_{\overline{z}} f)(z_0) = 0$.

Proposition VIII.1.5. *Si $\ell \leq m$, on a*

On a aussi $D_z^\ell z^{[m]} = z^{[m-\ell]}$.

$$D_z^\ell \frac{z^m}{m!} = \frac{z^{m-\ell}}{(m-\ell)!}$$

et si $\ell > m$,

$$D_z^\ell \frac{z^m}{m!} = 0.$$

En particulier, si $P = c_0 + c_1 z + \cdots + c_k z^k$, alors

$$\frac{1}{m!} D_z^m P = \sum_{i=m}^{k} c_i\, \mathrm{C}_i^m\, z^{i-m},\ m \in \{0, \ldots, k\}$$

et

$$c_m = \frac{1}{m!}(D_z^m P)(0),\ m \in \{0, \ldots, k\}.$$

Ensuite, si l'on se rappelle que $a^m - b^m = (a-b)(a^{m-1} + a^{m-2}b + \cdots + b^{m-1})$, alors on trouve

$$D_x z^m = \lim_{h \to 0} \frac{h\,[(x+iy+h)^{m-1} + (x+iy+h)^{m-2}(x+iy) + \cdots + (x+iy)^{m-1}]}{h} = m(x+iy)^{m-1}.$$

Démonstration. Les deux premières formules sont immédiates. Soient $m \in \{0, \dots, k\}$ et $i \geq m$, il vient

$$\frac{1}{m!} D_z^m (c_i\, z^i) = \frac{i!}{m!} D_z^m (c_i\, \frac{z^i}{i!}) = c_i\, \frac{i!}{m!}\, \frac{z^{i-m}}{(i-m)!} = c_i\, \mathrm{C}_i^m\, z^{i-m}$$

d'où la conclusion par linéarité de D_z. De plus, $c_i\, \mathrm{C}_i^m\, z^{i-m}$ évalué en 0 est nul si $i > m$.

■

Définition VIII.1.6. Si le polynôme $P = c_0 + c_1 z + \cdots + c_k z^k$ diffère de la fonction nulle, alors au moins un de ses coefficients c_m est non nul[3]. On définit le *degré* de $P \neq 0$ comme étant le plus grand entier $m \geq 0$ tel que $c_m \neq 0$. Ce nombre m est noté $\deg P$ et on dit que c_m est le *coefficient dominant* de P. Dans cette définition, on n'attribue pas de degré à la fonction nulle. Par convention[4], le degré de la fonction nulle est $-\infty$. On désigne par $\mathbb{C}[z]_k$, l'ensemble des polynômes de degré au plus k.

Remarque VIII.1.7. Une conséquence de la proposition VIII.1.5 est que si deux fonctions polynomiales $P = c_0 + \cdots + c_k z^k$ et $Q = d_0 + \cdots + d_\ell z^\ell$ sont égales (i.e., si pour tout $z \in \mathbb{C}$, on a $P(z) = Q(z)$), alors $\deg P = \deg Q$. En effet, supposons $k > \ell$. Dans ce cas, $D_z^k P \neq 0$ et $D_z^k Q = 0$, ce qui est impossible car si deux fonctions sont égales, leurs dérivées le sont aussi. De plus, il est aisé de vérifier[5], en appliquant le même raisonnement, que pour tout $i \in \{0, \dots, k\}$ et en évaluant les dérivées D_z^i en 0,

On serait à présent en mesure de redémontrer le théorème multinomial de la remarque I.9.9.

$$c_i = d_i.$$

Proposition VIII.1.8. *Soient $P = c_0 + \cdots + c_k\, z^k$ et $Q = d_0 + \cdots + d_\ell\, z^\ell$ deux polynômes. Pour tous $\alpha, \beta \in \mathbb{C}$, on a*

$$\deg(\alpha P + \beta Q) \leq \sup(\deg P, \deg Q).$$

Si P et Q sont non nuls, alors le produit de P et de Q est un polynôme et

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

Démonstration. C'est immédiat.

■

[3]En effet, par contraposition, si tous les coefficients sont nuls, alors le polynôme est la fonction nulle.

[4]La justification de cette convention prendra tout son sens lorsqu'on introduira la division euclidienne des polynômes, cf. théorème VIII.5.1. En fait, elle permet d'étendre la proposition VIII.1.8 au cas de polynômes nuls. En effet, si cette proposition s'applique à $Q = 0$, alors pour tout $P \in \mathbb{C}[z]$, $\deg(P.0) = \deg 0 = \deg P + \deg 0$, ce qui n'a de sens qu'en posant $\deg 0 = -\infty$ et en supposant que $r + (-\infty) = -\infty$ pour tout réel r.

[5]Cette remarque qui montre l'équivalence entre polynôme (donné par une suite finie de coefficients $c_0, \dots, c_k$) et fonction polynomiale ($P : \mathbb{C} \to \mathbb{C}$) est uniquement valable pour les polynômes à coefficients complexes (ou réels). En effet, nous avons rencontré des situations où deux polynômes distincts donnaient lieu à la même fonction polynomiale.

Proposition VIII.1.9 (Formule de Taylor). *Soient P un polynôme de degré k et $z_0 \in \mathbb{C}$. Pour tout $z \in \mathbb{C}$, on a*

$$\boxed{P(z) = \sum_{i=0}^{k} \frac{(D_z^i P)(z_0)}{i!} \, (z - z_0)^i.}$$

Exemple VIII.1.10. La formule de Taylor permet d'exprimer un polynôme, non pas en termes de puissances de z, mais comme une combinaison linéaire de puissances de $(z - z_0)$ pour un z_0 choisi. Ainsi considérons le polynôme $P(z) = z^2 + 2i\,z - 3$. Nous voudrions, par exemple, l'exprimer sous la forme $P(z) = a(z-1)^2 + b(z-1) + c$. Au vu de la formule ci-dessus, on a

$$c = P(1) = -2 + 2i, \;\; b = (D_z P)(1) = 2 + 2i, \;\; a = \frac{(D_z^2 P)(1)}{2} = 1$$

et donc

$$P(z) = z^2 + 2i\,z - 3 = (z-1)^2 + (2+2i)(z-1) - 2 + 2i.$$

Démonstration. Supposons que

$$P(z) = \sum_{i=0}^{k} c_i \, z^i.$$

Il vient

$$\begin{aligned}
P(z) &= \sum_{i=0}^{k} c_i \, (z - z_0 + z_0)^i \\
&= \sum_{i=0}^{k} c_i \sum_{j=0}^{i} \mathrm{C}_i^j \, (z - z_0)^j \, z_0^{i-j} \\
&= \sum_{j=0}^{\mathbf{k}} \left(\sum_{i=\mathbf{j}}^{k} c_i \, \mathrm{C}_i^j \, z_0^{i-j} \right) (z - z_0)^j, \text{ en permutant les sommes} \\
&= \sum_{j=0}^{k} \frac{(D_z^j P)(z_0)}{j!} (z - z_0)^j
\end{aligned}$$

où, à la deuxième ligne, on a utilisé la formule du binôme de Newton (cf. proposition I.9.7) et à la dernière ligne, on a utilisé la proposition VIII.1.5.

■

2. Zéros d'un polynôme

Dans un cadre général de polynômes à coefficients dans un corps quelconque $\mathbb{K}$, il est naturel définir un élément $z_0 \in \mathbb{K}$ comme zéro α-uple d'un polynôme $P \in \mathbb{K}[z]$, si $(z - z_0)^\alpha$ divise P et $(z - z_0)^{\alpha+1}$ ne divise pas P. Dans le cas de polynômes de $\mathbb{C}[z]$, on peut également prendre une définition faisant intervenir les dérivées de P. La proposition VIII.2.3 nous montrera rapidement que les deux approches sont équivalentes.

Définition VIII.2.1. Soient $P \in \mathbb{C}[z]$ et $z_0 \in \mathbb{C}$. On dit que z_0 est un *zéro* de P si

$$P(z_0) = 0.$$

On dit que la *multiplicité* de z_0 est α ou encore que z_0 est un zéro α-uple ($\alpha \in \mathbb{N} \setminus \{0\}$), si

$$P(z_0) = (D_z P)(z_0) = \cdots = (D_z^{\alpha-1} P)(z_0) = 0 \quad \text{et} \quad (D_z^{\alpha} P)(z_0) \neq 0.$$

Ainsi, si $\alpha = 1$ (resp. 2, 3), on parle de zéro *simple* (resp. *double*, *triple*).

Exemple VIII.2.2. Le polynôme

$$P(z) = z^4 + (6-2i)z^3 + (12-10i)z^2 + (8-16i)z - 8i = (z+1-i)^2(z+2)^2$$

possède $-1+i$ comme zéro double. En effet, $P(-1+i) = 0$,

$$D_z P = 4z^3 + (18-6i)z^2 + (24-20i)z + 8 - 16i = (z+1-i)(z+2)(4z+6-2i)$$

et donc $(D_z P)(-1+i) = 0$. Enfin,

$$D_z^2 P = 12z^2 + (36-12i)z + 24 - 20i \quad \text{et } (D_z^2 P)(-1+i) = 4i \neq 0.$$

Proposition VIII.2.3. *Un nombre complexe z_0 est zéro α-uple d'un polynôme P si et seulement s'il existe un polynôme Q tel que*

$$P(z) = (z - z_0)^{\alpha} Q(z) \quad \text{et} \quad Q(z_0) \neq 0.$$

De plus, les zéros de P distincts de z_0 sont les zéros de Q et la multiplicité d'un tel zéro de P est égale à la multiplicité de ce zéro en tant que zéro de Q.

Démonstration. Soit P un polynôme de degré k. Montrons que la condition est nécessaire et supposons que z_0 est un zéro α-uple de P. Par la formule de Taylor, il vient

$$P(z) = \sum_{i=\alpha}^{k} \frac{(D_z^i P)(z_0)}{i!} (z - z_0)^i = (z - z_0)^{\alpha} \underbrace{\left(\sum_{i=\alpha}^{k} \frac{(D_z^i P)(z_0)}{i!} (z - z_0)^{i-\alpha} \right)}_{:= Q(z)}.$$

On conclut en remarquant que $Q(z_0)$ diffère de zéro car $(D_z^{\alpha} P)(z_0) \neq 0$.

Passons à la réciproque et supposons que

$$P(z) = (z - z_0)^{\alpha} Q(z) \quad \text{avec} \quad Q(z_0) \neq 0.$$

Par la formule de Leibniz[6], il vient pour $m \leq \alpha$,

$$D_z^m((z - z_0)^{\alpha} Q(z)) = \sum_{i=0}^{m} \mathrm{C}_m^i \, D_z^i (z - z_0)^{\alpha} \; D_z^{m-i} Q(z).$$

Si on évalue cette dérivée en z_0, on trouve

$$D_z^m((z - z_0)^{\alpha} Q(z))(z_0) = \begin{cases} \alpha! \, Q(z_0) & \text{si } m = \alpha \\ 0 & \text{si } 0 \leq m < \alpha \end{cases}$$

[6] cf. le cours d'analyse.

car si $0 \leq i < \alpha$, alors $(D_z^i(z-z_0)^\alpha)(z_0) = 0$. Cela signifie ainsi que z_0 est un zéro α-uple de P.

Passons à la seconde partie de la preuve. Tout d'abord, il est clair que les zéros de P distincts de z_0 et les zéros de Q coïncident. Soit z_1 un zéro de Q de multiplicité β. En appliquant une fois encore la formule de Leibniz, on a

$$D_z^m P(z) = \sum_{i=0}^{m} \mathrm{C}_m^i \, D_z^{m-i}(z-z_0)^\alpha \, D_z^i Q(z).$$

Si $m < \beta$, alors $(D_z^i Q)(z_1) = 0$ pour tout $i \leq m$ et on en conclut que $(D_z^m P)(z_1) = 0$. Si $m = \beta$, alors

$$(D_z^\beta P)(z_1) = (z_1 - z_0)^\alpha (D_z^\beta Q)(z_1) \neq 0.$$

Ceci signifie que z_1 est un zéro β-uple de P.

■

3. Théorème fondamental de l'algèbre

Nous arrivons à présent au résultat, appelé *théorème fondamental de l'algèbre* ou encore théorème de Gauss-d'Alembert, qui stipule qu'un polynôme à coefficients complexes de degré k possède exactement k zéros (comptés avec leur multiplicité). Deux lemmes utilisant quelque peu l'analyse (et la topologie de $\mathbb{C}$) sont tout d'abord nécessaires.

Lemme VIII.3.1 (Lemme de Gauss). *Soient Ω un ouvert[7] de $\mathbb{C}$ et P un polynôme à coefficients complexes de degré $m \geq 1$. Si $z_0 \in \Omega$ est tel que*

$$|P(z_0)| = \inf_{z \in \Omega} |P(z)|,$$

alors z_0 est un zéro de P.

Démonstration. Procédons par l'absurde et supposons que $P(z_0) \neq 0$. Puisque P est un polynôme de degré au moins un, il existe[8] un entier $k \geq 1$ tel que $(D_z^k P)(z_0) \neq 0$. On peut même supposer que k est le plus petit entier ayant cette propriété. Ainsi, pour tout ℓ tel que $\ell \in \{1, \ldots, k-1\}$, on a

$$(D_z^\ell P)(z_0) = 0.$$

En appliquant la formule de Taylor, on obtient

$$\begin{aligned} P(z) &= \sum_{i=0}^{m} \frac{(D_z^i P)(z_0)}{i!} (z-z_0)^i \\ &= P(z_0) + \frac{(D_z^k P)(z_0)}{k!} (z-z_0)^k + \sum_{i=k+1}^{m} \frac{(D_z^i P)(z_0)}{i!} (z-z_0)^i. \end{aligned}$$

[7] Pour rappel, un ensemble Ω est un ouvert si tout point de Ω est le centre d'une boule incluse dans Ω.

[8] Justifier!

Puisque $P(z_0) \neq 0$, cela se réécrit

$$P(z) = P(z_0)\left(1 + \frac{(D_z^k P)(z_0)}{k!\,P(z_0)}\,(z-z_0)^k + (z-z_0)^{k+1}\,Q(z)\right)$$

où Q est un polynôme. Soit α un nombre complexe tel que

$$\alpha^k = -\frac{k!\,P(z_0)}{(D_z^k P)(z_0)}.$$

Au vu de la formule précédente, pour tout $t \in]0,1[$,

$$P(z_0 + t\,\alpha) = P(z_0)\left(1 + \underbrace{\frac{(D_z^k P)(z_0)}{k!\,P(z_0)}\,\alpha^k}_{=-1}\,t^k + t^{k+1}\,\alpha^{k+1}\,Q(z_0 + t\,\alpha)\right).$$

Ainsi[9],

$$|P(z_0 + t\,\alpha)| \leq (1-t^k)\,|P(z_0)| + t^{k+1}\,|P(z_0)\,\alpha^{k+1}\,Q(z_0 + t\,\alpha)|.$$

Observons que[10]

$$\lim_{t\to 0^+} t\,\alpha^{k+1}\,Q(z_0 + t\,\alpha) = 0.$$

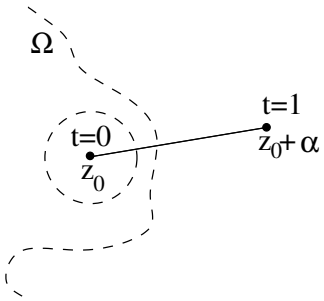


FIGURE VIII.2. Un point du segment $\{(1-t)z_0 + t(z_0+\alpha) = z_0 + t\alpha \mid t \in [0,1]\}$.

En d'autres termes, cela signifie[11] qu'il existe ε tel que, si $0 < t < \varepsilon$,

$$z_0 + t\,\alpha \in \Omega \quad \text{et} \quad t\,|\alpha^{k+1}\,Q(z_0 + t\,\alpha)| < 1.$$

Par conséquent, si $0 < t < \varepsilon$, on a

$$|P(z_0 + t\,\alpha)| < (1-t^k)|P(z_0)| + t^k|P(z_0)| = |P(z_0)|.$$

On vient donc de trouver un point de Ω tel que le module de P évalué en ce point soit strictement inférieur à $|P(z_0)| = \inf_{z\in\Omega} |P(z)|$. C'est impossible.

■

[9]Puisque $t \in]0,1[$, on a $1 - t^k > 0$ et $|1 - t^k| = 1 - t^k$.

[10]En effet, $P(z_0)$ et α^{k+1} ne dépendent pas de t et Q est une fonction polynomiale donc continue. Ainsi, $\lim_{t\to 0^+} Q(z_0 + t\,\alpha) = Q(z_0)$.

[11]On utilise ici le fait que Ω est un ouvert et que $z_0 \in \Omega$. L'autre observation est une simple traduction de la limite.

Exemple VIII.3.2. Voici une illustration graphique du lemme de Gauss. On considère le polynôme

$$P(z) = z^3 - 1$$

qui possède les zéros $1, \omega, \omega^2$ (cf. le chapitre sur les nombres complexes et la figure I.9). On a représenté à la figure VIII.3 le graphique de la fonction $|P(z)|$ et les courbes de niveau correspondantes. Nous espérons que cet exemple pourra donner une interprétation visuelle du lemme de Gauss.

Lemme VIII.3.3 (d'Alembert). *Tout polynôme P de $\mathbb{C}[z]$ de degré au moins 1 possède un zéro dans $\mathbb{C}$.*

Démonstration. Nous devons montrer que tout polynôme P de degré au moins un possède au moins un zéro. D'une part, on sait que

$$\lim_{z\to\infty} P(z) = \infty.$$

Ainsi, il existe $R > 0$ tel que

$$|z| \geq R \Rightarrow |P(z)| \geq |P(0)| + 1.$$

D'autre part, vu le théorème des bornes atteintes[12], la borne inférieure de la fonction $z \mapsto |P(z)|$ réelle et continue sur le compact $K = \{z \in \mathbb{C} : |z| \leq R\}$ est réalisée en un point z_0, i.e.,

$$|P(z_0)| = \inf_{z\in K} |P(z)|.$$

En particulier, 0 appartient à K et donc

$$|P(z_0)| \leq |P(0)|.$$

Cela entraîne donc[13] que $|z_0| < R$ et donc z_0 est un point de l'ouvert $\Omega = \{z \in \mathbb{C} : |z| < R\}$ tel que

$$|P(z_0)| = \inf_{z\in\Omega} |P(z)|.$$

En vertu du lemme de Gauss, z_0 est un zéro de P.

■

[12] cf. le cours d'analyse : si la fonction f est réelle et continue sur le compact non vide K de $\mathbb{R}^n$, alors il existe x_0 et y_0 dans K tels que

$$f(x_0) = \inf_{x\in K} f(x) \quad \text{et} \quad f(y_0) = \sup_{x\in K} f(x).$$

[13] C'est simplement la contraposition de

$$|z| \geq R \Rightarrow |P(z)| \geq |P(0)| + 1.$$

En effet, nous avons ici $|P(z_0)| \leq |P(0)|$, ce qui signifie que $|P(z_0)| < |P(0)| + 1$. En particulier, cela précise pourquoi nous avions introduit, au début de cette démonstration et de manière un peu artificielle, cette constante 1.

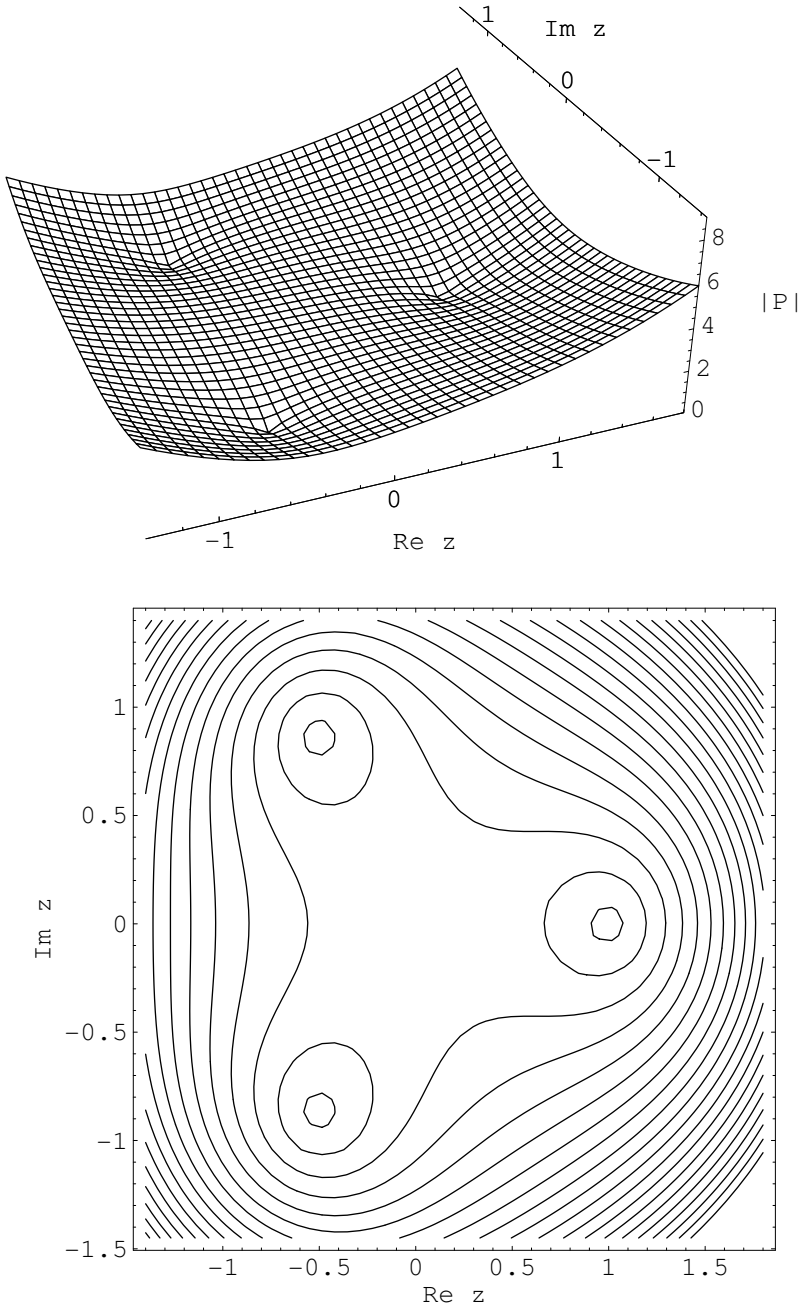


FIGURE VIII.3. Le graphique de $|z^3 - 1|$ et les courbes de niveau correspondantes.

Théorème VIII.3.4 (Théorème fondamental de l'algèbre). *Tout polynôme P de degré $k \geq 1$ possède exactement k zéros si on les compte avec leur multiplicité. Ainsi, si $z_1, \ldots, z_m$ sont les m $(m \leq k)$ zéros de P de multiplicité*

respective $\alpha_1, \ldots, \alpha_m$, *alors*

$$\alpha_1 + \cdots + \alpha_m = k,$$

et si c_k *est le coefficient dominant de* P, *alors*

$$P(z) = c_k \prod_{i=1}^{m} (z - z_i)^{\alpha_i}.$$

Démonstration. On procède par récurrence sur k. Si $k = 1$, le polynôme P est de la forme

$$c_1\, z + c_0, \quad c_1 \neq 0.$$

Ainsi, $-c_0/c_1$ est l'unique zéro simple de P. Supposons le résultat satisfait pour les polynômes de degré strictement inférieur à k et vérifions-le pour un polynôme P de degré $k > 1$. Au vu du lemme précédent, P possède au moins un zéro z_1 de multiplicité $\alpha_1 \geq 1$. Ainsi, par la proposition VIII.2.3, on a

$$P(z) = (z - z_1)^{\alpha_1}\, Q(z)$$

avec $Q(z)$ un polynôme tel que $Q(z_1) \neq 0$. De la proposition VIII.1.8, on tire

$$\deg Q = \deg P - \alpha_1 < \deg P.$$

On peut donc appliquer l'hypothèse de récurrence à Q. Ce dernier polynôme possède des zéros $z_2, \ldots, z_m$ de multiplicité respective $\alpha_2, \ldots, \alpha_m$ tels que

$$\alpha_2 + \cdots + \alpha_m = \deg Q = \deg P - \alpha_1$$

et

$$Q(z) = d \prod_{i=2}^{m} (z - z_i)^{\alpha_i}$$

où d est le coefficient dominant de Q. La proposition VIII.2.3 stipule en outre que les zéros de P distincts de z_1 coïncident avec ceux de Q et possèdent la même multiplicité. Ainsi, les zéros de P sont $z_1, z_2, \ldots, z_m$ de multiplicité $\alpha_1, \alpha_2, \ldots, \alpha_m$ et on a

$$\alpha_1 + (\alpha_2 + \cdots + \alpha_m) = \alpha_1 + (\deg_P - \alpha_1) = \deg P.$$

Il est clair que le coefficient dominant de Q est égal à celui de P, donc

$$P = d \prod_{i=1}^{m} (z - z_i)^{\alpha_i}.$$

■

Remarque VIII.3.5. Le théorème précédent est *existentiel*. Cela signifie simplement qu'il assure, pour un polynôme de degré k, l'existence de k zéros comptés avec leur multiplicité. La preuve ne fournit pas de moyen explicite pour la recherche de ces zéros. Nous avons vu dans le chapitre dédié aux nombres complexes qu'il existait des méthodes pour la recherche des zéros d'un polynôme de degré au plus 4 (se rappeler en particulier la méthode de Cardan). Pour un polynôme arbitraire de degré 5 ou plus, on utilise alors

des méthodes d'analyse numérique pour la recherche de valeurs approchées des zéros.

Voici quelques conséquences directes du résultat précédent.

Corollaire VIII.3.6. *Soient P et Q deux polynômes.*

i) *Si P et Q ont les mêmes zéros avec les mêmes multiplicités, alors il existe une constante $c \in \mathbb{C} \setminus \{0\}$ telle que $P = cQ$.*

ii) *Si P et Q sont deux polynômes de degré k égaux en $k+1$ points, alors ils sont égaux.*

Démonstration. Le premier point découle directement du théorème fondamental de l'algèbre. Passons au second point. Si P et Q sont égaux en $k+1$ points, alors le polynôme $P - Q$ est un polynôme de degré au plus k qui possède $k+1$ zéros distincts. Cela implique que $P - Q = 0$.

■

La proposition suivante généralise la règle de la somme et du produit des racines d'une équation polynomiale du deuxième degré.

Proposition VIII.3.7 (Formules de Viète[14]). *Soit $P = c_0 + \cdots + c_n z^n$ un polynôme de $\mathbb{C}[z]$ ayant $z_1, \ldots, z_n$ comme zéros répétés selon leur multiplicité. On a*

$$\begin{aligned}
\textstyle\sum_{1 \le i \le n} z_i &= -\tfrac{c_{n-1}}{c_n} \\
\textstyle\sum_{1 \le i_1 < i_2 \le n} z_{i_1} z_{i_2} &= \tfrac{c_{n-2}}{c_n} \\
\textstyle\sum_{1 \le i_1 < i_2 < i_3 \le n} z_{i_1} z_{i_2} z_{i_3} &= -\tfrac{c_{n-3}}{c_n} \\
&\vdots \\
\textstyle\sum_{1 \le i_1 < \cdots < i_{n-1} \le n} z_{i_1} \cdots z_{i_{n-1}} &= (-1)^{n-1} \tfrac{c_1}{c_n} \\
z_1 \cdots z_n &= (-1)^n \tfrac{c_0}{c_n}.
\end{aligned}$$

Démonstration. Au vu du théorème fondamental de l'algèbre, P s'écrit aussi

$$c_n (z - z_1)(z - z_2) \cdots (z - z_n).$$

En distribuant les différents produits et en identifiant le coefficient de z^j avec c_j, $j = 0, \ldots, n-1$, on trouve immédiatement le résultat annoncé. Par exemple, en distribuant, le terme indépendant est $c_n (-1)^n z_1 \cdots z_n$ or ce terme vaut c_0.

■

4. Estimation des zéros

Nous avons vu que le théorème fondamental de l'algèbre est existentiel (cf. remarque VIII.3.5). Il ne fournit aucun renseignement sur les n zéros d'un polynôme de degré n. Cependant, il est possible d'obtenir des estimations quant à la localisation de ces zéros.

[14] François Viète, mathématicien français du XVIè siècle.

Théorème VIII.4.1 (Règle de Descartes). *Soit $P \in \mathbb{C}[z]$ un polynôme de degré n de la forme $c_0 + c_1\, z + \cdots + c_n\, z^n$. Les zéros de P appartiennent au disque fermé $\{z \in \mathbb{C} : |z| \leq R\}$ où*

$$R = 1 + \max_{k\in\{0,\ldots,n-1\}} \left|\frac{c_k}{c_n}\right|.$$

Démonstration. Posons $C = \max_{k\in\{0,\ldots,n-1\}} |c_k|$. Ainsi, $R = 1 + \frac{C}{|c_n|}$. Supposons $|z| > R$. Nous allons montrer que $P(z) \neq 0$. D'où le résultat annoncé en considérant la contraposée[15] ($P(z) = 0 \Rightarrow |z| \leq R$). Puisque $|z| > R$, en particulier, $|z| > 1$. On a

$$|P(z) - c_n\, z^n| = |c_0 + \cdots + c_{n-1}\, z^{n-1}| \leq C \sum_{j=0}^{n-1} |z|^j.$$

Puisque nous sommes en présence d'une progression géométrique de raison $|z|$, il vient

$$\sum_{j=0}^{n-1} |z|^j = \frac{|z|^n - 1}{|z| - 1} = \frac{|z|^n}{|z| - 1} - \frac{1}{|z| - 1} < \frac{|z|^n}{|z| - 1}$$

où pour obtenir la dernière inégalité, nous avons utilisé le fait que $|z| > 1$. En conclusion, il vient

$$|P(z) - c_n\, z^n| < \frac{C\,|z|^n}{|z| - 1}.$$

Or $|z| > R$. Donc $|z| - 1 > \frac{C}{|c_n|}$ et

$$|P(z) - c_n\, z^n| < |c_n\, z^n|.$$

Au vu de la proposition I.4.5 iii), on a

$$|\,|P(z)| - |c_n\, z^n|\,| \leq |P(z) - c_n\, z^n| < |c_n\, z^n|.$$

En particulier, on a $|c_n\, z^n| - |P(z)| < |c_n\, z^n|$ et donc $|P(z)| > 0$. Ceci achève la preuve.

si $|a - b| < c$, alors $a - b < c$ et $b - a < c$.

■

Corollaire VIII.4.2. *Avec les mêmes notations que dans le théorème précédent, les éventuels zéros réels de P appartiennent à l'intervalle $[-R, R]$.*

5. Division de polynômes

On peut munir l'ensemble $\mathbb{C}[z]$ de la division euclidienne de la manière suivante.

Théorème VIII.5.1 (Division euclidienne). *Soit D un polynôme non nul. Pour tout polynôme P, il existe des polynômes uniques Q et R tels que*

$$P = Q\, D + R, \quad \textit{avec } \deg R < \deg D.$$

Quelques remarques avant de passer à la démonstration de ce résultat.

[15] Si $A \Rightarrow B$, alors $\neg B \Rightarrow \neg A$.

Définition VIII.5.2. Les polynômes Q et R de l'énoncé précédent sont appelés respectivement *quotient* et *reste* de la division de P par D. Si le reste de la division de P par D est nul, on dit que D *divise* P ou encore que P est *divisible* par D.

Exemple VIII.5.3. Si on effectue la division euclidienne de $2z^4 + 2z^3 + z^2 + 1$ par $2z^2 - 1$, on peut vérifier que

$$2z^4 + 2z^3 + z^2 + 1 = \underbrace{(z^2 + z + 1)}_{Q}\underbrace{(2z^2 - 1)}_{D} + \underbrace{z + 2}_{R}$$

et $\deg R < \deg D$.

Remarque VIII.5.4. Si $\deg D = 0$, i.e., si D est une constante $c \in \mathbb{C} \setminus \{0\}$, alors

$$P = \underbrace{\frac{1}{c}P}_{Q}\ D + \underbrace{0}_{R}.$$

Par convention, le degré de la fonction nulle étant $-\infty$, on a bien $\deg 0 < \deg D = 0$. Ceci justifie donc notre choix concernant le degré de la fonction nulle. En effet, avec une telle convention, on a encore $\deg(P.Q) = \deg P + \deg Q$ même lorsque P ou Q est nul (en supposant que $-\infty + r = -\infty$ pour tout $r \in \mathbb{R} \cup \{-\infty\}$).

Passons à la preuve du théorème VIII.5.1.

Démonstration. Commençons par démontrer l'existence de polynômes Q et R répondant à la question. Si $\deg P < \deg D$, alors $Q = 0$ et $R = P$ conviennent. Sinon, on procède par récurrence sur $\deg P$. Supposons que

$$n = \deg P \geq \deg D = m.$$

Il existe[16] $c \in \mathbb{C}$ tel que

$$P(z) - c\, z^{n-m}\, D(z) \tag{8}$$

est un polynôme de degré au plus $n-1$ auquel on peut appliquer l'hypothèse de récurrence. Il existe donc des polynômes Q' et R tels que

$$P - c\, z^{n-m}\, D = Q'\ D + R, \quad \text{avec } \deg R < \deg D.$$

Ainsi,

$$P = (Q' + c\, z^{n-m})D + R$$

et $Q = Q' + c\, z^{n-m}$ répond à la question.

Montrons à présent l'unicité. Supposons que

$$P = Q\ D + R = Q'\ D + R', \quad \text{avec } \deg R, \deg R' < \deg D.$$

On a

$$(Q - Q')\, D = R' - R.$$

[16] Si p (resp. d) est le coefficient dominant de P (resp. D), il est clair que $c = p/d$ convient.

Si $Q-Q' \neq 0$, alors le membre de gauche est un polynôme de degré supérieur ou égal à $\deg D$. Ceci est impossible car le membre de droite est un polynôme de degré strictement inférieur à $\deg D$. Par conséquent, $Q = Q'$ et cela entraîne $R = R'$.

■

La disposition pratique de la division euclidienne s'inspire directement du raisonnement utilisé dans la preuve ci-dessus et plus particulièrement de la formule (8).

Exemple VIII.5.5. Soient

$$P = z^5 + 3z^3 + z - 1 \quad \text{et} \quad D = z^3 - 2z^2 + 1.$$

On a

$$\begin{array}{rrrrrr|l}
z^5 & & +3z^3 & & +z & -1 & z^3-2z^2+1 \\
\cline{7-7}
z^5 & -2z^4 & & +z^2 & & & z^2+2z+7 \\
\cline{1-4}
 & 2z^4 & +3z^3 & -z^2 & +z & -1 & \\
 & 2z^4 & -4z^3 & & +2z & & \\
\cline{2-5}
 & & 7z^3 & -z^2 & -z & -1 & \\
 & & 7z^3 & -14z^2 & & +7 & \\
\cline{3-6}
 & & & 13z^2 & -z & -8 &
\end{array}$$

Ainsi, le quotient de la division de P par D est $z^2 + 2z + 7$ et le reste est $13z^2 - z - 8$.

Considérons un second exemple. Soient

$$P = 2iz^4 + z^3 - iz^2 + z - 1 \quad \text{et} \quad D = 3z^2 + z + 1.$$

On a

$$\begin{array}{rrrrrrrrr|l}
2i\,z^4 & + & z^3 & - & i\,z^2 & + & z & -1 & & 3\,z^2+z+1 \\
\cline{10-10}
2i\,z^4 & + & \tfrac{2i}{3}\,z^3 & + & \tfrac{2i}{3}\,z^2 & & & & & \tfrac{2i}{3}\,z^2+\tfrac{3-2i}{9}\,z-\tfrac{3+13i}{27} \\
\cline{1-5}
 & & \tfrac{3-2i}{3}\,z^3 & - & \tfrac{5i}{3}\,z^2 & + & z & -1 & & \\
 & & \tfrac{3-2i}{3}\,z^3 & + & \tfrac{3-2i}{9}\,z^2 & + & \tfrac{3-2i}{9}\,z & & & \\
\cline{3-7}
 & & & - & \tfrac{3+13i}{9}\,z^2 & + & \tfrac{6+2i}{9}\,z & -1 & & \\
 & & & - & \tfrac{3+13i}{9}\,z^2 & - & \tfrac{3+13i}{27}\,z & -\tfrac{3+13i}{27} & & \\
\cline{5-8}
 & & & & & & \tfrac{21+19i}{27}\,z & -\tfrac{24-13i}{27} &
\end{array}$$

Ici, le reste et le quotient de la division de P par D sont respectivement

$$\frac{21+19i}{27}z - \frac{24-13i}{27} \quad \text{et} \quad \frac{2i}{3}\,z^2 + \frac{3-2i}{9}\,z - \frac{3+13i}{27}.$$

La preuve donnée précédemment fournit donc un algorithme pour calculer de manière effective la division euclidienne de deux polynômes. En utilisant la théorie des systèmes linéaires, nous pouvons cependant donner une preuve plus courte du théorème VIII.5.1.

Démonstration. (Preuve alternative du théorème VIII.5.1) Supposons $n = \deg P \geq \deg D$. La relation $P = QD + R$ peut être vue comme un

système linéaire de $n+1$ équations à $n+1$ inconnues qui sont les coefficients des polynômes Q et R (on a $\deg P - \deg D + 1$ coefficients pour Q et $\deg D$ coefficients pour R). Le système homogène associé est $QD + R = 0$. La seule solution de ce dernier système est $Q = R = 0$ (pour montrer l'unicité de la solution, on procède avec la même argumentation que dans la preuve précédente). Au vu de la proposition VI.2.4, le système est de Cramer et le système $P = QD + R$ possède bien une et une seule solution.

■

Proposition VIII.5.6. *Soient P et D des polynômes non nuls. Le polynôme D divise P si et seulement si tout zéro de D est aussi zéro de P et si sa multiplicité comme zéro de D est inférieure ou égale à celle de P.*

Démonstration. La condition est suffisante. Soient $z_1, \ldots, z_p$ les zéros de D de multiplicité $\alpha_1, \ldots, \alpha_p$. Soient $z_{p+1}, \ldots, z_q$ les zéros de P qui ne sont pas zéros de D, de multiplicité $\beta_{p+1}, \ldots, \beta_q$. On note $\beta_1, \ldots, \beta_p$ les multiplicités de $z_1, \ldots, z_p$ comme zéros de P. Par hypothèse, pour tout $i \in \{1, \ldots, p\}$, $\alpha_i \leq \beta_i$. En vertu du théorème fondamental de l'algèbre,

$$P = r\,(z - z_1)^{\beta_1} \cdots (z - z_p)^{\beta_p}\,(z - z_{p+1})^{\beta_{p+1}} \cdots (z - z_q)^{\beta_q}$$

et

$$D = s\,(z - z_1)^{\alpha_1} \cdots (z - z_p)^{\alpha_p}.$$

Ainsi,

$$P = \frac{r}{s}(z - z_1)^{\beta_1 - \alpha_1} \cdots (z - z_p)^{\beta_p - \alpha_p}\,(z - z_{p+1})^{\beta_{p+1}} \cdots (z - z_q)^{\beta_q}\; D$$

ce qui montre bien que D divise P.

Montrons à présent que la condition est nécessaire et supposons que D divise P. Cela signifie qu'il existe un polynôme Q tel que

$$P = Q\; D.$$

Soit z_0 un zéro de D de multiplicité $\alpha \geq 1$. Si z_0 est également zéro de Q, on note β, la multiplicité de z_0 comme zéro de Q. Si $Q(z_0) \neq 0$, alors on pose $\beta = 0$. En vertu de la proposition VIII.2.3, il existe des polynômes S et T tels que

$$D(z) = (z - z_0)^{\alpha}\, S(z), \quad \text{avec } S(z_0) \neq 0$$

et

$$Q(z) = (z - z_0)^{\beta}\, T(z), \quad \text{avec } T(z_0) \neq 0.$$

Ainsi,

$$P = (z - z_0)^{\alpha+\beta}\, S(z)\, T(z) \quad \text{et } S(z_0)\, T(z_0) \neq 0.$$

Dès lors, z_0 est un zéro de P de multiplicité $\alpha + \beta \geq \alpha$. Ceci suffit pour conclure la preuve.

■

Définition VIII.5.7. Soient $P_1, \ldots, P_n$ des polynômes non nuls. Le polynôme D est un *plus grand commun diviseur* (p.g.c.d.) de $P_1, \ldots, P_n$ si D divise $P_1, \ldots, P_n$ et si tout autre polynôme D' qui divise $P_1, \ldots, P_n$, divise D.

Remarque VIII.5.8. On peut observer que le p.g.c.d. des polynômes $P_1, \ldots, P_n$ n'est défini qu'à une constante multiplicative non nulle près. Si D est un p.g.c.d. de $P_1, \ldots, P_n$, pour tout $c \in \mathbb{C} \setminus \{0\}$, cD est aussi un p.g.c.d. de $P_1, \ldots, P_n$.

Proposition VIII.5.9. *Soient $P_1, \ldots, P_n$ des polynômes non nuls et $z_1, \ldots, z_t$ leurs zéros communs. Si on note α_{ij} la multiplicité de z_i comme zéro de P_j et $\alpha_i = \inf_{j\in\{1,\ldots,n\}} \alpha_{ij}$, alors D est un p.g.c.d. de $P_1, \ldots, P_n$ si et seulement si*

$$D = c\,(z - z_1)^{\alpha_1} \cdots (z - z_t)^{\alpha_t}, \quad c \in \mathbb{C} \setminus \{0\}.$$

Démonstration. C'est une conséquence immédiate de la proposition VIII.5.6. ∎

Définition VIII.5.10. Deux polynômes sont *premiers entre eux* s'ils ont 1 comme p.g.c.d. Au vu de la proposition précédente, cela signifie qu'ils n'ont pas de zéro commun.

On appelle parfois ce résultat *théorème de Gauss.*

Proposition VIII.5.11. *Soient A, B, C trois polynômes non nuls. Si A divise BC et est premier avec B, alors A divise C.*

Démonstration. Si $z_1, \ldots, z_p$ sont les zéros de A de multiplicité respective $\alpha_1, \ldots, \alpha_p$, alors $z_1, \ldots, z_p$ sont aussi zéros de BC de multiplicité respective $\beta_1, \ldots, \beta_p$ avec $\beta_i \geq \alpha_i$, (c'est une conséquence de la proposition VIII.5.6). Puisque A est premier avec B, ils n'ont pas de zéro commun. Par conséquent, $z_1, \ldots, z_p$ sont des zéros de C de multiplicité $\beta_1, \ldots, \beta_p$ et donc A divise C. ∎

Proposition VIII.5.12 (Algorithme d'Euclide). [17] *Soient A et B deux polynômes non nuls tels que* $\deg A \geq \deg B$. *En appliquant successivement la division euclidienne, on obtient la suite d'équations*

$$\begin{array}{rcll} A &=& Q_1\,B + R_1 & \deg R_1 < \deg B \\ B &=& Q_2\,R_1 + R_2 & \deg R_2 < \deg R_1 \\ R_1 &=& Q_3\,R_2 + R_3 & \deg R_3 < \deg R_2 \\ & \vdots & & \\ R_{j-2} &=& Q_j\,R_{j-1} + R_j & \deg R_j < \deg R_{j-1} \\ R_{j-1} &=& Q_{j+1}\,R_j & R_j \neq 0. \end{array}$$

Un p.g.c.d. de A et de B est le dernier reste non nul R_j.

Démonstration. La dernière égalité nous montre que R_j divise R_{j-1}. Montrons de proche en proche que R_j divise $R_{j-2}, \ldots, R_1$. Soit $k \in \{j, \ldots, 3\}$. Si R_j divise $R_{j-1}, \ldots, R_k, R_{k-1}$, alors R_j divise R_{k-2} car

$$R_{k-2} = Q_k\,R_{k-1} + R_k.$$

[17] Le lecteur ayant lu le chapitre consacré aux entiers modulo n pourra faire le parallèle entre l'algorithme d'Euclide et le théorème de Bezout vus dans ce chapitre avec leur contrepartie dans le cas des entiers.

Ainsi, R_j divise R_1 et R_2. Il divise donc B et par le même raisonnement, il divise aussi A. C'est un diviseur commun, il nous reste à prouver qu'il est le plus grand.

Si T divise A et B, alors T divise R_1 car

$$R_1 = A - Q_1\, B.$$

Puisque T divise B et R_1, on tire de la deuxième équation qu'il divise aussi R_2. De proche en proche, on en conclut que T divise R_j. Par conséquent, R_j est un p.g.c.d. de A et de B.

■

Exemple VIII.5.13. Considérons les polynômes

$$A = 4 + 2\,z - 12\,z^2 - 8\,z^3 + 8\,z^4 + 6\,z^5$$

et

$$B = -4 + 2\,z + 4\,z^2 + z^3 + 3\,z^4$$

et appliquons leurs l'algorithme d'Euclide. Nous utilisons les mêmes notations que dans ce dernier,

$$A = \underbrace{(2 + 2\,z)}_{:=Q_1}\, B + \underbrace{12 + 6\,z - 24\,z^2 - 18\,z^3}_{:=R_1},$$

$$B = \underbrace{(1/6 - z/6)}_{:=Q_2}\, R_1 \underbrace{-6 + 3\,z + 9\,z^2}_{:=R_2}$$

$$R_1 = \underbrace{(-2 - 2z)}_{:=Q_3}\, R_2.$$

Ainsi, un p.g.c.d. de A et de B est donné par R_2.

Théorème VIII.5.14 (Théorème de Bezout). *Soient A et B deux polynômes non nuls et D un p.g.c.d. de A et de B. Il existe des polynômes S et T tels que*

$$D = S\,A + T\,B.$$

Démonstration. En appliquant l'algorithme d'Euclide à A et à B (nous supposons ici que $\deg A \geq \deg B$), on obtient deux suites finies de polynômes $Q_1, \ldots, Q_{j+1}$ et $R_1, \ldots, R_j$ (nous utilisons les mêmes notations que dans l'énoncé de la proposition VIII.5.12). La première égalité permet d'exprimer R_1 comme combinaison de A et de B,

$$R_1 = A - Q_1 B.$$

En remplaçant R_1 dans la deuxième égalité, on peut aussi exprimer R_2 comme combinaison de A et de B,

$$R_2 = B - Q_2 R_1 = B - Q_2(A - Q_1 B) = (1 + Q_1 Q_2)B - Q_2\, A.$$

En procédant de proche en proche, on arrive à exprimer R_j comme combinaison de A et de B.

■

Exemple VIII.5.15. Poursuivons l'exemple VIII.5.13 et exprimons un p.g.c.d. de A et de B comme combinaison de ceux-ci. On a

$$R_2 = B - Q_2\,R_1 = B - Q_2\,(A - Q_1\,B) = (1 + Q_1\,Q_2)\,B - Q_2\,A$$

et en remplaçant, on trouve

$$R_2 = (4/3 - z^2/3)\,B - (1/6 - z/6)\,A.$$

6. Fractions rationnelles

Définition VIII.6.1. Une *fraction rationnelle* à coefficients complexes est une fonction telle qu'il existe deux polynômes A et B premiers entre eux (et où $B \neq 0$) tels que

$$R(z) = \frac{A(z)}{B(z)}.$$

Cette fonction est définie dans le complémentaire d'un nombre fini de points $\mathbb{C} \setminus \{z_1, \ldots, z_p\}$ où $z_1, \ldots, z_p$ sont les zéros de B.

Remarque VIII.6.2. Dans la définition précédente, nous avons supposé que A et B étaient premiers entre eux. Ceci ne constitue pas une véritable restriction. En effet, si A et B ne sont pas premiers entre eux, prenons D un p.g.c.d. de A et de B, alors

$$A = A'\,D \quad \text{et} \quad B = B'D.$$

Si $B(z) \neq 0$, alors

$$R(z) = \frac{A(z)}{B(z)} = \frac{A'(z)}{B'(z)}.$$

Il est donc clair qu'on peut étendre continûment la fonction $\frac{A(z)}{B(z)}$ définie sur $\mathbb{C} \setminus \{z \mid B(z) = 0\}$ en la fonction $\frac{A'(z)}{B'(z)}$ définie sur $\mathbb{C} \setminus \{z \mid B'(z) = 0\}$. Il est de plus évident que

$$\mathbb{C} \setminus \{z \mid B(z) = 0\} \subset \mathbb{C} \setminus \{z \mid B'(z) = 0\}.$$

Remarque VIII.6.3. Les polynômes A et B (premiers entre eux) qui représentent la fraction rationnelle

$$R = \frac{A(z)}{B(z)}$$

sont uniques à une même constante multiplicative non nulle près. En effet, si A' et B' sont deux polynômes satisfaisant les mêmes conditions que A et B, alors

$$AB' = A'B$$

dans le complémentaire d'un nombre fini de points[18]. En vertu du corollaire VIII.3.6, l'égalité entre les polynômes AB' et $A'B$ a lieu dans $\mathbb{C}$. Puisque

[18]En fait, dans l'intersection des deux domaines de définition. Ainsi, si $z_1, \ldots, z_p$ (resp.$z'_1, \ldots, z'_q$) sont les zéros de B (resp. B'), alors l'égalité a lieu sur $\mathbb{C} \setminus \{z_1, \ldots, z_p, z'_1, \ldots, z'_q\}$. Si AB' et $A'B$ sont deux polynômes de degré n, l'égalité ayant lieu dans le complémentaire d'un nombre fini de points, elle est en particulier satisfaite en $n+1$ points et les deux polynômes sont donc égaux partout.

A est premier avec B, au vu de la proposition VIII.5.11, A divise A', i.e., $A' = QA$. De la même manière, B' divise B, i.e., $B = Q'B'$. Puisque $AB' = QQ'AB'$, on en tire que Q et Q' sont des constantes non nulles et qu'il existe donc une constante $c \neq 0$ telle que $A' = cA$ et $B' = cA$.

Définition VIII.6.4. Une fraction rationnelle $R = \frac{A}{B}$ est *propre* si $\deg A < \deg B$. On appelle *pôle* de R tout zéro de B. L'*ordre* d'un pôle est sa multiplicité comme zéro de B. Au vu de la remarque précédente, ces définitions sont indépendantes des polynômes A et B qui représentent la fraction rationnelle R.

Remarque VIII.6.5. Une conséquence immédiate de la division euclidienne est que toute fraction rationnelle est la somme d'un polynôme et d'une fraction rationnelle propre. Au vu de la remarque précédente, cette décomposition est unique.

Le résultat suivant explicite le comportement d'une fraction rationnelle au voisinage d'un de ses pôles : au voisinage d'un pôle d'ordre α, elle tend vers l'infini comme z^α.

Proposition VIII.6.6. *Soit $R = \frac{A}{B}$ une fraction rationnelle. Le nombre complexe z_0 est un pôle d'ordre α de R, si et seulement si*

$$\lim_{z \to z_0} (z - z_0)^\alpha \, R(z) \in \mathbb{C} \setminus \{0\}.$$

Démonstration. Puisque z_0 est un zéro de multiplicité α de B, en vertu de la proposition VIII.2.3, $B(z) = (z - z_0)^\alpha C(z)$ où $C(z_0) \neq 0$. Ainsi,

$$\lim_{z \to z_0} (z - z_0)^\alpha \, R(z) = \lim_{z \to z_0} (z - z_0)^\alpha \, \frac{A(z_0)}{(z - z_0)^\alpha C(z)}$$

De plus, z_0 n'est pas zéro de A car R une fraction rationnelle (A et B sont premiers entre eux et donc z_0 n'est pas zéro de A). Ainsi, la limite cherchée vaut $A(z_0)/C(z_0) \neq 0$.

Si z_0 est un zéro de multiplicité μ de B, alors

$$\lim_{z \to z_0} (z - z_0)^\alpha \, \frac{A(z)}{B(z)} = \lim_{z \to z_0} \frac{(z - z_0)^\alpha \, A(z)}{(z - z_0)^\mu \, C(z)}.$$

Dès lors,

$$\lim_{z \to z_0} (z - z_0)^\alpha \, \frac{A(z)}{B(z)} = \begin{cases} 0 & , \text{si } \alpha > \mu \\ \infty & , \text{si } \alpha < \mu. \end{cases}$$

Ceci conclut la preuve.

■

Exemple VIII.6.7. Considérons la fraction rationnelle

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

La figure VIII.4 donne le graphique de la fonction $|R| : \mathbb{C} \to \mathbb{R} : z \mapsto |R(z)|$ ainsi qu'une représentation en courbes de niveau.

On est forcé de représenter la fonction $|R|$ et non R car $R : \mathbb{C} \to \mathbb{C}$ et nous ne sommes pas en mesure de représenter un espace à 4 dimensions.

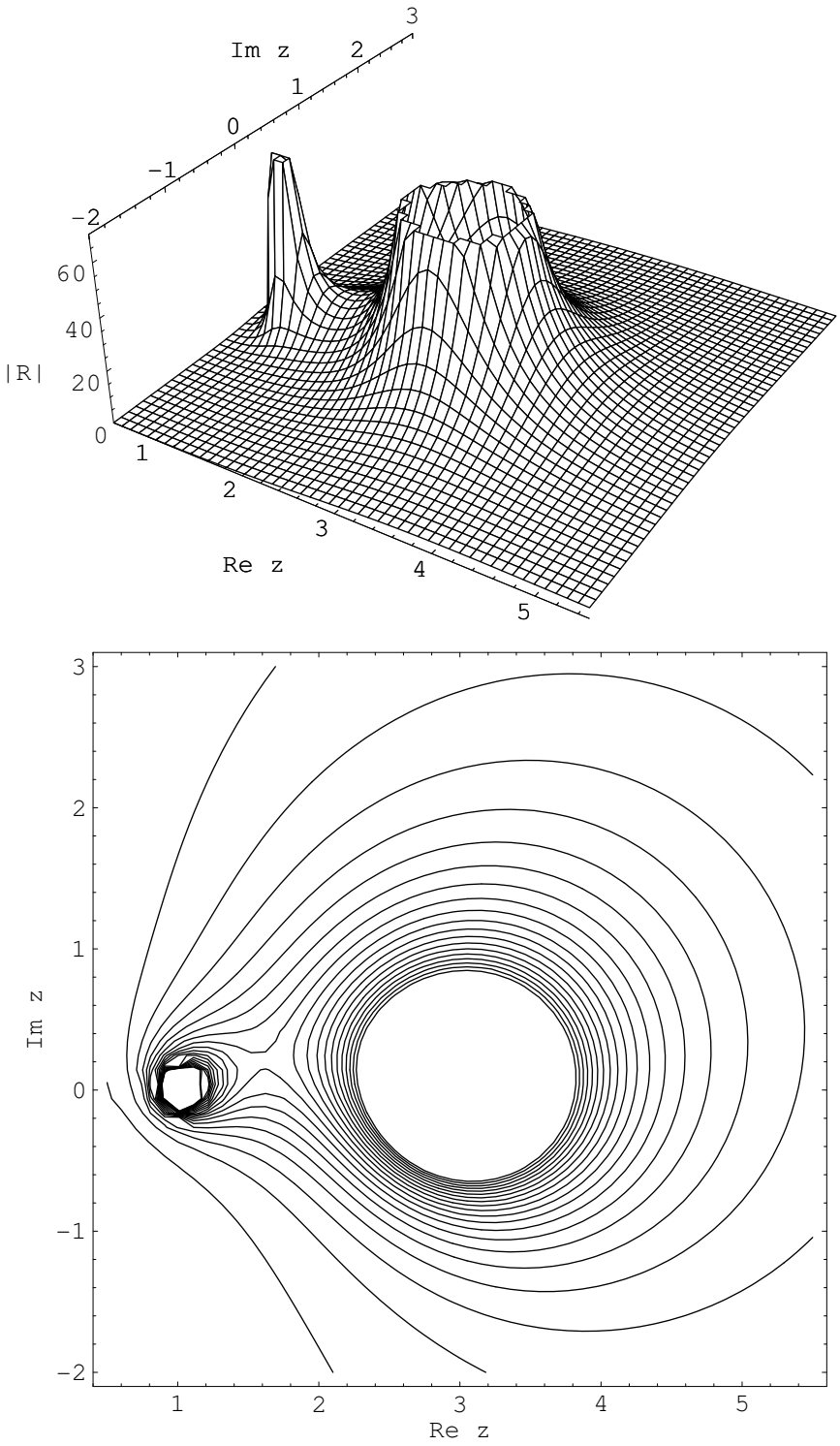


FIGURE VIII.4. Comportement d'une fraction rationnelle au voisinage de ses pôles, graphique tronqué et courbes de niveau.

Proposition VIII.6.8. *Toute fraction rationnelle R est une fonction de classe C_∞ dans le complémentaire Ω de l'ensemble de ses pôles. On a*

$$D_{\overline{z}}R = 0.$$

De plus, D_zR est une fraction rationnelle qui a les mêmes pôles que R, l'ordre de chacun d'entre eux étant augmenté d'une unité.

Exemple VIII.6.9. Avant de procéder à la démonstration de ce résultat, illustrons cette propriété sur un exemple. En considérant la fraction rationnelle $R(z)$ de l'exemple VIII.6.7. On trouve

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

Ainsi, les dénominateurs de R et de D_zR ont bien les mêmes zéros, les multiplicités de ceux de D_zR étant d'une unité supérieure à ceux de R.

Démonstration. La fraction rationnelle R s'écrit $\frac{A}{B}$ où A et B sont deux fonctions de classe C_∞ sur $\mathbb{C}$ (cf. proposition VIII.1.3). De plus, B ne s'annule pas sur Ω. Dès lors, R est de classe C_∞ sur Ω comme quotient de deux fonctions de classe C_∞ dans Ω, le dénominateur ne s'annulant pas. Sur Ω, on a

$$D_{\overline{z}}R = \frac{B\,D_{\overline{z}}A - A\,D_{\overline{z}}B}{B^2}.$$

Or si P est un polynôme, nous savons que $D_{\overline{z}}P$ est nul. Par conséquent, $D_{\overline{z}}R = 0$. On a aussi

$$D_zR = \frac{B\,D_zA - A\,D_zB}{B^2}.$$

Remarquons que si B possède un zéro multiple, alors le numérateur et le dénominateur ne sont pas premiers entre eux. En effet, si z_0 est un zéro de B de multiplicité au moins deux, alors $B(z_0) = (D_zB)(z_0) = 0$ et dès lors, z_0 est un zéro commun du numérateur et du dénominateur de D_zR. Soit Δ, un p.g.c.d. de B et de D_zB. Ainsi, $B = \Delta\,B_0$ et $D_zB = \Delta\,B_1$ avec B_0 et B_1 deux polynômes premiers entre eux. Le polynôme B_0 possède les mêmes zéros que B mais tous ses zéros sont simples. En effet, si z_0 est un zéro simple de B, alors z_0 n'est pas zéro de D_zB et il n'est donc pas non plus zéro de Δ. Si z_0 est un zéro α-uple de B, $\alpha > 1$, alors z_0 est zéro $(\alpha-1)$-uple de D_zB et de Δ (c'est une conséquence de la proposition VIII.5.9). Dans Ω, on a donc

$$D_zR = \frac{B_0\,D_zA - A\,B_1}{B\,B_0}.$$

Le numérateur et le dénominateur de cette dernière expression sont premiers entre eux. En effet, si z_0 est un zéro de B ou B_0 (ce qui revient au même puisqu'ils ont les mêmes zéros), alors $B_0(z_0) = 0$ mais $A(z_0) \neq 0$ (car A et B sont premiers entre eux) et $B_1(z_0) \neq 0$ (car B_0 et B_1 sont premiers entre eux), donc le numérateur ne s'annule pas en z_0. Ceci prouve que D_zR est une fraction rationnelle et le résultat annoncé concernant ses pôles (puisque, rappelons-le une fois encore, tous les zéros de B_0 sont simples).

■

Remarque VIII.6.10. Si

$$R(z) = \frac{A(z)}{B(z)}$$

est une fraction rationnelle, alors

$$\lim_{z\to\infty} R(z) = \begin{cases} \infty & \text{si } \deg A > \deg B \\ a/b & \text{si } \deg A = \deg B \\ 0 & \text{si } \deg A < \deg B, \text{ i.e., } R \text{ est propre} \end{cases}$$

où a et b sont les coefficients dominants de A et B respectivement. Pour s'en apercevoir, il suffit de mettre en évidence le terme de plus haut degré.

Exemple VIII.6.11. Considérons la fraction rationnelle

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

La figure VIII.5 montre le graphique de la fonction $|R| : \mathbb{C} \to \mathbb{R} : z \mapsto |R(z)|$ ainsi qu'une représentation en courbes de niveau.

7. Décomposition d'une fraction rationnelle propre

Le théorème suivant (tant la décomposition que l'unicité) est à la base de toutes les constructions développées dans cette section.

Théorème VIII.7.1. *Soit $R = \frac{A}{B}$ une fraction rationnelle propre. Supposons que $B = B_1 B_2$ avec B_1 et B_2 premiers entre eux. Il existe une et une seule décomposition de R de la forme*

$$R = \frac{A_1}{B_1} + \frac{A_2}{B_2}$$

où $\frac{A_1}{B_1}$ et $\frac{A_2}{B_2}$ sont des fractions rationnelles propres.

Démonstration. Montrons d'abord l'existence de la décomposition. Puisque B_1 et B_2 sont premiers entre eux, en vertu du théorème de Bezout, il existe des polynômes T_1 et T_2 tels que

$$1 = T_1\, B_1 + T_2\, B_2.$$

Ainsi, il vient[19]

$$\frac{A}{B} = \frac{A\,T_1\,B_1}{B} + \frac{A\,T_2\,B_2}{B} = \frac{A\,T_1}{B_2} + \frac{A\,T_2}{B_1}.$$

Au vu de la remarque VIII.6.5, il existe des polynômes uniques P_1 et P_2 et des fractions rationnelles propres $\frac{A_1}{B_1}$ et $\frac{A_2}{B_2}$ tels que

$$\frac{A}{B} = P_1 + \frac{A_1}{B_1} + P_2 + \frac{A_2}{B_2}.$$

[19] A est premier avec B_2 car A est premier avec B. De plus, T_1 est premier avec B_2 car sinon, ils auraient un facteur commun P (de degré ≥ 1) et de là, on pourrait en conclure que $1 = T_1\, B_1 + T_2\, B_2$ est divisible par P. Ainsi, AT_1/B_2 est une "vraie" fraction rationnelle. Idem pour AT_2/B_1.

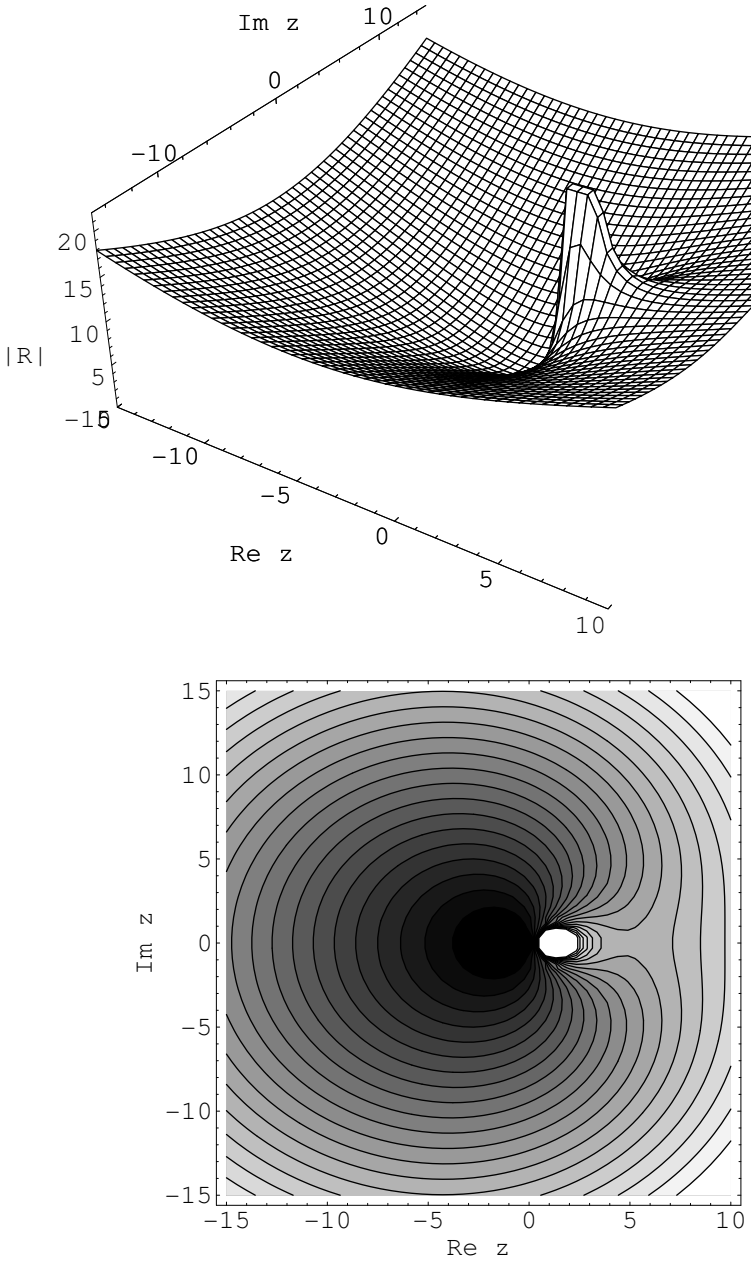


FIGURE VIII.5. Comportement d'une fraction rationnelle à l'infini.

En réduisant au même dénominateur, il vient

$$\frac{A}{B} = \frac{(P_1 + P_2)\, B + A_1\, B_2 + A_2\, B_1}{B}.$$

Comme A/B est une fraction rationnelle propre, il s'ensuit que $P_1 + P_2 = 0$ car sinon le degré du numérateur serait supérieur ou égal au degré du dénominateur. Ceci montre donc l'existence de la décomposition.

Passons à l'unicité de la décomposition et supposons que

$$R = \frac{A_1}{B_1} + \frac{A_2}{B_2} = \frac{A_1'}{B_1} + \frac{A_2'}{B_2}$$

où les deux décompositions ont les propriétés annoncées. On a

$$\frac{A_1 - A_1'}{B_1} = \frac{A_2' - A_2}{B_2} \quad \text{et} \quad (A_1 - A_1')\, B_2 = (A_2' - A_2)\, B_1.$$

Si $A_1 \neq A_1'$, alors $A_2 \neq A_2'$. Dans ce cas, comme B_2 est premier avec B_1, il divise $A_2' - A_2$. Ceci est impossible car $\deg A_2 < \deg B_2$, $\deg A_2' < \deg B_2$ et donc, $\deg(A_2' - A_2) < \deg B_2$. Ainsi, B_2 ne peut pas diviser $A_2' - A_2$. Par conséquent, $A_1 = A_1'$ et $A_2 = A_2'$.

■

Corollaire VIII.7.2. *Soit $R = \frac{A}{B}$ une fraction rationnelle propre. Supposons que $B = B_1 \cdots B_m$ avec B_j premiers entre eux deux à deux. Il existe une et une seule décomposition de R de la forme*

$$R = \frac{A_1}{B_1} + \cdots + \frac{A_m}{B_m}$$

où $\frac{A_1}{B_1}, \ldots, \frac{A_m}{B_m}$ sont des fractions rationnelles propres.

Démonstration. On procède par récurrence sur m. Le cas $m = 2$ a été vérifié dans le théorème précédent. Les polynômes B_1 et $B' = B_2 \cdots B_m$ étant premiers entre eux, il existe une unique décomposition de R sous la forme

$$R = \frac{A_1}{B_1} + \frac{A'}{B'}$$

où les termes du second membre sont des fractions rationnelles propres. Par hypothèse de récurrence, il existe une unique décomposition de $\frac{A'}{B'}$ sous la forme

$$\frac{A'}{B'} = \frac{A_2}{B_2} + \cdots + \frac{A_m}{B_m}$$

où $\frac{A_2}{B_2}, \ldots, \frac{A_m}{B_m}$ sont des fractions rationnelles propres.

■

Remarque VIII.7.3. Dans cette dernière démonstration, on s'aperçoit que A_j est caractérisé par le fait que

$$\frac{A}{B} = \frac{A_j}{B_j} + \frac{A'}{B'}$$

avec A_j/B_j et A'/B' des fractions rationnelles propres et A_j ne dépend que du facteur B_j de la décomposition de B. En effet, il suffit de reproduire la démonstration avec B_j et $B' = B_1 \cdots \widehat{B_j} \cdots B_m$.

Remarque VIII.7.4. Pour calculer les polynômes A_j apparaissant dans la décomposition

$$\frac{A}{B} = \frac{A_1}{B_1} + \cdots + \frac{A_m}{B_m},$$

on procède en général par identification des coefficients. Si $d_1, \dots, d_m$ sont les degrés de $B_1, \dots, B_m$, alors, puisque les fractions rationnelles sont propres, pour tout $j \in \{1, \dots, m\}$, il existe des coefficients $a_{j,i} \in \mathbb{C}$ tels que

$$A_j = a_{j,0} + a_{j,1}\, z + \cdots + a_{j,d_j-1}\, z^{d_j-1}.$$

En réduisant au même dénominateur, il vient

$$\frac{A}{B} = \frac{A_1}{B_1} + \cdots + \frac{A_m}{B_m} = \frac{\sum_{j=1}^m A_j B_1 \cdots \widehat{B_j} \cdots B_m}{B}.$$

Or l'identité polynomiale

$$A = \sum_{j=1}^m A_j B_1 \cdots \widehat{B_j} \cdots B_m$$

n'ayant lieu que si les coefficients des différentes puissances de z sont égaux dans les deux membres, on obtient un système d'équations linéaires pour les $a_{j,i}$. La décomposition en fractions rationnelles étant unique, ce système possède une et une seule solution.

Définition VIII.7.5. Une décomposition de A/B dans laquelle tous les numérateurs sont des constantes s'appelle décomposition de A/B en somme de *fractions simples*.

Proposition VIII.7.6 (Décomposition en fractions simples sur $\mathbb{C}$). *Si R est une fraction rationnelle propre ayant $z_1, \dots, z_p$ pour pôles d'ordre $\alpha_1, \dots, \alpha_p$, alors R se décompose de manière unique sous la forme*

$$R = \frac{c_{1,1}}{z - z_1} + \cdots + \frac{c_{1,\alpha_1}}{(z - z_1)^{\alpha_1}} + \cdots + \frac{c_{p,1}}{z - z_p} + \cdots + \frac{c_{p,\alpha_p}}{(z - z_p)^{\alpha_p}}.$$

Démonstration. La fraction rationnelle propre R peut se mettre sous la forme A/B avec

$$B = b\,(z - z_1)^{\alpha_1} \cdots (z - z_p)^{\alpha_p}.$$

Par le corollaire VIII.7.2, R se décompose de manière unique sous la forme

$$R = \frac{A_1}{(z - z_1)^{\alpha_1}} + \cdots + \frac{A_p}{(z - z_p)^{\alpha_p}}$$

avec, pour tout $j \in \{1, \dots, p\}$, $\deg A_j < \alpha_j$. Par la formule de Taylor, on a

$$A_j = \sum_{k=0}^{\alpha_j - 1} \frac{(D_z^k A_j)(z_j)}{k!} (z - z_j)^k.$$

Par conséquent,

$$\frac{A_j}{(z - z_j)^{\alpha_j}} = \sum_{k=0}^{\alpha_j - 1} \frac{(D_z^k A_j)(z_j)}{k!} \frac{1}{(z - z_j)^{\alpha_j - k}}$$

et en renommant l'indice sommatoire, il vient

$$\frac{A_j}{(z - z_j)^{\alpha_j}} = \sum_{k=1}^{\alpha_j} \frac{(D_z^{\alpha_j - k} A_j)(z_j)}{(\alpha_j - k)!} \frac{1}{(z - z_j)^k}.$$

On obtient donc une décomposition du type recherché en posant

$$c_{j,k} = \frac{(D_z^{\alpha_j - k} A_j)(z_j)}{(\alpha_j - k)!}.$$

Il nous reste à montrer que cette décomposition est unique. Pour ce faire, il suffit de prouver[20] que

$$\sum_{j=1}^{p} \sum_{k=1}^{\alpha_j} \frac{d_{j,k}}{(z - z_j)^k} = 0 \quad \text{entraîne} \quad d_{j,k} = 0,\ \forall j, k.$$

En réduisant (partiellement) au même dénominateur,

$$\sum_{j=1}^{p} \sum_{k=1}^{\alpha_j} \frac{d_{j,k}}{(z - z_j)^k} = \sum_{j=1}^{p} \frac{\sum_{k=1}^{\alpha_j} d_{j,k} (z - z_j)^{\alpha_j - k}}{(z - z_j)^{\alpha_j}} = 0.$$

Or la décomposition en fractions rationnelles propres étant unique (cf. corollaire VIII.7.2), il s'ensuit que

$$\sum_{k=1}^{\alpha_j} d_{j,k} (z - z_j)^{\alpha_j - k} = 0,\ \forall j \in \{1, \ldots, p\}.$$

On en tire directement que pour tout $j \in \{1, \ldots, p\}$, $d_{j,k} = 0$ pour tout $k \in \{1, \ldots, \alpha_j\}$.

■

Remarque VIII.7.7. Pour calculer les coefficients $c_{j,k}$ apparaissant dans la décomposition en fractions simples de $R = A/B$, on peut procéder comme à la remarque VIII.7.4. Il est cependant possible de diminuer le nombre de calculs nécessaires en utilisant les zéros du dénominateur B. Supposons que la décomposition en fractions simples de R est

$$R = \frac{c_{1,1}}{z - z_1} + \cdots + \frac{c_{1,\alpha_1}}{(z - z_1)^{\alpha_1}} + \cdots + \frac{c_{p,1}}{z - z_p} + \cdots + \frac{c_{p,\alpha_p}}{(z - z_p)^{\alpha_p}}.$$

Dès lors, il existe des polynômes[21] $A_1, \ldots, A_p$ tels que

$$R = \frac{A_1}{(z - z_1)^{\alpha_1}} + \cdots + \frac{A_p}{(z - z_p)^{\alpha_p}}.$$

[20] En effet, si on dispose de deux telles décompositions

$$\sum_{j=1}^{p} \sum_{k=1}^{\alpha_j} \frac{c_{j,k}}{(z - z_j)^k} = \sum_{j=1}^{p} \sum_{k=1}^{\alpha_j} \frac{c'_{j,k}}{(z - z_j)^k},$$

alors

$$\sum_{j=1}^{p} \sum_{k=1}^{\alpha_j} \frac{c_{j,k} - c'_{j,k}}{(z - z_j)^k} = 0$$

et pour que la décomposition soit unique, il suffit de vérifier que chacun des numérateurs est nul. Dans la preuve ci-dessus, $d_{j,k}$ joue le rôle de $c_{j,k} - c'_{j,k}$

[21] Il est clair que, pour tout $j \in \{1, \ldots, p\}$,

$$A_j = \sum_{k=1}^{\alpha_j} c_{j,k} (z - z_j)^{\alpha_j - k}.$$

Posons

$$N_j = A_j(z-z_1)^{\alpha_1}\cdots\widehat{(z-z_j)^{\alpha_j}}\cdots(z-z_p)^{\alpha_p}.$$

De cette façon, on a

$$R = \frac{A}{B} = \frac{N_1+\cdots+N_p}{B}$$

et on en tire

$$A = N_1+\cdots+N_p.$$

Donc en particulier,

$$A(z_j) = N_1(z_j)+\cdots+N_p(z_j)$$

et par définition même des N_k, pour tout $i\neq j$, z_j est un zéro α_j-uple de N_i. Cela signifie que pour tout $j\in\{1,\dots,p\}$,

$$\left\{\begin{array}{rcl} A(z_j) &=& N_j(z_j)\\ (D_zA)(z_j) &=& (D_zN_j)(z_j)\\ &\vdots&\\ (D_z^{\alpha_j-1}A)(z_j) &=& (D_z^{\alpha_j-1}N_j)(z_j)\end{array}\right.$$

Ce système linéaire est un système triangulaire en $c_{j,1},\dots,c_{j,\alpha_j}$. Pour le voir, il suffit de remarquer que $c_{j,1},\dots,c_{j,\alpha_j}$ sont les seuls coefficients apparaissant[22] dans $A(z_j),\dots,(D_z^{\alpha_j-1}A)(z_j)$. En effet, en mettant $(z-z_j)^{\alpha_j}$ en évidence dans les N_i $(i\neq j)$, on trouve

$$\begin{array}{rcl} A &=& N_j+N_1+\cdots+\widehat{N_j}+\cdots+N_p\\ &=& A_j\underbrace{(z-z_1)^{\alpha_1}\cdots\widehat{(z-z_j)^{\alpha_j}}\cdots(z-z_p)^{\alpha_p}}_{:=S_j}+(z-z_j)^{\alpha_j}T_j.\end{array}$$

Pour tout $\ell\in\{0,\dots,\alpha_j-1\}$, par la formule de Leibniz, on a

$$(D_z^\ell A)(z_j) = \sum_{k=0}^{\ell}\mathrm{C}_\ell^k\ (D_z^kA_j)(z_j)\ (D_z^{\ell-k}S_j)(z_j).$$

Puisque $A_j=\sum_{k=1}^{\alpha_j}c_{j,k}(z-z_j)^{\alpha_j-k}$ et qu'en vertu de la formule de Taylor, on a aussi

$$A_j = \sum_{i=0}^{\alpha_j-1}\frac{(D_z^iA_j)(z_j)}{i!}(z-z_j)^i,$$

alors, en identifiant les coefficients, il vient

$$c_{j,k} = \frac{(D_z^{\alpha_j-k}A_j)(z_j)}{(\alpha_j-k)!},\ k=1,\dots,\alpha_j.$$

Ceci montre bien que les seuls coefficients apparaissant dans $(D_z^\ell A)(z_j)$ sont $c_{j,1},\dots,c_{j,\alpha_j}$.

[22] Vu la forme de A_j et N_j, il est par ailleurs clair que $c_{j,1},\dots,c_{j,\alpha_j}$ sont les seuls coefficients apparaissant dans $N_j(z_j),\dots,(D_z^{\alpha_j-1}N_j)(z_j)$.

Exemple VIII.7.8. Dans cet exemple, nous mettons en pratique la technique évoquée dans la remarque précédente. Soit la fraction rationnelle

$$R(z) = \frac{1}{(z-1)^2(z^2+1)}.$$

Pour utiliser les mêmes notations que dans la remarque, on pose

$$z_1 = 1,\ \alpha_1 = 2,\ z_2 = i,\ z_3 = -i \ \text{ et } \ \alpha_2 = \alpha_3 = 1.$$

Ainsi, la décomposition de R en fractions simples est de la forme

$$R(z) = \frac{a}{z-1} + \frac{b}{(z-1)^2} + \frac{c}{z-i} + \frac{d}{z+i}.$$

Pour déterminer les polynômes A_i, on peut réécrire R sous la forme

$$R(z) = \frac{\overbrace{a(z-1)+b}^{A_1}}{(z-1)^2} + \overbrace{\frac{c}{z-i}}^{A_2} + \overbrace{\frac{d}{z+i}}^{A_3}.$$

Ainsi,

$$\begin{array}{rclcl} N_1 & = & A_1\,(z-i)(z+i) & = & a\,(z-1)(z^2+1) + b\,(z^2+1) \\ N_2 & = & A_2\,(z-1)^2(z+i) & = & c\,(z-1)^2(z+i) \\ N_3 & = & A_3\,(z-1)^2(z-i) & = & d\,(z-1)^2(z-i) \end{array}$$

et

$$\left\{ \begin{array}{rcl} A(1) & = & N_1(1) \\ (D_zA)(1) & = & (D_zN_1)(1) \end{array} \right. , \quad A(i) = N_2(i), \quad A(-i) = N_3(-i).$$

Par conséquent, puisque $D_zN_1 = 3a\,z^2 + 2(b-a)\,z + a$, on a

$$\left\{ \begin{array}{rcl} 1 & = & 2\,b \\ 0 & = & 2a + 2b \end{array} \right. , \quad 1 = 2\,c\,i\,(i-1)^2, \quad 1 = -2\,d\,i\,(-1-i)^2.$$

et on trouve

$$a = -\frac{1}{2},\ b = \frac{1}{2},\ c = \frac{1}{4} \ \text{ et } \ d = \frac{1}{4}.$$

8. Polynômes et fractions rationnelles réels

Dans cette section, nous nous intéressons aux polynômes et fractions rationnelles à coefficients réels et nous mettons en évidence les différences essentielles avec le cas complexe.

Définition VIII.8.1. Un polynôme est *réel* si tous ses coefficients sont réels. L'ensemble des polynômes à coefficients réels se note $\mathbb{R}[z]$. Ainsi, l'ensemble des polynômes à coefficients réels est un sous-ensemble de $\mathbb{C}[z]$. Une fraction rationnelle $R = A/B$ est *réelle* si les polynômes A et B sont réels.

Soit

$$P = a_0 + a_1\,z + \cdots + a_k\,z^k$$

un polynôme à coefficients complexes. On pose, le *conjugué* de P, comme

$$\overline{P}(z) = \overline{a_0} + \overline{a_1}\,z + \cdots + \overline{a_k}\,z^k.$$

Ainsi, un polynôme P est réel si $\overline{P} = P$. De plus, il est clair que

$$\overline{P}(z) = \overline{P(\overline{z})}.$$

Proposition VIII.8.2. *Soit P un polynôme à coefficients réels. Si $z \in \mathbb{C}$ est un zéro α-uple de P, alors $\overline{z}$ est aussi un zéro α-uple de P.*

Démonstration. Soit $\mathcal{Z}$ l'ensemble des zéros de P. Puisque P est réel,

$$P(z) = \overline{P}(z) = \overline{P(\overline{z})}$$

et si z_0 est un zéro de P, alors $\overline{z_0}$ est aussi un zéro de P (si $P(z_0) = 0$, alors $\overline{P(\overline{z_0})} = 0$ et donc $P(\overline{z_0}) = 0$). Ainsi, $\mathcal{Z}$ est stable par conjugaison. C'est un ensemble de la forme

$$\mathcal{Z} = \{z_1, \ldots, z_r, z_{r+1}, \ldots, z_{r+s}, \overline{z_{r+1}}, \ldots, \overline{z_{r+s}}\}$$

où $z_1, \ldots, z_r \in \mathbb{R}$ et $z_{r+1}, \ldots, z_{r+s} \in \mathbb{C} \setminus \mathbb{R}$. Comme

$$D_z P = D_z \overline{P} = \overline{(D_z P)},$$

on a pour tout i

$$(D_z^i P)(z_j) = \overline{(D_z^i P)(\overline{z_j})}$$

et donc, la multiplicité d'un zéro z_j de P est la même que celle de $\overline{z_j}$.

■

Remarque VIII.8.3. Si on utilise les mêmes notations que dans la preuve précédente, on a

$$\begin{aligned} P(z) &= c\,(z-z_1)^{\alpha_1} \cdots (z-z_r)^{\alpha_r} (z-z_{r+1})^{\alpha_{r+1}} \cdots (z-z_{r+s})^{\alpha_{r+s}} \\ &\quad (z-\overline{z_{r+1}})^{\alpha_{r+1}} \cdots (z-\overline{z_{r+s}})^{\alpha_{r+s}} \end{aligned}$$

où c est le coefficient dominant de P et donc réel. De plus, pour tout $i \in \{r+1, \ldots, r+s\}$, on a

$$(z-z_i)\,(z-\overline{z_i}) = z^2 - 2\,(\mathfrak{Re}\, z_i)\, z + |z_i|^2 := Q_i(z)$$

avec $Q_i(z)$ un polynôme de degré 2 à coefficients réels et ainsi,

$$P(z) = c\,(z-z_1)^{\alpha_1} \cdots (z-z_r)^{\alpha_r}\, Q_{r+1}^{\alpha_{r+1}} \cdots Q_{r+s}^{\alpha_{r+s}}.$$

Les polynômes

$$(z-z_1), \ldots, (z-z_r), Q_{r+1}, \ldots, Q_{r+s}$$

ne peuvent pas être factorisés en produits de polynômes réels de degré strictement inférieur. C'est pour cette raison qu'on dit que ce sont des *polynômes irréductibles* sur $\mathbb{R}$. On dit que P a été décomposé en facteurs irréductibles sur $\mathbb{R}$.

Dans le cas d'une fraction rationnelle à coefficients réels, la décomposition en fractions rationnelles propres possède les propriétés suivantes.

Proposition VIII.8.4. *Soit $R = A/B$ une fraction rationnelle réelle et propre avec $B = B_1 \cdots B_m$ où les B_i sont des polynômes*[23] *deux à deux premiers entre eux. Supposons que*

$$\frac{A}{B} = \frac{A_1}{B_1} + \cdots + \frac{A_m}{B_m}$$

est une décomposition en fractions rationnelles propres de R. Si $B_j = \overline{B_k}$, alors $A_j = \overline{A_k}$. En particulier, si B_j est réel, alors A_j l'est aussi.

Démonstration. Puisque R est réel, on a

$$\begin{aligned}\frac{A_1}{B_1} + \cdots + \frac{A_j}{B_j} + \cdots + \frac{A_k}{B_k} + \cdots + \frac{A_m}{B_m} = \frac{A}{B}\\ = \frac{\overline{A}}{\overline{B}} = \frac{\overline{A_1}}{\overline{B_1}} + \cdots + \frac{\overline{A_j}}{\overline{B_j}} + \cdots + \frac{\overline{A_k}}{\overline{B_k}} + \cdots + \frac{\overline{A_m}}{\overline{B_m}}.\end{aligned}$$

Ceci montre que nous avons deux décomposition en fractions rationnelles propres de la même fraction. Or vu la remarque VIII.7.3, le numérateur A_j ne dépend que de B_j et ainsi, si $B_j = \overline{B_k}$, alors $A_j = \overline{A_k}$. En effet, cela résulte de l'unicité de la décomposition énoncée au théorème VIII.7.1

$$\frac{A}{B} = \frac{A_j}{B_j} + \frac{A'}{B_1 \cdots \widehat{B}_j \cdots B_m} = \frac{\overline{A_k}}{\overline{B_k}} + \frac{A'}{\overline{B_1 \cdots \widehat{B}_k \cdots B_m}}$$

et $B_j = \overline{B_k}$ et puisque $B = \overline{B}$, $B_1 \cdots \widehat{B}_j \cdots B_m = \overline{B_1 \cdots \widehat{B}_k \cdots B_m}$.

■

Si $R = A/B$ est une fraction rationnelle réelle, le dénominateur B ne peut pas nécessairement être factorisé en un produit de polynômes réels de degré 1. Par conséquent, la décomposition en fractions rationnelles simples prend une forme particulière.

Proposition VIII.8.5 (Décomposition en fractions simples sur $\mathbb{R}$). *Soit $R = A/B$ une fraction rationnelle propre réelle. Si la décomposition en facteurs irréductibles sur $\mathbb{R}$ de B est de la forme*

$$B = c\,(z - z_1)^{\alpha_1} \cdots (z - z_r)^{\alpha_r} Q_{r+1}^{\alpha_{r+1}} \cdots Q_{r+s}^{\alpha_{r+s}}$$

où les Q_i sont des polynômes réels irréductibles de degré 2, alors R se décompose de manière unique sous la forme

$$\begin{aligned}R \;=\; & \frac{c_{1,1}}{z - z_1} + \cdots + \frac{c_{1,\alpha_1}}{(z - z_1)^{\alpha_1}} + \cdots + \frac{c_{r,1}}{z - z_r} + \cdots + \frac{c_{r,\alpha_r}}{(z - z_r)^{\alpha_r}}\\ & + \frac{T_{r+1,1}}{Q_{r+1}} + \cdots + \frac{T_{r+1,\alpha_{r+1}}}{Q_{r+1}^{\alpha_{r+1}}} + \cdots + \frac{T_{r+s,1}}{Q_{r+s}} + \cdots + \frac{T_{r+s,\alpha_{r+s}}}{Q_{r+s}^{\alpha_{r+s}}}\end{aligned}$$

où les $c_{j,k}$ sont des nombres réels et les $T_{j,k}$ des polynômes réels de degré au plus 1.

[23] Dans cet énoncé, rien n'empêche les polynômes B_i d'avoir des coefficients complexes.

Démonstration. Au vu de la remarque VIII.8.3, les polynômes

$$(z-z_1)^{\alpha_1},\dots,(z-z_r)^{\alpha_r},Q_{r+1}^{\alpha_{r+1}},\dots,Q_{r+s}^{\alpha_{r+s}}$$

sont premiers entre eux. La fraction rationnelle R possède une décomposition en fractions rationnelles propres de la forme

$$R=\frac{A_1}{(z-z_1)^{\alpha_1}}+\cdots+\frac{A_r}{(z-z_r)^{\alpha_r}}+\frac{A_{r+1}}{Q_{r+1}^{\alpha_{r+1}}}+\cdots+\frac{A_{r+s}}{Q_{r+s}^{\alpha_{r+s}}}$$

où $\deg A_1<\alpha_1,\dots,\deg A_r<\alpha_r$ et $\deg A_{r+1}<2\,\alpha_{r+1},\dots,\deg A_{r+s}<2\,\alpha_{r+s}$. Au vu de la proposition VIII.8.4, pour $i\in\{1,\dots,r+s\}$, les polynômes A_i sont réels. On peut décomposer les r premiers polynômes A_i en utilisant la formule de Taylor. La démarche est identique à celle développée dans la preuve de la proposition VIII.7.6 et le résultat obtenu est semblable. Considérons à présent un terme de la forme

$$\frac{A_i}{Q_i^{\alpha_i}},\ i\in\{r+1,\dots,r+s\}.$$

Envisageons les divisions euclidiennes successives suivantes

$$\begin{aligned}
A_i &= T_{i,1}\,Q_i^{\alpha_i-1}+A_{i,1} && \text{, avec } \deg A_{i,1}<\deg Q_i^{\alpha_i-1}\\
A_{i,1} &= T_{i,2}\,Q_i^{\alpha_i-2}+A_{i,2} && \text{, avec } \deg A_{i,2}<\deg Q_i^{\alpha_i-2}\\
&\vdots\\
A_{i,\alpha_i-2} &= T_{i,\alpha_i-1}\,Q_i+A_{i,\alpha_i-1} && \text{, avec } \deg A_{i,\alpha_i-1}<\deg Q_i.
\end{aligned}$$

On pose $T_{i,\alpha_i}=A_{i,\alpha_i-1}$. Il est clair que pour tout j, $\deg T_{i,j}\le 1$ et

$$A_i=T_{i,1}\,Q_i^{\alpha_i-1}+T_{i,2}\,Q_i^{\alpha_i-2}+\cdots+T_{i,\alpha_i-1}\,Q_i+T_{i,\alpha_i}.$$

Il vient donc

$$\frac{A_i}{Q_i^{\alpha_i}}=\frac{T_{i,1}}{Q_i}+\frac{T_{i,2}}{Q_i^2}+\cdots+\frac{T_{i,\alpha_i-1}}{Q_i^{\alpha_i-1}}+\frac{T_{i,\alpha_i}}{Q_i^{\alpha_i}}.$$

On obtient ainsi l'existence de la décomposition annoncée. La démonstration de l'unicité de la décomposition est laissée en exercice au lecteur. Le raisonnement est semblable à celui développé dans la preuve de la proposition VIII.7.6.

∎

Remarque VIII.8.6. Pour calculer les coefficients $c_{j,k}$ et les coefficients des polynômes $T_{j,k}$, on procède essentiellement comme dans la remarque VIII.7.7. Si la décomposition en fractions simples sur $\mathbb{R}$ de la fraction rationnelle réelle $R=A/B$ est de la forme

$$\begin{aligned}
R &= \frac{c_{1,1}}{z-z_1}+\cdots+\frac{c_{1,\alpha_1}}{(z-z_1)^{\alpha_1}}+\cdots+\frac{c_{r,1}}{z-z_r}+\cdots+\frac{c_{r,\alpha_r}}{(z-z_r)^{\alpha_r}}\\
&\quad+\frac{T_{r+1,1}}{Q_{r+1}}+\cdots+\frac{T_{r+1,\alpha_{r+1}}}{Q_{r+1}^{\alpha_{r+1}}}+\cdots+\frac{T_{r+s,1}}{Q_{r+s}}+\cdots+\frac{T_{r+s,\alpha_{r+s}}}{Q_{r+s}^{\alpha_{r+s}}},
\end{aligned}$$

on pose, pour $j\in\{1,\dots,r\}$,

$$N_j=A_j(z-z_1)^{\alpha_1}\cdots\widehat{(z-z_j)^{\alpha_j}}\cdots(z-z_r)^{\alpha_r}\,Q_{r+1}^{\alpha_{r+1}}\cdots Q_{r+s}^{\alpha_{r+s}}$$

et pour $j \in \{r+1, \dots, r+s\}$,

$$M_j = A_j \, (z - z_1)^{\alpha_1} \cdots (z - z_r)^{\alpha_r} \, Q_{r+1}^{\alpha_{r+1}} \cdots \widehat{Q_j^{\alpha_j}} \cdots Q_{r+s}^{\alpha_{r+s}}.$$

Ainsi, en réduisant au même dénominateur, on obtient

$$\frac{A}{B} = \frac{N_1 + \cdots + N_r + M_{r+1} + \cdots + M_{r+s}}{B}.$$

Pour $j \in \{1, \dots, r\}$, on procède comme à la remarque VIII.7.7. Puisque $z_j \in \mathbb{R}$ est un zéro α_j-uple de N_i pour $i \in \{1, \dots, r\} \setminus \{j\}$ et de M_i pour $i \in \{r+1, \dots, r+s\}$, pour trouver les coefficients $c_{j,1}, \dots, c_{j,\alpha_j}$, on résout le système linéaire triangulaire

$$\left\{ \begin{array}{rcl} A(z_j) & = & N_j(z_j) \\ (D_z A)(z_j) & = & (D_z N_j)(z_j) \\ & \vdots & \\ (D_z^{\alpha_j - 1} A)(z_j) & = & (D_z^{\alpha_j - 1} N_j)(z_j). \end{array} \right.$$

Pour $j \in \{r+1, \dots, r+s\}$, puisque $z_j \in \mathbb{C}$ est zéro α_j-uple de M_i pour $i \in \{r+1, \dots, r+s\} \setminus \{j\}$ et de N_i pour $i \in \{1, \dots, r\}$, pour trouver les deux coefficients réels de chacun des polynômes $T_{j,1}, \dots, T_{j,\alpha_j}$, on résout le système à coefficients complexes

$$\left\{ \begin{array}{rcl} A(z_j) & = & M_j(z_j) \\ (D_z A)(z_j) & = & (D_z M_j)(z_j) \\ & \vdots & \\ (D_z^{\alpha_j - 1} A)(z_j) & = & (D_z^{\alpha_j - 1} M_j)(z_j). \end{array} \right.$$

Exemple VIII.8.7. Appliquons la méthode précédente à un exemple. Soit la fraction rationnelle réelle

$$R(z) = \frac{1}{(z-1)^2 \, (z^2+1)^2}.$$

La décomposition en fractions simples sur $\mathbb{R}$ est de la forme

$$R = \frac{a}{z-1} + \frac{b}{(z-1)^2} + \frac{cz+d}{z^2+1} + \frac{ez+f}{(z^2+1)^2}.$$

Avec les notations de la remarque, on a

$$z_1 = 1, \ \alpha_1 = 2, \ z_2 = i, \ \alpha_2 = 2.$$

Puisque

$$R = \frac{\overbrace{a(z-1)+b}^{A_1}}{(z-1)^2} + \frac{\overbrace{(cz+d)(z^2+1)+ez+f}^{A_2}}{(z^2+1)^2},$$

on trouve

$$N_1 = A_1 \, (z^2+1)^2 = (az + b - a) \, (z^2+1)^2$$

et

$$M_2 = A_2 \, (z-1)^2 = (cz^3 + dz^2 + (c+e)z + d + f) \, (z-1)^2.$$

Pour déterminer a et b, puisque $\alpha_1 = 2$, il suffit de résoudre

$$\left\{\begin{array}{rcl} A(1) & = & N_1(1) \\ (D_zA)(1) & = & (D_zN_1)(1) \end{array}\right. , \text{ i.e., } \left\{\begin{array}{rcl} 1 & = & 4b \\ 0 & = & 4a+8b \end{array}\right.$$

et ainsi, on trouve $a = -\frac{1}{2}$ et $b = \frac{1}{4}$. Pour déterminer c, d, e, f, on résout

$$\left\{\begin{array}{rcl} A(i) & = & M_2(i) \\ (D_zA)(i) & = & (D_zM_2)(i) \end{array}\right.$$

c'est-à-dire

$$\left\{\begin{array}{rcl} 1 & = & (ei+f)(i-1)^2 \\ 0 & = & (e-2c+2di)(i-1)^2 + 2(ei+f)(i-1) \end{array}\right.$$

et donc

$$\left\{\begin{array}{rcl} 1 & = & 2e-2f\,i \\ 0 & = & 4d-2e-2f+(4c-4e+2f)\,i \end{array}\right.$$

En égalant les parties réelles et imaginaires des deux membres de chacune des équations (c, d, e, f sont réels), on trouve

$$e = \frac{1}{2},\ f = 0,\ c = \frac{1}{2},\ d = \frac{1}{4}.$$

CHAPITRE IX

Polynômes à coefficients dans un champ quelconque

1. Premières définitions

Nous quittons ici le cadre des polynômes à coefficients réels ou complexes pour considérer la situation générale de polynômes dont les coefficients appartiennent à un champ quelconque $\mathbb{K}$.

Définition IX.1.1. Un *polynôme* à coefficients dans $\mathbb{K}$ est la donnée d'une suite $(c_j)_{j\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ dont seul un nombre fini d'entre eux sont non nuls. On note de manière symbolique un polynôme comme suit

$$P = \sum_{j\geq 0} c_j\, X^j.$$

On dit souvent que X est une *indéterminée*. Dans une telle écriture, il suffit de représenter uniquement les termes ayant un coefficient non nul. Si la suite $(c_j)_{j\in\mathbb{N}}$ possède un unique élément c_k non nul, on parle du *monôme* $c_k\, X^k$.

Ainsi, si la suite de coefficients définissant un polynôme P est différente de la suite nulle, il existe un plus petit entier $N \geq 0$ tel que

$$\forall j > N,\ c_j = 0.$$

Cet entier N est le *degré* du polynôme et on le note $\deg P$. Dans ce cas, c_N s'appelle le *coefficient dominant* de P et $c_N\, X^N$ s'appelle le *monôme de plus haut degré*. Dans le cas où la suite $(c_j)_{j\in\mathbb{N}}$ est la suite nulle, on pose[1] le degré du polynôme nul comme étant $-\infty$. L'ensemble des polynômes à coefficients dans $\mathbb{K}$ se note $\mathbb{K}[X]$.

Exemple IX.1.2. Soit $\mathbb{K} = \mathbb{Z}_5$. Le polynôme P déterminé par la suite de coefficients $(1, 0, 3, 4, 0, 0, \ldots)$ se note

$$1 + 3\, X^2 + 4X^3.$$

Il s'agit d'un polynôme de degré 3.

Définition IX.1.3. Si

$$P = \sum_{j\geq 0} c_j\, X^j$$

est un polynôme de $\mathbb{K}[x]$ et si $x \in \mathbb{K}$, alors on note

$$P(x) = \sum_{j\geq 0} c_j\, x^j$$

[1] Cette convention est identique à celle prise dans la définition VIII.1.6.

l'élément de $\mathbb{K}$ obtenu en substituant x à l'indéterminée dans P. Une *fonction polynomiale* est une fonction $f : \mathbb{K} \to \mathbb{K}$ telle que

$$f(x) = P(x),\ \forall x \in \mathbb{K}$$

et où P est un polynôme à coefficients dans $\mathbb{K}$.

Exemple IX.1.4. Si on poursuit l'exemple IX.1.2, la fonction polynomiale associée à $P = 1 + 3\,X^2 + 4X^3$ est telle que

x	0	1	2	3	4
$P(x)$	1	3	0	1	0

.

Remarque IX.1.5. Nous avons vu que pour les polynômes à coefficients réels ou complexes, il n'y avait aucune distinction entre polynôme et fonction polynomiale (deux fonctions polynomiales sont différentes si et seulement si les suites de coefficients des deux polynômes correspondants sont distinctes). La situation est différente dans $\mathbb{K}[x]$. Par exemple, considérons le champ $\mathbb{K} = \mathbb{Z}_3$ et les polynômes P et Q définis respectivement par les suites $(1, 2, 1, 0, \ldots)$ et $(1, 1, 2, 1, 2, 0, \ldots)$. Ces deux polynômes définissent la même fonction polynomiale

x	0	1	2
$P(x)$	1	1	0

x	0	1	2
$Q(x)$	1	1	0

.

En effet, dans $\mathbb{Z}_3$,

$$1 + 2.0 + 1.0^2 = 1, \quad 1 + 2.1 + 1.1^2 = 1 \quad \text{et} \quad 1 + 2.2 + 1.2^2 = 0;$$

$$1 + 1.0 + 2.0^2 + 1.0^3 + 2.0^4 = 1, \quad 1 + 1.1 + 2.1^2 + 1.1^3 + 2.1^4 = 1$$

et

$$1 + 1.2 + 2.2^2 + 1.2^3 + 2.2^4 = 0.$$

On peut même être plus précis. Si $\mathbb{K}$ est un champ fini contenant p éléments, le nombre de fonctions distinctes définies sur $\mathbb{K}$ et à valeurs dans $\mathbb{K}$ est fini et vaut exactement p^p. Le nombre de polynômes à coefficients dans $\mathbb{K}$ de degré n est p^{n+1}. Ainsi, pour n suffisamment grand, on a $p^{n+1} > p^p$ et il existe donc au moins deux polynômes distincts donnant lieu à la même fonction polynomiale. Par contre, on peut montrer[2] que si $\mathbb{K}$ est un champ infini, alors deux polynômes distincts donnent lieu à des fonctions polynomiales différentes.

On peut munir l'ensemble $\mathbb{K}[X]$ d'une structure d'anneau commutatif. Pour cela, nous devons définir l'addition et la multiplication de deux polynômes. Ainsi, si P et Q sont deux polynômes donnés respectivement par les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$, alors la somme de P et de Q est le polynôme

$$P + Q = \sum_{j\geq 0} (a_j + b_j)\, X^j$$

[2]En utilisant par exemple la notion de dérivée.

et le produit des deux polynômes est défini, de manière naturelle, par

$$P.Q = \sum_{j\geq 0} \left(\sum_{k+\ell=j} a_k\, b_\ell \right) X^j.$$

Pour tout $a \in \mathbb{K}$, la suite $(a, 0, 0, 0, \ldots)$ est un polynôme de $\mathbb{K}[X]$. Ainsi, l'application

$$\mathbb{K} \to \mathbb{K}[X] : a \mapsto \sum_{j\geq 0} (a\, \delta_{j,0})\, X^j$$

est injective. De cette manière, on peut identifier $\mathbb{K}$ et l'ensemble des polynômes sur $\mathbb{K}$ de degré 0. Par abus de langage, on s'autorise à parler du polynôme a lorsque a est un élément de $\mathbb{K}$.

Proposition IX.1.6. *L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients sur $\mathbb{K}$ possède une structure d'anneau commutatif ayant*

$$\sum_{j\geq 0} 0\, X^j$$

comme neutre pour l'addition et 1 comme unité pour la multiplication.

Remarque IX.1.7. Le lecteur attentif pourrait espérer trouver en $\mathbb{K}[X]$ une structure de champ. Il n'en est rien. En effet, par exemple, le polynôme X ne possède pas d'inverse. Supposons que

$$P = \sum_{j\geq 0} a_j\, X^j$$

soit l'inverse de X (avec au moins un des a_j non nul). Dès lors,

$$P.X = \sum_{j\geq 0} a_j\, X^{j+1} \neq 1.$$

Proposition IX.1.8. *Soient P, Q deux polynômes de $\mathbb{K}[X]$. On a*[3]

- $\deg(P+Q) \leq \sup\{\deg P, \deg Q\}$,
- $\deg(P.Q) = \deg P + \deg Q$.

Démonstration. Cela découle directement de la définition du degré d'un polynôme. Comme le montre l'exemple ci-dessous, le degré de la somme de deux polynômes peut diminuer. Pour $\mathbb{K} = \mathbb{Z}_3$, $P = 2X^2 + X + 1$, $Q = X^2 + X + 1$, on trouve $P + Q = 2X + 2$. Par contre, si P et Q sont deux polynômes ayant respectivement $a_M\, X^M$ et $b_N\, X^N$ comme monôme de plus haut degré, alors $P.Q$ possède $a_M b_N\, X^{M+N}$ comme monôme de plus haut degré. En effet, puisque $\mathbb{K}$ est un champ[4], $a_M b_N$ ne peut être nul.

■

[3] Si l'un des polynômes est nul, on pose $\sup\{-\infty, n\} = n$ et $-\infty + n = -\infty$.

[4] Si $\mathbb{K}$ n'est pas un champ, mais simplement un anneau, cela n'est plus nécessairement vrai. En effet, pour $\mathbb{K} = \mathbb{Z}^4$, si $P = 2X^2 + 3$ et $Q = 2X^2 + 3X + 1$, on trouve $P.Q = 2\,X^3 + X + 3$.

Corollaire IX.1.9. *Soient P, Q deux polynômes de $\mathbb{K}[X]$. L'égalité $P.Q = 0$ entraîne que $P = 0$ ou que $Q = 0$.*

Démonstration. Procédons par contraposition. Si $P \neq 0$ et $Q \neq 0$, alors $\deg P \geq 0$ et $\deg Q \geq 0$. Au vu de la proposition précédente, on a alors $\deg(P.Q) \geq 0$ et $P.Q$ n'est donc pas le polynôme nul.

■

Remarque IX.1.10. Le corollaire précédent nous montre que la seule façon d'obtenir le polynôme nul comme produit de deux polynômes P et Q est qu'au moins un de ces deux polynômes soit nul. Un anneau jouissant d'une telle propriété est appelé *intègre*[5].

Tout comme dans $\mathbb{C}[z]$ (cf. théorème VIII.5.1), on dispose de la division euclidienne.

Proposition IX.1.11 (Division euclidienne). *Soit $D \in \mathbb{K}[X]$ un polynôme non nul. Pour tout $P \in \mathbb{K}[X]$, il existe des polynômes uniques Q et R tels que*

$$P = Q\,D + R, \quad \textit{avec } \deg R < \deg D.$$

Démonstration. On procède comme dans le cas de $\mathbb{C}[z]$.

■

Tout comme dans $\mathbb{C}[z]$, si le reste R de la division de P par D est nul, on dit que D *divise* P.

2. Idéal d'un anneau

Pour étudier plus en avant la divisibilité dans $\mathbb{K}[X]$, nous allons introduire la notion d'idéal d'un anneau A. Nous supposerons dans cette section que A est un anneau commutatif muni, comme à l'habitude, de deux opérations notées $+$ et $\cdot$ ayant pour neutre respectivement 0 et 1.

Définition IX.2.1. Un sous-ensemble I de A est un *idéal* de A si les deux conditions suivantes sont satisfaites :

- I est un sous-groupe additif de A, i.e., l'ensemble I muni de l'opération $+$ de A restreinte aux éléments de I jouit d'une structure de groupe
  - $0 \in I$,
  - $\forall i, j \in I : i + j \in I$,
  - $\forall i \in I : -i \in I$.
- Pour tout $a \in A$ et tout $i \in I$, $a.i \in I$.

Remarque IX.2.2. Si I est non vide, pour vérifier que I est un idéal de A, il suffit de vérifier que

[5] Un anneau quelconque n'est pas nécessairement intègre. En effet, on a vu dans l'exemple II.3.23 que dans $\mathbb{Z}_{21}$, on avait $[3].[7] = [0]$. Ainsi, bien que les classes $[3]$ et $[7]$ soient toutes deux différentes de la classe $[0]$, leur produit donne $[0]$. Ces éléments de $\mathbb{Z}_{21}$ sont appelés des *diviseurs de zéro* et $\mathbb{Z}_{21}$ n'est donc pas un anneau intègre.

- I est stable par addition : $\forall i, j \in I : i + j \in I$,
- le produit d'un élément quelconque de A par un élément quelconque de I appartient encore à I.

En effet, il suffit de remarquer que si $i \in I$, on a toujours $-1 \in A$ et donc $-i = (-1).i$ doit appartenir à I au vu de la seconde propriété. De là, on en conclut aussi que 0 appartient à I.

Proposition IX.2.3. *Soit I un idéal de A. Si 1 appartient à I, alors $I = A$.*

Démonstration. Puisque $1 \in I$, pour tout $a \in A$, $1.a$ doit appartenir à I.

■

Définition IX.2.4. Un idéal I d'un anneau A est dit *propre* s'il est distinct de A. Ainsi, un idéal I est propre si et seulement si $1 \notin I$.

Exemple IX.2.5. Les ensembles $\{0\}$ et A sont des idéaux. On les appelle *idéaux triviaux* de A. Remarquons que si A est un champ, au vu de la proposition précédente, ce sont les seuls idéaux de A. En effet, si I est un idéal non vide de A distinct de $\{0\}$, il contient un élément $i \neq 0$. L'élément i^{-1} appartient à A (car A est un champ) et donc, puisque I est un idéal, $i.i^{-1} = 1$ appartient à I. On conclut en utilisant la proposition précédente.

Exemple IX.2.6. Dans $\mathbb{Z}$, l'ensemble $I = \{m\,r \mid r \in \mathbb{Z}\}$ des multiples de $m \geq 0$ est un idéal[6]. En effet,

$$m\,r + m\,s = m\,(r + s) \in I$$

et, pour tout $t \in \mathbb{Z}$

$$(m\,r).t = m\,(tr) \in I.$$

Exemple IX.2.7. Dans $\mathbb{C}[z]$, il est facile de vérifier que

$$\{P \in \mathbb{C}[z] \mid P(0) = 0\}$$

et

$$\{P \in \mathbb{C}[z] \mid P(0) = P(1) = 0\}$$

sont des idéaux de $\mathbb{C}[z]$. Par contre,

$$B = \{P \in \mathbb{C}[z] \mid P(0) = P(1)\}$$

n'est pas un idéal. En effet, $1+z(z-1) \in B$ mais $z.[1+z(z-1)]$ n'appartient pas à B.

Définition IX.2.8. Soient $a_1, \ldots, a_k$ des éléments de A. Il est aisé de vérifier que l'ensemble

D'où l'intérêt d'avoir supposé A commutatif.

$$\langle a_1, \ldots, a_k \rangle = \{b_1 a_1 + \cdots + b_k a_k \mid b_1, \ldots, b_k \in A\}$$

est un idéal. On l'appelle l'*idéal engendré*[7] par $a_1, \ldots, a_k$.

[6] On note parfois cet ensemble $m\mathbb{Z}$.

[7] D'une certaine façon, l'idéal engendré par $a_1, \ldots, a_k$ dans un anneau commutatif est le pendant de la notion d'enveloppe linéaire développée dans le cadre des espaces vectoriels (cf. proposition VII.5.12). Cela dépend simplement des opérations dont on dispose.

Définition IX.2.9. Si un idéal I est engendré par un unique élément, i.e., si I est de la forme $\langle a\rangle$, $a \in A$, alors I est dit *principal*.

Exemple IX.2.10. Dans $\mathbb{Z}$, l'ensemble I des multiples de $m > 0$ est un idéal principal,

$$I = \langle m\rangle = \{m\, r \mid r \in \mathbb{Z}\}.$$

Exemple IX.2.11. Dans $\mathbb{Z}$, soient les idéaux principaux $\langle 3\rangle$, $\langle 6\rangle$ et $\langle 7\rangle$. On a par exemple,

Tout multiple de 6 est multiple de 3.

$$\langle 6\rangle \subset \langle 3\rangle,$$
$$\langle 6\rangle \cap \langle 7\rangle = \langle 42\rangle$$

ou encore

$$\langle 6, 7\rangle = \mathbb{Z} \text{ car } 7 - 6 = 1 \in \langle 6, 7\rangle.$$

Exemple IX.2.12. Soit le polynôme $X^2 + 1 \in \mathbb{C}[X]$. Par définition,

$$\langle X^2 + 1\rangle = \{(X^2 + 1).Q(X) \mid Q \in \mathbb{C}[X]\}.$$

Ainsi,

$$X^2{+}1, 2X^2{+}2, iX^2{+}i, X^3{+}X, X^4{+}X^2, (X^2{+}1)^2, (X^2{+}1)(X^3{-}5X{+}i), \ldots$$

Tout multiple de $X^3 + X$ est un multiple de $X^2 + 1$.

sont des éléments de $\langle X^2 + 1\rangle$. Par exemple,

$$\langle X^3 + X\rangle \subset \langle X^2 + 1\rangle$$

et cette inclusion est stricte. Par contre

$$\langle 2X^2 + 2\rangle = \langle X^2 + 1\rangle.$$

Enfin,

$$\langle X^2 - 1, X^2 + X - 2\rangle = \langle X - 1\rangle.$$

$X^2 + X - 2 = (X - 1)(X + 2)$.

Il est clair que $\langle X^2 - 1, X^2 + X - 2\rangle \subset \langle X - 1\rangle$ car quels que soient $P, Q \in \mathbb{C}[X]$, un élément quelconque du premier ensemble s'écrit

$$P.(X^2 - 1) + Q.(X^2 + X - 2) = [P.(X + 1) + Q.(X + 2)].(X - 1)$$

et appartient donc au second. Pour l'autre inclusion, on remarque que, quel que soit $P \in \mathbb{C}[X]$, un élément quelconque du second idéal $P.(X - 1) = P.(X^2 + X - 2) - P.(X^2 - 1)$ appartient donc à $\langle X^2 - 1, X^2 + X - 2\rangle$.

Définition IX.2.13. Un anneau intègre A (i.e., tel que pour tous $a, b \in A$, $ab = 0$ implique $a = 0$ ou $b = 0$) qui est tel que tout idéal de A est principal est qualifié d'*anneau principal*.

Cela nous permettra de définir la notion de polynôme minimum...

Proposition IX.2.14. *L'anneau des polynômes $\mathbb{K}[X]$ est principal.*

Démonstration. Il est tout d'abord clair que $\mathbb{K}[X]$ est intègre. Cela résulte du corollaire IX.1.9. Nous devons à présent vérifier que tout idéal de $\mathbb{K}[X]$ est principal. Soit I un idéal de $\mathbb{K}[X]$. Si $I = \{0\}$, alors $I = \langle 0 \rangle$. Sinon, I contient au moins un polynôme non nul. Soit D un polynôme de degré minimum appartenant à I. Il est évident[8] que $\langle D \rangle \subset I$. Pour conclure cette preuve, il nous reste à montrer que $\langle D \rangle \supset I$. Soit P un élément de I. En effectuant la division euclidienne de P par D, on obtient

$$P = Q.D + R \quad \text{avec} \quad \deg R < \deg D.$$

Puisque D appartient à I, on en conclut que $Q.D$ et $R = P - Q.D$ aussi. Or on a choisi D de degré minimum parmi les éléments de I. Par conséquent, $R = 0$ et $P = Q.D$. Ceci conclut la preuve.

■

Proposition IX.2.15. *L'anneau $\mathbb{Z}$ est principal.*

Démonstration. Puisque $\mathbb{Z}$ est lui aussi muni de la division euclidienne, on peut refaire le même raisonnement que dans la preuve de la proposition précédente. Il suffit de remplacer les degrés des polynômes par les modules des entiers considérés.

■

La proposition suivante relie la notion d'idéal à celle de la divisibilité.

Proposition IX.2.16. *Soient A un anneau principal*[9] *et $a, b \in A \setminus \{0\}$. On a*

- *$\langle a \rangle \supset \langle b \rangle$ si et seulement si a divise b.*
- *$\langle a \rangle = \langle b \rangle$ si et seulement si $a = ub$ avec u inversible dans A. (Dans ce cas, on dit que a et b sont associés*[10]*.)*

Démonstration. Supposons que $\langle a \rangle \supset \langle b \rangle$. En particulier, b appartient à $\langle a \rangle$ et il existe donc $c \in A$ tel que $b = ca$. Ainsi, a divise b. Réciproquement, si a divise b, il existe $c \in A$ tel que $b = ca$. Dès lors, pour tout $t \in A$, $tb = tca$ ce qui montre que $\langle b \rangle$ est inclus dans $\langle a \rangle$.

Pour la seconde partie, si $a = ub$ avec u inversible dans A, on a aussi $u^{-1}a = b$ (avec u^{-1} l'inverse de u, i.e., $u^{-1}.u = 1$). Ainsi, a divise b et b divise a. Donc par le premier point, $\langle a \rangle = \langle b \rangle$. Réciproquement, si $\langle a \rangle = \langle b \rangle$, alors il existe u et v dans A tels que $a = ub$ et $b = va$. De là, $b = vub$ et donc, puisque l'anneau est intègre, $b(vu - 1) = 0$ implique $vu = 1$. Ceci signifie que u et v sont inversibles et inverses l'un de l'autre.

■

[8] En effet, $D \in I$ et $\langle D \rangle = \{P.D \mid P \in \mathbb{K}[X]\}$. Puisque I est un idéal, il est clair que pour tout $P \in \mathbb{K}[X]$, $P.D \in I$.

[9] On suppose l'anneau principal muni d'une division euclidienne comme par exemple $\mathbb{Z}$ ou $\mathbb{K}[X]$.

[10] Vérifier que "être associé" est une relation d'équivalence

Exemple IX.2.17. Illustrons la propriété précédente. Dans l'exemple IX.2.11, on avait montré que $\langle 6\rangle \subset \langle 3\rangle$ et il est clair que 3 divise 6.

De même, $\langle 2X^2+2\rangle = \langle X^2+1\rangle$. Il s'agit de deux polynômes sont associés. En effet, $2\,(X^2+1) = 2X^2+2$ et 2 est inversible dans $\mathbb{C}[X]$ (d'inverse 1/2).

Remarque IX.2.18. Si I est un idéal propre d'un anneau principal A, il peut y avoir plusieurs éléments $a \in A$ tels que $I = \langle a\rangle$. Si a est un tel élément, les autres éléments $b \in A$ tels que $I = \langle b\rangle$ sont associés à a.

Par exemple, dans $\mathbb{Z}$, les seuls éléments inversibles sont 1 et -1 (ils sont leur propre inverse). Ainsi deux entiers x et y sont associées si et seulement si $x = \pm y$.

De même, dans $\mathbb{K}[X]$, deux polynômes non nuls P et Q sont associés si et seulement si il existe $\alpha \in \mathbb{K}\setminus\{0\}$ tel que $P = \alpha Q$. En effet, les seuls éléments inversibles de $\mathbb{K}[X]$ sont les constantes $\alpha \in \mathbb{K}\setminus\{0\}$. Ainsi, parmi tous les polynômes associés à un polynôme P, il en existe un seul tel que son coefficient dominant soit 1. Un tel polynôme est dit *unitaire* ou *monique*. En effet, si P est un polynôme de coefficient dominant α, alors $\alpha^{-1}P$ est un polynôme monique associée à P.

Enfin, notez que dans un anneau principal A, $a \in A$ est inversible si et seulement si a est associé à 1.

Proposition IX.2.19. *Soient A un anneau principal et a, b deux éléments non nuls de A. Un p.g.c.d. d de a et de b est donné par*

$$\langle d\rangle = \langle a, b\rangle.$$

De plus, tout autre p.g.c.d. de a et de b est associé à d et il existe $\alpha, \beta \in A$ tels que

Pensez au théorème de Bezout.

$$d = \alpha\, a + \beta\, b.$$

Démonstration. Vérifions que d est un p.g.c.d. de a et de b. Il est clair que $\langle a\rangle$ et $\langle b\rangle$ sont inclus dans $\langle d\rangle = \langle a, b\rangle$. Par la proposition précédente, d divise donc a et b. Si d' divise aussi a et b, alors $\langle a\rangle$ et $\langle b\rangle$ sont inclus dans $\langle d'\rangle$. De là[11], $\langle a, b\rangle$ est aussi inclus dans $\langle d'\rangle$ et donc d' divise d. Le reste de la preuve est immédiat. En effet, si e est aussi un p.g.c.d. de a et de b, alors $\langle d\rangle = \langle a, b\rangle = \langle e\rangle$ et d et e sont donc associés.

■

Exemple IX.2.20. Par exemple, $\langle 6, 7\rangle = \mathbb{Z} = \langle 1\rangle$ (cf. exemple IX.2.11). Il est clair que 6 et 7 sont premiers entre eux. Dans l'exemple IX.2.12, on a vu que

$$\langle X^2-1, X^2+X-2\rangle = \langle X-1\rangle.$$

Il est facile de voir que ces deux polynômes ont $X-1$ comme p.g.c.d.

[11] Un élément quelconque de $\langle a, b\rangle$ est de la forme $r.a + s.b$. Or $a = t.d'$ et $b = u.d'$. De là, $r.a + s.b = (rt + su)d'$ appartient bien à $\langle d'\rangle$.

De la même manière, les polynômes de $\mathbb{R}[X]$

$$A = 2X^2+5X+2 = (2X+1)(X+2) \text{ et } B = 2X^2+7X+3 = (2X+1)(X+3)$$

sont tels que

$$\langle A, B\rangle = \langle 2X+1\rangle$$

et tout polynôme de la forme $\alpha(2X+1)$, $\alpha \in \mathbb{R}$, est un p.g.c.d. de A et de B. En particulier, le polynôme monique $\frac{1}{2}(2X+1) = X + \frac{1}{2}$ est aussi un p.g.c.d. de A et de B.

3. Décomposition en facteurs premiers

Définition IX.3.1. Soit A un anneau principal. Deux éléments non nuls $a, b \in A$ sont *premiers entre eux* si les p.g.c.d. de a et de b sont associés à 1, autrement dit, si 1 est un de leur p.g.c.d.

Définition IX.3.2. Soit A un anneau intègre. Un élément $a \in A$ non nul est *irréductible* s'il est non associé à 1 et s'il s'écrit $a = bc$ avec $b, c \in A$, alors b ou c est associé à 1. Autrement dit, tout diviseur de a est associé à 1 ou à a.

Définition IX.3.3. Soit A un anneau intègre. Un élément $a \in A$ est *premier*, s'il est non nul et non associé à 1 et si a divise bc, alors a divise b ou c. En termes d'idéaux, cela revient à dire $\langle a\rangle \neq A$ et si $bc \in \langle a\rangle$, alors $b \in \langle a\rangle$ ou $c \in \langle a\rangle$. Un idéal jouissant d'une telle propriété est qualifié d'*idéal premier*.

Remarque IX.3.4. Dans un anneau intègre A, *tout élément premier est irréductible*. Soit a un élément premier. Supposons que $a = bc$, $b, c \in A$. Alors $bc \in \langle a\rangle$ implique $b \in \langle a\rangle$ ou $c \in \langle a\rangle$. Supposons être dans le premier cas, il existe $d \in A$ tel que $b = ad$ donc $a = acd$. Puisque A est intègre, on conclut que $cd = 1$, i.e., c est associé à 1. comme dans la propostion IX.2.16

La réciproque n'est pas toujours vraie[12]. Par exemple, dans l'anneau $\mathbb{Z}[i\sqrt{5}]$ des polynômes à coefficients entiers évalués en $i\sqrt{5}$, on peut montrer[13] que l'élément 3 est irréductible. Cependant, il n'est pas premier, 3 divise $9 = (2+i\sqrt{5})(2-i\sqrt{5})$ mais ne divise aucun des deux facteurs.

Lemme IX.3.5. *Soient a, b et c des éléments non nuls d'un anneau principal A. Si a divise bc et est premier avec b, alors a divise c.*

Démonstration. Au vu de la proposition IX.2.19, il existe α et β dans A tels que $1 = \alpha a + \beta b$. De plus, a divise bc. Il existe donc $t \in A$ tel que $bc = ta$. Ainsi, $c = \alpha ac + \beta bc = \alpha ac + \beta ta = (\alpha c + \beta t)a$ et a divise c.

■

Dans un anneau principal, les deux notions d'élément premier et d'élément irréductible coïncident.

[12] Il faut se placer dans un anneau factoriel (ou à factorisation unique). Tout anneau principal est factoriel.

[13] En recourant à la notion algébrique de norme, par exemple.

Proposition IX.3.6. *Soit A un anneau principal. Tout élément irréductible est premier. Par conséquent, un élément est premier si et seulement si il est irréductible.*

Démonstration. Procédons par l'absurde. Soit a un élément irréductible non premier. Supposons que $bc \in \langle a \rangle$, $b, c \in A$ avec $b \notin \langle a \rangle$ et $c \notin \langle a \rangle$. Considérons l'idéal $\langle a, b \rangle$. Puisque A est principal, il existe d tel que $\langle a, b \rangle = \langle d \rangle$. Il existe donc $e, f \in A$ tels que $a = de$ et $b = df$. Puisque a est irréductible, d ou e est associé à 1. Dans le premier cas, cela signifie que a et b sont premiers entre eux. Or a divise bc, donc a divise c, ce qui contredit $c \notin \langle a \rangle$. Dans l'autre cas, si e est associé à 1, alors $\langle a \rangle = \langle d \rangle = \langle a, b \rangle$ contient b, ce qui contredit $b \notin \langle a \rangle$.

■

Exemple IX.3.7. Dans $\mathbb{Z}$, les seuls éléments inversibles sont 1 et -1 (ils sont d'ailleurs leur propre inverse). Ainsi, deux *entiers positifs* sont *premiers entre eux* si leur p.g.c.d. est 1. Par exemple, 3 et 16 sont premiers entre eux mais 3 et 15 ne le sont pas. Enfin, un *nombre* $p > 1$ est *premier* si ses seuls diviseurs sont 1 et p (et bien sûr -1 et $-p$). Par exemple, $2, 3, 5, 7$ sont premiers mais 8 et 9 ne le sont pas.

Exemple IX.3.8. Dans $\mathbb{K}[X]$, nous avons déjà observé que les seuls éléments inversibles sont les éléments non nuls de $\mathbb{K}$ (i.e., les polynômes constants non nuls). Ainsi, un polynôme non nul est associé à 1 si et seulement s'il est constant. Par conséquent, deux polynômes sont *premiers entre eux* s'ils ne sont pas tous deux divisibles par un polynôme non constant et un polynôme $P \in \mathbb{K}[X]$ non constant est *irréductible* si et seulement si ses seuls diviseurs sont de la forme α ou αP avec $\alpha \in \mathbb{K} \setminus \{0\}$.

Autrement dit, un polynôme P de $\mathbb{K}[X]$ est *irréductible* s'il est non constant (i.e., de degré au moins 1) et s'il ne peut pas s'écrire comme produit de deux polynômes de degré strictement inférieur à $\deg P$.

Dans la suite de cette section, A est un anneau principal. On ne distinguera donc pas les notions d'élément premier et d'élément irréductible. Le but de cette section est de montrer que tout élément non nul de A peut s'écrire de manière unique comme produit d'éléments premiers. Par exemple, dans $\mathbb{Z}$, $1176 = 2^3.3.7^2$.

Lemme IX.3.9. *Toute suite croissante $I_1 \subset I_2 \subset I_3 \subset \cdots$ d'idéaux de A est stationnaire, i.e., il existe $N \geq 1$ tel que pour tout $n \geq N$, $I_n = I_N$.*

On dit aussi "se stabilise".

Démonstration. Il est facile de vérifier que

$$I = \bigcup_{n \geq 1} I_n$$

est encore un idéal de A. Or A étant un anneau principal, cela signifie qu'il existe $d \in A$ tel que $I = \langle d \rangle$. Puisque d appartient à I, il existe N tel que

d appartienne à I_N. La suite d'idéaux étant croissante, d appartient aussi à I_n pour tout $n \geq N$. Ainsi, pour tout $n \geq N$,

$$\langle d \rangle \subset I_n \subset I = \langle d \rangle,$$

ce qui suffit.

■

Proposition IX.3.10. *Si $a \in A$ est un élément non nul et non associé à 1, alors il existe des éléments premiers $p_1, \ldots, p_m$ tels que*

$$a = p_1 \cdots p_m.$$

A l'ordre des facteurs près, cette décomposition est unique (sous-entendu qu'il est autorisé de remplacer les facteurs apparaissant dans cette décomposition par des facteurs qui leur sont associés).

Démonstration. Nous allons utiliser le lemme précédent pour démontrer l'existence d'une telle décomposition. Procédons par l'absurde et supposons que a ne possède pas une telle décomposition. Par conséquent, a n'est pas premier et il possède un diviseur a_1 qui n'est associé ni à 1 ni à a. Dès lors,

$$a = a_1 b_1$$

où ni a_1 ni b_1 n'est associé à 1. En effet, b_1 ne peut être associé à 1 car sinon, il existerait u inversible tel que $ub_1 = 1$ et de là, $ua = a_1$ et a_1 serait associé à a ce qui est impossible. Les éléments a_1 et b_1 ne peuvent avoir tous les deux des décompositions en facteurs premiers car sinon a lui-même en aurait une. Supposons que a_1 ne possède pas une telle décomposition (cela est toujours possible quitte à renommer a_1 et b_1). En particulier, $\langle a \rangle$ est inclus strictement dans $\langle a_1 \rangle$ car a et a_1 ne sont pas associés (donc $\langle a \rangle \neq \langle a_1 \rangle$). On peut alors répéter le raisonnement qui vient d'être fait et trouver des éléments a_2 et b_2 non associés à 1 tels que $a_1 = a_2 b_2$. En continuant de la sorte, on obtient des suites d'éléments a_n et b_n non associés à 1 tels que $a_n = a_{n+1} b_{n+1}$ et que la suite d'idéaux

$$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \langle a_3 \rangle \subset \cdots$$

soit strictement croissante. Or le lemme précédent stipule que dans A, il n'existe aucune suite infinie strictement croissante d'idéaux, d'où une contradiction.

Pour montrer l'unicité de la décomposition, supposons que l'on dispose de deux décompositions en facteurs premiers

$$a = p_1 \cdots p_m = q_1 \cdots q_n.$$

Si $m = 1$, alors a est premier et $n = 1$. Sinon, p_m divise $a = q_1 \cdots q_n$ et il ne peut donc être premier avec tous les q_i (car sinon, il ne diviserait pas a). Or $q_1, \ldots, q_n$ sont premiers. Par conséquent, un des q_i est associé à p_m. Il existe u inversible tel que $q_i = up_m$. De là,

$$p_1 \cdots p_{m-1} = (uq_1) \cdots \widehat{q_i} \cdots q_n$$

et uq_1, étant associé à q_1, est encore premier. En continuant de la sorte, on obtient $m = n$ et chaque p_j est associé à un q_{μ_j} où μ est une permutation.

■

Corollaire IX.3.11 (Théorème fondamental de l'arithmétique). *Dans $\mathbb{Z}$, tout entier n différent de ± 1 s'écrit de manière unique sous la forme*

$$n = \pm\, p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

où les p_i sont des nombres premiers, $\alpha_i \in \mathbb{N} \setminus \{0\}$.

Corollaire IX.3.12. *Soient m et n deux entiers positifs dont les décompositions en facteurs premiers sont*

$$m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}\, q_1^{\beta_1} \cdots q_t^{\beta_t} \quad et \quad n = p_1^{\gamma_1} \cdots p_s^{\gamma_s}\, r_1^{\delta_1} \cdots r_u^{\delta_u}$$

où les p_i, q_i et r_i sont des nombres premiers distincts. Le p.g.c.d. de m et de n est donné par

$$p_1^{\inf\{\alpha_1,\gamma_1\}} \cdots p_s^{\inf\{\alpha_s,\gamma_s\}}$$

et le p.p.c.m. de m et de n par

$$p_1^{\sup\{\alpha_1,\gamma_1\}} \cdots p_s^{\sup\{\alpha_s,\gamma_s\}} q_1^{\beta_1} \cdots q_t^{\beta_t} r_1^{\delta_1} \cdots r_u^{\delta_u}.$$

Corollaire IX.3.13. *Dans $\mathbb{K}[X]$, tout polynôme P non constant s'écrit de manière unique sous la forme*

$$P = \lambda\, P_1^{\alpha_1} \cdots P_k^{\alpha_k}$$

où les P_i sont des polynômes irréductibles et moniques de $\mathbb{K}[X]$, $\alpha_i \in \mathbb{N} \setminus \{0\}$ et $\lambda \in \mathbb{K} \setminus \{0\}$.

Remarque IX.3.14. Le corollaire IX.3.12 se réexprime immédiatement dans le cas du p.g.c.d. et du p.p.c.m. de deux polynômes.

Exemple IX.3.15. Par exemple, on a les décompositions suivantes en facteurs premiers, $6248 = 2^3.11.71$ et $128720912 = 2^4.683.11779$. Dans $\mathbb{C}[X]$, le polynôme $X^5 - 2X^4 + X^3 - X^2 + 1$ se factorise en

$$(X + i)(X - i)(X - 1)(X - \frac{1 + \sqrt{5}}{2})(X - \frac{1 - \sqrt{5}}{2}).$$

Noter que dans $\mathbb{R}[X]$, la factorisation est donnée par

$$(X^2 + 1)(X - 1)(X - \frac{1 + \sqrt{5}}{2})(X - \frac{1 - \sqrt{5}}{2}).$$

4. Résultant de deux polynômes

Comme vu plus haut, $X^2 + 1$ est irréductible sur $\mathbb{R}[X]$ mais pas sur $\mathbb{C}[X]$.

Dans l'anneau des polynômes $\mathbb{K}[X]$, rappelons qu'un polynôme P de $\mathbb{K}[X]$ est irréductible s'il est non constant (i.e., de degré au moins 1) et s'il ne peut pas s'écrire comme produit de deux polynômes de degré strictement inférieur à $\deg P$.

Pour que deux polynômes non constants $A, B \in \mathbb{K}[X]$ possèdent un facteur irréductible en commun (et ne soient dès lors pas premiers entre eux),

au vu du corollaire IX.3.13, il est nécessaire et suffisant que leur p.g.c.d. soit de degré strictement positif. Pour répondre à cette question, on peut bien évidemment calculer un p.g.c.d. au moyen de l'algorithme d'Euclide vu précédemment. Cependant, comme nous allons le montrer, on peut également procéder par un calcul de déterminant (qui en pratique, peut s'avérer plus simple[14]).

Définition IX.4.1. Soient $A, B \in \mathbb{K}[X]$ deux polynômes non constants de la forme

Remarquez que nous avons débuté par le terme indépendant.

$$A = a_0 + a_1 X + \cdots + a_m X^m, \quad a_m \neq 0$$

et

$$B = b_0 + b_1 X + \cdots + b_n X^n, \quad b_n \neq 0.$$

Le *résultant* de A et de B est le déterminant

La matrice correspondante est appelée *matrice de Sylvester*.

$$\operatorname{res}(A,B) = \det \begin{pmatrix} a_0 & a_1 & \cdots & a_m & & & \\ & a_0 & a_1 & \cdots & a_m & & \\ & & \ddots & \ddots & & \ddots & \\ & & & a_0 & a_1 & \cdots & a_m \\ b_0 & b_1 & \cdots & b_n & & & \\ & b_0 & b_1 & \cdots & b_n & & \\ & & \ddots & \ddots & & \ddots & \\ & & & b_0 & b_1 & \cdots & b_n \end{pmatrix}$$

où la matrice carrée est de dimension $m+n$. Les coefficients de A occupent les n premières lignes et ceux de B, les m dernières.

Exemple IX.4.2. Soient les polynômes de $\mathbb{R}[X]$, $A(X) = X^3+X^2+2X+2$ et $B(X) = X^4 - 2X^2 + X + 3$. Leur résultant est

$$\det \begin{pmatrix} 2 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 2 & 2 & 1 & 1 & 0 & 0 \\ 0 & 0 & 2 & 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 1 & 1 \\ 3 & 1 & -2 & 0 & 1 & 0 & 0 \\ 0 & 3 & 1 & -2 & 0 & 1 & 0 \\ 0 & 0 & 3 & 1 & -2 & 0 & 1 \end{pmatrix} = 123.$$

La proposition liant la valeur du résultant de A et de B à l'existence d'un facteur irréductible commun aux deux polynômes est la suivante.

Proposition IX.4.3. *Deux polynômes non constants $A, B \in \mathbb{K}[X]$ possèdent un facteur irréductible commun si et seulement si leur résultant est nul.*

Pour démontrer ce résultat, nous aurons besoin d'un lemme préalable.

[14] Si la question posée est uniquement de savoir s'ils ont un facteur commun, sans nécessairement déterminer ce facteur.

Lemme IX.4.4. *Deux polynômes non constants $A, B \in \mathbb{K}[X]$ possèdent un facteur irréductible commun si et seulement si il existe des polynômes non nuls U et V tels que*

$$UA + VB = 0, \quad \textit{avec} \quad \deg U < \deg B \ \textit{et} \ \deg V < \deg A.$$

Démonstration. Soit D le p.g.c.d. monique de A et de B. Ainsi, il existe des polynômes non nuls U et V tels que $A = VD$ et $B = -UD$.

Montrons que la condition est nécessaire. Si A et B possèdent un facteur irréductible commun, cela signifie que $\deg D \geq 1$. De là, on trouve $\deg V < \deg A$, $\deg U < \deg B$ et $UA + VB = 0$.

La condition est suffisante. Supposons qu'il existe des polynômes U et V satisfaisant les conditions prescrites et supposons de plus que A et B sont premiers entre eux. De là, $UA = -VB$ et puisque A et B sont premiers entre eux, A divise V. C'est impossible car $\deg V < \deg A$. Ceci permet de conclure.

■

Il s'agit d'une belle application de la notion d'indépendance linéaire...

Démontrons à présent le résultat proprement dit.

Démonstration. Posons $m = \deg A$ et $n = \deg B$. On sait à présent que A et B ont un facteur irréductible commun si et seulement si il existe des polynômes non nuls U et V tels que

$$UA + VB = 0, \quad \text{avec} \quad \deg U < n \ \text{et} \ \deg V < m.$$

Si $U(X) = u_0 + u_1X + \cdots + u_{n-1}X^{n-1}$ et $V(X) = v_0 + v_1X + \cdots + v_{m-1}X^{m-1}$, alors cette condition se réexprime en affirmant qu'il existe des coefficients $u_0, \ldots, u_{n-1}, v_0, \ldots, v_{m-1} \in \mathbb{K}$ non tous nuls tels que

$$u_0A + u_1XA + \cdots + u_{n-1}X^{n-1}A + v_0B + v_1XB + \cdots + v_{m-1}X^{m-1}B = 0.$$

Autrement dit, A et B ont un facteur irréductible commun si et seulement si les polynômes

$$A, XA, \ldots, X^{n-1}A, B, XB, \ldots, X^{m-1}B$$

sont linéairement dépendants dans l'espace vectoriel des polynômes à coefficients dans $\mathbb{K}$ et de degré au plus $m+n-1$. Les composantes de ces vecteurs dans la base $1, X, X^2, \ldots, X^{m+n-1}$ étant exactement les lignes de la matrice $\operatorname{res}(A, B)$, on conclut aisément[15].

■

Exemple IX.4.5. Ainsi, les deux polynômes $A(X) = X^3 + X^2 + 2X + 2$ et $B(X) = X^4 - 2X^2 + X + 3$ ayant un résultant non nul, ne possèdent pas de facteur commun.

Cependant, contrairement à l'algorithme d'Euclide, la valeur du résultant ne nous apprend rien sur leurs éventuels facteurs communs. On pourrait vérifier que

$$A(X) = X^3 + X^2 + 2X + 2 = (X + 1)(X^2 + 2)$$

[15] Se rappeler la proposition V.3.1.

et

B et C diffèrent d'un terme X^3.

$$C(X) = X^4 + X^3 - 2X^2 + X + 3 = (X+1)(X^3 - 2X + 3)$$

ont pour résultant

$$\det \begin{pmatrix} 2 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 2 & 2 & 1 & 1 & 0 & 0 \\ 0 & 0 & 2 & 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 1 & 1 \\ 3 & 1 & -2 & 1 & 1 & 0 & 0 \\ 0 & 3 & 1 & -2 & 1 & 1 & 0 \\ 0 & 0 & 3 & 1 & -2 & 1 & 1 \end{pmatrix} = 0.$$

Ainsi, même si on ne disposait pas de la factorisation de A et C (qui est ici triviale à obtenir), ce calcul de déterminant prouverait que ces deux polynômes possède un facteur commun.

Remarque IX.4.6. Pour les polynômes

$$A = a_0 + a_1 X + \cdots + a_m X^m, \quad a_m \neq 0$$

et

$$B = b_0 + b_1 X + \cdots + b_n X^n, \quad b_n \neq 0,$$

il est facile de voir qu'une définition du résultant donnée par

$$\det \begin{pmatrix} a_m & a_{m-1} & \cdots & a_0 & & & \\ & a_m & a_{m-1} & \cdots & a_0 & & \\ & & \ddots & \ddots & & \ddots & \\ & & & a_m & a_{m-1} & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & & & \\ & b_n & b_{n-1} & \cdots & b_0 & & \\ & & \ddots & \ddots & & \ddots & \\ & & & b_n & b_{n-1} & \cdots & b_0 \end{pmatrix}$$

aurait fourni le même résultat.

CHAPITRE X

Opérateurs linéaires

1. Définitions

Définition X.1.1. Soient E et F, deux espaces vectoriels sur le même champ $\mathbb{K}$. Une application[1] T de E dans F est dite *linéaire*[2] si, pour tous $x, y \in E$ et tous $\lambda, \mu \in \mathbb{K}$, on a

$$T(\lambda\, x + \mu\, y) = \lambda\, T(x) + \mu\, T(y).$$

On parle généralement d'*application linéaire* ou d'*opérateur linéaire*. Si $E = F$, on dit alors que T est une *transformation linéaire* ou un *endomorphisme*. L'ensemble des opérateurs linéaires de E dans F est noté $\mathcal{L}(E; F)$. L'ensemble des endomorphismes de E se note $\mathcal{L}(E) = \mathcal{L}(E; E)$.

Dans le cas particulier où $F = \mathbb{K}$, on dit que l'application linéaire $T : E \to \mathbb{K}$ est une *forme linéaire*[3] sur E. L'ensemble $\mathcal{L}(E; \mathbb{K})$ des formes linéaires sur E s'appelle l'*espace dual* de E ou simplement le *dual* de E et est noté E^*.

Dans le cas des opérateurs linéaires, on omet souvent les parenthèses. Ainsi, on écrira simplement Tx pour $T(x)$.

Remarque X.1.2. Pour vérifier que $T : E \to F$ est un opérateur linéaire, il suffit de vérifier que pour tous $x, y \in E$ et tout $\lambda \in \mathbb{K}$, on a

$$T(x + y) = Tx + Ty$$

et

$$T(\lambda\, x) = \lambda\, Tx.$$

Si T est un opérateur linéaire, on a $T(0) = 0$ et

$$T\left(\sum_{i=1}^{p} \lambda_i x_i\right) = \sum_{i=1}^{p} \lambda_i T x_i$$

pour toute combinaison linéaire d'éléments de E.

[1] On réserve souvent le mot fonction à des applications à valeurs dans $\mathbb{R}$ ou $\mathbb{C}$.

[2] Il est naturel d'introduire les applications linéaires dans le cadre des espaces vectoriels. En effet, un espace vectoriel est muni de deux opérations : l'addition de vecteurs et la multiplication d'un vecteur par un scalaire. Si une application est linéaire, elle préserve alors exactement ces deux opérations. On peut noter que, dans le cadre des groupes (resp. des anneaux), on rencontre les mêmes notions. Les applications préservant l'opération du groupe (resp. les opérations de l'anneau) s'appellent alors "homomorphisme". Un homomorphisme d'un groupe ou d'un anneau dans lui-même est appelé endomorphisme.

[3] On emploie parfois l'expression *fonctionnelle linéaire*.

Exemple X.1.3. Voici quelques exemples d'applications linéaires.

- Soient n, p et q des entiers positifs et A une matrice appartenant à $\mathbb{K}_p^n$. D'après les règles du calcul matriciel, l'application
$$T : \mathbb{K}_q^p \to \mathbb{K}_q^n : x \mapsto T(x) = Ax$$
est linéaire.
- Soit E l'espace vectoriel de fonctions de classe C^∞ sur un intervalle ouvert I de $\mathbb{R}$ et à valeurs dans $\mathbb{R}$. L'application de E dans E qui à $f \in E$ associe sa dérivée f' est linéaire. En effet, $(f+g)' = f' + g'$ et pour tout $\lambda \in \mathbb{R}$, $(\lambda f)' = \lambda f'$.
- Soient a, b des nombres réels tels que $a < b$. Si E est l'espace vectoriel des fonctions continues sur $[a, b]$, alors l'application
$$\varphi : E \to \mathbb{R} : f \mapsto \int_a^b f(t)\,dt$$
est une forme linéaire. Cela résulte des propriétés de l'intégrale vues au cours d'analyse.

Exemple X.1.4. A présent, des exemples "numériques". Soit l'application
$$f : \mathbb{R}^2 \to \mathbb{R}^2 : (x, y) \mapsto f(x, y) = (x + 2y, y - x).$$
A titre indicatif, $f(1, 3) = (7, 2)$. Cette application est linéaire. En effet, si $(x, y), (x', y') \in \mathbb{R}^2$ et $\lambda \in \mathbb{R}$, alors
$$\begin{aligned} f((x, y) + (x', y')) &= f(x + x', y + y') = (x + x' + 2(y + y'), y + y' - (x + x')) \\ &= (x + 2y, y - x) + (x' + 2y', y' - x') = f(x, y) + f(x', y') \end{aligned}$$
et
$$f(\lambda(x, y)) = f(\lambda x, \lambda y) = (\lambda x + 2\lambda y, \lambda y - \lambda y x) = \lambda f(x, y).$$
On pourrait remarquer que les valeurs de cette application peuvent aussi s'obtenir matriciellement,
$$f : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + 2y \\ y - x \end{pmatrix}.$$
L'explication de ce phénomène viendra très bientôt.

Ce n'est pas la seule façon de le montrer.

Soit l'application $g : \mathbb{R}^2 \to \mathbb{R}^2 : (x, y) \mapsto (x, y^2)$. Cette application n'est pas linéaire. En effet, $g(1, 1) = (1, 1)$ mais $g(2(1, 1)) = g(2, 2) = (2, 4) \neq 2g(1, 1) = (2, 2)$.

De la même manière, $h : \mathbb{R}^2 \to \mathbb{R}^2 : (x, y) \mapsto (x + 1, y)$ n'est pas linéaire. En effet, $h(1, 0) = (2, 0)$ mais $h(2(1, 0)) = h(2, 0) = (3, 0) \neq 2h(1, 0) = (4, 0)$.

Définition X.1.5. L'*opérateur nul* (de E dans F) est celui qui, à tout vecteur x de E associe le vecteur nul de F. On le note 0_{EF} ou simplement 0. L'*opérateur identité* (de E) est celui qui, à tout vecteur x de E associe x. On le note id_E ou simplement id, si aucune confusion sur E n'est possible.

On peut munir $\mathcal{L}(E;F)$ d'une structure d'espace vectoriel sur $\mathbb{K}$ de la manière suivante. On définit la *somme* de deux opérateurs $S,T \in \mathcal{L}(E;F)$ par

$$(S+T)x = Sx + Tx, \quad \forall x \in E$$

et le *produit* de $T \in \mathcal{L}(E;F)$ par le scalaire $\lambda \in \mathbb{K}$ par

$$(\lambda T)x = \lambda(Tx), \quad \forall x \in E.$$

En effet, on vérifie facilement que ces opérateurs appartiennent encore à $\mathcal{L}(E;F)$. Par exemple, si T est linéaire, alors λT est linéaire car

$$\begin{aligned}(\lambda T)(\alpha x + \mu y) &= \lambda(T(\alpha x + \mu y)) = \lambda(\alpha Tx + \mu Ty) \\ &= \lambda\alpha Tx + \lambda\mu Ty = \alpha(\lambda T)x + \mu(\lambda T)y.\end{aligned}$$

On procède de manière analogue pour la somme.

Remarque X.1.6. En particulier, l'espace dual E^* est aussi un espace vectoriel.

Soient E, F et G des espaces vectoriels et $S \in \mathcal{L}(E;F)$, $T \in \mathcal{L}(F;G)$. On définit[4] le *produit* $TS = T \circ S$ par

$$(TS)x = T(Sx),\ x \in E.$$

On vérifie facilement que TS est un opérateur linéaire de E dans G. Le produit d'opérateurs est associatif car la composition de fonctions est associative. L'opérateur id_E est un neutre dans $\mathcal{L}(E)$. Enfin, il est aisé de vérifier que le produit d'opérateurs est distributif par rapport aux combinaisons linéaires,

$$T\left(\sum_{i=1}^{p} \lambda_i S_i\right) = \sum_{i=1}^{p} \lambda_i T S_i$$

et

$$\left(\sum_{i=1}^{p} \lambda_i T_i\right) S = \sum_{i=1}^{p} \lambda_i T_i S.$$

Dans le cas où E est de dimension finie, un opérateur linéaire T est entièrement déterminé par les valeurs qu'il attribue aux éléments d'une base de E.

Théorème X.1.7. *Supposons que E est un espace vectoriel de dimension finie n. Soient $(u_1,\dots,u_n)$ une base de E, $v_1,\dots,v_n$ des vecteurs de F et l'application $T : E \to F$ définie par*

$$Tx = x_1v_1 + \cdots + x_nv_n$$

pour tout $x \in E$ tel que $x = x_1u_1 + \cdots + x_nu_n$. Alors, l'application T est linéaire. De plus, T est l'unique application linéaire de E dans F telle que $Tu_i = v_i$ pour tout $i \in \{1,\dots,n\}$.

[4] L'ensemble $\mathcal{L}(E)$ des endomorphismes de E muni de la somme et du produit d'opérateurs possède alors une structure d'anneau.

Démonstration. Soient $x, y \in E$ et $\lambda \in \mathbb{K}$. Puisque $(u_1, \ldots, u_n)$ est une base de E, il existe des scalaires $x_1, \ldots, x_n, y_1, \ldots, y_n$ tels que $x = x_1u_1 + \cdots + x_nu_n$ et $y = y_1u_1 + \cdots + y_nu_n$. On a

$$x + y = (x_1 + y_1)u_1 + \cdots + (x_n + y_n)u_n$$

et

$$\lambda x = \lambda x_1 u_1 + \cdots + \lambda x_n u_n.$$

Il vient, par définition de T,

$$\begin{aligned} T(x+y) &= (x_1+y_1)v_1 + \cdots + (x_n+y_n)v_n \\ &= (x_1v_1 + \cdots + x_nv_n) + (y_1v_1 + \cdots + y_nv_n) = Tx + Ty \end{aligned}$$

et

$$T(\lambda x) = \lambda x_1 v_1 + \cdots + \lambda x_n v_n = \lambda(x_1v_1 + \cdots + x_nv_n) = \lambda Tx.$$

L'application T est donc linéaire. Il est clair que $Tu_i = v_i$ pour tout $i \in \{1, \ldots, n\}$.

Il reste à montrer l'unicité de T. Supposons que $S : E \to F$ soit aussi une application linéaire vérifiant $S(u_i) = v_i$ pour tout $i \in \{1, \ldots, n\}$. Puisque S est linéaire, pour tous $x_1, \ldots, x_n \in \mathbb{K}$,

$$S(x_1u_1 + \cdots + x_nu_n) = x_1S(u_1) + \cdots + x_nS(u_n) = x_1v_1 + \cdots + x_nv_n.$$

Il s'ensuit que $T(x_1u_1 + \cdots + x_nu_n) = S(x_1u_1 + \cdots + x_nu_n)$ pour tous $x_1, \ldots, x_n \in \mathbb{K}$ et donc $Sx = Tx$ pour tout $x \in E$. Cela signifie que $S = T$.

■

Définition X.1.8. Soient E et F deux espaces vectoriels sur $\mathbb{K}$. Un *isomorphisme* de E sur F est une application linéaire de E dans F qui est bijective.

Proposition X.1.9. *Si T est un isomorphisme de E sur F, alors la bijection T^{-1} est un isomorphisme de F sur E.*

Démonstration. L'application T^{-1} est bijective. Il reste à montrer que $T^{-1} : F \to E$ est linéaire. Soient y, y' appartenant à F. Puisque T est bijective, il existe $x, x' \in E$ uniques tels que $Tx = y$ et $Tx' = y'$. Par définition de T^{-1}, il vient $x = T^{-1}(y)$ et $x' = T^{-1}(y')$, donc $x + x' = T^{-1}(y) + T^{-1}(y')$. Puisque l'application T est linéaire,

$$T(x + x') = T(T^{-1}(y)) + T(T^{-1}(y')) = y + y'.$$

Ainsi, $T^{-1}(y + y') = x + x'$ et donc

$$T^{-1}(y + y') = T^{-1}(y) + T^{-1}(y').$$

De la même façon, on vérifie que pour tout $\lambda \in \mathbb{K}$,

$$T^{-1}(\lambda y) = \lambda T^{-1}(y),$$

ce qui prouve que T^{-1} est linéaire.

■

Définition X.1.10. On dit que E et F sont *isomorphes* ou que E est *isomorphe* à F, s'il existe un isomorphisme de E sur F. Dans ce cas, on note souvent $E \simeq F$.

Proposition X.1.11. *Soit E un espace vectoriel de dimension finie n. Soient $(u_1, \ldots, u_n)$ une base de E et $T : E \to F$ une application linéaire. L'application T est un isomorphisme si et seulement si $(Tu_1, \ldots, Tu_n)$ est une base de F.*

Démonstration. Supposons que $(Tu_1, \ldots, Tu_n)$ est une base de l'espace vectoriel F. Soit $x \in E$ de composantes $x_1, \ldots, x_n$ dans la base $(u_1, \ldots, u_n)$. Puisque T est linéaire et $x = x_1u_1 + \cdots + x_nu_n$, il vient

$$Tx = x_1Tu_1 + \cdots + x_nTu_n.$$

Les composantes de Tx dans la base $(Tu_1, \ldots, Tu_n)$ sont ainsi $x_1, \ldots, x_n$. Il s'ensuit que si x et x' sont des vecteurs de E tels que $Tx = Tx'$, alors x et x' ont les mêmes composantes dans la base $(u_1, \ldots, u_n)$ et par suite $x = x'$. L'application T est donc injective. Soit $y \in F$ de composantes $y_1, \ldots, y_n$ dans la base $(Tu_1, \ldots, Tu_n)$. Le vecteur $x = y_1u_1 + \cdots + y_nu_n$ de E a pour image y par T. Cela signifie que T est surjectif.

Réciproquement, supposons que T est un isomorphisme. Soit $y \in F$. Puisque T est surjective, il existe $x \in E$ tel que $y = Tx$. Si $x_1, \ldots, x_n$ sont les composantes de x dans la base $(u_1, \ldots, u_n)$, on a

$$y = T(x_1u_1 + \cdots + x_nu_n) = x_1Tu_1 + \cdots + x_nTu_n.$$

L'espace vectoriel F est donc engendré par les vecteurs $Tu_1, \ldots, Tu_n$. Soient des scalaires $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ tels que

$$\lambda_1Tu_1 + \cdots + \lambda_nTu_n = 0.$$

Il vient

$$T(\lambda_1u_1 + \cdots + \lambda_nu_n) = 0 = T0.$$

Puisque T est injectif, $\lambda_1u_1 + \cdots + \lambda_nu_n = 0$. Or $(u_1, \ldots, u_n)$ est une base de E et donc, $\lambda_1 = \cdots = \lambda_n = 0$. Ainsi, les vecteurs $Tu_1, \ldots, Tu_n$ sont linéairement indépendants ce qui conclut la preuve.

■

Exemple X.1.12. Soit $T : \mathbb{C}_2^2 \to \mathbb{C}[z]_3$ l'application linéaire définie par

$$T\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} = z^3,\ T\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} = z^2,\ T\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix} = z,\ T\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix} = 1.$$

Au vu de la proposition précédente, il est immédiat que T est un isomorphisme entre $\mathbb{C}_2^2$ et $\mathbb{C}[z]_3$. Par contre l'application linéaire S donnée par

$$S\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} = z^3,\ S\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} = z^2,\ S\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix} = 2,\ S\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix} = 1$$

n'est pas un isomorphisme.

Corollaire X.1.13. *Soient E et F deux espaces vectoriels de dimension finie sur $\mathbb{K}$. Les espaces E et F sont isomorphes si et seulement si* $\dim E = \dim F$.

Démonstration. Le résultat est clair si $E = \{0\}$. Nous pouvons donc supposer $E \neq \{0\}$. Soit $(u_1, \ldots, u_n)$ une base de E.

Si T est un isomorphisme de E sur F, alors, d'après la proposition précédente, $(Tu_1, \ldots, Tu_n)$ est une base de F et donc $\dim E = \dim F = n$.

Supposons à présent que $(v_1, \ldots, v_n)$ est une base de F. Par le théorème X.1.7, il existe une unique application linéaire $S : E \to F$ telle que $Su_i = v_i$ pour tout $i \in \{1, \ldots, n\}$. En conséquence de la proposition précédente, S est un isomorphisme.

■

Remarque X.1.14. Soit E un $\mathbb{K}$-vectoriel. Cet espace est de dimension finie n si et seulement si il est isomorphe à $\mathbb{K}^n$. Ainsi, on voit une fois encore que $\mathbb{K}^n$ est un exemple fondamental d'espace vectoriel de dimension finie sur $\mathbb{K}$.

Proposition X.1.15. *Si $S : E \to F$ est un isomorphisme de E sur F et $T : F \to G$ est un isomorphisme de F sur G, alors $T \circ S : E \to G$ est un isomorphisme de E sur G.*

Démonstration. Il s'agit d'une vérification immédiate.

■

2. Image et noyau

Soient E et F deux espaces vectoriels sur le champ $\mathbb{K}$ et T une application linéaire de E dans F.

Proposition X.2.1. *Si G est un sous-espace vectoriel de E, alors $T(G)$ est un sous-espace vectoriel de F.*

Démonstration. Le vecteur nul de E appartient à tout sous-espace vectoriel de E et $T0 = 0$. On en déduit que le vecteur nul de F appartient à $T(G)$. Soient $y, y' \in T(G)$. Il existe $x, x' \in G$ tels que $y = Tx$ et $y' = Tx'$. Il vient

$$y + y' = Tx + Tx' = T(x + x')$$

car T est linéaire. Comme G est un sous-espace vectoriel de E, $x + x'$ appartient encore à G. De là, $y + y'$ appartient donc à $T(G)$. De manière semblable, on démontre que si $\lambda \in \mathbb{K}$, alors λy appartient à $T(G)$. Ceci prouve que $T(G)$ est un sous-espace vectoriel de F.

■

Définition X.2.2. On appelle *image* de T le sous-espace vectoriel $T(E)$ de F et on le note $\operatorname{Im} T$. Le *rang* est la dimension de $\operatorname{Im} T$ et on le note $\operatorname{rg}(T)$.

Il faudra attendre la section suivante pour faire le lien avec la notion matricielle de rang.

Proposition X.2.3. *Si H est un sous-espace vectoriel de F, alors*

$$T^{-1}(H) = \{x \in E \mid Tx \in H\}$$

est un sous-espace vectoriel de E.

Démonstration. La démonstration est analogue à la précédente.

■

Définition X.2.4. On appelle *noyau* de T le sous-espace vectoriel

$$T^{-1}(\{0\})$$

de E et on le note $\operatorname{Ker} T$.

Exemple X.2.5. Soient E un espace vectoriel ayant (e_1, e_2) pour base et l'application linéaire $T : E \to E$ définie par $Te_1 = e_1$ et $Te_2 = -e_1$. Un vecteur quelconque $x \in E$ se décompose sous la forme $\alpha_1 e_1 + \alpha_2 e_2$. Par linéarité de T, $Tx = \alpha_1 Te_1 + \alpha_2 Te_2 = (\alpha_1 - \alpha_2)e_1$. De là, on en conclut que $\operatorname{Im} T = \rangle e_1 \langle$ et $\operatorname{Ker} T = \rangle e_1 + e_2 \langle$.

Ces notions d'image et de noyau ne se rencontrent pas uniquement dans le contexte des espaces vectoriels et des applications linéaires. Considérons la fonction $f : \mathbb{R} \to \mathbb{R} : x \mapsto (x-1)^2$; par définition, $\operatorname{Ker} f = \{x \in \mathbb{R} \mid f(x) = 0\}$ et $\operatorname{Im} f = \{y \in \mathbb{R} \mid \exists x \in \mathbb{R} : f(x) = y\}$. Pour cet exemple,

On a quitté pour un court instant les espaces vectoriels. Par exemple, $\{1\}$ n'est pas un sous-vectoriel.

$$\operatorname{Ker} f = \{1\} \text{ et } \operatorname{Im} f = [0, +\infty[.$$

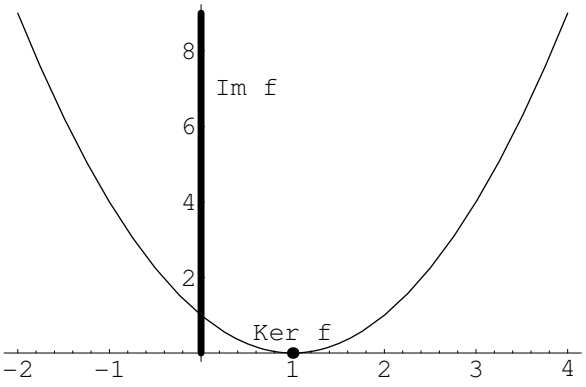


FIGURE X.1. Image et noyau de $f : x \mapsto x^2$.

Pour la fonction $f : x \mapsto \sin x$, il est clair que $\operatorname{Ker} f = \{n\pi \mid n \in \mathbb{Z}\}$ et $\operatorname{Im} f = [-1, 1]$.

Enfin, pour la fonction sgn, on a $\operatorname{Ker} \operatorname{sgn} = \{0\}$ et $\operatorname{Im} \operatorname{sgn} = \{-1, 1\}$.

Pour rappel, $\operatorname{sgn} x = \begin{cases} 1 & ,si\ x > 0 \\ 0 & ,si\ x = 0 \\ -1 & ,si\ x < 0. \end{cases}$

Proposition X.2.6. *Soit $T \in \mathcal{L}(E; F)$.*

- *L'application T est surjective si et seulement si $\operatorname{Im} T = F$,*
- *T est injectif si et seulement si $\operatorname{Ker} T = \{0\}$.*

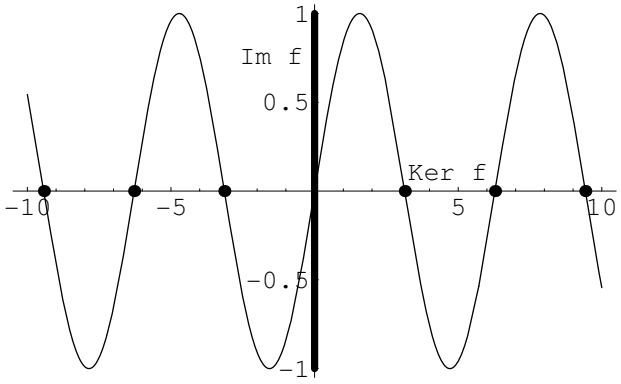


FIGURE X.2. Image et noyau de $f : x \mapsto \sin x$.

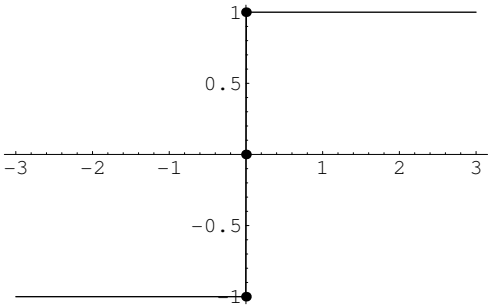


FIGURE X.3. Image et noyau de $f : x \mapsto \operatorname{sgn} x$.

Démonstration. La première partie est immédiate. Passons à la seconde. Supposons T injectif. L'équation

$$Tx = 0 = T0$$

entraîne $x = 0$ et donc $\operatorname{Ker} T = \{0\}$. Réciproquement, si $\operatorname{Ker} T = \{0\}$ et si $Tx = Ty$, alors, puisque T est linéaire,

$$T(x - y) = T0 = 0$$

et donc $x - y = 0$. De là, $x = y$, ce qui prouve l'injectivité de T.

■

Le théorème suivant stipule que tout supplémentaire de $\operatorname{Ker} T$ est isomorphe à $\operatorname{Im} T$.

Théorème X.2.7 (Théorème de la dimension). *Supposons E de dimension finie. Si $T \in \mathcal{L}(E; F)$, alors*

$$\boxed{\dim E = \dim \operatorname{Ker} T + \dim \operatorname{Im} T.}$$

Démonstration. [5] Puisque E est de dimension finie, par la proposition VII.5.20, le sous-espace vectoriel $\operatorname{Ker} T$ possède un supplémentaire G. On a

[5] Au vu de la proposition X.3.7, on dispose d'une autre preuve du théorème de la dimension. Soient U une base de E et V une base de F. Si A représente l'opérateur T

alors

$$E = \operatorname{Ker} T \oplus G.$$

Soit

$$S : G \to \operatorname{Im} T$$

l'application définie par $Sx = Tx$ pour tout $x \in G$. Puisque T est linéaire, l'application S l'est aussi. Soit $x \in G$ tel que $Sx = 0$, c'est-à-dire tel que $Tx = 0$. On a donc $x \in G \cap \operatorname{Ker} T$. Ainsi $x = 0$ car la somme de G et $\operatorname{Ker} T$ est directe. D'après la proposition précédente, l'application S est donc injective.

Soit $y \in \operatorname{Im} T$. Par définition de l'image, il existe $x \in E$ tel que $y = Tx$. Puisque $E = \operatorname{Ker} T \oplus G$, on a $x = x_1 + x_2$ avec $x_1 \in \operatorname{Ker} T$ et $x_2 \in G$. Il vient

$$y = Tx = T(x_1 + x_2) = Tx_1 + Tx_2 = 0 + Tx_2 = Tx_2 = Sx_2.$$

L'application S est donc surjective.

Il s'ensuit que S est un isomorphisme de G sur $\operatorname{Im} T$. Par le corollaire X.1.13, $\dim G = \dim \operatorname{Im} T$. Enfin, puisque $E = \operatorname{Ker} T \oplus G$, on a $\dim E = \dim \operatorname{Ker} T + \dim G = \dim \operatorname{Ker} T + \dim \operatorname{Im} T$.

■

Remarque X.2.8. Si on considère le système homogène $Ax = 0$ à p inconnues, alors l'ensemble des solutions de ce système n'est autre que $\operatorname{Ker} A$ et sa dimension est donnée par $p - \dim \operatorname{Im} A = p - \operatorname{rg} A$. On retrouve ainsi une partie de la remarque VI.4.1.

Corollaire X.2.9. *Supposons E et F de même dimension. Si une application linéaire $T : E \to F$ est injective ou surjective, alors T est un isomorphisme.*

Démonstration. L'application T est injective si et seulement si $\operatorname{Ker} T = \{0\}$, c'est-à-dire $\dim \operatorname{Ker} T = 0$. D'autre part, l'application T est surjective si et seulement si $\operatorname{Im} T = F$, c'est-à-dire $\dim \operatorname{Im} T = \dim F$, ou encore $\dim \operatorname{Im} T = \dim E$. Grâce au théorème de la dimension, l'application T est injective si et seulement si elle est surjective, d'où le résultat.

■

Exemple X.2.10. Appliquons le théorème de la dimension en supposant E de dimension finie $n \geq 1$ et $F = \mathbb{K}$. Si T est une forme linéaire non nulle sur E, on a alors $\operatorname{Im} T \neq \{0\}$ et donc $\dim \operatorname{Im} T \geq 1$. Or $\operatorname{Im} T \subset \mathbb{K}$ et par conséquent, $\dim \operatorname{Im} T \leq 1$. Il vient $\dim \operatorname{Im} T = 1$ et par suite, $\dim \operatorname{Ker} T = n - 1$.

---

dans les bases U et V, alors la dimension de $\operatorname{Ker} T$ est la même que celle de $\{X : AX = 0\}$. Pour rappel, A est de forme $\dim F \times \dim E$. Au vu de la remarque VI.4.1, puisque $AX = 0$ est un système homogène de $\dim F$ équations à $\dim E$ inconnues, l'ensemble $\{X : AX = 0\}$ est un sous-espace vectoriel de dimension $\dim E - \operatorname{rg} A$. On conclut en remarquant que $\operatorname{rg} A = \operatorname{rg} T = \dim \operatorname{Im} T$.

Le corollaire suivant est lui aussi immédiat.

Corollaire X.2.11. *Soit $T \in \mathcal{L}(E;F)$. On a*

- $\operatorname{rg} T \leq \inf(\dim E, \dim F)$,
- *T est surjectif si et seulement si* $\operatorname{rg} T = \dim F$,
- *T est injectif si et seulement si* $\operatorname{rg} T = \dim E$,
- *T est un isomorphisme si et seulement si* $\operatorname{rg} T = \dim E = \dim F$.

Démonstration. Nous devons uniquement démontrer le premier point. Puisque $\operatorname{Im} T$ est un sous-espace vectoriel de F, il est clair que $\operatorname{rg} T \leq \dim F$. Soit $(u_1, \ldots, u_n)$ une base de E. Les vecteurs $Tu_1, \ldots, Tu_n$ formant une partie génératrice de $\operatorname{Im} T$, on a bien $\operatorname{rg} T \leq \dim E$.

■

3. Représentation matricielle

Nous avons déjà vu dans la première section de ce chapitre que, dans le cas où E est de dimension finie, un opérateur linéaire $T : E \to F$ est entièrement déterminé par les valeurs qu'il attribue aux éléments d'une base de E (cf. théorème X.1.7).

Soient $U = (u_1, \ldots, u_n)$ et $V = (v_1, \ldots, v_p)$ des bases respectives des $\mathbb{K}$-vectoriels E et F et $T \in \mathcal{L}(E;F)$.

Puisque U est une base, tout élément $x \in E$ s'écrit sous la forme

$$x = \sum_{j=1}^{n} x_j \, u_j.$$

Puisque V est une base de F, il existe des scalaires $a_{ij} \in \mathbb{K}$ tels que

$$Tu_j = \sum_{i=1}^{p} a_{ij} \, v_i.$$

Pour tout $x \in E$, on a donc

$$Tx = \sum_{j=1}^{n} x_j \, Tu_j = \sum_{i=1}^{p} \left(\sum_{j=1}^{n} a_{ij} \, x_j \right) v_i.$$

Ce calcul nous montre que, connaissant la matrice $A = (a_{ij})$ et le vecteur

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \Phi_U(x)$$

des composantes de x dans la base U, on trouve le vecteur

$$Y = \begin{pmatrix} y_1 \\ \vdots \\ y_p \end{pmatrix} = \Phi_V(Tx)$$

A est $p \times n$.

des composantes de Tx dans la base V par

$$Y = AX.$$

On remarquera encore que la j-ième colonne de A est formée des composantes de $T(u_j)$ dans la base V. On dit que A est la *matrice associée* à T dans les bases U et V ou que A *représente* T dans les bases U et V.

Si T est une transformation linéaire appartenant à $\mathcal{L}(E)$, on ne choisit évidemment qu'une seule base de E.

Remarque X.3.1. Il est parfois judicieux de donner une notation plus explicite à la matrice A associée à T dans les bases U et V. Par exemple, une notation comme

$$A = \mathcal{M}_{U,V}(T)$$

a l'avantage de préciser les bases choisies et l'application considérée. Cependant, dans ces notes, les bases et l'application étant souvent explicitées par le contexte et une telle notation ne sera que rarement utilisée. Ainsi, $\mathcal{M}_{U,V}$ est une application définie sur $\mathcal{L}(E;F)$ et à valeurs dans $\mathbb{K}_n^p$.

Proposition X.3.2. *Soient $U = (u_1, \ldots, u_n)$ et $V = (v_1, \ldots, v_p)$ des bases respectives des $\mathbb{K}$-vectoriels E et F et $T \in \mathcal{L}(E;F)$.*

i) *Pour tout $x \in E$, on a $\Phi_V(Tx) = \mathcal{M}_{U,V}(T)\Phi_U(x)$.*
ii) *Si $B \in \mathbb{K}_n^p$ satisfait, pour tout x dans E, $\Phi_V(Tx) = B\,\Phi_U(x)$, alors $B = \mathcal{M}_{U,V}(T)$.*

Démonstration. Nous devons uniquement montrer le point ii). Si $x = u_i$, $i = 1, \ldots, n$, on a $\Phi_V(Tu_i) = Be_i$. Ainsi, la i-ème colonne de B est complétement déterminée par Tu_i. On conclut par le théorème X.1.7 précisant qu'une application linéaire $T \in \mathcal{L}(E;F)$ est entièrement déterminée par les images par T des vecteurs d'une base de E.

■

Tout l'intérêt de ces représentations est que les opérations matricielles correspondent exactement aux opérations définies sur les opérateurs linéaires.

Proposition X.3.3. *Soient E, F, G trois espaces vectoriels de bases respectives $U = (u_1, \ldots, u_n)$, $V = (v_1, \ldots, v_p)$, $W = (w_1, \ldots, w_q)$. Pour tous $T, S \in \mathcal{L}(E;F)$, $T' \in \mathcal{L}(F;G)$ et $\lambda \in \mathbb{K}$, on a*

$$\mathcal{M}_{U,V}(T+S) = \mathcal{M}_{U,V}(T) + \mathcal{M}_{U,V}(S),$$
$$\mathcal{M}_{U,V}(\lambda T) = \lambda \mathcal{M}_{U,V}(T),$$
$$\mathcal{M}_{U,W}(T'T) = \mathcal{M}_{V,W}(T')\mathcal{M}_{U,V}(T).$$

Démonstration. Nous considérons ici le cas du produit $T'T$. Pour tout $x \in E$, on a $\Phi_V(Tx) = \mathcal{M}_{U,V}(T)\Phi_U(x)$ et pour tout $y \in F$, $\Phi_W(Ty) = \mathcal{M}_{V,W}(T')\Phi_V(y)$. On conclut en applicant la proposition précédente :

$$\forall x \in E,\ \mathcal{M}_{V,W}(T')\mathcal{M}_{U,V}(T)\Phi_U(x) = \mathcal{M}_{V,W}(T')\Phi_U(Tx) = \Phi_W(T'Tx).$$

■

Exemple X.3.4. Soient deux espaces vectoriels E et F ayant respectivement $U = (u_1, u_2, u_3)$ et $V = (v_1, v_2)$ pour bases et l'application linéaire $T : E \to F$ définie par $Tu_1 = v_1$, $Tu_2 = v_1 + v_2$ et $Tu_3 = -v_2$. Un élément quelconque $x \in E$ se décompose sous la forme $x = \alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_3$. Par linéarité de T, il vient

$$Tx = \alpha_1 v_1 + \alpha_2(v_1 + v_2) + \alpha_3(-v_2) = (\alpha_1 + \alpha_2)v_1 + (\alpha_2 - \alpha_3)v_2.$$

Clairement,

$$\Phi_U(x) = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix},$$

La matrice représentant T dans les bases U et V est

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

et

$$A\Phi_U(x) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 + \alpha_2 \\ \alpha_2 - \alpha_3 \end{pmatrix} = \Phi_V(Tx).$$

L'exemple qui suit réapparaîtra de manière récurrente. Considérons le même espace vectoriel E et l'endomorphisme $S : E \to E$ défini par $Su_1 = 0$, $Su_2 = u_1$ et $Su_3 = u_2$. La matrice représentant S est simplement

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Théorème X.3.5. *Soient $U = (u_1, \ldots, u_n)$ et $V = (v_1, \ldots, v_p)$ des bases respectives des $\mathbb{K}$-vectoriels E et F et $T \in \mathcal{L}(E; F)$. L'application $\mathcal{M}_{U,V} : \mathcal{L}(E; F) \to \mathbb{K}_n^p$ est un* **isomorphisme** *d'espaces vectoriels.*

De plus, muni du produit de composition, l'ensemble $\mathcal{L}(E)$ possèdant une structure naturelle d'anneau, l'application $\mathcal{M}_{U,U} : \mathcal{L}(E) \to \mathbb{K}_n^n$ est un isomorphisme d'anneaux.

Démonstration. Montrons l'injectivité. Soient $S, T \in \mathcal{L}(E; F)$. Si $\mathcal{M}_{U,V}(S) = \mathcal{M}_{U,V}(T)$, alors $\Phi_V(Su_i) = \Phi_V(Tu_i)$ pour tout $i = 1, \ldots, n$. On conclut que $S = T$.

Passons à la surjectivité : à des coefficients $\alpha_{j,i}$ donnés, $j = 1, \ldots, p$, $i = 1, \ldots, n$, il correspond (cf. théorème X.1.7) une unique application linéaire T satisfaisant

$$\forall i \in \{1, \ldots, n\}, \quad Tu_i = \sum_{j=1}^{p} \alpha_{j,i}\, v_j.$$

Il est clair que $\mathcal{M}_{U,V}(T) = (\alpha_{j,i})$.

Enfin, la stabilité par rapport aux opérations d'espace vectoriel et d'anneau résulte de la proposition précédente.

■

Deux espaces vectoriels de dimension finie isomorphes étant de même dimension, on a directement le résultat suivant.

Proposition X.3.6. *Si E et F sont deux espaces vectoriels de dimension finie, alors l'espace vectoriel $\mathcal{L}(E;F)$ est de dimension finie et*

$$\dim \mathcal{L}(E;F) = \dim E . \dim F.$$

Proposition X.3.7. *Si A est la matrice représentant T dans des bases U et W de E et de F et si $X = \Phi_U(x)$ et $Y = \Phi_W(y)$ sont les vecteurs des composantes de $x \in E$ dans U et de $y \in F$ dans W, alors*

- $x \in \operatorname{Ker} T$ *si et seulement si* $AX = 0$,
- $y \in \operatorname{Im} T$ *si et seulement s'il existe* $X \in \mathbb{K}^n$ *tel que* $Y = AX$.

En particulier,

$$\operatorname{rg}(T) = \operatorname{rg}(A).$$

Démonstration. C'est évident. La situation se résume comme sur le schéma ci-contre

$$\begin{array}{ccccc} & x \in E & \xrightarrow{\ T\ } & y = Tx \in F & \\ E \simeq \mathbb{K}^n & {\scriptstyle \Phi_U}\downarrow & & \downarrow{\scriptstyle \Phi_W} & F \simeq \mathbb{K}^m \\ & X \in \mathbb{K}^n & \xrightarrow{\ A\ } & Y \in \mathbb{K}^m & \end{array}$$

Du deuxième point, il résulte que $\operatorname{Im} T$ est isomorphe au sous-espace vectoriel de $\mathbb{K}^p$ engendré[6] par les colonnes de A. Comme par définition, ce sous-espace vectoriel est de dimension $\operatorname{rg} T$, la conclusion en résulte.

∎

4. Changement de base

Positionnons le problème. Soit $T \in \mathcal{L}(E;F)$. L'espace vectoriel E (resp. F) dispose de deux bases $U = (u_1, \dots, u_n)$ et $U' = (u'_1, \dots, u'_n)$ (resp. $V = (v_1, \dots, v_p)$ et $V' = (v'_1, \dots, v'_p)$). Supposons que la matrice A représente T dans les bases U et V. Supposons que B (resp. C) est la matrice de changement de base de U à U' (resp. de V à V').

$$\begin{array}{ccc} \Phi_U(x) \in \mathbb{K}^n & \xrightarrow{\ A\ } & \Phi_V(Tx) \in \mathbb{K}^p \\ {\scriptstyle B}\downarrow & & \downarrow{\scriptstyle C} \\ \Phi_{U'}(x) \in \mathbb{K}^n & \xrightarrow{\ ?\ } & \Phi_{V'}(Tx) \in \mathbb{K}^p \end{array}$$

Peut-on à partir de A, B, C déterminer la matrice qui représente T dans les bases U' et V' ?

On a

$$\Phi_{U'}(x) = B\Phi_U(x) \quad \text{et} \quad \Phi_{V'}(Tx) = C\Phi_V(Tx).$$

[6] Si $A = (C_1 \cdots C_n)$, alors $\{A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \sum_i x_i C_i \mid x_1, \dots, x_n \in \mathbb{K}\} = \rangle C_1, \dots, C_n \langle$.

De plus,

$$\Phi_V(Tx) = A\Phi_U(x).$$

Il vient ainsi

$$\Phi_{V'}(Tx) = C\Phi_V(Tx) = CA\Phi_U(x) = CAB^{-1}\Phi_{U'}(x).$$

L'opérateur T se représente donc dans les bases U' et V' par

$$CAB^{-1}.$$

Remarque X.4.1. Il arrive souvent que l'on dispose des composantes des vecteurs de U' (resp. V') dans la base U (resp. V). Si ces composantes forment une matrice B' (resp. C'), alors

$$\Phi_{U'}(x) = B'^{-1}\Phi_U(x) \quad \text{et} \quad \Phi_{V'}(Tx) = C'^{-1}\Phi_V(Tx).$$

De là, on voit que l'opérateur T se représente par

$$C'^{-1}AB'.$$

Considérons à présent le cas particulier d'un endomorphisme $T \in \mathcal{L}(E)$. Ici, on prend $U = V$ et $U' = V'$. Supposons disposer d'une matrice S formée des composantes des vecteurs de U' dans U. Dans ce cas,

$$\Phi_{U'}(x) = S^{-1}\Phi_U(x).$$

De là, il vient

$$\Phi_{U'}(Tx) = S^{-1}AS\Phi_{U'}(x).$$

L'opérateur T se représente donc dans la base U' par

$$A' = S^{-1}AS.$$

Notion intrinsèque : indépendante de la base choisie.

En particulier,

$$\det A' = \det A.$$

Ce scalaire est appelé le *déterminant de la transformation linéaire* T, on le note $\det T$.

Définition X.4.2. Deux matrices $A, A' \in \mathbb{K}_n^n$ sont dites *semblables* s'il existe une matrice inversible $S \in \mathbb{K}_n^n$ telle que[7]

$$A' = S^{-1}AS.$$

Exemple X.4.3. Soit $\mathbb{R}^3$ muni de la base canonique (e_1, e_2, e_3). Considérons l'endomorphisme de $\mathbb{R}^3$ défini par

$$T : xe_1 + ye_2 + ze_3 \mapsto (x + z)e_1 + (-x + 2y + z)e_2 + 2ze_3.$$

Dans la base canonique, T se représente par la matrice

$$A = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

[7] Remarquer que l'on a aussi $A = SA'S^{-1}$ ou encore, si on pose $R = S^{-1}$, $A' = S^{-1}AS$ se réécrit $A' = RAR^{-1}$ et $A = R^{-1}A'R$.

Les vecteurs

$$u_1 = \begin{pmatrix}1\\1\\0\end{pmatrix},\ u_2 = \begin{pmatrix}0\\1\\0\end{pmatrix} \quad \text{et} \quad u_3 = \begin{pmatrix}1\\0\\1\end{pmatrix}$$

forment aussi une base[8] de $\mathbb{R}^3$. On dispose ici des composantes de u_1, u_2, u_3 dans la base canonique (e_1, e_2, e_3), si

$$S = \begin{pmatrix}1 & 0 & 1\\1 & 1 & 0\\0 & 0 & 1\end{pmatrix},$$

alors l'opérateur T se représente dans la base (u_1, u_2, u_3) par la matrice

$$S^{-1}AS = \begin{pmatrix}1 & 0 & -1\\-1 & 1 & 1\\0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0 & 1\\-1 & 2 & 1\\0 & 0 & 2\end{pmatrix}\begin{pmatrix}1 & 0 & 1\\1 & 1 & 0\\0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0 & 0\\0 & 2 & 0\\0 & 0 & 2\end{pmatrix}.$$

Cet exemple nous montre qu'un choix judicieux[9] de la base permet d'obtenir une représentation matricielle de l'opérateur particulièrement simple.

5. Projecteurs

Soient E un espace vectoriel et F, G des sous-espaces vectoriels tels que

$$E = F \oplus G.$$

Définition X.5.1. Puisque $E = F \oplus G$, tout $x \in E$ se décompose de manière unique[10] sous la forme $x = x_F + x_G$, $x_F \in F$, $x_G \in G$. On appelle *projection de E sur F parallèlement à G*, l'application

$$P_F : E \to E : x \mapsto x_F$$

et de manière analogue, on appelle *projection de E sur G parallèlement à F*, l'application

$$P_G : E \to E : x \mapsto x_G.$$

Proposition X.5.2. *Les applications P_F et P_G sont linéaires et on a*

$$\operatorname{Ker} P_F = G,\ \operatorname{Ker} P_G = F,\ \operatorname{Im} P_F = F,\ \operatorname{Im} P_G = G.$$

De plus,

$$id_E = P_F + P_G,\ P_F^2 = P_F,\ P_G^2 = P_G,\ P_F \circ P_G = 0 = P_G \circ P_F.$$

[8] Il est laissé au lecteur le soin de vérifier que (u_1, u_2, u_3) est une base de $\mathbb{R}^3$.

[9] Nous verrons plus loin (cf. le chapitre sur la diagonalisation) sous quelles conditions et comment il est possible de choisir une base pour obtenir une représentation matricielle sous forme diagonale. En effet, ici le choix de u_1, u_2, u_3 paraît artificiel.

[10] cf. proposition VII.5.17.

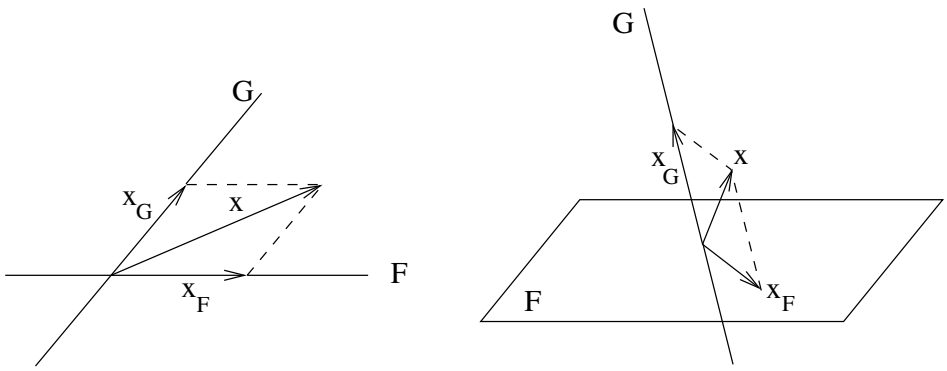


FIGURE X.4. Projecteurs.

Démonstration. Soient $x_1, \ldots, x_n$ des vecteurs de E et $\lambda_1, \ldots, \lambda_n$ des scalaires. On a, pour tout $j \in \{1, \ldots, n\}$,

$$x_j = P_F(x_j) + P_G(x_j).$$

De là,

$$\sum_{j=1}^{n} \lambda_j \, x_j = \sum_{j=1}^{n} \lambda_j \, (P_F(x_j) + P_G(x_j)) = \sum_{j=1}^{n} \lambda_j \, P_F(x_j) + \sum_{j=1}^{n} \lambda_j \, P_G(x_j).$$

Or,

$$\sum_{j=1}^{n} \lambda_j \, P_F(x_j) \in F \text{ et } \sum_{j=1}^{n} \lambda_j \, P_G(x_j) \in G.$$

Dès lors, puisque la décomposition d'un élément de E comme somme d'un élément de F et d'un élément de G est unique,

$$P_F \left(\sum_{j=1}^{n} \lambda_j \, x_j \right) = \sum_{j=1}^{n} \lambda_j \, P_F(x_j)$$

et

$$P_G \left(\sum_{j=1}^{n} \lambda_j \, x_j \right) = \sum_{j=1}^{n} \lambda_j \, P_G(x_j)$$

ce qui prouve que les applications P_F et P_G sont linéaires.

Il est clair que $P_F(x) = 0$ si et seulement si $x \in G$, ainsi $\operatorname{Ker} P_F = G$. On procède de manière analogue pour le noyau de P_G. On a $\operatorname{Im} P_F \subset F$. Si $x \in F$, alors $P_F(x) = x$. On a donc aussi $F \subset \operatorname{Im} P_F$. De là, il vient $\operatorname{Im} P_F = F$ et $P_F^2 = P_F$. De façon identique, $\operatorname{Im} P_G = G$ et $P_G^2 = P_G$. Le fait que $id_E = P_F + P_G$ résulte de la définition même des projecteurs. Enfin, puisque $\operatorname{Ker} P_F = G = \operatorname{Im} P_G$, on trouve $P_F \circ P_G = 0$.

■

Définition X.5.3. Un endomorphisme $P \in \mathcal{L}(E)$ est un *projecteur* si

$$P^2 = P.$$

La proposition suivante lie les notions de projecteur et de projection parallèlement à un sous-espace vectoriel.

Proposition X.5.4. *Soit $P \in \mathcal{L}(E)$ un projecteur. On a*

$$E = \operatorname{Ker} P \oplus \operatorname{Im} P$$

et P est la projection de E sur $\operatorname{Im} P$ parallèlement à $\operatorname{Ker} P$. De plus,

$$Q = id_E - P$$

est un projecteur de E qui coïncide avec la projection de E sur $\operatorname{Ker} P$ parallèlement à $\operatorname{Im} P$.

Démonstration. Il est clair que

$$Q^2 = (id_E - P) \circ (id_E - P) = id_E - P - P + P^2 = Q,$$
$$Q \circ P = P \circ Q = 0$$

et

$$id_E = P + Q.$$

Ainsi, pour tout $x \in E$, $x = Px + Qx$ et

$$E \subset \operatorname{Im} P + \operatorname{Im} Q.$$

Puisque $P \circ Q = 0$, on a $\operatorname{Im} Q \subset \operatorname{Ker} P$. De plus, si $x \in \operatorname{Ker} P$, alors $Qx = x - Px = x$, ce qui signifie que $\operatorname{Ker} P \subset \operatorname{Im} Q$. Donc, $\operatorname{Im} Q = \operatorname{Ker} P$ et

$$E \subset \operatorname{Im} P + \operatorname{Ker} P$$

(l'autre inclusion étant immédiate). Il nous reste à montrer que

$$\operatorname{Im} P \cap \operatorname{Ker} P = \{0\}.$$

Pour ce faire, remarquons que si $x = Py \in \operatorname{Ker} P$, alors

$$Px = 0 = P^2 y = Py = x.$$

Ce qui permet de conclure que la somme $\operatorname{Im} P + \operatorname{Ker} P$ est directe. De là, il découle que P est la projection de E sur $\operatorname{Im} P$ parallèlement à $\operatorname{Ker} P$. En effet, puisque $E = \operatorname{Im} P \oplus \operatorname{Ker} P$, pour tout $x \in E$, il existe $y \in \operatorname{Im} P$ et $z \in \operatorname{Ker} P$ tels que $x = y + z$. Puisque $y \in \operatorname{Im} P$, il existe $w \in E$ tel que $y = Pw$. Ainsi, $x = Pw + z$ et

$$Px = P^2 w + Pz = Pw = y.$$

Par conséquent, $x = Px + z$ d'où la conclusion.

On sait déjà que Q est un projecteur car $Q^2 = Q$. Pour montrer que Q est la projection de E sur $\operatorname{Ker} P$ parallèlement à $\operatorname{Im} P$, il suffit d'échanger les rôles de P et Q car $P = id_E - Q$.

■

Exemple X.5.5. Voici quelques exemples de projecteurs

- La matrice
$$M = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}$$
est un projecteur de $\mathbb{C}^2$. En effet,
$$M\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} z_1 - iz_2 \\ iz_1 + z_2 \end{pmatrix}$$
et
$$M^2\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} z_1 - iz_2 \\ iz_1 + z_2 \end{pmatrix} = M\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$$
En fait, $M = M^2$.
- La transformation linéaire
$$A \mapsto \frac{1}{2}(A + \widetilde{A})$$
est un projecteur de $\mathbb{K}_n^n$. Son image est formée par les matrices symétriques et son noyau par les matrices antisymétriques.

La notion de projecteur peut se généraliser à plus de deux projecteurs de la manière suivante.

Définition X.5.6. Soit $n \geq 1$. Des endomorphismes $P_1, \ldots, P_n$ de E forment un *système de projecteurs* si
$$P_j P_k = \delta_{jk} P_j, \quad j, k \in \{1, \ldots, n\}$$
et
$$P_1 + \cdots + P_n = id_E. \tag{9}$$

La proposition X.5.4 se généralise dans le cas des systèmes de projecteurs de la manière suivante.

Proposition X.5.7. *Si $P_1, \ldots, P_n$ est un système de projecteurs de E, alors*
$$E = \operatorname{Im} P_1 \oplus \cdots \oplus \operatorname{Im} P_n$$
et pour tout $j \in \{1, \ldots, n\}$,
$$\operatorname{Ker} P_j = \operatorname{Im} P_1 \oplus \cdots \oplus \widehat{\operatorname{Im} P_j} \oplus \cdots \oplus \operatorname{Im} P_n.$$
Inversement, si E est la somme directe de sous-espaces $E_1, \ldots, E_n$,
$$E = E_1 \oplus \cdots \oplus E_n,$$
alors, il existe un unique système de projecteurs $P_1, \ldots, P_n$ tel que
$$E_1 = \operatorname{Im} P_1, \ \ldots, \ E_n = \operatorname{Im} P_n.$$

Démonstration. Supposons tout d'abord que $P_1, \ldots, P_n$ forment un système de projecteurs de E. Si $x \in E$, alors vu (9)
$$x = \sum_{j=1}^{n} P_j\, x \in \operatorname{Im} P_1 + \cdots + \operatorname{Im} P_n$$

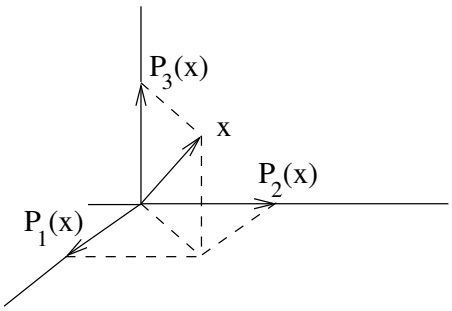


FIGURE X.5. Système de projecteurs

et de là, on trouve

$$E = \operatorname{Im} P_1 + \cdots + \operatorname{Im} P_n.$$

Montrons que la somme est directe. Par la définition VII.5.23, nous devons vérifier que si

$$\sum_{j=1}^{n} x_j = 0 \quad \text{avec } x_j \in \operatorname{Im} P_j,\ \forall j \in \{1, \ldots, n\},$$

alors

$$x_1 = \cdots = x_n = 0.$$

Par hypothèse, on a $P_k\, x_j = \delta_{jk} x_j$. Dès lors, pour tout $k \in \{1, \ldots, n\}$, il vient

$$P_k \sum_{j=1}^{n} x_j = x_k = 0.$$

Ceci montre que la somme est directe. Prouvons à présent la seconde égalité. Si $x \in \operatorname{Ker} P_j$, alors

$$x = \sum_{k=1}^{n} P_k\, x = \sum_{k \neq j} P_k\, x \in \operatorname{Im} P_1 \oplus \cdots \oplus \widehat{\operatorname{Im} P_j} \oplus \cdots \oplus \operatorname{Im} P_n.$$

On a donc

$$\operatorname{Ker} P_j \subset \operatorname{Im} P_1 \oplus \cdots \oplus \widehat{\operatorname{Im} P_j} \oplus \cdots \oplus \operatorname{Im} P_n.$$

Inversement, par définition d'un système de projecteurs, si $j \neq k$, alors $P_j P_k = 0$ et $\operatorname{Im} P_k \subset \operatorname{Ker} P_j$.

Passons à la deuxième partie de la proposition et supposons que E est la somme directe de sous-espaces $E_1, \ldots, E_n$. Si $x \in E$, alors il existe[11] des éléments uniques $x_j \in E_j$, $1 \leq j \leq n$, tels que

$$x = \sum_{j=1}^{n} x_j.$$

[11] Se rappeler la proposition VII.5.25.

Définissons pour tout $j \in \{1, \dots, n\}$ un opérateur P_j qui à x associe l'élément $x_j \in E_j$ apparaissant dans cette décomposition. Il est clair que P_j est linéaire. On a

$$\operatorname{Im} P_j = E_j$$

et il est aisé de vérifier que $P_1, \dots, P_n$ forment un système de projecteurs.

■

6. Quelques compléments sur l'espace dual

Pour rappel, si une application linéaire du $\mathbb{K}$-vectoriel E est à valeurs dans $\mathbb{K}$, on dit que $T : E \to \mathbb{K}$ est une forme linéaire sur E. L'ensemble $E^* = \mathcal{L}(E; \mathbb{K})$ des formes linéaires sur E s'appelle l'espace dual de E.

Exemple X.6.1. Soit $U = (u_1, \dots, u_n)$ une base de E. Pour tous scalaires $\alpha_1, \dots, \alpha_n \in \mathbb{K}$, vu le théorème X.1.7, il existe une unique application linéaire $T : E \to \mathbb{K}$ telle que

$$Tu_i = \alpha_i.$$

Cette forme linéaire est définie par

$$Tx = \alpha_1 x_1 + \cdots + \alpha_n x_n$$

si $x = x_1 u_1 + \cdots + x_n u_n$.

La proposition suivante n'est en fait qu'un particulier des développements réalisés dans la preuve de la proposition X.3.6.

Proposition X.6.2. *Soit $U = (u_1, \dots, u_n)$ une base de E. Pour tout entier $i \in \{1, \dots, n\}$, soit la forme linéaire $u_i^* : E \to \mathbb{K}$ telle que*

$$u_i^*(u_j) = \delta_{ij}.$$

Alors $(u_1^*, \dots, u_n^*)$ est une base de E^*.

Démonstration. Soient $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ des scalaires. La forme linéaire $\alpha_1 u_1^* + \cdots + \alpha_n u_n^*$ est définie par

$$(\alpha_1 u_1^* + \cdots + \alpha_n u_n^*)x = \alpha_1 u_1^*(x) + \cdots \alpha_n u_n^*(x), \ \forall x \in E.$$

Si $x = u_i$, alors dans cette somme, le terme $\alpha_j u_j^*(u_i)$ est nul dès que $j \neq i$. On a donc

$$(\alpha_1 u_1^* + \cdots + \alpha_n u_n^*)u_i = \alpha_i u_i^*(u_i) = \alpha_i.$$

Montrons que $u_1^*, \dots, u_n^*$ forment une partie libre. Supposons[12] que

$$\alpha_1 u_1^* + \cdots + \alpha_n u_n^* = 0.$$

En particulier,

$$\alpha_i = (\alpha_1 u_1^* + \cdots + \alpha_n u_n^*)u_i = 0$$

pour tout $i \in \{1, \dots, n\}$.

Montrons que $u_1^*, \dots, u_n^*$ forment une partie génératrice de E^*. Soit T une forme linéaire sur E. Si l'on pose $\alpha_i = Tu_i$, alors les formes linéaires T

[12] Encore une fois, ici 0 est la forme linéaire nulle.

et $\alpha_1 u_1^* + \cdots + \alpha_n u_n^*$ coïncident sur chaque u_i. Puisque U est une base de E,

$$Tx = (\alpha_1 u_1^* + \cdots + \alpha_n u_n^*)x, \ \forall x \in E.$$

Ceci prouve que les formes linéaires $u_1^*, \ldots, u_n^*$ engendrent E^*.

■

Remarque X.6.3. Si $U = (u_1, \ldots, u_n)$ est une base de E, la forme linéaire u_i^* est définie par

$$u_i^*(\alpha_1 u_1 + \cdots + \alpha_n u_n) = \alpha_i$$

pour tous scalaires $\alpha_1, \ldots, \alpha_n$.

Corollaire X.6.4. *Si E est de dimension finie, l'espace vectoriel E^* est aussi de dimension finie et*

$$\dim E^* = \dim E.$$

Démonstration. Cela découle directement de la proposition précédente.

■

Exemple X.6.5. Supposons par exemple que $E = \mathbb{R}_2$ et que $u_1 = (1, 0)$ et $u_2 = (1, 1)$. Alors les formes linéaires u_1^* et u_2^* sont définies par $u_1^*(x, y) = x - y$ et $u_2^*(x, y) = y$ pour tous $(x, y) \in \mathbb{R}^2$, car on a $(x, y) = (x - y)u_1 + yu_2$.

Définition X.6.6. Soit $U = (u_1, \ldots, u_n)$ une base de E. La base $(u_1^*, \ldots, u_n^*)$ s'appelle la *base duale* de la base U.

Exemple X.6.7. Considérons encore un exemple. Soit la forme linéaire

$$f : \mathbb{R}^3 \to \mathbb{R} : \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto x_1 + x_2 + x_3.$$

Soit U la base canonique de $\mathbb{R}^3$ formée des vecteurs unitaires e_1, e_2, e_3. Pour $i = 1, 2, 3$, on considère la forme linéaire $u_i : \mathbb{R}^3 \to \mathbb{R}$ définie par

$$u_i(e_j) = \delta_{ij}, \quad \text{pour } j = 1, 2, 3.$$

Ces formes linéaires déterminent une base de l'espace dual et f doit donc se décomposer dans cette base. Déterminons cette décomposition. Soit, un élément quelconque de $\mathbb{R}^3$,

$$x = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} = \lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3.$$

Il est clair que $f(x) = \lambda_1 + \lambda_2 + \lambda_3$. De plus par linéarité, pour $i = 1, 2, 3$, $u_i(x) = \lambda_i$. Par conséquent, pour tout $x \in \mathbb{R}^3$,

$$f(x) = u_1(x) + u_2(x) + u_3(x).$$

Faisons à présent les mêmes développements dans la base $U' = (e'_1, e'_2, e'_3)$ où

$$e'_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \; e'_2 = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} \quad \text{et} \quad e'_3 = \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}.$$

Considérons la base du dual formée des formes linéaires u'_i, $i = 1, 2, 3$, avec

$$u'_i(e'_j) = \delta_{ij}, \quad \text{pour } j = 1, 2, 3.$$

Pour tous $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$, il est facile de vérifier que

$$\lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3 = (\lambda_1 - 2\lambda_2 + \lambda_3) e'_1 + (\lambda_2 - 2\lambda_3) e'_2 + \lambda_3 e'_3.$$

Ceci nous donne la formule de changement de base de la base U à la base U'. Puisque les u'_i forment une base du dual,

$$f(x) = \alpha_1 u'_1(x) + \alpha_2 u'_2(x) + \alpha_3 u'_3(x), \; \forall x \in \mathbb{R}^3$$

et nous devons déterminer les coefficients α_i, $i = 1, 2, 3$. Pour tout x de la forme $\lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3$, au vu de ce qui précède, on a

$$u'_1(x) = \lambda_1 - 2\lambda_2 + \lambda_3, \; u'_2(x) = \lambda_2 - 2\lambda_3 \quad \text{et} \quad u'_3(x) = \lambda_3.$$

De là,

$$f(x) = \lambda_1 + \lambda_2 + \lambda_3 = \alpha_1 (\lambda_1 - 2\lambda_2 + \lambda_3) + \alpha_2 (\lambda_2 - 2\lambda_3) + \alpha_3 \lambda_3.$$

Cette dernière égalité étant satisfaite pour toute valeur de λ_i, on en tire que $\alpha_1 = 1$, $\alpha_2 = 3$ et $\alpha_3 = 6$. Le calcul effectué ci-dessus est long et fastidieux. En appliquant le raisonnement effectué dans la preuve de la proposition X.6.2, on aurait directement obtenu

$$\alpha_1 = f(e'_1) = 1, \; \alpha_2 = f(e'_2) = 2 + 1 = 3, \; \alpha_3 = f(e'_3) = 3 + 2 + 1 = 6.$$

Proposition X.6.8. *Si P est la matrice de changement de base de la base $U = (u_1, \ldots, u_n)$ à la base $V = (v_1, \ldots, v_n)$ de E, alors la matrice de changement de base de la base $V^* = (v_1^*, \ldots, v_n^*)$ à la base $U^* = (u_1^*, \ldots, u_n^*)$ de E^* est $\widetilde{P}$.*

Démonstration. Posons[13] $P = (p_{ij})$ de sorte que $u_j = p_{1j} v_1 + \cdots + p_{nj} v_n$ pour tout entier $j \in \{1, \ldots, n\}$. Puisque l'application v_k^* est linéaire, il vient

$$v_k^*(u_j) = p_{1j} v_k^*(v_1) + \cdots + p_{nj} v_k^*(v_n) = p_{kj}.$$

Les formes linéaires v_k^* et $p_{k1} u_1^* + \cdots + p_{kn} u_n^*$ coïncident ainsi sur chaque vecteur de la base U. Par suite, elles sont égales. On a par conséquent

$$v_k^* = p_{k1} u_1^* + \cdots + p_{kn} u_n^*$$

et la matrice de changement de base de la base $V^* = (v_1^*, \ldots, v_n^*)$ à la base $U^* = (u_1^*, \ldots, u_n^*)$ de E^* est donc $\widetilde{P}$.

■

[13] Pour rappel, la j-ième colonne de la matrice de changement de base de la base U à la base V contient les composantes du j-ième vecteur de l'ancienne base U dans la nouvelle base V.

Corollaire X.6.9. *Toute base de E^* est la base duale d'une base de E.*

Démonstration. Soient $U = (u_1, \dots, u_n)$ une base de E et $(\ell_1, \dots, \ell_n)$ une base de E^*. Notons Q la matrice de changement de base de la base $(u_1^*, \dots, u_n^*)$ à la base $(\ell_1, \dots, \ell_n)$ de E^* et posons $P = \widetilde{Q}$. Pour tout $j \in \{1, \dots, n\}$, notons v_j le vecteur de E dont les composantes dans la base U sont les coefficients de la j-ième colonne de P. Puisque P est une matrice inversible, les vecteurs $v_1, \dots, v_n$ sont linéairement indépendants et forment donc une base de E. La matrice P est la matrice de changement de base de la base $V = (v_1, \dots, v_n)$ à la base U. D'après la proposition précédente, $\widetilde{P} = Q$ est la matrice de changement de base de la base $(u_1^*, \dots, u_n^*)$ à la base $(v_1^*, \dots, v_n^*)$. Par définition de Q, il vient

$$(\ell_1, \dots, \ell_n) = (v_1^*, \dots, v_n^*).$$

■

Exemple X.6.10. Considérons les quatre formes linéaires $\ell_1, \ell_2, \ell_3, \ell_4 : \mathbb{R}^4 \to \mathbb{R}$ définies par

$$\begin{cases} \ell_1(x,y,z,t) &= x - y + 2z + 3t \\ \ell_2(x,y,z,t) &= y + z + t \\ \ell_3(x,y,z,t) &= z + t \\ \ell_4(x,y,z,t) &= 2z + 3t \end{cases}$$

pour tout $(x, y, z, t) \in \mathbb{R}^4$. Notons (e_1, e_2, e_3, e_4) la base canonique de $\mathbb{R}^4$ et P la matrice dont les **lignes** sont les composantes des formes $\ell_1, \ell_2, \ell_3, \ell_4$ dans la base $(e_1^*, e_2^*, e_3^*, e_4^*)$. Il vient

$$P = \begin{pmatrix} 1 & -1 & 2 & 3 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 2 & 3 \end{pmatrix}$$

et $\det P = 1$. La matrice P est donc inversible et $\widetilde{P}$ aussi. Les colonnes de la matrice $\widetilde{P}$ sont les composantes des formes $\ell_1, \ell_2, \ell_3, \ell_4$ dans la base $(e_1^*, e_2^*, e_3^*, e_4^*)$.

Cela signifie que $(\ell_1, \ell_2, \ell_3, \ell_4)$ est aussi une base de $(\mathbb{R}^4)^*$ et que $\widetilde{P}$ est la matrice de changement de base de la base $(\ell_1, \ell_2, \ell_3, \ell_4)$ à la base $(e_1^*, e_2^*, e_3^*, e_4^*)$.

Cherchons la base (u_1, u_2, u_3, u_4) de $\mathbb{R}^4$ dont la base duale est la base $(\ell_1, \ell_2, \ell_3, \ell_4)$. Pour chaque $j \in \{1, 2, 3, 4\}$, on doit résoudre le système

$$\ell_i(u_j) = \delta_{i,j}.$$

Considérons le système linéaire $Px = f$ ayant pour second membre

$$f = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}.$$

Il vient

$$\left\{\begin{array}{rcl}\ell_1(x,y,z,t) &=& a\\ \ell_2(x,y,z,t) &=& b\\ \ell_3(x,y,z,t) &=& c\\ \ell_4(x,y,z,t) &=& d\end{array}\right. \Leftrightarrow \left\{\begin{array}{rcl}x-y+2z+3t &=& a\\ y+z+t &=& b\\ z+t &=& c\\ 2z+3t &=& d\end{array}\right.$$

$$\Leftrightarrow \left\{\begin{array}{rcl}x &=& a+b-c-d\\ y &=& b-c\\ z &=& 3c-d\\ t &=& -2c+d\end{array}\right. .$$

En donnant à a, b, c, d les valeurs $1, 0, 0, 0$, on trouve $u_1 = (1, 0, 0, 0)$. De manière semblable, on trouve $u_2 = (1, 1, 0, 0)$, $u_3 = (-1, -1, 3, -2)$ et $u_4 = (-1, 0, -1, 1)$. Si on considère la matrice M dont les colonnes sont les composantes de u_1, u_2, u_3, u_4 dans la base (e_1, e_2, e_3, e_4),

$$M = \begin{pmatrix}1 & 1 & -1 & -1\\ 0 & 1 & -1 & 0\\ 0 & 0 & 3 & -1\\ 0 & 0 & -2 & 1\end{pmatrix}$$

Cette matrice est donc l'inverse de la matrice de changement de base de la base (e_1, e_2, e_3, e_4) à la base (u_1, u_2, u_3, u_4).

Pour vérifier la proposition X.6.8, $\widetilde{M^{-1}}$ doit être la matrice de changement de base de la base $(\ell_1, \ell_2, \ell_3, \ell_4)$ à la base $(e_1^*, e_2^*, e_3^*, e_4^*)$, c'est-à-dire $\widetilde{P}$. Pour le voir, il suffit de vérifier que

$$MP = I.$$

CHAPITRE XI

Opérateurs linéaires, diagonalisation et réduction

1. Introduction

Le but principal de ce chapitre est de représenter (matriciellement) les endomorphismes d'un espace vectoriel sur $\mathbb{C}$ de dimension finie de la manière *la plus simple possible*. Dès lors, nous recherchons le cas échéant une base dans laquelle l'opérateur se représente par une matrice diagonale. On parlera alors d'*opérateur diagonalisable*. Si un endomorphisme n'est pas diagonalisable, la situation n'est pas désespérée pour autant. Il existe une forme canonique, appelée *forme de Jordan*, pour laquelle le choix d'une base "spéciale" permet de représenter l'opérateur sous une forme particulièrement simple. On considérera dans tout ce chapitre, un espace vectoriel E sur $\mathbb{C}$ de dimension finie n.

La diagonalisation apparaît dans de très nombreuses branches des mathématiques et ce, tant d'un point de vue théorique qu'appliqué (étude des extrema locaux pour des fonctions à plusieurs variables, théorie des graphes, comportement asymptotique de systèmes dynamiques, analyse en composantes principales en statistique multivariée, etc.). Ce genre de problème apparaît bien évidemment également en physique, par exemple en mécanique quantique.

Remarque XI.1.1. Notons dès à présent que la diagonalisation des matrices de $\mathbb{C}_n^n$ n'est qu'un cas particulier du problème étudié ici. En effet, toute matrice $A \in \mathbb{C}_n^n$ définit un endomorphisme de $\mathbb{C}^n$, $T_A : \mathbb{C}^n \to \mathbb{C}^n : x \mapsto Ax$. Cet endomorphisme T_A se représente trivialement, dans la base canonique, par la matrice A. Ainsi, les définitions et théorèmes de ce chapitre s'appliqueront en particulier à $E = \mathbb{C}^n$.

Diagonaliser une matrice $A \in \mathbb{C}_n^n$ revient à trouver (si possible) une matrice inversible S telle que $S^{-1}AS$ soit une matrice diagonale, i.e.,

$$S^{-1}AS = \operatorname{diag}(\lambda_1, \ldots, \lambda_n), \quad \lambda_1, \ldots, \lambda_n \in \mathbb{C}.$$

Si l'on peut répondre à cette question par l'affirmative, on dit alors que A est une *matrice diagonalisable* et que S *diagonalise* A. En fait, on remarquera que cela revient à trouver une base U de $\mathbb{C}^n$ telle que S est la matrice de changement de bases pour passer de la base U à la base canonique. En effet, si A représente T_A dans la base canonique, alors $S^{-1}AS$ représente T_A dans la base U :

$$\forall x \in \mathbb{C}^n,\ S^{-1}AS\,\Phi_U(x) = S^{-1}Ax = S^{-1}T_Ax = \Phi_U(T_Ax).$$

Pour commencer, considérons un exemple numérique.

Exemple XI.1.2. Soit la matrice

$$A = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

La matrice S donnée ci-dessous est inversible

$$S = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

et on calcule facilement que

$$S^{-1}AS = \begin{pmatrix} 1 & 0 & -1 \\ -1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ -1 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Ainsi A est diagonalisable. Dans cet exemple, le choix de S paraît quelque peu miraculeux. Notre but sera donc de réussir à trouver d'une manière générale une matrice S qui diagonalise A. Lorsque A est diagonalisable, certains calculs fastidieux sont grandement simplifiés. En effet, pour calculer A^n, il vient

$$A^n = (S \operatorname{diag}(1,2,2)\, S^{-1})^n = S\,(\operatorname{diag}(1,2,2))^n\, S^{-1} = S \operatorname{diag}(1, 2^n, 2^n)\, S^{-1}.$$

2. Vecteurs propres et valeurs propres

Définition XI.2.1. Soit $T \in \mathcal{L}(E)$ un endomorphisme. Le nombre complexe λ est une *valeur propre* de T s'il existe $x \in E \setminus \{0\}$ tel que $Tx = \lambda x$. L'ensemble des valeurs propres de T s'appelle le *spectre* de T et se note $\operatorname{sp}(T)$.

Soit λ une valeur propre de T. Le vecteur $x \in E$ est *vecteur propre* de T de valeur propre λ si $Tx = \lambda x$. L'ensemble E_λ des vecteurs propres de T de valeur propre λ est un sous-espace vectoriel de E appelé le *sous-espace propre* de T associé à la valeur propre λ,

$$E_\lambda = E_\lambda(T) = \{x \in E \mid Tx = \lambda x\} = \ker(T - \lambda\, id).$$

La dimension de E_λ est la *multiplicité géométrique* de λ.

Soient U une base de E et A la matrice représentant T dans cette base. Remarquons que $Tx = \lambda x$ si et seulement si $A\Phi_U(x) = \Phi_U(\lambda x) = \lambda \Phi_U(x)$. Ainsi, T et toute matrice représentant T possèdent exactement les mêmes valeurs propres.

Remarque XI.2.2. Remarquons en outre que des notions comme celles de vecteurs et valeurs propres se rencontrent fréquemment dans un contexte plus général. Par exemple, l'application dérivée D_x est un endomorphisme[1]

[1] Il est clair que $D_x(f+g) = D_x f + D_x g$ et que $D_x \lambda f = \lambda D_x f$. Cependant, nous limitons notre étude au cadre des espaces vectoriels de dimension finie. Par la suite, nous n'étudierons donc pas l'espace vectoriel $C_\infty(\mathbb{R})$.

du $\mathbb{R}$-vectoriel $C_\infty(\mathbb{R})$ et résoudre l'équation différentielle

Les solutions de l'équation sont donc des vecteurs propres.

$$D_x f = \lambda f$$

revient donc à chercher les vecteurs f de $C_\infty(\mathbb{R})$ ayant une image proportionnelle à f par l'endormorphisme D_x.

Définition XI.2.3. Un endomorphisme T est *diagonalisable* s'il existe une base dans laquelle T se représente par une matrice diagonale.

Exemple XI.2.4. Soit un endomorphisme T d'un espace vectoriel E de dimension 2. Dans la base $B = (e_1, e_2)$, T est défini par

$$Te_1 = 2e_1 \quad \text{et} \quad Te_2 = e_1 + e_2.$$

Ainsi, il s'y représente par la matrice (non diagonale)

$$A = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}.$$

Considérons à présent la base $U = (u_1 = e_1, u_2 = e_2 - e_1)$. Il vient

$Tu_1 = Te_1 = 2e_1 = 2u_1$ et $Tu_2 = Te_2 - Te_1 = e_1 + e_2 - 2e_1 = e_2 - e_1 = u_2$.

Ainsi, dans la base U, T se représente par la matrice diagonale

$$\Delta = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

La matrice de changement de base de la base B à la base U est

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

Son inverse est

$$S^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad S^{-1}AS = \Delta.$$

Le lien entre la diagonalisation d'un endomorphisme et ses vecteurs propres est le suivant.

Proposition XI.2.5. *Un endomorphisme $T \in \mathcal{L}(E)$ est diagonalisable si et seulement si E possède une base formée de vecteurs propres.*

Démonstration. La preuve est immédiate. Si $U = (u_1, \ldots, u_n)$ est une base de E, la matrice qui représente T dans la base U a pour j-ième colonne $\Phi_U(Tu_j)$. En particulier, si u_j est un vecteur propre de T de valeur propre λ, cela signifie que $Tu_j = \lambda u_j$ et donc $\Phi_U(Tu_j) = \lambda e_j$.

■

Remarque XI.2.6. Si T est diagonalisable, toute matrice représentant T est diagonalisable. En effet, soit U (resp. U') une base de E dans laquelle T se représente par une matrice diagonale Δ (resp. par une matrice A). Si S est la matrice de changement de base permettant de passer de la base U' à la base U, alors $\Delta = S^{-1}AS$ et A est diagonalisable.

Exemple XI.2.7. On peut reprendre l'exemple XI.1.2 et vérifier que les colonnes de S sont bien trois vecteurs propres de A linéairement indépendants.

3. Polynôme caractéristique

Rappelons que si T est un endomorphisme de E et si les matrices A et B représentent T dans deux bases quelconques de E, alors $\det A = \det B$. On peut dès lors parler du *déterminant* de T que l'on note simplement $\det T$ (cf. page 206). Ainsi, la définition suivante est intrinsèque : elle ne dépend pas de la base choisie pour représenter T.

Définition XI.3.1. Soit $T \in \mathcal{L}(E)$. Si A représente T dans une base $e_1, \ldots, e_n$ de E, le polynôme en λ

$$\chi_T(\lambda) = \det(T - \lambda\, id) = \det(A - \lambda I)$$

est le *polynôme caractéristique* de T. Si λ est une valeur propre de T, la *multiplicité algébrique* de λ est sa multiplicité comme zéro de $\det(T - \lambda I)$.

Exemple XI.3.2. Poursuivons l'exemple XI.1.2. Le polynôme caractéristique de A est donné par

$$\chi_A(\lambda) = \det \begin{pmatrix} 1-\lambda & 0 & 1 \\ -1 & 2-\lambda & 1 \\ 0 & 0 & 2-\lambda \end{pmatrix} = -\lambda^3 + 5\lambda^2 - 8\lambda + 4.$$

Proposition XI.3.3. *Soit $T \in \mathcal{L}(E)$. Le nombre complexe λ est valeur propre de T si et seulement si $\chi_T(\lambda) = 0$.*

Démonstration. Soit U une base de E. Le nombre complexe λ est valeur propre de T, s'il existe un vecteur non nul $x \in E$ tel que $Tx = \lambda\, x$. Cette relation est équivalente à

$$(A - \lambda I)\Phi_U(x) = 0$$

où A représente T dans la base U. Ce système linéaire homogène ayant $\Phi_U(x)$ comme vecteur des inconnues possède une solution non nulle si et seulement si il n'est pas de Cramer (cf. proposition VI.2.4), c'est-à-dire, si et seulement si $\det(A - \lambda I) = 0$.

■

Remarque XI.3.4. Si $S \in \mathbb{C}_n^n$ est inversible, les matrices $S^{-1}AS$ et A ont le même polynôme caractéristique car

$$\begin{aligned} \det(S^{-1}AS - \lambda I) &= \det(S^{-1}(A - \lambda I)S) \\ &= \det S^{-1} \det(A - \lambda I) \det S = \det(A - \lambda I). \end{aligned}$$

Ainsi, cela montre une fois encore que $\chi_T(\lambda)$ est indépendant de la base choisie pour représenter T. En particulier, deux matrices semblables ont les mêmes valeurs propres (avec les mêmes multiplicités algébriques).

Passons à présent en revue quelques propriétés du polynôme caractéristique d'une matrice. Ces propriétés pouvant en grande partie être transposées aux applications linéaires correspondantes.

Proposition XI.3.5. *On dispose des propriétés suivantes.*

- *Soient $A, B \in \mathbb{C}_n^n$. Les matrices AB et BA ont le même polynôme caractéristique. En particulier, le polynôme caractéristique d'un produit de matrices carrées est invariant si on permute circulairement les facteurs.*
- *Le polynôme caractéristique de $\widetilde{A}$ est égal à celui de A.*
- *Les polynômes caractéristiques de $\overline{A}$ et A^* sont égaux au polynôme conjugué du polynôme caractéristique de A.*

Démonstration. Pour le premier point, on considère la matrice carrée de dimension $2n$

$$\begin{pmatrix} -\lambda I & A \\ B & -I \end{pmatrix}$$

et si $\lambda \neq 0$, on lui applique les deux formules de Frobenius-Schur. Il vient

$$\underbrace{\det(-\lambda I)}_{(-\lambda)^n} \det(\underbrace{-I - B(-\lambda I)^{-1}A}_{-I+\frac{1}{\lambda}BA}) = \underbrace{\det(-I)}_{(-1)^n} \det(-\lambda I + AB).$$

De là,

$$\det(BA - \lambda I) = \det(AB - \lambda I).$$

L'égalité étant vérifiée pour tout λ non nul, elle l'est aussi si $\lambda = 0$.

Pour les deux derniers points, on a

$$\det(\widetilde{A} - \lambda I) = \det(\widetilde{A} - \lambda \widetilde{I}) = \det(\widetilde{A - \lambda I}) = \det(A - \lambda I)$$

et

$$\det(\overline{A} - \lambda I) = \det((\overline{A} - \lambda I)^{\sim}) = \det(A^* - \lambda I) = \overline{\det(A - \overline{\lambda} I)}.$$

■

Rappelons qu'une sous-matrice diagonale de dimension k est une sous-matrice de A de la forme

$$A_{(i_1,\ldots,i_k;i_1,\ldots,i_k)}.$$

Par exemple

$$\begin{pmatrix} 1 & 3 \\ 7 & 9 \end{pmatrix}$$

est une sous-matrice diagonale de la matrice

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

La proposition suivante précise la forme des coefficients du polynôme caractéristique χ_A de A. Elle peut aussi s'appliquer à toute matrice A représentant un endomorphisme $T \in \mathcal{L}(E)$.

Proposition XI.3.6. *Soit $A \in \mathbb{C}_n^n$ Si on pose*

$$\det(A - \lambda I) = \sum_{i=0}^{n} \alpha_i (-\lambda)^i = \sum_{i=0}^{n} (-1)^i \alpha_i \lambda^i,$$

alors $\alpha_n = 1$ et pour tout $i < n$, α_i est la somme des déterminants des sous-matrices diagonales de A de dimension $n - i$. En particulier, $\alpha_0 = \det A$ et

$$\alpha_{n-1} = \sum_{j=1}^{n} a_{jj}.$$

Démonstration. Si on considère les colonnes de A,

$$\det(A - \lambda I) = \det\begin{pmatrix} C_1 - \lambda e_1 & \cdots & C_n - \lambda e_n \end{pmatrix}.$$

Vu la multilinéarité du déterminant, on a

$$\det(A - \lambda I) = \sum_{i=0}^{n} (-\lambda)^i \sum_{1 \leq \nu_1 < \cdots < \nu_i \leq n} \det\begin{pmatrix} C_1 & \cdots & e_{\nu_1} & \cdots & e_{\nu_i} & \cdots & C_n \end{pmatrix}.$$

En effet, un terme faisant apparaître du $(-\lambda)^i$ est obtenu en considérant dans la matrice $A - \lambda I$, i vecteurs unitaires $e_{\nu_1}, \ldots, e_{\nu_i}$ et $n - i$ colonnes de A. Pour calculer $\det\begin{pmatrix} C_1 & \cdots & e_{\nu_1} & \cdots & e_{\nu_i} & \cdots & C_n \end{pmatrix}$, on applique i fois la règle des mineurs[2] aux colonnes qui ont été remplacées par $e_{\nu_1}, \ldots, e_{\nu_i}$. Cela revient à calculer le déterminant de la matrice A privée des lignes et des colonnes d'indices $\nu_1, \ldots, \nu_i$. En d'autres termes, α_i est la somme des déterminants des sous-matrices diagonales de A de dimension $n - i$.

■

Remarque XI.3.7. La seule difficulté de cette dernière démonstration réside dans la manipulation d'une matrice de dimension arbitraire n. Pour se convaincre des développements utilisés, nous présentons le cas d'une matrice de dimension 3. Il vient,

$$\begin{aligned}
& \det\begin{pmatrix} C_1 - \lambda e_1 & C_2 - \lambda e_2 & C_3 - \lambda e_3 \end{pmatrix} \\
= \; & \det\begin{pmatrix} C_1 & C_2 - \lambda e_2 & C_3 - \lambda e_3 \end{pmatrix} - \lambda \det\begin{pmatrix} e_1 & C_2 - \lambda e_2 & C_3 - \lambda e_3 \end{pmatrix} \\
= \; & \det\begin{pmatrix} C_1 & C_2 & C_3 - \lambda e_3 \end{pmatrix} - \lambda \begin{pmatrix} C_1 & e_2 & C_3 - \lambda e_3 \end{pmatrix} \\
& - \lambda \det\begin{pmatrix} e_1 & C_2 & C_3 - \lambda e_3 \end{pmatrix} + \lambda^2 \det\begin{pmatrix} e_1 & e_2 & C_3 - \lambda e_3 \end{pmatrix} \\
= \; & \det\begin{pmatrix} C_1 & C_2 & C_3 \end{pmatrix} - \lambda \det\begin{pmatrix} C_1 & C_2 & e_3 \end{pmatrix} - \lambda \begin{pmatrix} C_1 & e_2 & C_3 \end{pmatrix} \\
& + \lambda^2 \begin{pmatrix} C_1 & e_2 & e_3 \end{pmatrix} - \lambda \det\begin{pmatrix} e_1 & C_2 & C_3 \end{pmatrix} + \lambda^2 \det\begin{pmatrix} e_1 & C_2 & e_3 \end{pmatrix} \\
& + \lambda^2 \det\begin{pmatrix} e_1 & e_2 & C_3 \end{pmatrix} - \lambda^3 \det\begin{pmatrix} e_1 & e_2 & e_3 \end{pmatrix}.
\end{aligned}$$

D'où la conclusion en regroupant les termes en $(-\lambda)^i$.

[2] Remarquons que e_{ν_k} se trouve dans la ν_k-ième colonne de la matrice. Par conséquent, le cofacteur correspondant à l'élément ν_k, ν_k de cette matrice est égal au déterminant de la matrice privée de sa ν_k-ième ligne et de sa ν_k-ième colonne (multiplié par $(-1)^{2\nu_k} = 1$).

Exemple XI.3.8. Illustrons cette dernière proposition en considérant une fois encore la matrice de l'exemple XI.1.2 (nous en connaissons déjà par ailleurs le polynôme caractéristique, cf. exemple XI.3.2). Avec les notations de la proposition XI.3.6, $\alpha_3 = 1$. Pour obtenir α_2, il faut calculer la somme des déterminants des sous-matrices diagonales de dimension $3-2$, i.e., la somme des éléments diagonaux de A. Ainsi, $\alpha_2 = 1+2+2 = 5$. Pour obtenir α_1, il faut calculer la somme des déterminants des sous-matrices diagonales de dimension $3-1=2$,

$$\alpha_1 = \det \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} + \det \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} + \det \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} = 2+2+4 = 8.$$

Enfin, $\alpha_0 = \det A = 4$.

Définition XI.3.9. Le coefficient α_{n-1} apparaissant dans la proposition précédente comme somme des éléments diagonaux d'une matrice carrée $A = (a_{ij})$, s'appelle la *trace* de A, i.e.,

$$\operatorname{tr} A = \sum_{j=1}^{n} a_{jj}.$$

Puisque le polynôme caractéristique d'un endomorphisme T est invariant par changement de base, nous pouvons aussi définir, de cette manière, la trace de T. Au vu de la proposition XI.3.11, la trace de T est parfois définie comme la somme des valeurs propres de T (répétées selon leur multiplicité).

Passons en revue les premières propriétés de la trace d'une matrice.

Proposition XI.3.10. *La trace jouit des propriétés suivantes.*

- $\operatorname{tr} \widetilde{A} = \operatorname{tr} A$,
- $\operatorname{tr} \overline{A} = \operatorname{tr} A^* = \overline{\operatorname{tr} A}$,
- *la trace est linéaire, i.e., si* $A_1, \ldots, A_p \in \mathbb{C}_n^n$ *et* $\lambda_1, \ldots, \lambda_p \in \mathbb{C}$, *alors*
$$\operatorname{tr} \left(\sum_{j=1}^{p} \lambda_j A_j \right) = \sum_{j=1}^{p} \lambda_j \operatorname{tr} A_j,$$
- $\operatorname{tr}(AB) = \operatorname{tr}(BA)$,
- $\operatorname{tr}(S^{-1}AS) = \operatorname{tr} A$.

Démonstration. Il s'agit de simples vérifications. ∎

Proposition XI.3.11. *Si* $\lambda_1, \ldots, \lambda_n$ *sont les valeurs propres de* A *répétées selon leur multiplicité comme racine du polynôme caractéristique de* A, *alors les coefficients* α_i $(i < n)$ *sont donnés par*

Même notation α_i qu'à la proposition XI.3.6.

$$\alpha_i = \sum_{1 \le \nu_1 < \cdots < \nu_{n-i} \le n} \lambda_{\nu_1} \cdots \lambda_{\nu_{n-i}}.$$

En particulier,

$$\det A = \alpha_0 = \prod_{j=1}^{n} \lambda_j \quad \textit{et} \quad \operatorname{tr} A = \alpha_{n-1} = \sum_{j=1}^{n} \lambda_j.$$

Prenons μ comme variable pour éviter toute confusion avec les valeurs propres λ_i.

Démonstration. Au vu du théorème fondamental de l'algèbre, on a

$$\chi_A(\mu) = \det(A - \mu I) = (-1)^n \prod_{j=1}^{n} (\mu - \lambda_j).$$

Si on développe ce produit, on trouve

$$\det(A - \mu I) = (-1)^n \sum_{i=0}^{n} \mu^i \sum_{1 \le \nu_1 < \cdots < \nu_{n-i} \le n} (-1)^{n-i} \lambda_{\nu_1} \cdots \lambda_{\nu_{n-i}}$$

$$= \sum_{i=0}^{n} \underbrace{(-1)^n (-1)^{n-i}}_{=(-1)^i} \mu^i \sum_{1 \le \nu_1 < \cdots < \nu_{n-i} \le n} \lambda_{\nu_1} \cdots \lambda_{\nu_{n-i}}.$$

D'où la conclusion, par définition même des α_i.

■

Exemple XI.3.12. Illustrons une fois encore cette dernière proposition à l'aide de la matrice de l'exemple XI.1.2. Puisque

$$\chi_A(\lambda) = -\lambda^3 + 5\lambda^2 - 8\lambda + 4 = -(\lambda - 1)(\lambda - 2)^2,$$

avec les notations de la proposition précédente, on a $\lambda_1 = 1$ et $\lambda_2 = \lambda_3 = 2$. Il vient

$$\alpha_2 = \lambda_1 + \lambda_2 + \lambda_3 = 5,$$
$$\alpha_1 = \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3 = 8,$$
$$\alpha_0 = \lambda_1\lambda_2\lambda_3 = 4.$$

Il suffit de comparer ces résultats avec les coefficients de $\chi_A(\lambda)$ obtenus dans l'exemple XI.3.2.

4. Diagonalisation

La proposition suivante montre que la multiplicité géométrique d'une valeur propre est toujours inférieure ou égale à sa multiplicité algébrique.

Proposition XI.4.1. *Soit λ une valeur propre de $T \in \mathcal{L}(E)$ de multiplicité algébrique μ. On a*

$$\dim E_\lambda \le \mu.$$

Démonstration. Soit $p = \dim E_\lambda$. Il existe des vecteurs $x_1, \ldots, x_p \in E$ qui forment une base de E_λ. Il existe également des vecteurs $y_{p+1}, \ldots, y_n$ tels que $x_1, \ldots, x_p, y_{p+1}, \ldots, y_n$ forment une base de E. Dans cette base, T se représente par

$$M = \begin{pmatrix} \lambda I_p & B \\ 0 & C \end{pmatrix}$$

où C est une matrice carrée de dimension $n-p$. Le polynôme caractéristique de T est $\chi_T(\beta) = \det(M - \beta I) = (\lambda - \beta)^p \det(C - \beta I_{n-p})$ et λ en est un zéro de multiplicité au moins p.

■

Proposition XI.4.2. *Des vecteurs propres non nuls associés à des valeurs propres distinctes sont linéairement indépendants.*

Démonstration. Soient $x_1, \ldots, x_p$ des vecteurs propres non nuls associés à des valeurs propres distinctes $\lambda_1, \ldots, \lambda_p$. Supposons que

$$\sum_{i=1}^{p} \beta_i x_i = 0. \tag{10}$$

Pour $k \in \{1, \ldots, p\}$, on définit l'opérateur

$$T_k = (T - \lambda_1 id) \cdots (\widehat{T - \lambda_k id}) \cdots (T - \lambda_p id).$$

On a

$$T_k x_i = 0 \text{ si } i \neq k$$

et

$$T_i x_i = (\lambda_i - \lambda_1) \cdots (\widehat{\lambda_i - \lambda_i}) \cdots (\lambda_i - \lambda_p) x_i \neq 0.$$

En appliquant T_k à (10), on trouve pour tout $k \in \{1, \ldots, p\}$,

$$\beta_k T_k x_k = 0$$

et donc $\beta_1 = \cdots = \beta_p = 0$, ce qui suffit.

■

Corollaire XI.4.3. *Si $\lambda_1, \ldots, \lambda_p$ sont les valeurs propres distinctes de T, alors la somme $E_{\lambda_1} + \cdots + E_{\lambda_p}$ est directe. De plus, T est diagonalisable si et seulement si $E = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_p}$.*

Démonstration. C'est immédiat. Si l'on disposait de deux décompositions différentes du vecteur nul comme somme d'éléments des sous-espaces E_{λ_i}, alors on mettrait en défaut la proposition précédente.

Pour la deuxième partie, il suffit d'appliquer la proposition XI.2.5. Si $E \supsetneq E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_p}$, alors on ne peut trouver une base de E formée uniquement de vecteurs propres de T. Par contre, si $E = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_p}$, alors il est aisé d'obtenir une base de E formée de vecteurs propres (se rappeler la remarque VII.5.26).

■

Corollaire XI.4.4. *Un endomorphisme $T \in \mathcal{L}(E)$ est diagonalisable si et seulement si les multiplicités algébrique et géométrique de chaque valeur propre de T coïncident.*

Démonstration. Soient $\lambda_1, \ldots, \lambda_p$ les valeurs propres distinctes de T de multiplicité algébrique respective $\mu_1, \ldots, \mu_p$. Au vu du corollaire précédent, T est diagonalisable si et seulement si

$$E = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_p}$$

ou encore, si et seulement si

$$\dim E = \dim E_{\lambda_1} + \cdots + \dim E_{\lambda_p}.$$

Si $\dim E_{\lambda_j} = \mu_j$ pour tout $j \in \{1, \ldots, p\}$, alors T est diagonalisable car $\mu_1 + \cdots + \mu_p = \dim E$. En effet, le polynôme caractéristique de T est de degré égal à la dimension de E.

Réciproquement, si T est diagonalisable, alors $\dim E_{\lambda_j} = \mu_j$ car sinon, au vu de la proposition XI.4.1, on aurait $\dim E = \dim E_{\lambda_1} + \cdots + \dim E_{\lambda_p} < \mu_1 + \cdots + \mu_p = \dim E$ ce qui est impossible.

■

Corollaire XI.4.5. *Un endomorphisme dont toutes les valeurs propres sont simples est diagonalisable.*

Démonstration. C'est immédiat, toute valeur propre possède au moins un vecteur propre non nul.

■

5. Exemples et applications

Considérons tout d'abord quelques exemples numériques.

Exemple XI.5.1. Reprenons la matrice A donnée dans l'exemple XI.1.2,

$$A = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

Les valeurs propres de A sont les zéros de

$$\chi_A(\lambda) = -\lambda^3 + 5\lambda^2 - 8\lambda + 4 = -(\lambda - 1)(\lambda - 2)^2.$$

Ainsi, 1 (resp. 2) est valeur propre de multiplicité algébrique égale à 1 (resp. 2). Nous ne pouvons pas directement conclure que A est diagonalisable car nous avons une valeur propre multiple. Recherchons les espaces propres associés à 1 et à 2 :

$$E_1 = \{x \in \mathbb{C}^3 \mid (A - I)x = 0\}$$

et

$$E_2 = \{x \in \mathbb{C}^3 \mid (A - 2I)x = 0\}.$$

Pour le premier, on a

$$\begin{pmatrix} 0 & 0 & 1 \\ -1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

et on trouve $x_3 = 0$ et $x_1 = x_2$. Ainsi,

$$E_1 = \left\langle \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\rangle.$$

Encore dit autrement, puisque la matrice $A - I$ est de rang deux, on aurait pu en conclure directement que $\dim E_1 = 3 - 2 = 1$. Pour le second espace propre, il vient

$$\begin{pmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

et on trouve $x_1 = x_3$ comme unique condition. Les vecteurs

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

appartiennent tous les deux à E_2 et sont linéairement indépendants. Par conséquent, la multiplicité géométrique de la valeur propre 2 est bien 2. Ceci montre que A est diagonalisable et on construit alors facilement une matrice qui la diagonalise. Par exemple, la matrice

$$S = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

est telle que $S^{-1}AS = \operatorname{diag}(1, 2, 2)$. De même, la matrice

$$T = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

où l'on a permuté les deux premières colonnes de S est telle que $T^{-1}AT = \operatorname{diag}(2, 1, 2)$.

Exemple XI.5.2. Considérons la matrice

$$A = \begin{pmatrix} 2 & 4 & 3 \\ -4 & -6 & -3 \\ 3 & 3 & 1 \end{pmatrix}.$$

Les valeurs propres de A sont les zéros de son polynôme caractéristique,

$$\chi_A(\lambda) = -\lambda^3 - 3\lambda^2 + 4 = -(\lambda - 1)(\lambda + 2)^2.$$

Pour que A soit diagonalisable, il faut nécessairement que la dimension de l'espace propre E_2 soit 2. Les vecteurs propres x de valeur propre -2 satisfont $(A + 2I)x = 0$, c'est-à-dire,

$$\begin{pmatrix} 4 & 4 & 3 \\ -4 & -4 & -3 \\ 3 & 3 & 3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

et donc $x_1 = -x_2$ et $x_3 = 0$. Ainsi,

$$E_{-2} = \left\langle \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \right\rangle$$

et la multiplicité géométrique est strictement inférieure à 2. La matrice A n'est donc pas diagonalisable. Pour le voir, on aurait pu aussi remarquer que le rang de la matrice $A + 2I$ est deux et dès lors, $\dim E_{-2} = 3 - 2 = 1 < 2$.

Exemple XI.5.3. Nous reprenons à présent un exemple présenté au début de ces notes de cours. A savoir, l'exemple III.6.3 dans lequel trois partis politiques R, S et T s'opposent. On y décrit un modèle de prédiction de répartition des votes d'une élection à l'élection suivante. Grâce à la diagonalisation, nous allons proposer des prédictions à long terme pour ce modèle (on parle parfois de comportement asymptotique). La matrice P du modèle était

$$\begin{pmatrix} 0,6 & 0,2 & 0,2 \\ 0,3 & 0,6 & 0,1 \\ 0,3 & 0,2 & 0,5 \end{pmatrix}.$$

Son polynôme caractéristique est

$$-(\lambda - 1)(\lambda - 0,4)(\lambda - 0,3).$$

Puisque P possède trois valeurs propres simples, cette matrice est diagonalisable. Pour calculer P^n, diagonalisons P. Il est facile de voir que

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} -4/3 \\ 1 \\ 1 \end{pmatrix}$$

sont des vecteurs propres de valeur propre respective 1; 0,4 et 0,3. Si

$$S = \begin{pmatrix} 1 & 1 & -4/3 \\ 1 & -2 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \text{ alors } S^{-1} = \begin{pmatrix} 3/7 & 1/3 & 5/21 \\ 0 & -1/3 & 1/3 \\ -3/7 & 0 & 3/7 \end{pmatrix}.$$

Puisque $\operatorname{diag}(1; 0,4; 0,3) = S^{-1}PS$, on trouve

$$P^n = S \operatorname{diag}(1; 0,4^n; 0,3^n)\ S^{-1}.$$

Ainsi, la répartition des votes à long terme est donnée par

$$\begin{aligned} \lim_{n\to\infty} \begin{pmatrix} 0,3 & 0,5 & 0,2 \end{pmatrix} P^n &= \begin{pmatrix} 0,3 & 0,5 & 0,2 \end{pmatrix} S \operatorname{diag}(1,0,0)\ S^{-1} \\ &= \begin{pmatrix} 3/7 & 1/3 & 5/21 \end{pmatrix} \end{aligned}$$

où $\begin{pmatrix} 0,3 & 0,5 & 0,2 \end{pmatrix}$ est le vecteur des répartitions initiales au sein des trois partis.

Remarque XI.5.4. Si $A \in \mathbb{C}_n^n$ est une matrice diagonalisable par une matrice inversible S, i.e., $S^{-1}AS = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$, alors

$$A^k = S\operatorname{diag}(\lambda_1^k, \ldots, \lambda_n^k)S^{-1}$$

et on en déduit que tout élément d'une puissance k-ième de A s'exprime comme combinaison linéaire de puissances k-ièmes des valeurs propres de A, i.e.,

$$\boxed{(A^k)_{i,j} = \sum_{\ell=1}^{n} c_{i,j}^{(\ell)}\, \lambda_\ell^k}$$

où les $c_{i,j}$ sont des nombres complexes. Bien évidemment, on obtient exactement le même type d'expression en ne considérant que les valeurs propres distinctes de A.

Exemple XI.5.5. Le dernier exemple concerne la résolution de systèmes d'équations différentiels linéaires. Nous énoncerons sans démonstration des résultats classiques d'analyse et les appliquerons à un exemple d'une particule se déplaçant dans un champ de force. Soient $x_1, \ldots, x_n$ des fonctions continûment dérivables en la variable t. Nous noterons x_i' la dérivée de x_i par rapport à t. Le système d'équations différentielles homogène

$$\begin{cases} x_1' &= a_{11}x_1 + \cdots + a_{1n}x_n \\ &\vdots \\ x_n' &= a_{n1}x_1 + \cdots + a_{nn}x_n \end{cases}$$

où les a_{ij} sont des constantes, peut se mettre sous forme matricielle

$$\mathbf{x}'(t) = A\,\mathbf{x}(t)$$

où $\mathbf{x}$ désigne le vecteur des fonctions $x_1, \ldots, x_n$ et $A = (a_{ij})$. Il est clair que si $\mathbf{u}$ et $\mathbf{v}$ sont des solutions de $\mathbf{x}' = A\,\mathbf{x}$, alors toute combinaison linéaire $\alpha\mathbf{u} + \beta\mathbf{v}$ l'est aussi[3]. En effet,

$$(\alpha\mathbf{u} + \beta\mathbf{v})' = \alpha\mathbf{u}' + \beta\mathbf{v}' = \alpha A\mathbf{u} + \beta A\mathbf{v} = A(\alpha\mathbf{u} + \beta\mathbf{v}).$$

Supposons qu'une solution de $\mathbf{x}' = A\,\mathbf{x}$ soit de la forme

Cette supposition devrait paraître naturelle au lecteur habitué aux équations différentielles.

$$\mathbf{x}(t) = e^{\lambda t}\mathbf{c}$$

avec $\mathbf{c}$ un vecteur constant. Dans ce cas, on a nécessairement

$$\mathbf{x}'(t) = \lambda\, e^{\lambda t}\mathbf{c} \quad \text{et} \quad A\mathbf{x}(t) = A\, e^{\lambda t}\mathbf{c}.$$

Puisque l'exponentielle ne s'annule jamais, $\mathbf{c}\, e^{\lambda t}$ est solution de $\mathbf{x}' = A\,\mathbf{x}$ si $A\mathbf{c} = \lambda\mathbf{c}$. Ainsi, chaque couple formé par une valeur propre λ de A et un vecteur propre $\mathbf{c}$ correspondant fournit une solution de l'équation $\mathbf{x}' = A\,\mathbf{x}$. Ces fonctions sont parfois appelées les *fonctions propres* de l'équation différentielle $\mathbf{x}' = A\,\mathbf{x}$. On peut montrer que si la matrice A est diagonalisable et si des vecteurs propres $\mathbf{c}_1, \ldots, \mathbf{c}_n$ de A associés respectivement aux valeurs propres $\lambda_1, \ldots, \lambda_n$ forment une base de $\mathbb{R}^n$, alors toute solution de l'équation $\mathbf{x}' = A\,\mathbf{x}$ s'obtient comme combinaison linéaire des fonctions propres, i.e., $\mathbf{x} = \sum_{i=1}^{n} \alpha_i\, e^{\lambda_i t}\mathbf{c}_i$.

[3] On exprime simplement la linéarité de l'équation. Certains auteurs parlent parfois de la propriété de *superposition* des solutions.

Considérons à présent le cas d'une masse (supposée ponctuelle) attachée à un ressort. Ce système évoluant au sein d'un milieu hautement visqueux[4], si on écarte la masse de la position d'équilibre du ressort, alors son vecteur position $\mathbf{x}$ satisfait la loi de mouvement $\mathbf{x}' = A\,\mathbf{x}$ où

$$A = \begin{pmatrix} 4 & -5 \\ -2 & 1 \end{pmatrix}$$

et où la position initiale de la masse au temps $t = 0$ est

$$\mathbf{x}_0 = \begin{pmatrix} 4 \\ 3 \end{pmatrix}.$$

Un calcul aisé donne 6 et -1 comme valeurs propres et on trouve comme vecteurs propres respectifs

$$\begin{pmatrix} -5 \\ 2 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Vu ce qui précède,

$$\mathbf{x}(t) = C \begin{pmatrix} -5 \\ 2 \end{pmatrix} e^{6t} + D \begin{pmatrix} 1 \\ 1 \end{pmatrix} e^{-t}.$$

Les constantes peuvent être déterminées par les conditions initiales $\mathbf{x}_0$. Ainsi,

$$C \begin{pmatrix} -5 \\ 2 \end{pmatrix} + D \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ 3 \end{pmatrix} \quad \text{ou} \quad \begin{pmatrix} -5 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} C \\ D \end{pmatrix} = \begin{pmatrix} 4 \\ 3 \end{pmatrix}.$$

En inversant cette dernière matrice, on trouve

$$C = -\frac{1}{7} \quad \text{et} \quad D = \frac{23}{7}$$

d'où

$$\mathbf{x}(t) = -\frac{1}{7} \begin{pmatrix} -5 \\ 2 \end{pmatrix} e^{6t} + \frac{23}{7} \begin{pmatrix} 1 \\ 1 \end{pmatrix} e^{-t}.$$

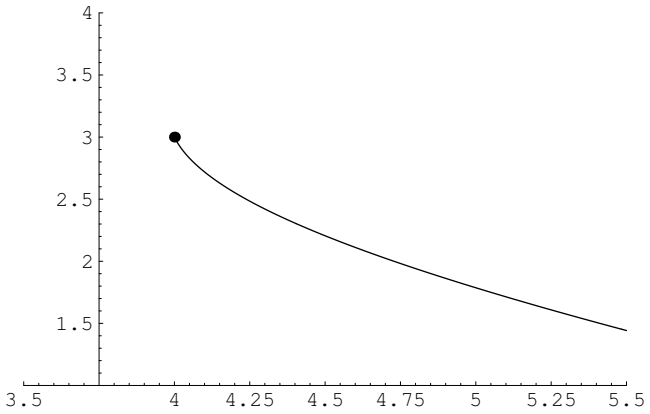


FIGURE XI.1. Mouvement d'une masse en milieu visqueux.

[4]On a choisi une telle situation physique pour obtenir une équation différentielle du premier ordre ne faisant pas intervenir l'accélération.

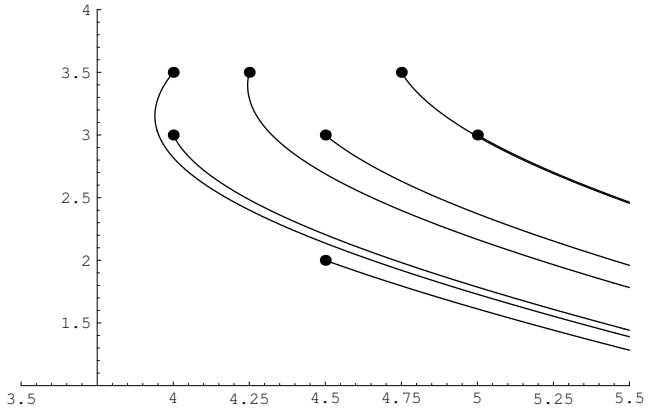


FIGURE XI.2. Mouvement d'une masse en milieu visqueux pour diverses positions intiales $\mathbf{x}_0$.

6. Estimation des valeurs propres

Tout comme la règle de Descartes (cf. théorème VIII.4.1) permet de localiser les zéros d'un polynôme en fonction de ses coefficients, un résultat analogue permet de localiser les valeurs propres d'une matrice de $\mathbb{C}_n^n$ en fonction des éléments de celle-ci.

Définition XI.6.1. Soit $A = (a_{ij}) \in \mathbb{C}_n^n$, le k-ième *disque de Gerschgorin* $\mathcal{D}_k$ de la matrice A, $k \in \{1, \ldots, n\}$, est donné par

$$\mathcal{D}_k = \{z \in \mathbb{C} : |z - a_{kk}| \leq r_k\} \text{ où } r_k = \sum_{\ell \neq k} |a_{k\ell}|.$$

De manière analogue, on peut également privilégier les colonnes de la matrice A et définir

$$\mathcal{E}_k = \{z \in \mathbb{C} : |z - a_{kk}| \leq s_k\} \text{ où } s_k = \sum_{\ell \neq k} |a_{\ell k}|.$$

Théorème XI.6.2. *Les valeurs propres de $A \in \mathbb{C}_n^n$ appartiennent à l'union des disques de Gerschgorin de A. Autrement dit, si λ est une valeur propre de A, alors*

$$\lambda \in \bigcup_{k=1}^{n} \mathcal{D}_k.$$

Démonstration. Soit λ une valeur propre de A et x un vecteur propre non nul de A de valeur propre λ. Puisque tout multiple de x est encore vecteur propre de A, on peut supposer[5] qu'il existe k tel que $|x_k| = 1$ et pour tout $j \neq k$, $|x_j| \leq 1$. Ainsi,

$$\lambda x_k = (\lambda x)_k = (Ax)_k = \sum_{\ell=1}^{n} a_{k\ell}\, x_\ell \quad \text{et} \quad (\lambda - a_{kk})x_k = \sum_{\ell \neq k} a_{k\ell}\, x_\ell.$$

[5]Il suffit de considérer le vecteur $x / \max_{i=1,\ldots,n} |x_i|$. On trouve la notation $||x||_\infty = \max_{i=1,\ldots,n} |x_i|$ (on pourra vérifier qu'il s'agit d'une norme).

Par conséquent,

$$|\lambda - a_{kk}| = \left| \sum_{\ell \neq k} a_{k\ell}\, x_\ell \right| \leq \sum_{\ell \neq k} |a_{k\ell}| = r_k.$$

■

Corollaire XI.6.3. *Si λ est une valeur propre de $A \in \mathbb{C}_n^n$, alors*

$$\lambda \in (\bigcup_{k=1}^{n} \mathcal{D}_k) \cap (\bigcup_{k=1}^{n} \mathcal{E}_k).$$

Démonstration. Puisque A et $\widetilde{A}$ possèdent les mêmes valeurs propres, on peut dans le résultat précédent remplacer $\mathcal{D}_k$ par $\mathcal{E}_k$. En particulier, si λ est valeur propre de A, elle doit appartenir simultanément à

$$\bigcup_{k=1}^{n} \mathcal{D}_k \quad \text{et à} \quad \bigcup_{k=1}^{n} \mathcal{E}_k.$$

■

Remarque XI.6.4. On peut montrer[6] que si l'union $\mathcal{U}$ de t disques de Gerschgorin de A n'intersecte pas l'union des $n - t$ autres disques, alors $\mathcal{U}$ contient exactement t valeurs propres de A comptées avec leur multiplicité.

Exemple XI.6.5. Considérons la matrice

$$A = \begin{pmatrix} 5 & 1 & 1 \\ 0 & 6 & 1 \\ 1 & 2 & -3 \end{pmatrix}.$$

Avec les notations introduites précédemment, on a

$$r_1 = 2,\ r_2 = 1,\ r_3 = 3,$$

$$\mathcal{D}_1 = \{z : |z - 5| \leq 2\},\ \mathcal{D}_2 = \{z : |z - 6| \leq 1\} \ \text{ et } \ \mathcal{D}_3 = \{z : |z + 3| \leq 3\}.$$

Les disques correspondants sont représentés sur la figure XI.3. Un rapide

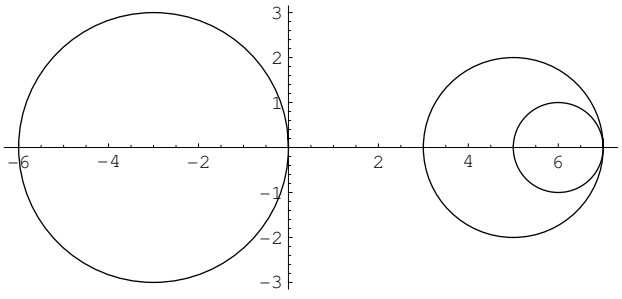


FIGURE XI.3. Disques de Gerschgorin.

[6] voir par exemple, C. D. Meyer, *Matrix Analysis and Applied Linear Algebra*, Siam, Philapeldhia, 2000.

calcul montre en outre que les valeurs propres de A sont

$$5;\ \frac{3-\sqrt{93}}{2} \simeq -3,32 \ \text{ et } \ \frac{3-\sqrt{93}}{2} \simeq 6,32.$$

On aurait pu aussi rechercher les disques

$$\mathcal{E}_1 = \{z : |z-5| \leq 1\},\ \mathcal{E}_2 = \{z : |z-6| \leq 3\} \ \text{ et } \ \mathcal{E}_3 = \{z : |z+3| \leq 2\}.$$

Sur la figure XI.4, on a représenté les deux types de disques (les $\mathcal{E}_k$ étant en gras). Sur cet exemple, on voit que $\mathcal{E}_3$ donne une meilleure approximation de la valeur propre $\frac{3-\sqrt{93}}{2}$ (en effet, le rayon de $\mathcal{E}_3$ est inférieur à celui de $\mathcal{D}_3$), alors que pour les deux autres valeurs propres, $\mathcal{D}_1 \cup \mathcal{D}_2$ donne une meilleure localisation que $\mathcal{E}_1 \cup \mathcal{E}_2$.

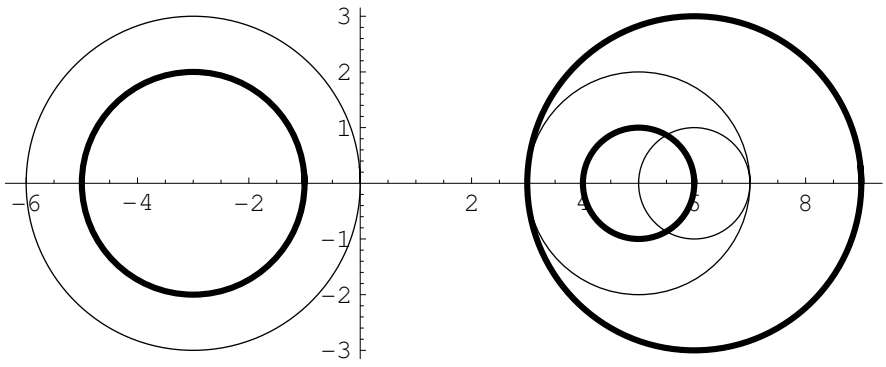


FIGURE XI.4. Disques de Gerschgorin $\mathcal{D}_k$ et $\mathcal{E}_k$.

7. Polynômes d'endomorphismes

Définition XI.7.1. Soit P un polynôme à coefficients complexes,

$$P(z) = a_0 + a_1 z + \cdots + a_m z^m.$$

Soit T un endomorphisme de E. On pose

$$P(T) = a_0\, id + a_1 T + \cdots a_m T^m.$$

Il est clair que $P(T)$ est encore un endomorphisme de E. On dit que $P(T)$ est un *polynôme de l'endomorphisme* T.

Remarque XI.7.2. Si $P, Q \in \mathbb{C}[z]$, $\lambda, \mu \in \mathbb{C}$,

$$(\lambda P + \mu Q)(T) = \lambda P(T) + \mu Q(T)$$

et

$$P(T) \circ Q(T) = (PQ)(T).$$

En effet, les deux membres sont des combinaisons linéaires de puissances de T. Les coefficients sont égaux par définition de la combinaison linéaire et du produit de polynômes. Ainsi, tout identité entre polynôme d'une variable reste valable pour les polynômes d'endomorphismes correspondants. En particulier, les endomorphismes $P(T)$ et $Q(T)$ commutent.

Proposition XI.7.3. *Soient $P \in \mathbb{C}[z]$ et $T \in \mathcal{L}(E)$ un endomorphisme dont les valeurs propres répétées selon leur multiplicité (algébrique) sont $\lambda_1, \ldots, \lambda_n$. On a*

$$\det P(T) = \prod_{j=1}^{n} P(\lambda_j).$$

En particulier, l'endomorphisme $P(T)$ est inversible si et seulement si aucune valeur propre de T n'est un zéro de P.

Démonstration. Au vu du théorème fondamental de l'algèbre, si P est un polynôme de degré m ayant $z_1, \ldots, z_m$ comme zéros (répétés selon leur multiplicité), alors

$$P(z) = \alpha \prod_{i=1}^{m} (z - z_i).$$

Dès lors,

$$P(T) = \alpha\,(T - z_1\,id) \circ \cdots \circ (T - z_m\,id)$$

et[7]

$$\det P(T) = \alpha^n \prod_{i=1}^{m} \det(T - z_i\,id).$$

Par définition des valeurs propres[8] de T, on a

$$\det(T - z_i\,id) = \prod_{j=1}^{n} (\lambda_j - z_i).$$

Donc

$$\det P(T) = \alpha^n \prod_{i=1}^{m} \prod_{j=1}^{n} (\lambda_j - z_i) = \prod_{j=1}^{n} \underbrace{\alpha \prod_{i=1}^{m} (\lambda_j - z_i)}_{P(\lambda_j)}.$$

■

Corollaire XI.7.4. *Soient $P \in \mathbb{C}[z]$ et $T \in \mathcal{L}(E)$ un endomorphisme ayant $\lambda_1, \ldots, \lambda_p$ comme valeurs propres distinctes.*

- $\mathrm{sp}(P(T)) = P(\mathrm{sp}(T)) = \{P(\lambda_1), \ldots, P(\lambda_p)\}$.
- *La multiplicité (algébrique) d'une valeur propre λ de $P(T)$ est égale à la somme des multiplicités des valeurs propres λ_j de T telles que $P(\lambda_j) = \lambda$.*
- *Tout vecteur propre de valeur propre λ_j de T est vecteur propre de $P(T)$ de valeur propre $P(\lambda_j)$,*

$$E_{\lambda_j}(T) \subset E_{P(\lambda_j)}(P(T)).$$

[7] Pensez que $P(T)$ est un endomorphisme. Il peut donc être représenté dans une base U de E. Si T est représenté par A, alors $P(T)$ est représenté par $P(A) = \alpha(A - z_1 I) \cdots (A - z_m I)$ et par définition, $\det(P(T)) = \det(P(A))$. Enfin, il suffit de remarquer que pour une matrice $M \in \mathbb{C}_n^n$, $\det(\alpha M) = \alpha^n \det M$.

[8] Si λ est valeur propre de T, $\lambda - z_i$ est valeur propre de $T - z_i\,id$. En effet, si $x \neq 0$ est tel que $Tx = \lambda x$, alors $(T - z_i\,id)x = (\lambda - z_i)x$. De plus, $\det(T - z_i\,id)$ est égal au produit des valeurs propres de $T - z_i\,id$ en vertu de la proposition XI.3.11.

- *La dimension de l'espace propre associé à une valeur propre λ de $P(T)$ est au moins égale à la somme des dimensions des espaces propres associés aux valeurs propres λ_j de T telles que $P(\lambda_j) = \lambda$,*

$$\sum_{j:P(\lambda_j)=\lambda} \dim E_{\lambda_j}(T) \leq \dim E_\lambda(P(T)).$$

- *Si T est diagonalisable, alors $P(T)$ l'est aussi.*

Démonstration. Si $\mu_1, \ldots, \mu_p$ sont les multiplicités algébriques des valeurs propres $\lambda_1, \ldots, \lambda_p$ de T, au vu de la proposition précédente, on a

$$\det(P(T) - \lambda\, id) = \det((P-\lambda)(T)) = \prod_{j=1}^{p}((P-\lambda)(\lambda_j))^{\mu_j} = \prod_{j=1}^{p}(P(\lambda_j)-\lambda)^{\mu_j}.$$

Ainsi, λ est valeur propre de $P(T)$ si et seulement si il existe $j \in \{1, \ldots, p\}$ tel que $P(\lambda_j) = \lambda$. De cette constatation découle les deux premiers points.

Etablissons le troisième point. Soit $x \in E_{\lambda_j}(T)$. Cela signifie que $Tx = \lambda_j x$ et donc $T^k x = \lambda_j^k x$ pour tout $k \in \mathbb{N}$. Par linéarité, on a donc bien $P(T)x = P(\lambda_j)x$.

Les deux derniers points découlent du fait que les sous-espaces propres E_{λ_j} sont en somme directe. En effet, si $\lambda_{j_1}, \ldots, \lambda_{j_k}$ sont les valeurs propres de T telles que $P(\lambda_{j_1}) = \cdots = P(\lambda_{j_k}) = \lambda$, alors par le point précédent,

$$E_{\lambda_{j_i}}(T) \subset E_\lambda(P(T)),\ \forall i = 1, \ldots, k.$$

Puisque nous sommes en présence de sous-espaces vectoriels, il est clair que

$$E_{\lambda_{j_1}}(T) \oplus \cdots \oplus E_{\lambda_{j_k}}(T) \subset E_\lambda(P(T)).$$

Par conséquent,

$$\dim(\bigoplus_{i=1}^{k} E_{\lambda_{j_i}}(T)) = \sum_{i=1}^{k} \dim E_{\lambda_{j_i}}(T) \leq \dim E_\lambda(P(T)).$$

Pour le dernier point, si T est diagonalisable, alors $E = \bigoplus_{j=1}^{p} E_{\lambda_j}(T)$. Notons[9] $\mu_1, \ldots, \mu_r$ les valeurs propres distinctes de $P(T)$. Par le point précédent, on a alors

$$\dim E = \sum_{j=1}^{p} \dim E_{\lambda_j}(T) \leq \sum_{j=1}^{r} \dim E_{\mu_j}(P(T)) \leq \dim E$$

où la dernière inégalité provient du fait que $E_{\mu_1}(P(T)) + \cdots + E_{\mu_r}(P(T)) \subset E$. On en conclut donc que $E = \bigoplus_{j=1}^{r} E_{\mu_j}(P(T))$ et $P(T)$ est bien diagonalisable.

■

A titre d'exercice sur les polynômes d'endomorphismes, on peut démontrer la proposition suivante.

Se rappeler le théorème de Bezout.

[9] $\mathrm{sp}(P(T)) = \{\mu_1, \ldots, \mu_r\} = \{P(\lambda_1), \ldots, P(\lambda_p)\}$, $r \leq p$.

Remarque XI.7.5. Soit $T \in L(E)$. Si $P, Q \in \mathbb{C}[z]$ sont deux polynômes premiers entre eux, alors

$$\ker\left(PQ(T)\right) = \ker P(T) \oplus \ker Q(T).$$

8. Polynôme minimum d'un endomorphisme

Théorème XI.8.1 (Cayley-Hamilton). *Soit $T \in \mathcal{L}(E)$ un endomorphisme ayant χ_T pour polynôme caractéristique. On a*

$$\chi_T(T) = 0.$$

Autrement dit, tout endomorphisme annule son polynôme caractéristique.

Démonstration. On procède par récurrence sur $n = \dim E$. Le cas $n = 1$ est immédiat[10]. Supposons le résultat vérifié pour $n-1$ et démontrons-le pour n. Soit λ une valeur propre de T. Si e_1 est un vecteur propre non nul de valeur propre λ, on considère alors une base $e_1, e_2, \ldots, e_n$ de E. Dans cette base, T se représente alors par une matrice A de la forme

$$A = \begin{pmatrix} \lambda & * \\ 0 & B \end{pmatrix}$$

où B est une matrice $(n-1) \times (n-1)$. Le polynôme caractéristique $\chi_T(\mu)$ de T est égal à $\det(T - \mu\, id) = \det(A - \mu I)$ et donc

$$\chi_T(\mu) = (\lambda - \mu)\det(B - \mu I) = (\lambda - \mu)\, Q(\mu)$$

où Q est le polynôme caractéristique d'un endomorphisme défini sur un espace vectoriel de dimension $n-1$ et représenté par B. Par conséquent[11],

$$\chi_T(A) = (\lambda I - A)\, Q(A) = \begin{pmatrix} 0 & * \\ 0 & \lambda I - B \end{pmatrix} \begin{pmatrix} Q(\lambda) & * \\ 0 & Q(B) \end{pmatrix}.$$

Par hypothèse de récurrence, $Q(B) = 0$ et donc $\chi_T(A) = 0$. Puisque $\chi_T(A)$ représente l'endomorphisme $\chi_T(T)$ dans la base $e_1, \ldots, e_n$, cela signifie que $\chi_T(T) = 0$.

■

Remarque XI.8.2. Pour le cas matriciel, on en déduit que toute matrice de $\mathbb{C}_n^n$ annule son polynôme caractéristique.

[10] Dans un espace vectoriel de dimension 1, un endomorphisme est toujours de la forme $T = \alpha\, id$. Ainsi, $\chi_T(\mu) = \alpha - \mu$ et $\chi_T(T) = \alpha\, id - T = 0$.

[11] On trouve la forme particulière de $Q(A)$ à cause de la forme particulière de A. En effet, il est facile de voir que

$$A^n = \begin{pmatrix} \lambda^n & * \\ 0 & B^n \end{pmatrix}.$$

Exemple XI.8.3. Soit la matrice

$$A = \begin{pmatrix} 1 & 2 & 3 & 1 \\ 2 & 0 & 0 & 1 \\ 1 & -1 & -2 & 0 \\ 4 & 1 & 0 & -1 \end{pmatrix}.$$

Le polynôme caractéristique de A est donné par

$$\det(A - \lambda I) = -5 - 30\lambda - 13\lambda^2 + 2\lambda^3 + \lambda^4$$

et on peut vérifier que

$$-5I - 30A - 13A^2 + 2A^3 + A^4 = 0.$$

Corollaire XI.8.4. *Soit $T \in \mathcal{L}(E)$. L'ensemble*

$$I = \{P \in \mathbb{C}[z] \mid P(T) = 0\}$$

On appelle cet ensemble l'*idéal annulateur* de T.

est un idéal propre de $\mathbb{C}[z]$.

Démonstration. Il est clair qu'il s'agit d'un idéal contenant au moins un polynôme non nul, à savoir le polynôme caractéristique de T. Il est propre car $1 \notin I$ et donc $I \neq \mathbb{C}[z]$.

■

Définition XI.8.5. Puisque $I = \{P \in \mathbb{C}[z] \mid P(T) = 0\}$ est un idéal propre d'un anneau principal[12], il existe un polynôme monique[13] $\mathcal{M}_T$ tel que $I = \langle \mathcal{M}_T \rangle$. On l'appelle le *polynôme minimum* de T.

Remarque XI.8.6. Il est clair que le polynôme minimum de T divise tout polynôme appartenant à I et donc en particulier, il divise le polynôme caractéristique de T.

Exemple XI.8.7. Lorsqu'on aura à sa disposition des outils plus puissants, on pourra vérifier (cf. exemple XI.14.4) que la matrice

$$A = \begin{pmatrix} 5 & -1 & -3 & 2 & -5 \\ 0 & 2 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & -2 \\ 0 & -1 & 0 & 3 & 1 \\ 1 & -1 & -1 & 1 & 1 \end{pmatrix}$$

a $-(\lambda - 2)^3(\lambda - 3)^2$ pour polynôme caractéristique et $-(\lambda - 2)^{\mathbf{2}}(\lambda - 3)^2$ pour polynôme minimum. A ce stade, on peut se borner à vérifier que $(A - 2I)^2(A - 3I)^2 = 0$. (Nous ne sommes pas encore en mesure de prouver aisément qu'il n'y a pas un polynôme de degré inférieur annulé par A.)

Proposition XI.8.8. *Soit $T \in \mathcal{L}(E)$. Le polynôme caractéristique de T et le polynôme minimum de T ont les mêmes zéros.*

[12] Nous savons que $\mathbb{C}[z]$ est principal.

[13] i.e., de coefficient principal égal à 1.

Démonstration. Soit χ_T (resp. $\mathcal{M}_T$) le polynôme caractéristique (resp. minimum) de T. Soit λ un zéro de χ_T. En particulier, λ est valeur propre de T et il existe $x \in E \setminus \{0\}$ tel que $Tx = \lambda x$. Par conséquent[14],

$$\underbrace{\mathcal{M}_T(T)}_{=0} x = \mathcal{M}_T(\lambda)\, x$$

et puisque x est non nul, on en déduit que $\mathcal{M}_T(\lambda) = 0$.

■

Remarque XI.8.9. Nous savons à présent que les valeurs propres distinctes $\lambda_1, \ldots, \lambda_p$ de T sont exactement les zéros de son polynôme minimum. Si

$$\det(T - \lambda I) = (-1)^n \prod_{j=1}^{p} (\lambda - \lambda_j)^{\mu_j} = \prod_{j=1}^{p} (\lambda_j - \lambda)^{\mu_j}$$

$$\mathcal{M}_T(\lambda) = \prod_{j=1}^{p} (\lambda - \lambda_j)^{m_j},$$

alors $1 \leq m_j \leq \mu_j$.

En particulier, si toutes les valeurs propres de T sont simples, le polynôme minimum de T coïncide avec son polynôme caractéristique.

9. Sous-espaces caractéristiques

Définition XI.9.1. Soit $T \in \mathcal{L}(E)$. Un sous-espace vectoriel F de E est *stable* si

$$T(F) \subset F.$$

Par exemple, les espaces propres de T sont stables pour T. En effet, $x \in E_\lambda$ si et seulement si $(T - \lambda\, id)x = 0$. Ainsi, si $x \in E_\lambda$, alors le vecteur Tx appartient encore à E_λ car $(T - \lambda\, id)Tx = T(T - \lambda\, id)x = 0$.

Soient $\lambda_1, \ldots, \lambda_p$ les valeurs propres distinctes de $T \in \mathcal{L}(E)$. Nous savons déjà qu'en général la somme des sous-espaces propres E_{λ_j} n'est pas E tout entier (en fait, la somme diffère de E, lorsque T n'est pas diagonalisable). Nous verrons à la fin de la section suivante qu'il existe d'autres sous-espaces vectoriels stables pour T et dont la somme est toujours E. Ces espaces seront appelés *sous-espaces caractéristiques*. Rappelons que notre but ultime est de représenter un endomorphisme T de la manière la plus simple possible. Nous pouvons déjà préciser que la base choisie pour représenter T sera construite sur des bases particulières de ces fameux sous-espaces caractéristiques. Avant d'arriver à ce théorème de réduction, plusieurs étapes sont encore nécessaires.

Pour définir les sous-espaces caractéristiques, on introduit au préalable les opérateurs

$$\boxed{T_j = T - \lambda_j\, id, \quad j = 1, \ldots, p.}$$

[14] On utilise le même raisonnement qu'à la fin de la preuve du corollaire XI.7.4.

Puisqu'il s'agit de polynômes de T, ils commutent entre eux et avec T.

Théorème XI.9.2 (Stabilisation des images et des noyaux). *Soit m_j, la multiplicité de λ_j comme zéro du polynôme minimum de T. On a*

$$\ker(T_j^0) \subsetneq \ker(T_j) \subsetneq \ker(T_j^2) \subsetneq \cdots \subsetneq \ker(T_j^{m_j}) = \ker(T_j^{m_j+1}) = \ker(T_j^{m_j+2}) = \cdots$$

et

$$\mathrm{Im}(T_j^0) \supsetneq \mathrm{Im}(T_j) \supsetneq \mathrm{Im}(T_j^2) \supsetneq \cdots \supsetneq \mathrm{Im}(T_j^{m_j}) = \mathrm{Im}(T_j^{m_j+1}) = \mathrm{Im}(T_j^{m_j+2}) = \cdots .$$

De plus,

$$E = \ker(T_j^{m_j}) \oplus \mathrm{Im}(T_j^{m_j}).$$

Démonstration. Si $x \in E$ est tel que $T_j^k x = 0$, alors $T_j^{k+1} x = 0$ et donc

$$\ker(T_j^k) \subset \ker(T_j^{k+1}), \quad \forall k > 0.$$

Montrons que si k est tel que $\ker(T_j^k) = \ker(T_j^{k+1})$, alors on a aussi

$$\ker(T_j^{k+1}) = \ker(T_j^{k+2}). \tag{11}$$

Il suffit de montrer que $\ker(T_j^{k+1}) \supset \ker(T_j^{k+2})$. Soit $x \in E$ tel que $T_j^{k+2} x = 0$. Dès lors, $T_j x$ appartient à $\ker(T_j^{k+1}) = \ker(T_j^k)$ et donc x appartient à $\ker(T_j^{k+1})$. Ceci montre donc que si on a stabilisation des noyaux pour une valeur k, la suite devient stationnaire à partir de k.

De plus, on a

$$\ker(T_j^{m_j-1}) \neq \ker(T_j^{m_j}).$$

Pour le montrer, il suffit de trouver un élément appartenant à $\ker(T_j^{m_j})$ mais pas à $\ker(T_j^{m_j-1})$. L'opérateur

$$S_j = T_1^{m_1} \cdots T_j^{m_j-1} \cdots T_p^{m_p}$$

n'est pas nul (car $\mathcal{M}_T = T_1^{m_1} \cdots T_j^{m_j} \cdots T_p^{m_p}$ est le polynôme minimum de T). Soit x tel que $S_j x \neq 0$. Le vecteur

$$y = T_1^{m_1} \cdots \widehat{[j]} \cdots T_p^{m_p} x$$

est annulé par $T_j^{m_j}$ mais pas par $T_j^{m_j-1}$. En particulier, cela montre que $\ker(T_j^{k-1}) \neq \ker(T_j^k)$ pour tout $k \leq m_j$ car sinon, au vu de (11), on aurait $\ker(T_j^{m_j-1}) = \ker(T_j^{m_j})$, ce qui est impossible.

On a aussi

$$\ker(T_j^{m_j}) = \ker(T_j^{m_j+1}).$$

Il suffit une fois encore de montrer que $\ker(T_j^{m_j}) \supset \ker(T_j^{m_j+1})$. Soit x tel que $T_j^{m_j+1} x = 0$. Ainsi,

$$(T - \lambda_j\, id) T_j^{m_j} x = 0$$

ce qui signifie que $T_j^{m_j} x$ est un vecteur propre de T de valeur propre λ_j. De là,

$$T_k(T_j^{m_j} x) = (T - \lambda_k\, id)(T_j^{m_j} x) = (\lambda_j - \lambda_k) T_j^{m_j} x, \quad \forall k \in \{1, \ldots, p\}.$$

Par conséquent,

$$\underbrace{T_1^{m_1}\cdots T_j^{m_j}\cdots T_p^{m_p}}_{=0}x = (\lambda_j-\lambda_1)^{m_1}\cdots\widehat{[j]}\cdots(\lambda_j-\lambda_p)^{m_p}T_j^{m_j}x,$$

l'égalité à zéro résultant de la définition même du polynôme minimum. Or puisque les valeurs propres sont distinctes, on en déduit que $T_j^{m_j}x = 0$.

On a $\mathrm{Im}(T_j^k) \supset \mathrm{Im}(T_j^{k+1})$ pour tout $k \geq 0$ car si $x = T_j^{k+1}y$, on a aussi $x = T_j^k(T_j y)$. La deuxième partie de la preuve résulte du théorème de la dimension (théorème X.2.7),

$$\dim(\mathrm{Im}(T_j^k)) = n - \dim(\ker(T_j^k)).$$

Il nous reste à montrer que

$$E = \ker(T_j^{m_j}) \oplus \mathrm{Im}(T_j^{m_j}).$$

Pour ce faire, il suffit de vérifier que $\ker(T_j^{m_j}) \cap \mathrm{Im}(T_j^{m_j}) = \{0\}$ car nous savons déjà que $\ker(T_j^{m_j}) + \mathrm{Im}(T_j^{m_j}) \subset E$ et vu le théorème de la dimension, on a aussi que $\dim(\mathrm{Im}(T_j^{m_j})) + \dim(\ker(T_j^{m_j})) = \dim E$ (ce qui suffit alors pour conclure que $E = \ker(T_j^{m_j}) + \mathrm{Im}(T_j^{m_j})$). Si x appartient à $\ker(T_j^{m_j}) \cap \mathrm{Im}(T_j^{m_j})$, alors il existe y tel que

$$x = T_j^{m_j}y \quad \text{et} \quad T_j^{m_j}x = 0.$$

De là, $T_j^{2m_j}y = 0$ et y appartient à $\ker(T_j^{2m_j}) = \ker(T_j^{m_j})$. On en conclut que x est nul.

■

Définition XI.9.3. Soit $T \in \mathcal{L}(E)$. On appelle *sous-espace caractéristique*[15] associé à la valeur propre λ_j de T, le sous-espace vectoriel

$$F_{\lambda_j} = F_{\lambda_j}(T) = \ker(T_j^{m_j})$$

où m_j est la multiplicité de λ_j comme zéro du polynôme minimum de T. Au vu de la remarque XI.8.9 et du théorème précédent, on a que $F_{\lambda_j} = \ker(T_j^k)$ pour tout $k \geq m_j$ et en particulier, pour k égal à la multiplicité algébrique de T.

Remarque XI.9.4. Les sous-espaces caractéristiques sont stables pour T. En effet, x appartient à F_{λ_j} si et seulement si $T_j^{m_j}x = 0$. De là, Tx appartient encore à F_{λ_j} car

$$T_j^{m_j}Tx = TT_j^{m_j}x = 0$$

et rappelons que $T_j^{m_j}$ et T commutent.

Le lecteur pourrait à ce stade s'interroger sur l'importance d'avoir des sous-espaces stables pour T. La raison provient une fois encore de notre désir de représenter T de manière simple. En effet, si $E = G_1 \oplus \cdots \oplus G_t$ et si les sous-espaces vectoriels G_i sont stables pour T, alors la représentation

[15] Certains auteurs utilisent parfois le terme *sous-espace principal*.

de T dans une base $g_{1,1},\dots,g_{1,d_1},\dots,g_{t,1},\dots,g_{t,d_t}$ où $g_{i,j}\in G_i$ pour tout i, sera une matrice composée diagonale

$$\operatorname{diag}(A_1,\dots,A_t) \quad \text{avec } A_i\in\mathbb{C}^{d_i}_{d_i}.$$

Exemple XI.9.5. Soient une base $U=(u_1,u_2,u_3,u_4)$ de $\mathbb{C}^4$, $G_1=\rangle u_1,u_2\langle$, $G_2=\rangle u_3,u_4\langle$ et $T:\mathbb{C}^4\to\mathbb{C}^4$ un endomorphisme tel que $Tu_1=u_2$, $Tu_2=u_1+u_2$, $Tu_3=0$ et $Tu_4=u_3$. Il est clair que $TG_1\subset G_1$ et $TG_2\subset G_2$ et la représentation de T dans la base U est

$$\left(\begin{array}{cc|cc} 0&1&0&0\\ 1&1&0&0\\ \hline 0&0&0&1\\ 0&0&0&0 \end{array}\right)$$

qui est bien une matrice composée diagonale.

Remarque XI.9.6. Veillez à ne pas confondre les sous-espaces propres et caractéristiques. On a

$$E_{\lambda_j}=\ker(T_j) \quad \text{et} \quad F_{\lambda_j}=\ker(T_j^{m_j})$$

et en particulier, au vu du théorème précédent, $E_{\lambda_j}\subset F_{\lambda_j}$, l'inclusion étant stricte si et seulement si $m_j>1$.

10. Projecteurs spectraux

On emploie les mêmes notations qu'à la section précédente : les valeurs propres de T sont $\lambda_1,\dots,\lambda_p$, leur multiplicité comme zéro du polynôme caractéristique (resp. minimum) de T sont $\mu_1,\dots,\mu_p$ (resp. $m_1,\dots,m_p$).

Les projecteurs que nous allons présenter ici sont en relation directe avec les sous-espaces caractéristiques qui viennent d'être introduits à la section précédente. En particulier, c'est grâce aux projecteurs spectraux que nous allons pouvoir montrer que E se décompose en somme directe des sous-espaces caractéristiques de T.

Soit $\mathcal{M}_T(\lambda)$, le polynôme minimum de $T\in\mathcal{L}(E)$. Si on décompose $1/\mathcal{M}_T(\lambda)$ en fractions rationnelles propres (cf. corollaire VIII.7.2), on a

$$\frac{1}{\mathcal{M}_T(\lambda)}=\sum_{j=1}^{p}\frac{A_j(\lambda)}{(\lambda-\lambda_j)^{m_j}}, \quad \text{avec } \deg A_j<m_j.$$

En réduisant au même dénominateur, on a

$$1=\sum_{j=1}^{p}A_j(\lambda)\,(\lambda-\lambda_1)^{m_1}\cdots\widehat{[j]}\cdots(\lambda-\lambda_p)^{m_p}$$

sur $\mathbb{C}\setminus\{\lambda_1,\dots,\lambda_p\}$ et donc sur $\mathbb{C}$. Cette identité reste valable si on remplace λ par T et donc,

$$id=\sum_{j=1}^{p}\underbrace{A_j(T)\,T_1^{m_1}\cdots\widehat{[j]}\cdots T_p^{m_p}}_{:=P_j}.$$

Définition XI.10.1. On pose

$$\boxed{P_j = A_j(T)\, T_1^{m_1} \cdots \widehat{[j]} \cdots T_p^{m_p}.}$$

On appelle $P_1, \ldots, P_p$, les *projecteurs spectraux* de T.

Proposition XI.10.2. *Les applications $P_1, \ldots, P_p$ forment un système de projecteurs.*

Démonstration. Voir le point X.5.6 pour la définition d'un système de projecteurs. Il est clair que $id = \sum_{j=1}^{p} P_j$. De plus, $P_j P_k = 0$ si $j \neq k$. En effet,

$$P_j P_k = A_j(T) A_k(T)\, T_1^{m_1} \cdots \widehat{[j]} \cdots T_p^{m_p} T_1^{m_1} \cdots \widehat{[k]} \cdots T_p^{m_p}$$

fait donc apparaître le polynôme minimum de T. Enfin, $P_j^2 = P_j$ car

$$P_j\, id = P_j \sum_{k=1}^{p} P_k = P_j^2.$$

■

La proposition suivante précise le lien entre les projecteurs spectraux et les sous-espaces caractéristiques.

Proposition XI.10.3. *On a*

$$\ker(P_j) = \mathrm{Im}(T_j^{m_j}) \quad \textit{et} \quad \mathrm{Im}(P_j) = \ker(T_j^{m_j}) = F_{\lambda_j}.$$

Démonstration. Si x appartient à $\ker(P_j)$, on a

$$x = id\, x = \sum_{k=1}^{p} P_k\, x = \sum_{k \neq j} P_k\, x = T_j^{m_j} \sum_{k \neq j} A_k(T) T_1^{m_1} \cdots \widehat{[j]} \cdots \widehat{[k]} \cdots T_p^{m_p} x$$

et donc $x \in \mathrm{Im}(T_j^{m_j})$. Réciproquement, si $x \in \mathrm{Im}(T_j^{m_j})$, il existe y tel que $T_j^{m_j} y = x$. On a

$$P_j x = P_j T_j^{m_j} y = A_j(T) \mathcal{M}_T(T) y = 0$$

et donc $\ker(P_j) = \mathrm{Im}(T_j^{m_j})$.

Pour l'autre égalité, $T_j^{m_j} P_j = A_j(T) \mathcal{M}_T(T) = 0$ et donc $\mathrm{Im}(P_j)$ est inclus dans $\ker(T_j^{m_j})$. Réciproquement, si $x \in \ker(T_j^{m_j})$, alors $P_k\, x = 0$ si $k \neq j$. Par conséquent, on a $x = id\, x = P_j\, x \in \mathrm{Im}(P_j)$. Ceci conclut la preuve.

Vu la définition de P_k.

■

Théorème XI.10.4. *La dimension du sous-espace caractéristique de T associé à la valeur propre λ_j est égale à la multiplicité de λ_j comme zéro du polynôme caractéristique de T,*

$$\dim F_{\lambda_j} = \mu_j.$$

On a

$$\boxed{E = F_{\lambda_1} \oplus \cdots \oplus F_{\lambda_p}}$$

et les projecteurs associés à cette décomposition sont les projecteurs spectraux de T.

Démonstration. Soit le polynôme P défini par $P(z) = (z - \lambda_j)^{m_j}$. On peut alors considérer $T_j^{m_j}$ comme un polynôme d'endomorphisme,

$$P(T) = (T - \lambda_j\, id)^{m_j} = T_j^{m_j}$$

et tirer parti du corollaire XI.7.4. Il est clair que

$$E_0(T_j^{m_j}) = \{x \mid T_j^{m_j} x = 0\} = \ker T_j^{m_j} = F_{\lambda_j}.$$

Par le deuxième point du corollaire XI.7.4, la multiplicité[16] de 0 comme valeur propre de $T_j^{m_j} = P(T)$ est égale à la somme des multiplicités des valeurs propres β de T telles que $P(\beta) = (\beta - \lambda_j)^{m_j} = 0$, c'est-à-dire μ_j car $\lambda_1, \ldots, \lambda_p$ sont distincts (et donc, la seule façon d'avoir l'égalité à zéro, c'est d'avoir $\beta = \lambda_j$).

Rappelons que si x est un vecteur propre de $T_j^{m_j}$ de valeur propre 0, alors $T_j^{m_j} x = 0$. Autrement dit, $F_{\lambda_j} = \ker(T_j^{m_j}) = E_0(T_j^{m_j})$. On sait que la dimension d'un sous-espace propre est inférieure ou égale à la multiplicité algébrique de la valeur propre correspondante, ainsi

$$\dim F_{\lambda_j} \leq \mu_j.$$

Les applications $P_1, \ldots, P_p$ forment un système de projecteurs, ce qui signifie que $E = \mathrm{Im}(P_1) \oplus \cdots \oplus \mathrm{Im}(P_p)$ (cf. proposition X.5.7). Dès lors, au vu de la proposition précédente,

$$n = \sum_{j=1}^{p} \dim(\mathrm{Im}(P_j)) = \sum_{j=1}^{p} \dim(F_{\lambda_j}) \leq \sum_{j=1}^{p} \mu_j = n.$$

Par conséquent, $\dim(F_{\lambda_j}) = \mu_j$ pour tout $j \in \{1, \ldots, p\}$.

La deuxième partie découle directement de la proposition X.5.7.

■

Corollaire XI.10.5. *Un endomorphisme T est diagonalisable si et seulement si son polynôme minimum ne possède que des zéros simples.*

Démonstration. Nous savons (cf. corollaire XI.4.4) que T est diagonalisable si et seulement si, pour tout $j \in \{1, \ldots, p\}$, $\dim E_{\lambda_j} = \mu_j$. De plus, au vu de la remarque XI.9.6, $E_{\lambda_j} \subset F_{\lambda_j}$ et par le théorème précédent, $\dim F_{\lambda_j} = \mu_j$. Par conséquent, T est diagonalisable si et seulement si

$$E_{\lambda_j} = F_{\lambda_j}.$$

Ceci a lieu si et seulement si $m_j = 1$ pour tout $j \in \{1, \ldots, p\}$ (cf. remarque XI.9.6).

■

[16] sous-entendu multiplicité algébrique.

Remarque XI.10.6. Soit $T \in \mathcal{L}(E)$. Il existe une base de E dans laquelle T se représente par une matrice composée diagonale

$$B = \operatorname{diag}(B_1, \dots, B_p), \quad B_i \in \mathbb{C}^{\mu_i}_{\mu_i}.$$

Il suffit de considérer comme base de E, une base construite sur des vecteurs

$$\underbrace{x_1, \dots, x_{\mu_1}}_{\text{base de } F_{\lambda_1}}, \underbrace{x_{\mu_1+1}, \dots, x_{\mu_1+\mu_2}}_{\text{base de } F_{\lambda_2}}, \dots, \underbrace{x_{n-\mu_p+1}, \dots, x_n}_{\text{base de } F_{\lambda_p}}$$

d'où la conclusion car les sous-espaces caractéristiques sont stables pour T (cf. remarque XI.9.4).

De plus, on a

$$\det(B_j - \lambda I) = (\lambda_j - \lambda)^{\mu_j}.$$

En effet, la matrice B_j représente la restriction de T à F_{λ_j}. Elle ne peut donc pas avoir d'autre valeur propre que λ_j car les sous-espaces caractéristiques sont en somme directe.

11. Endomorphismes nilpotents

Les endomorphismes nilpotents sont fondamentaux dans l'étude de la réduction des endomorphismes à la forme de Jordan. En effet, l'étude de ces endomorphismes particuliers permet de mieux appréhender le cas des endomorphismes non diagonalisables.

Définition XI.11.1. Un endomorphisme $N \in \mathcal{L}(E)$ est *nilpotent*[17] s'il existe un entier positif k tel que $N^k = 0$. Le plus petit entier k vérifiant cette égalité est appelé l'*indice de nilpotence*.

Exemple XI.11.2. Soit la matrice N donnée par

$$N = \begin{pmatrix} 0 & 1 & 2 & 1 \\ 0 & 0 & -2 & 3 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Ses puissances sont

$$N^2 = \begin{pmatrix} 0 & 0 & -2 & 11 \\ 0 & 0 & 0 & -8 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \; N^3 = \begin{pmatrix} 0 & 0 & 0 & -8 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ et } N^4 = 0.$$

Il s'agit donc d'un endomorphisme nilpotent de $\mathbb{C}^4$.

Proposition XI.11.3. *Soit N un endomorphisme nilpotent.*

- *Son indice de nilpotence est toujours inférieur ou égal à la dimension de E.*
- *N n'est pas inversible.*
- *Son spectre est réduit à $\{0\}$.*

[17] En latin, *nihil, nil* : rien et *potentia,æ* : puissance.

Démonstration. Soit k le plus grand entier tel que $N^{k-1} \neq 0$. Il existe donc $x \in E$ tel que $N^{k-1}x \neq 0$. Les vecteurs

$$x, Nx, \ldots, N^{k-1}x$$

sont linéairement indépendants et de là, $k \leq \dim E$. En effet, supposons que

$$\sum_{i=0}^{k-1} \alpha_i N^i x = 0,$$

avec les $\alpha_i \in \mathbb{C}$ non tous nuls. Soit j le plus petit entier tel que $\alpha_j \neq 0$.

De là,

$$N^{k-j-1}\left(\sum_{i=j}^{k-1} \alpha_i N^i x\right) = \sum_{i=j}^{k-1} \alpha_i N^{k+i-(j+1)} x = 0.$$

Or $N^{k+i-(j+1)} = 0$ dès que $i > j$. La somme se réduit donc à

$$\alpha_j \underbrace{N^{k-1}x}_{\neq 0} = 0$$

et on en conclut que $\alpha_j = 0$ ce qui est absurde.

Passons au deuxième point. Si N était inversible, on aurait

$$N^{k-1} = N^{-1} \circ N^k = N^{-1} \circ 0 = 0$$

ce qui contredit la définition de k.

Enfin, pour le dernier point, $N^k = 0$ et donc N^k n'a que zéro comme valeur propre. En conséquence du corollaire XI.7.4, si λ est valeur propre de N, alors λ^k est valeur propre de N^k. On en tire que $\lambda = 0$.

■

Proposition XI.11.4. *Si S et N sont deux endomorphismes nilpotents qui commutent, alors $S + N$ et SN sont aussi nilpotents.*

Démonstration. Soit ℓ un entier[18] tel que $S^\ell = N^\ell = 0$. Puisque S et N commutent, on trouve

$$(S + N)^{2\ell} = 0 \quad \text{et } (SN)^\ell = 0.$$

■

Proposition XI.11.5. *Un endomorphisme nilpotent N non nul n'est jamais diagonalisable.*

Démonstration. Si N est diagonalisable, 0 est racine simple du polynôme minimum de N (cf. corollaire XI.10.5). De là, $N = 0$.

■

Proposition XI.11.6. *Si E est de dimension n et si N est un endomorphisme nilpotent d'indice de nilpotence n, alors il existe une base $e_1, \ldots, e_n$ de E telle que*

Sans le dire, on introduit la notion de chaîne.

[18] Il suffit de prendre pour ℓ le plus grand des deux indices de nilpotence.

$$Ne_1 = 0 \quad et \quad Ne_j = e_{j-1},\ j \in \{2, \dots, n\}.$$

Autrement dit, N est représenté dans cette base par la matrice

$$J(n) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix}$$

Démonstration. Soit x un vecteur tel que $N^{n-1}x \neq 0$. Les vecteurs

$$N^{n-1}x, N^{n-2}x, \dots, Nx, x$$

forment une base[19] de E qui répond à la question.

■

12. Chaînes engendrées par un endomorphisme

Soit $T \in \mathcal{L}(E)$ un endomorphisme quelconque. Avec nos notations usuelles, rappelons que, par définition, $F_{\lambda_j} = \ker(T_j^{m_j})$. Ainsi, la restriction[20] de $T_j = T - \lambda_j\, id$ au sous-espace caractéristique F_{λ_j},

$$T_{j|F_{\lambda_j}} : F_{\lambda_j} \to F_{\lambda_j}$$

est nilpotent et son indice de nilpotence est m_j (c'est une conséquence du théorème de stabilisation des images et des noyaux). Par conséquent, les concepts introduits ci-dessous pour un opérateur nilpotent N quelconque se transposent aisément à la restriction à F_{λ_j} de T_j.

Définition XI.12.1. Soit $N \in \mathcal{L}(E)$ un opérateur nilpotent. On appelle *chaîne (engendrée par N)* toute suite finie de la forme

$$x, Nx, \dots, N^{\ell-1}x$$

où $N^{\ell-1}x \neq 0$ et $N^{\ell}x = 0$. On dit que x est la *tête* de la chaîne et que $N^{\ell-1}x$ en est la *queue*. L'entier ℓ est la *longueur* de la chaîne.

Remarque XI.12.2. Par définition, la longueur ℓ d'une chaîne est inférieure ou égale à l'indice de nilpotence k de N. Remarquons que pour tout $\ell \leq k$, il existe une chaîne de longueur ℓ. En effet, il suffit de prendre comme tête de chaîne un élément appartenant à $\ker(N^{\ell}) \setminus \ker(N^{\ell-1})$ et on se convainc aisément qu'un tel choix est toujours possible[21].

[19] L'argumentation est identique à celle développée dans la preuve de la proposition XI.11.3.

[20] On sait déjà que les sous-espaces caractéristiques sont stables pour T donc aussi pour T_j. En effet, si x appartient à F_{λ_j}, alors Tx et $\lambda_j x$ appartiennent tous deux à F_{λ_j} donc leur différence aussi.

[21] Par définition même de l'indice de nilpotence.

Exemple XI.12.3. Poursuivons l'exemple XI.11.2. On a

$$e_4 = \begin{pmatrix}0\\0\\0\\1\end{pmatrix},\ Ne_4 = \begin{pmatrix}1\\3\\4\\0\end{pmatrix},\ N^2e_4 = \begin{pmatrix}11\\-8\\0\\0\end{pmatrix},\ N^3e_4 = \begin{pmatrix}-8\\0\\0\\0\end{pmatrix} \text{ et } N^4e_4 = 0$$

et

$$e_3 = \begin{pmatrix}0\\0\\1\\0\end{pmatrix},\ Ne_3 = \begin{pmatrix}2\\-2\\0\\0\end{pmatrix},\ N^2e_3 = \begin{pmatrix}-2\\0\\0\\0\end{pmatrix} \text{ et } N^3e_3 = 0.$$

Ainsi, e_4 (resp. e_3) est la tête d'une chaîne de longueur 4 (resp. 3) engendrée par N. Remarquons qu'en prenant comme tête de chaîne le vecteur Ne_4 (resp. N^2e_4, N^3e_4, Ne_3, N^2e_3), on obtient une chaîne de longueur 3 (resp. 2, 1, 2, 1).

Exemple XI.12.4. Dans l'espace vectoriel $\mathbb{R}[x]_3$ des polynômes de degré au plus 3, on considère l'application dérivée D_x. Soit $P(x) = x^2 + 3x + 1$. Les élements

$$P,\ D_xP = 2x + 3,\ D_x^2P = 2$$

forment une chaîne de longueur 3 engendrée par D_x.

Proposition XI.12.5. *Les éléments d'une chaîne sont linéairement indépendants.*

Démonstration. On procède comme dans la preuve de la proposition XI.11.3.

■

On a même un résultat encore plus général.

Proposition XI.12.6. *Les éléments d'un ensemble C de chaînes sont linéairement indépendants si et seulement si les queues de ces chaînes sont linéairement indépendantes.*

Démonstration. La condition est trivialement nécessaire[22]

Il nous suffit donc de montrer que la condition est suffisante[23]. Soit L la longueur maximale des chaînes de C. Pour tout $\ell \in \{1, \ldots, L\}$, posons d_ℓ le nombre de chaînes de longueur ℓ de C. Soient

$$x_{\ell,1}, \ldots, x_{\ell,d_\ell}$$

les têtes des chaînes de longueur ℓ. Ainsi[24],

$$C = \{N^{\ell-k}x_{\ell,d} \mid \ell = 1, \ldots, L,\ d = 1, \ldots, d_\ell,\ k = 1, \ldots, \ell\}.$$

[22]Si des éléments sont linéairement indépendants, alors un sous-ensemble quelconque de ceux-ci est encore formé de vecteurs linéairement indépendants.

[23]Le raisonnement est encore une fois analogue à celui développé dans la preuve de la proposition XI.11.3.

[24]On adapte aisément la preuve dans le cas où C ne contient pas de chaîne d'une longueur ℓ donnée. Cette adaptation ne ferait qu'alourdir encore un peu plus les notations.

Supposons que

$$\sum_{\ell=1}^{L}\sum_{d=1}^{d_\ell}\sum_{k=1}^{\ell}\alpha_{\ell,d,k}\,N^{\ell-k}x_{\ell,d}=0$$

avec des coefficients $\alpha_{\ell,d,k}\in\mathbb{C}$ non tous nuls. Soit K le maximum des k pour lesquels il existe $\ell\in\{k,\dots,L\}$ et $d\in\{1,\dots,d_\ell\}$ tels que $\alpha_{\ell,d,k}\neq 0$. Alors,

$$N^{K-1}\left(\sum_{\ell=1}^{L}\sum_{d=1}^{d_\ell}\sum_{k=1}^{\ell}\alpha_{\ell,d,k}\,N^{\ell-k}x_{\ell,d}\right)=\sum_{\ell=1}^{L}\sum_{d=1}^{d_\ell}\sum_{k=1}^{\ell}\alpha_{\ell,d,k}\,N^{\ell-k+K-1}x_{\ell,d}=0.$$

En outre, $N^{\ell-k+K-1}x_{\ell,d}=0$ si $k<K$ car $x_{\ell,d}$ est la tête d'une chaîne de longueur ℓ et $k<K$ entraîne $\ell-k+K-1=\ell+K-(k+1)\geq\ell$. Si $k>K$, par définition même de K, les coefficients $\alpha_{\ell,d,k}$ sont nuls. Dès lors, on trouve

$$\sum_{\ell=K}^{L}\sum_{d=1}^{d_\ell}\alpha_{\ell,d,K}\,N^{\ell-1}x_{\ell,d}=0.$$

Or les queues des chaînes sont linéairement indépendantes et donc, pour tout $\ell\in\{K,\dots,L\}$ et pour tout $d\in\{1,\dots,d_\ell\}$, $\alpha_{\ell,d,K}=0$ ce qui contredit la définition de K.

■

On dit que des chaînes sont *linéairement indépendantes* si leurs queues sont linéairement indépendantes.

Théorème XI.12.7 (Base répartie en chaînes). *Soit N un endomorphisme nilpotent de E. Il existe une base de E formée des vecteurs de chaînes linéairement indépendantes réparties en longueurs décroissantes.*

Démonstration. Soit m l'indice de nilpotence de N. Pour une plus grande clarté, nous allons diviser la preuve en trois grandes étapes.

I. Construction de sous-espaces "S_k" et d'un tableau.

On sait que

$$\ker(N^k)\subsetneq\ker(N^{k+1}),\quad\text{si } k<m$$

et que $\ker(N^k)=E$, si $k\geq m$. Pour $k=m,m-1,\dots,2,1$, on construit de proche en proche des sous-espaces vectoriels[25] S_k de $\ker(N^k)$. Pour $k=m$, on choisit S_m de manière telle que

$$\ker(N^{m-1})\oplus S_m=\ker(N^m)=E.$$

Si on dispose de $S_m,S_{m-1},\dots,S_{k+1}$ (avec $k\leq m-1$), on choisit S_k de manière telle que

Cette formule est la clé de la preuve !

$$\left(\ker(N^{k-1})+\sum_{j=k+1}^{m}N^{j-k}(S_j)\right)\oplus S_k=\ker(N^k).\tag{12}$$

[25] On pourra observer qu'il n'est nullement gênant qu'un de ces sous-espaces vectoriels S_k soit réduit à $\{0\}$.

Observons que ce choix a un sens car les sous-espaces intervenant dans le membre de gauche sont tous des sous-espaces de $\ker(N^k)$,

$$\underbrace{\ker(N^{k-1})}_{\subset\ker(N^k)} + N\underbrace{\underbrace{(S_{k+1})}_{\subset\ker(N^{k+1})}}_{\subset\ker(N^k)} + N^2\underbrace{\underbrace{(S_{k+2})}_{\subset\ker(N^{k+2})}}_{\subset\ker(N^k)} + \cdots + N^{m-k}\underbrace{\underbrace{(S_m)}_{\subset\ker(N^m)}}_{\subset\ker(N^k)}.$$

Considérons une base[26]

$$x_{k,1},\dots,x_{k,d_k}$$

de chacun des sous-espaces vectoriels S_k, $k\in\{1,\dots,m\}$, d_k étant la dimension de S_k. On construit alors le tableau suivant formé de chaînes ayant les $x_{i,j}$ pour tête

$$\begin{array}{ccccc}
N^{m-1}x_{m,1} & \cdots & N^{m-k}x_{m,1} & \cdots & x_{m,1}\\
\vdots & & \vdots & & \vdots\\
N^{m-1}x_{m,d_m} & \cdots & N^{m-k}x_{m,d_m} & \cdots & x_{m,d_m}\\
\vdots & & & & \\
N^{k-1}x_{k,1} & \cdots & x_{k,1} & & \\
\vdots & & \vdots & & \\
N^{k-1}x_{k,d_k} & \cdots & x_{k,d_k} & & \\
\vdots & & & & \\
x_{1,1} & & & & \\
\vdots & & & & \\
x_{1,d_1} & & & &
\end{array} \tag{13}$$

II. Indépendance linéaire des éléments du tableau.

Au vu de la proposition précédente, les éléments du tableau sont linéairement indépendants si les éléments de la première colonne le sont. Supposons ces derniers linéairement dépendants et qu'il existe une relation linéaire

$$\sum_{k=1}^{m}\sum_{d=1}^{d_k}\alpha_{k,d}N^{k-1}x_{k,d}=0$$

avec les $\alpha_{k,d}$ non tous nuls. Soit K le minimum des k pour lesquels il existe $d\in\{1,\dots,d_k\}$ tel que $\alpha_{k,d}\neq 0$. Ainsi, la relation linéaire précédente peut se réécrire

$$\sum_{k=K}^{m}\sum_{d=1}^{d_k}\alpha_{k,d}\,N^{k-1}x_{k,d}=N^{K-1}\left(\sum_{k=K}^{m}\sum_{d=1}^{d_k}\alpha_{k,d}\,N^{k-K}x_{k,d}\right)=0$$

[26]Si $x_{k,j}$ est un vecteur d'une base de S_k, alors $N^k x_{k,j}=0$ car S_k est un sous-espace vectoriel de $\ker(N^k)$ et $N^{k-1}x_{k,j}\neq 0$ car S_k est en somme directe avec $\ker(N^{k-1})$. On peut donc construire une chaîne de longueur k de tête $x_{k,j}$.

ce qui signifie que

$$\sum_{k=K}^{m}\sum_{d=1}^{d_k}\alpha_{k,d}\,N^{k-K}x_{k,d}\in\ker(N^{K-1}).$$

On développe simplement la somme.

Dès lors,

$$\sum_{d=1}^{d_K}\alpha_{K,d}\,x_{K,d}+\sum_{d=1}^{d_{K+1}}\alpha_{K+1,d}\,N\underbrace{x_{K+1,d}}_{\in S_{K+1}}+\cdots+\sum_{d=1}^{d_m}\alpha_{m,d}\,N^{m-K}\underbrace{x_{m,d}}_{\in S_m}\in\ker(N^{K-1})$$

et donc[27]

$$\sum_{d=1}^{d_K}\alpha_{K,d}\,x_{K,d}\in\left(\ker(N^{K-1})+\sum_{k=K+1}^{m}N^{k-K}(S_k)\right).$$

Or $x_{K,1},\dots,x_{K,d_K}$ forment une base de S_K. Par conséquent, au vu de la relation (12), on a

$$\alpha_{K,1}=\cdots=\alpha_{K,d_K}=0$$

ce qui contredit la définition de K.

III. Partie génératrice.

Il est facile[28] de voir que les éléments des k premières colonnes ($k\geq 1$) du tableau (13) appartiennent tous à $\ker(N^k)$.

Nous allons montrer qu'ils forment en fait une base de ce sous-espace (en particulier, pour $k=m$, le tableau tout entier formé des m colonnes est alors une base de $\ker(N^m)=E$).

Nous avons au point précédent vérifié que l'ensemble des éléments du tableau (13) était une partie libre, il nous suffit dès lors de démontrer le résultat suivant.

Lemme XI.12.8. *les éléments des k premières colonnes du tableau* (13) *engendrent* $\ker(N^k)$, $k\geq 1$.

On procède par récurrence sur k. Mais commençons par une remarque préliminaire fort utile.

Remarque XI.12.9. L'espace $N^{j-\ell}(S_j)$, $1\leq\ell\leq j$, est engendré par

$$N^{j-\ell}x_{j,1},\dots,N^{j-\ell}x_{j,d_j}$$

et ces vecteurs appartiennent à la ℓ-ième colonne du tableau (13). En effet, $x_{j,1},\dots,x_{j,d_j}$ forment une base de S_j. Si y appartient $N^{j-\ell}(S_j)$, il existe donc $z\in S_j$ tel que $N^{j-\ell}z=y$ et des coefficients α_i tels que

$$z=\sum_{i=1}^{d_j}\alpha_i\,x_{j,i}\quad\text{et}\quad y=N^{j-\ell}z=\sum_{i=1}^{d_j}\alpha_i\,N^{j-\ell}x_{j,i}.$$

[27] L'argument est simple. Soient A,B deux sous-espaces vectoriels. Si $t+u\in A$ et $u\in B$, alors $t=(t+u)+(-u)\in A+B$.

[28] La première colonne de (13) est constituée de queues de chaînes engendrées par N et ses éléments appartiennent donc à $\ker(N)$. On obtient la conclusion en raisonnant de proche en proche.

Cas de base. Pour $k = 1$, la formule (12) devient

$$\ker N = S_1 \oplus \sum_{j=2}^{m} N^{j-1} S_j.$$

On conclut directement car $x_{1,1}, \ldots, x_{1,d_1}$ forment une base de S_1 et donc l'engendre. De plus, par la remarque précédente, pour $j = 2, \ldots, m$, $N^{j-1}S_j$ est engendré par $N^{j-1}x_{j,1}, \ldots, N^{j-1}x_{j,d_j}$.

Induction. Supposons à présent que les $k-1$ premières colonnes de (13) engendrent $\ker(N^{k-1})$ et montrons que les k premières colonnes engendrent $\ker(N^k)$. Au vu de (12),

$$\ker N^k = \left(\ker(N^{k-1}) + \sum_{j=k+1}^{m} N^{j-k}(S_j) \right) \oplus S_k = \ker(N^k).$$

Par hypothèse de récurrence, les $k-1$ premières colonnes de (13) engendrent $\ker N^{k-1}$. Par la remarque XI.12.9,

$$\begin{array}{ccc} Nx_{k+1,1}, \ldots, Nx_{k+1,d_{k+1}} & \text{engendrent} & NS_{k+1} \\ & \vdots & \\ N^{m-k}x_{m,1}, \ldots, N^{m-k}x_{m,d_m} & \text{engendrent} & N^{m-k}S_m. \end{array}$$

Enfin, $x_{k,1}, \ldots, x_{k,d_k}$ engendrent S_k. On en conclut que les k premières colonnes du tableau (13) engendrent $\ker N^k$.

Ceci achève la preuve. Les éléments du tableau tout entier forment une base de $\ker(N^m) = E$. Bien évidemment, ce tableau est formé de chaînes de longueur décroissante.

■

La base dont il est question dans le théorème précédent n'est pas unique (cf. la remarque XI.14.2 pour un exemple numérique). Cependant, toutes les bases réparties en chaînes ont des propriétés communes et en particulier, **la forme** du tableau (13) est bien déterminée.

Supposons que U est une base quelconque de E formée par des chaînes linéairement indépendantes et engendrées par N. On place les éléments de U dans un tableau semblable à (13). En d'autres termes, on ordonne les chaînes par longueur décroissante, une ligne du tableau correspondant à une chaîne de U et on écrit les chaînes en commençant par leur queue. Par exemple, si U est formé de deux chaînes de longueur 5, d'une chaîne de longueur 4, d'une chaîne de longueur 3, de deux chaînes de longueur 2 et

d'une chaîne de longueur 1, on a un tableau de la forme

$$\begin{array}{ccccc} N^4x_1 & N^3x_1 & N^2x_1 & Nx_1 & x_1 \\ N^4x_2 & aN^3x_2 & aN^2x_2 & aNx_2 & ax_2 \\ N^3x_3 & aN^2x_3 & aNx_3 & ax_3 & \\ N^2x_4 & aNx_4 & ax_4 & & \\ Nx_5 & ax_5 & & & \\ Nx_6 & x_6 & & & \\ x_7 & & & & \end{array}$$

On pourrait croire qu'on redémontre un résultat déjà connu ! Il n'en est rien. Dans la preuve précédente, on a considéré un tableau très particulier. Ici la proposition concerne une base **quelconque** répartie en chaînes.

Proposition XI.12.10. *Avec les notations précédentes, les k premières colonnes du tableau forment une base de* $\ker(N^k)$*. En particulier, la longueur de la plus longue chaîne du tableau est l'indice de nilpotence de N.*

Démonstration. Puisque tous les éléments du tableau sont linéairement indépendants, il suffit de montrer que tout vecteur x annulé par N^k est combinaison linéaire des vecteurs des k premières colonnes. Puisque U est une base de E, on peut écrire

$$x = \sum_{r=1}^{u} \alpha_r\, y_r + \sum_{s=1}^{v} \beta_s\, z_s$$

où $y_1, \ldots, y_u$ sont les vecteurs des k premières colonnes et $z_1, \ldots, z_v$ les vecteurs des autres colonnes du tableau. Il vient

$$N^k x = \sum_{r=1}^{u} \alpha_r\, \underbrace{N^k y_r}_{0} + \sum_{s=1}^{v} \beta_s\, N^k z_s.$$

Par construction du tableau, les éléments $N^k z_1, \ldots, N^k z_v$ sont des éléments distincts du tableau et sont donc linéairement indépendants. De là, on en conclut que $\beta_1 = \cdots = \beta_s = 0$.

Le cas particulier est immédiat. Soit t la longueur de la plus longue chaîne du tableau. En particulier cela signigie qu'il existe y tel que $N^{t-1}y \neq 0$. Tout élément x de E étant combinaison linéaire des éléments du tableau, il est clair que $N^t x = 0$ pour tout $x \in E$. Ceci termine la preuve.

■

Remarque XI.12.11. La proposition précédente nous a montré que quelle que soit la base répartie en chaînes considérée, les k premières colonnes du tableau correspondant à (13) forment une base de $\ker(N^k)$. Ainsi, le nombre d'éléments se trouvant dans les k premières colonnes est toujours

Ici, $N \in \mathcal{L}(E)$ et $\dim E = n$.

$$\dim(\ker(N^k)) = n - \underbrace{\dim(\mathrm{Im}(N^k))}_{\mathrm{rg}(N^k)}$$

Formule très utile dans les exercices...

et en particulier, le nombre d'éléments dans la k-ième colonne est

$$\begin{aligned} \dim(\ker(N^k)) - \dim(\ker(N^{k-1})) &= \dim(\mathrm{Im}(N^{k-1})) - \dim(\mathrm{Im}(N^k)) \\ &= \mathrm{rg}(N^{k-1}) - \mathrm{rg}(N^k). \end{aligned}$$

La forme du tableau de chaînes ne dépend donc pas de la base choisie. On peut la déterminer en calculant les rangs des opérateurs $N, N^2, \dots, N^m$.

Remarque XI.12.12. Nous avons déjà insisté sur l'importance d'avoir des sous-espaces stables pour T (cf. remarques XI.9.4 et XI.10.6) dans le but obtenir une représentation matricielle de T sous forme composée diagonale. Au vu du théorème XI.12.7, on peut trouver une base de F_{λ_j} répartie en chaînes engendrées par T_j. Notons que l'enveloppe linéaire des vecteurs d'une telle chaîne est stable pour T. En effet, $T = T_j + \lambda_j\, id.$

$$T(T_j^k x) = T_j^{k+1} x + \lambda_j T_j^k x.$$

Ainsi, une base de F_{λ_j} répartie en chaînes fournit une décomposition de F_{λ_j} en une somme directe de sous-espaces stables pour T (cette décomposition n'étant pas unique).

13. Réduction à la forme canonique de Jordan

Nous avons à présent à notre disposition l'ensemble des outils nécessaires pour représenter un endomorphisme T de la manière "la plus simple possible" (encore à définir). On sait notamment que

- $E = F_{\lambda_1} \oplus \cdots \oplus F_{\lambda_p}$,
- les sous-espaces caractéristiques F_{λ_j} sont stables pour T,
- l'opérateur T_j restreint à F_{λ_j} est nilpotent, on peut donc construire une base de F_{λ_j} répartie en chaînes engendrées par T_j,
- l'enveloppe linéaire des vecteurs d'une telle chaîne est stable pour T et une base de F_{λ_j} répartie en chaînes fournit donc une décomposition de F_{λ_j} en une somme directe de sous-espaces stables pour T.

Théorème XI.13.1. *Pour tout endomorphisme $T \in \mathcal{L}(E)$, il existe une base de E dans laquelle la matrice qui représente T est une matrice composée diagonale dont les blocs diagonaux sont de dimension* 1 *ou sont de la forme*

$$\begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix}$$

où λ est une valeur propre de A. Plusieurs blocs diagonaux peuvent correspondre à la même valeur propre. Cette forme canonique est unique à une permutation des blocs diagonaux près.

Démonstration. Soient $\lambda_1, \dots, \lambda_p$ les valeurs propres distinctes de T. L'opérateur $T_j = (T - \lambda_j\, id)$ restreint à F_{λ_j} est nilpotent, d'indice de nilpotence m_j. Au vu du théorème XI.12.7, il existe une base U_j de F_{λ_j} répartie en chaînes engendrées par T_j. Si le tableau formé par ces chaînes (ce tableau est

construit de manière analogue au tableau (13)) contient t lignes de longueur respective $\ell_1, \ldots, \ell_t$ (autrement dit, si U_j contient t chaînes[29]), alors, au vu de la remarque XI.12.12, la matrice qui représente $T_{j|F_{\lambda_j}}$ dans cette base de F_{λ_j} est de la forme

$$\begin{pmatrix} J(\ell_1) & & \\ & \ddots & \\ & & J(\ell_t) \end{pmatrix}$$

où, pour rappel,

$$J(n) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix}$$

est une matrice carrée de dimension n. La restriction de T à F_{λ_j} est telle que

$$T_{|F_{\lambda_j}} = \lambda_j \, id_{F_{\lambda_j}} + T_{j|F_{\lambda_j}}.$$

Dès lors, la représentation de $T_{|F_{\lambda_j}}$ dans la base U_j est de la forme

$$A_j = \begin{pmatrix} J'_{\lambda_j}(\ell_1) & & \\ & \ddots & \\ & & J'_{\lambda_j}(\ell_t) \end{pmatrix}$$

où

$$J'_\lambda(n) = J(n) + \lambda I_n = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix}$$

est appelée *matrice de Jordan*. Nous pouvons à présent conclure car, par le théorème XI.10.4, les sous-espaces caractéristiques sont en somme directe et leur somme donne E. Si on considère la base de E formée par les vecteurs des bases $U_1, \ldots, U_p$, alors l'endomorphisme T se représente dans cette base par une matrice composée diagonale

$$\operatorname{diag}(A_1, \ldots, A_p).$$

Si on dispose d'une autre décomposition en blocs de Jordan comme représentation de T dans une base U', il est clair que chaque bloc de Jordan de valeur propre λ_j et de dimension r provient de vecteurs de base correspondant à une chaîne engendrée par T_j de longueur r. La conclusion découle de la remarque XI.12.11.

[29] Rappelons que $\dim F_{\lambda_j} = \mu_j$ et donc $\ell_1 + \cdots + \ell_t$ est égal à la multiplicité de λ_j comme racine du polynôme caractéristique de T.

■

Remarque XI.13.2. Deux endomorphismes T et T' ont la même forme de Jordan s'ils ont les mêmes valeurs propres et si les formes des tableaux des bases de F_{λ_j} réparties en chaînes engendrées respectivement par les restrictions $(T-\lambda_j\,id)_{|F_{\lambda_j}(T)}$ et $(T'-\lambda_j\,id)_{|F_{\lambda_j}(T')}$ coïncident.

Remarque XI.13.3. Si dans les tableaux constituant une base répartie en chaînes, on avait commencé par les têtes au lieu des queues, on aurait obtenu dans la décomposition canonique de Jordan des blocs carrés ayant une valeur propre sur la diagonale et des 1 en dessous de la diagonale.

14. Quelques exemples

Exemple XI.14.1. Considérons la matrice

$$A=\begin{pmatrix}1&0&-1&1&0\\-4&1&-3&2&1\\-2&-1&0&1&1\\-3&-1&-3&4&1\\-8&-2&-7&5&4\end{pmatrix}$$

et réduisons-la à la forme canonique de Jordan. Il s'agit simplement d'un opérateur particulier $T:\mathbb{C}^5\to\mathbb{C}^5:x\mapsto Ax$. On calcule tout d'abord son polynôme caractéristique

$$\det(A-\lambda I)=\det\begin{pmatrix}1-\lambda&0&-1&1&0\\-4&1-\lambda&-3&2&1\\-2&-1&-\lambda&1&1\\-3&-1&-3&4-\lambda&1\\-8&-2&-7&5&4-\lambda\end{pmatrix}=-(\lambda-2)^5.$$

Ainsi, 2 est l'unique valeur propre de A de multiplicité algébrique $\mu=5$. Recherchons la dimension du sous-espace propre correspondant. On a

$$A-2I=\begin{pmatrix}-1&0&-1&1&0\\-4&-1&-3&2&1\\-2&-1&-2&1&1\\-3&-1&-3&2&1\\-8&-2&-7&5&2\end{pmatrix}.$$

On observe que, dans cette matrice, $L_5=L_1+L_2+L_4$ et $L_4=L_1+L_3$. Ainsi, si on remplace L_2 par $L_2-(L_1+L_3)$ et L_3 par L_3-L_1, on obtient un système suivant équivalent à $(A-2I)x=0$,

$$\begin{pmatrix}-1&0&-1&1&0\\-1&0&0&0&0\\-1&-1&-1&0&1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\x_5\end{pmatrix}=0$$

et les conditions $x_1 = 0$, $x_3 = x_4$ et $x_2 + x_3 = x_5$. Ainsi, le sous-espace propre E_2 est égal à

$$\rangle \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \langle$$

Pour calculer $\dim E_2$, on aurait pu procéder plus rapidement en calculant le rang de la matrice $A - 2I$ et en utilisant le fait que $\dim E_2 = 5 - \mathrm{rg}(A - 2I)$

et sa dimension vaut 2. On en conclut que A n'est pas diagonalisable puisque $\dim E_2 < 5$.

Calculons[30] à présent les puissances de $A - 2I$,

$$(A - 2I)^2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & -1 & 1 & 0 \\ -1 & 0 & -1 & 1 & 0 \\ -1 & 0 & -1 & 1 & 0 \end{pmatrix} \quad \text{et } (A - 2I)^3 = 0.$$

cf. remarque XI.12.11.

La forme du tableau d'une base de F_2 répartie en chaînes est donnée par les formules suivantes :

hauteur de la colonne 1 : $5 - \mathrm{rg}(A - 2I) = 5 - 3 = 2$,
hauteur de la colonne 2 : $\mathrm{rg}(A - 2I) - \mathrm{rg}(A - 2I)^2 = 3 - 1 = 2$,
hauteur de la colonne 3 : $\mathrm{rg}(A - 2I)^2 - \mathrm{rg}(A - 2I)^3 = 1 - 0 = 1$.

$\dim F_2 = \mu = 5$ et ici, on a $2 + 2 + 1 = 5$ vecteurs de base.

Ainsi, ce tableau est de la forme

*	*	*
*	*	

En particulier, puisque la longueur maximale des chaînes est 3, on peut retrouver le fait que le polynôme minimum de A est $(\lambda - 2)^3$. Il nous reste à présent à construire des chaînes linéairement indépendantes de longueur respective 2 et 3 engendrées par $A - 2I$. La tête d'une chaîne de longueur 3 est un vecteur x tel que $(A - 2I)^3 x = 0$ et $(A - 2I)^2 x \neq 0$. On peut prendre $x = e_1$ et on a la chaîne (en commençant par la queue)

$$(A - 2I)^2 e_1 = \begin{pmatrix} 0 \\ 0 \\ -1 \\ -1 \\ -1 \end{pmatrix}, \ (A - 2I)e_1 = \begin{pmatrix} -1 \\ -4 \\ -2 \\ -3 \\ -8 \end{pmatrix}, \ e_1.$$

La tête d'une chaîne de longueur 2 est un vecteur y tel que $(A-2I)^2 y = 0$ et $(A-2I)y \neq 0$. Il faut de plus s'assurer que les queues des chaînes $(A-2I)^2 x$ et $(A-2I)y$ sont linéairement indépendantes pour que les chaînes le soient et

[30] Puisque $(A - 2I)^3 = 0$, $A - 2I$ est un endomorphisme nilpotent de E et on a en particulier, $\ker((A - 2I)^3) = E$. On a même $\ker I = \{0\} \subsetneq \ker(A - 2I) \subsetneq \ker(A - 2I)^2 \subsetneq \ker(A - 2I)^3 = E = \ker(A - 2I)^4 = \ldots$.

forment une base. On peut prendre $y = e_2$ et on a la chaîne (en commençant par la queue)

$$(A-2I)e_2 = \begin{pmatrix} 0 \\ -1 \\ -1 \\ -1 \\ -2 \end{pmatrix}, \ e_2.$$

La matrice S formée sur ces chaînes est

$$S = \begin{pmatrix} 0 & -1 & 1 & 0 & 0 \\ 0 & -4 & 0 & -1 & 1 \\ -1 & -2 & 0 & -1 & 0 \\ -1 & -3 & 0 & -1 & 0 \\ -1 & -8 & 0 & -2 & 0 \end{pmatrix}.$$

A titre indicatif, on a

$$S^{-1} = \begin{pmatrix} 0 & 0 & 2 & -4 & 1 \\ 0 & 0 & 1 & -1 & 0 \\ 1 & 0 & 1 & -1 & 0 \\ 0 & 0 & -5 & 6 & -1 \\ 0 & 1 & -1 & 2 & -1 \end{pmatrix}.$$

Grâce aux constructions réalisées, il vient

$$S^{-1}AS = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

qui est constitué de deux blocs de Jordan car la base de F_2 contient deux chaînes.

Remarque XI.14.2. La base choisie n'est pas unique. On aurait pu prendre comme tête de chaîne de longueur 3, par exemple, le vecteur $x = e_3$ (ou aussi $x = e_4$) et construire la chaîne

$$(A-2I)^2e_3 = \begin{pmatrix} 0 \\ 0 \\ -1 \\ -1 \\ -1 \end{pmatrix}, \ (A-2I)e_3 = \begin{pmatrix} -1 \\ -3 \\ -2 \\ -3 \\ -7 \end{pmatrix}, \ e_3$$

et comme tête de chaîne de longueur 2, $y = e_5$,

$$(A-2I)e_5 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 2 \end{pmatrix}, \ e_5.$$

Il est clair que les queues $(A-2I)^2e_3$ et $(A-2I)e_5$ sont linéairement indépendantes. Ainsi, on pourrait vérifier que la matrice

$$S' = \begin{pmatrix} 0 & -1 & 0 & 0 & 0 \\ 0 & -3 & 0 & 1 & 0 \\ -1 & -2 & 1 & 1 & 0 \\ -1 & -3 & 0 & 1 & 0 \\ -1 & -7 & 0 & 2 & 1 \end{pmatrix}$$

réalise la même réduction.

Remarque XI.14.3. Connaissant la forme de Jordan de A, on peut calculer assez facilement A^n. En effet,

$$A^n = S \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}^n S^{-1}.$$

Il suffit donc de savoir calculer les puissances n-ièmes des différents blocs de Jordan. Une simple récurrence donne

Démontrez-le !

$$\begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}^n = \begin{pmatrix} 2^n & n2^{n-1} & n(n-1)2^{n-3} \\ 0 & 2^n & n2^{n-1} \\ 0 & 0 & 2^n \end{pmatrix}$$

et

$$\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}^n = \begin{pmatrix} 2^n & n2^{n-1} \\ 0 & 2^n \end{pmatrix}.$$

Exemple XI.14.4. Soit la matrice

$$A = \begin{pmatrix} 5 & -1 & -3 & 2 & -5 \\ 0 & 2 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & -2 \\ 0 & -1 & 0 & 3 & 1 \\ 1 & -1 & -1 & 1 & 1 \end{pmatrix}.$$

Une fois encore, on peut voir cette matrice comme un opérateur $T : \mathbb{C}^5 \to \mathbb{C}^5 : x \mapsto Ax$. Le polynôme caractéristique de A est donné par

$$\det(A-\lambda I) = \det \begin{pmatrix} 5-\lambda & -1 & -3 & 2 & -5 \\ 0 & 2-\lambda & 0 & 0 & 0 \\ 1 & 0 & 1-\lambda & 1 & -2 \\ 0 & -1 & 0 & 3-\lambda & 1 \\ 1 & -1 & -1 & 1 & 1-\lambda \end{pmatrix} = -(\lambda-2)^3(\lambda-3)^2.$$

La matrice A possède donc deux valeurs propres 2 et 3 de multiplicité algébrique respective 3 et 2. Déterminons les sous-espaces propres correspondants. Recherchons tout d'abord les solutions de $(A-2I)x=0$. Il vient

$$A-2I=\begin{pmatrix}3&-1&-3&2&-5\\0&0&0&0&0\\1&0&-1&1&-2\\0&-1&0&1&1\\1&-1&-1&1&-1\end{pmatrix}.$$

Cette matrice est de rang 3 car

$$\det\begin{pmatrix}-3&2&-5\\-1&1&-2\\0&1&1\end{pmatrix}=-2$$

et tous les déterminants bordés sont nuls,

$$\det\begin{pmatrix}3&-3&2&-5\\1&-1&1&-2\\0&0&1&1\\1&-1&1&-1\end{pmatrix}=0\quad\text{et}\quad\det\begin{pmatrix}-1&-3&2&-5\\0&-1&1&-2\\-1&0&1&1\\-1&-1&1&-1\end{pmatrix}=0.$$

Par conséquent, l'ensemble des solutions du système $(A-2I)x=0$ est un sous-espace vectoriel de dimension $5-3=2$ et $\dim E_2=2<3$. La matrice A n'est donc pas diagonalisable. On a

$$(A-2I)^2=\begin{pmatrix}1&0&-1&0&-2\\0&0&0&0&0\\0&0&0&0&0\\1&-2&-1&2&0\\1&-1&-1&1&-1\end{pmatrix}$$

qui est une matrice de rang 2 car $C_3=-C_1$, $C_4=-C_2$ et $C_5=-2C_1+C_2$.

En outre, on sait que $\ker((A-2I)^k)$ est égal à l'espace caractéristique F_2, pour tout $k\geq 3$, car 3 est la multiplicité algébrique de la valeur propre 2 (cf. la remarque faite à la fin de la définition XI.9.3). Il est donc inutile de calculer d'autres puissances de $A-2I$. En particulier, puisque F_2 a pour dimension la multiplicité algébrique de la valeur propre 2, c'est-à-dire 3, on en déduit[31]que le rang de $(A-2I)^k$ est $5-3=2$, pour tout $k\geq 3$.

La forme du tableau d'une base de F_2 répartie en chaînes est donnée par les formules suivantes[32] :

[31]On peut attirer l'attention du lecteur attentif sur une différence majeure avec l'exemple précédent. Dans ce dernier, on avait $(A-2I)^3=0$ et $F_2=E$. En d'autres termes, il s'agissait d'un opérateur nilpotent de E d'indice de nilpotence 3. Ici, il n'est pas possible d'avoir une telle situation car on sait que $E=F_2\oplus F_3$ et les deux sous-espaces F_2 et F_3 sont au moins de dimension 1. Par conséquent, il est impossible d'avoir $(A-2I)^k=0$ pour un k quelconque car sinon F_2 serait égal à E tout entier. Dit autrement, dans l'exemple précédent, le rang de $(A-2I)^k$ se stabilisait à 0 et ici, il se stabilise à 2.

[32]On veut encore une fois appliquer la formule de la remarque XI.12.11 pour calculer le nombre d'éléments dans la k-ième colonne du tableau. Cependant, cette formule s'applique

hauteur de la colonne 1 : $5 - \operatorname{rg}(A-2I) = 5-3 = 2$,
hauteur de la colonne 2 : $\operatorname{rg}(A-2I) - \operatorname{rg}(A-2I)^2 = 3-2 = 1$.

Ainsi, une base de F_2 répartie en chaînes sera de la forme

*	*
*	

Le vecteur $y = e_2 + e_4$ est la tête d'une chaîne de longueur 2 engendrée par $A - 2I$ car

$$(A-2I)^2(e_2+e_4) = 0 \text{ et } (A-2I)(e_2+e_4) = e_1 + e_3.$$

Le vecteur $z = e_1+e_3$ est la tête d'une chaîne de longueur 1 car $(A-2I)(e_1+e_3) = 0$, mais ce choix est incompatible avec le choix de y car les queues des deux chaînes seraient identiques et donc linéairement dépendantes. Par contre, on trouve aisément que

$$z = e_2 - 2e_3 + e_5$$

convient.

Recherchons à présent les solutions de $(A-3I)x = 0$. La matrice

$$A - 3I = \begin{pmatrix} 2 & -1 & -3 & 2 & -5 \\ 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & -2 & 1 & -2 \\ 0 & -1 & 0 & 0 & 1 \\ 1 & -1 & -1 & 1 & -2 \end{pmatrix}$$

est de rang 4, on le vérifie aisément en calculant le déterminant de la matrice privée de ses première colonne et deuxième ligne qui est non nul. De plus, la première colonne coïncidant avec la quatrième, le rang n'est pas 5. Par conséquent, le sous-espace propre associé à la valeur propre 3 est de dimension 1. On calcule

$$(A-3I)^2 = \begin{pmatrix} -4 & 2 & 5 & -4 & 8 \\ 0 & 1 & 0 & 0 & 0 \\ -2 & 0 & 3 & -2 & 4 \\ 1 & 0 & -1 & 1 & -2 \\ -1 & 1 & 1 & -1 & 2 \end{pmatrix}.$$

Son rang est nécessairement 3 car $\ker((A-3I)^2) = F_3$ qui est de dimension 2 (en effet, 2 est la multiplicité algébrique de la valeur propre 3). Ainsi, la

à un opérateur nilpotent et ici, l'opérateur $T_2 : \mathbb{C}^5 \to \mathbb{C}^5 : x \mapsto (A-2I)x$ n'est pas nilpotent sauf si on le restreint à l'espace caractéristique F_2. Si on considère une telle restriction, il est clair que

$$\dim\ker\left((A-2I)_{|F_2}\right)^k = \dim\ker(A-2I)^k = 5 - \operatorname{rg}(A-2I)^k;$$

en effet, c'est une conséquence du théorème de stabilisation des noyaux : si $(A-2I)^k x = 0$, alors $x \in F_2$. Cette remarque montre donc que l'on peut raisonner sur le rang des puissances de la matrice $A - 2I$ sans se préoccuper d'une éventuelle restriction,

$$\dim\ker\left((A-2I)_{|F_2}\right)^k - \dim\ker\left((A-2I)_{|F_2}\right)^{k-1} = \operatorname{rg}(A-2I)^{k-1} - \operatorname{rg}(A-2I)^k.$$

forme du tableau d'une base de F_3 répartie en chaînes est donnée par les formules suivantes :

hauteur de la colonne 1 : $5 - \mathrm{rg}(A - 3I) = 5 - 4 = 1$,
hauteur de la colonne 2 : $\mathrm{rg}(A - 3I) - \mathrm{rg}(A - 3I)^2 = 4 - 3 = 1$.

Ce tableau a donc la forme

*	*

Le vecteur $2e_1 + e_5$ est la tête d'une chaîne engendrée par $A - 3I$ de longueur 2. En effet,

$$(A - 3I)^2(2e_1 + e_5) = 0 \text{ et } (A - 3I)(2e_1 + e_5) = -e_1 + e_4.$$

Remarque XI.14.5. La longueur maximale d'une chaîne de la base de F_2 (resp. F_3) répartie en chaîne étant 2 (resp. 2), on en déduit que le polynôme minimum de A est

$$(\lambda - 2)^2(\lambda - 3)^2.$$

Nous pouvons à présent considérer la matrice S donnée par

$$\begin{pmatrix} 1 & 0 & 0 & -1 & 2 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & -2 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

A titre indicatif,

$$S^{-1} = \begin{pmatrix} -2 & 2 & 3 & -2 & 4 \\ 1 & 0 & -1 & 1 & -2 \\ -1 & 1 & 1 & -1 & 2 \\ -1 & 0 & 1 & 0 & 2 \\ 1 & -1 & -1 & 1 & -1 \end{pmatrix}.$$

Il est clair que

$$S^{-1}AS = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 3 \end{pmatrix}.$$

Remarque XI.14.6. Par des raisonnements analogues à ceux développés à la remarque XI.14.3, on trouve

$$A^n = S \begin{pmatrix} 2^n & n2^{n-1} & 0 & 0 & 0 \\ 0 & 2^n & 0 & 0 & 0 \\ 0 & 0 & 2^n & 0 & 0 \\ 0 & 0 & 0 & 3^n & n3^{n-1} \\ 0 & 0 & 0 & 0 & 3^n \end{pmatrix} S^{-1}.$$

Remarque XI.14.7. On aurait pu placer les colonnes de S dans un autre ordre (en plaçant bien évidemment les vecteurs d'une même chaîne de manière consécutive dans les colonnes de S'). Par exemple,

$$S' = \begin{pmatrix} -1 & 2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & -2 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix} \text{ et } S'^{-1} = \begin{pmatrix} -1 & 0 & 1 & 0 & 2 \\ 1 & -1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 2 \\ -2 & 2 & 3 & -2 & 4 \\ 1 & 0 & -1 & 1 & -2 \end{pmatrix}$$

donnent

$$S'^{-1}AS' = \begin{pmatrix} 3 & 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}.$$

On pourrait aussi renverser l'ordre des vecteurs au sein d'une même chaîne (en commençant par les têtes et non les queues). Par exemple, si on prend

$$S'' = \begin{pmatrix} 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & -2 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix},$$

on trouve

$$S''^{-1} = \begin{pmatrix} 1 & -1 & -1 & 1 & -1 \\ -1 & 0 & 1 & 0 & 2 \\ 1 & 0 & -1 & 1 & -2 \\ -2 & 2 & 3 & -2 & 4 \\ -1 & 1 & 1 & -1 & 2 \end{pmatrix}$$

Une réduction australienne...

et

$$S''^{-1}AS'' = \begin{pmatrix} 3 & 0 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}.$$

Remarque XI.14.8. Tout comme à la remarque XI.5.4 qui concernait les matrices diagonalisables, si $\lambda_1, \ldots, \lambda_p$ sont les valeurs propres distinctes de $A \in \mathbb{C}_n^n$, alors pour tout entier k

$$(A^k)_{i,j} = \sum_{\ell=1}^{p} P_{i,j}^{(\ell)} \lambda_\ell^k$$

où les $P_{i,j}^{(\ell)}$ est un polynôme tel que

$$\deg P_{i,j}^{(\ell)} < m_\ell.$$

On retrouve donc en particulier le résultat de la remarque XI.5.4, car si une matrice est diagonalisable, alors $m_\ell = 1$ pour tout $\ell = 1, \ldots, p$.

15. Résumé du chapitre

Soit T un endomorphisme de $\mathcal{L}(E)$ ayant $\lambda_1, \ldots, \lambda_p$ comme valeurs propres distinctes.

Premier cas :

L'endomorphisme T est diagonalisable si et seulement si

$$E = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_p}.$$

Dans ce cas, on a une base formée de vecteurs propres de E dans laquelle T se représente par une matrice diagonale (il suffit de prendre pour base de E une union de bases de chacun des E_{λ_j}).

Bien sûr, chaque E_{λ_j} est stable pour T, $T(E_{\lambda_j}) \subseteq E_{\lambda_j}$.

Rappelons que pour vérifier qu'un endomorphisme est diagonalisable, il faut et il suffit que les multiplicités algébrique et géométrique de chaque valeur propre coïncident.

Second cas :

L'endomorphisme T n'est pas diagonalisable, on a

$$E \supsetneq E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_p}.$$

Il nous faut alors introduire les sous-espaces caractéristiques $F_{\lambda_1}, \ldots, F_{\lambda_p}$ où

$$F_{\lambda_j} = \ker\left(T_j^{m_j}\right)$$

avec $T_j = T - \lambda_j\, id$ et m_j est la multiplicité de λ_j comme zéro du polynôme minimum de T. (Pour rappel, la notion de polynôme minimum découle du théorème de Cayley-Hamilton et du fait que $\mathbb{C}[z]$ est un anneau principal).
Ces sous-espaces caractéristiques ont deux propriétés fort agréables :

- $E = F_{\lambda_1} \oplus \cdots \oplus F_{\lambda_p}$,
- chaque F_{λ_j} est stable pour T, i.e., $T(F_{\lambda_j}) \subseteq F_{\lambda_j}$.

Pour la première, la démonstration fait appel aux projecteurs spectraux.

Ainsi, dans une base de E obtenue comme union de bases de chacun des F_{λ_j}, T se représente par une matrice composée diagonale (chaque bloc diagonal étant de dimension égale à la dimension de F_{λ_j}, à savoir la multiplicité algébrique μ_j de λ_j comme zéro du polynôme caractéristique de T).

On peut encore faire mieux qu'une réduction à une forme diagonale composée en choisissant des bases particulières des F_{λ_j}. Il est clair que T_j restreint à F_{λ_j} est un opérateur nilpotent. On peut donc construire une base de F_{λ_j} répartie en chaînes engendrées par T_j.

Pensez à la définition de F_{λ_j}.

On note que :

- Pour une base de F_{λ_j} répartie en chaînes mise sous forme d'un tableau où chaque ligne correspond à une chaîne, bien que la base ne soit pas unique, la forme du tableau est quant à elle unique — si les lignes sont disposées par longueur décroissante, la k-ième colonne du tableau contient exactement $\mathrm{rg}(T_{j|F_{\lambda_j}})^{k-1} - \mathrm{rg}(T_{j|F_{\lambda_j}})^k$ éléments.

  Dans le cas particulier d'une matrice $A \in \mathbb{C}_n^n$, il est facile de se convaincre que cette formule devient

$$\mathrm{rg}(A - \lambda_j I)^{k-1} - \mathrm{rg}(A - \lambda_j I)^k.$$

- L'enveloppe linéaire d'une chaîne engendrée par T_j est stable pour T.

Ce choix de base de E fournit une représentation de l'endomorphisme T réduit à la forme de Jordan. On a autant de blocs de Jordan

$$\begin{pmatrix} \lambda_j & 1 & 0 & \cdots & 0 \\ 0 & \lambda_j & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \lambda_j \end{pmatrix}$$

associés à la valeur propre λ_j que de lignes dans le tableau de la base de F_{λ_j} répartie en chaînes. Les tailles de ces blocs sont exactement les longueurs des chaînes de la base de F_{λ_j} répartie en chaînes.

CHAPITRE XII

Matrices particulières

1. Retour sur le produit scalaire

Commençons par quelques rappels concernant le produit scalaire de $\mathbb{C}^n$. Si x et y sont deux vecteurs de $\mathbb{C}^n$, le produit scalaire (canonique) de ceux-ci est donné par $\langle x, y\rangle = y^* x$. Ces deux vecteurs sont *orthogonaux* si $\langle x, y\rangle = 0$. Un vecteur x est normé, si sa norme $|x| = \sqrt{\langle x, x\rangle}$ vaut 1. Pour plus de détails, se rapporter à la définition III.5.3.

Définition XII.1.1. Des vecteurs $x_1, \ldots, x_p \in \mathbb{C}^n$ sont *orthonormés* s'ils sont normés et deux à deux orthogonaux, i.e.,

$$\langle x_i, x_j\rangle = \delta_{i,j}, \quad \forall i, j \in \{1, \ldots, p\}.$$

Proposition XII.1.2. *Des vecteurs non nuls $x_1, \ldots, x_p$ orthogonaux deux à deux sont linéairement indépendants.*

Démonstration. Soient des nombres complexes $\lambda_1, \ldots, \lambda_p$. Supposons que

$$\lambda_1 x_1 + \cdots + \lambda_p x_p = 0.$$

En considérant le produit scalaire avec x_i, $i \in \{1, \ldots, p\}$, on trouve

$$\langle \lambda_1 x_1 + \cdots + \lambda_p x_p, x_i\rangle = \lambda_1 \langle x_1, x_i\rangle + \cdots + \lambda_p \langle x_p, x_i\rangle = \lambda_i |x_i|^2 = 0.$$

Par conséquent, $\lambda_1 = \cdots = \lambda_p = 0$ et les vecteurs sont linéairement indépendants.

■

Le produit scalaire permet de calculer les composantes d'un vecteur dans une base donnée.

Proposition XII.1.3. *Soient $x_1, \ldots, x_p$ des vecteurs non nuls orthogonaux deux à deux. Si*

$$x = \sum_{i=1}^{p} \lambda_i \, x_i,$$

alors

$$\lambda_i = \frac{\langle x, x_i\rangle}{|x_i|^2}.$$

Démonstration. C'est immédiat. En multipliant par x_j, $j \in \{1, \ldots, p\}$, on a

$$\langle x, x_j\rangle = \sum_{i=1}^{p} \lambda_i \, \langle x_i, x_j\rangle = \sum_{i=1}^{p} \lambda_i \, \delta_{ij} |x_i|^2 = \lambda_j |x_j|^2.$$

Ceci achève la preuve.

■

Proposition XII.1.4. [1] *[Procédé d'orthogonalisation de Gram-Schmidt] Soit p vecteurs linéairement indépendants $x_1, \ldots, x_p$. Il existe p vecteurs combinaisons linéaires de ceux-ci qui sont non nuls et orthogonaux deux à deux.*

Démonstration. On procède par récurrence sur p. Si $p = 2$, on a

$$\langle x_2 + \lambda x_1, x_1 \rangle = \langle x_2, x_1 \rangle + \lambda |x_1|^2.$$

Ce produit scalaire est nul si et seulement si

$$\lambda = -\frac{\langle x_2, x_1 \rangle}{|x_1|^2}.$$

Les vecteurs x_1 et $x_2' = x_2 - \frac{\langle x_2, x_1 \rangle}{|x_1|^2} x_1$ sont orthogonaux. De plus, x_1 et x_2 étant linéairement indépendants, x_2' est non nul.

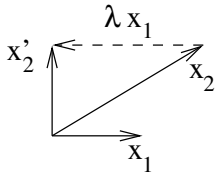


FIGURE XII.1. Orthogonalisation de Gram-Schmidt.

Supposons à présent que $x_1', \ldots, x_{p-1}'$ sont $p-1$ vecteurs orthogonaux deux à deux, non nuls, combinaisons linéaires de $x_1, \ldots, x_{p-1}$. Pour tout vecteur x et tout $j \in \{1, \ldots, p-1\}$, on a

$$\langle x - \sum_{i=1}^{p-1} \lambda_i x_i', x_j' \rangle = \langle x, x_j' \rangle - \sum_{i=1}^{p-1} \lambda_i \langle x_i', x_j' \rangle = \langle x, x_j' \rangle - \lambda_j |x_j'|^2.$$

Ainsi, $x - \sum_{i=1}^{p-1} \lambda_i x_i'$ est orthogonal à $x_1', \ldots, x_{p-1}'$ si et seulement si

$$\lambda_j = \frac{\langle x, x_j' \rangle}{|x_j'|^2}.$$

En particulier,

$$x_p - \sum_{i=1}^{p-1} \frac{\langle x_p, x_i' \rangle}{|x_i'|^2} x_i'$$

est un vecteur orthogonal à $x_1', \ldots, x_{p-1}'$. De plus, il est non nul car $x_1', \ldots, x_{p-1}'$ sont combinaisons linéaires de $x_1, \ldots, x_{p-1}$ et par hypothèse, x_p ne peut être combinaison linéaire de ceux-ci.

■

[1] Ce résultat s'énonce aussi en disant qu'à partir des vecteurs linéairement indépendants $x_1, \ldots, x_p$, on peut construire p vecteurs orthogonaux $y_1, \ldots, y_p$ tels que $\rangle x_1, \ldots, x_p \langle = \rangle y_1, \ldots, y_p \langle$.

Remarque XII.1.5. Si $x_1, \ldots, x_p$ sont des vecteurs non nuls orthogonaux deux à deux, alors $\frac{x_1}{|x_1|}, \ldots, \frac{x_p}{|x_p|}$ sont des vecteurs orthonormés. Ainsi, grâce au procédé d'orthogonalisation de Gram-Schmidt, il est clair que tout sous-espace vectoriel de $\mathbb{C}^n$ possède toujours une base orthonormée.

Proposition XII.1.6. *Si $B = (e_1, \ldots, e_p)$ est une base orthonormée d'un sous-espace vectoriel E de $\mathbb{C}^n$, alors pour tous $x, y \in E$,*

$$x = \sum_{i=1}^{p} \langle x, e_i \rangle \, e_i.$$

Autrement dit, la i-ième composante d'un vecteur x dans une base orthonormée est le produit scalaire de x avec le i-ième vecteur de base. De plus,

$$\langle x, y \rangle = \sum_{i=1}^{p} \langle x, e_i \rangle \, \overline{\langle y, e_i \rangle}.$$

Autrement dit, si $(x_1, \ldots, x_p)$ et $(y_1, \ldots, y_p)$ sont les composantes respectives de x et y dans B, alors

$$\langle x, y \rangle = \sum_{i=1}^{p} x_i \, \overline{y_i}, \quad \text{et} \quad |x|^2 = \sum_{i=1}^{p} |x_i|^2.$$

Démonstration. La première partie de cette proposition est une conséquence directe de la proposition XII.1.3.

Passons à la seconde partie. Puisque B est une base, $x = \sum_i x_i e_i$ et $y = \sum_j y_j e_j$. Ainsi, par linéarité du produit scalaire sur le premier facteur et antilinéarité sur le second facteur,

$$\langle x, y \rangle = \langle \sum_{i=1}^{p} x_i e_i, \sum_{j=1}^{p} y_j e_j \rangle = \sum_{i=1}^{p} \sum_{j=1}^{p} x_i \overline{y_j} \langle e_i, e_j \rangle.$$

Puisque B est orthonormé, il vient

$$\langle x, y \rangle = \sum_{i=1}^{p} x_i \, \overline{y_i} = \sum_{i=1}^{p} \langle x, e_i \rangle \, \overline{\langle y, e_i \rangle}$$

où, pour la dernière égalité, on a utilisé la première partie de cette proposition.

■

Exemple XII.1.7. Soient les trois vecteurs

$$x_1 = \begin{pmatrix} 1 \\ 0 \\ i \end{pmatrix}, \; x_2 = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}, \; x_3 = \begin{pmatrix} i \\ 1 \\ 0 \end{pmatrix}.$$

Construisons une base orthonormée de $\mathbb{C}^3$ de manière telle que les vecteurs de base soient combinaisons linéaires de x_1, x_2, x_3. Construisons une base

orthogonale au moyen du procédé d'orthogonalisation de Gram-Schmidt. Posons $x'_1 = x_1$,

$$x'_2 = x_2 - \frac{\langle x_2, x'_1\rangle}{|x'_1|^2} x'_1 = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} - \frac{(-i).(-1)}{2} \begin{pmatrix} 1 \\ 0 \\ i \end{pmatrix} = \begin{pmatrix} -i/2 \\ 1 \\ -1/2 \end{pmatrix}$$

et

$$x'_3 = x_3 - \frac{\langle x_3, x'_1\rangle}{|x'_1|^2} x'_1 - \frac{\langle x_3, x'_2\rangle}{|x'_2|^2} x'_2 = \begin{pmatrix} i \\ 1 \\ 0 \end{pmatrix} - \frac{i}{2} \begin{pmatrix} 1 \\ 0 \\ i \end{pmatrix} - \frac{1}{3} \begin{pmatrix} -i/2 \\ 1 \\ -1/2 \end{pmatrix} = \frac{2}{3} \begin{pmatrix} i \\ 1 \\ 1 \end{pmatrix}.$$

On vérifie aisément que x'_1, x'_2, x'_3 sont orthogonaux. On obtient une base orthonormée en normant ces vecteurs, $|x'_1| = \sqrt{2}$, $|x'_2| = \sqrt{3/2}$, $|x'_3| = 2/\sqrt{3}$. On a donc la base orthonormée suivante

$$e_1 = \frac{x'_1}{|x'_1|} = \frac{\sqrt{2}}{2} \begin{pmatrix} 1 \\ 0 \\ i \end{pmatrix},\ e_2 = \frac{x'_2}{|x'_2|} = \frac{\sqrt{6}}{3} \begin{pmatrix} -i/2 \\ 1 \\ -1/2 \end{pmatrix},\ e_3 = \frac{x'_3}{|x'_3|} = \frac{\sqrt{3}}{3} \begin{pmatrix} i \\ 1 \\ 1 \end{pmatrix}.$$

Recherchons à présent les composantes du vecteur

$$z = \begin{pmatrix} 2i \\ 1+i \\ 1 \end{pmatrix}$$

dans cette base orthonormée. Pour ce faire, il suffit de calculer les produits scalaires suivants,

$$\langle z, e_1\rangle = \frac{\sqrt{2}}{2} i,\ \langle z, e_2\rangle = -\frac{\sqrt{6}}{6} + \frac{\sqrt{6}}{3} i,\ \langle z, e_3\rangle = \frac{4\sqrt{3}}{3} + \frac{\sqrt{3}}{3} i.$$

On pourra vérifier que

$$z = \frac{\sqrt{2}}{2} i\, e_1 + (-\frac{\sqrt{6}}{6} + \frac{\sqrt{6}}{3} i)\, e_2 + (\frac{4\sqrt{3}}{3} + \frac{\sqrt{3}}{3} i)\, e_3.$$

2. Matrices normales, hermitiennes, unitaires

Proposition XII.2.1. *Soient A, B deux matrices de $\mathbb{C}^n_n$. On a*

$$\langle x, Ay\rangle = \langle Bx, y\rangle, \quad \forall x, y \in \mathbb{C}^n$$

si et seulement si $A = B^*$ (ou $A^* = B$).

Démonstration. La condition est suffisante car

$$\langle x, Ay\rangle = (Ay)^* x = y^*(A^* x) = \langle A^* x, y\rangle.$$

Elle est aussi nécessaire car si $\langle x, Ay\rangle = \langle Bx, y\rangle$ pour tous $x, y \in \mathbb{C}^n$, alors

$$\langle A^* x, y\rangle = \langle Bx, y\rangle$$

est satisfait en particulier pour $x = e_j$ et $y = e_k$ (e_j et e_k étant deux vecteurs unitaires, $j, k \in \{1, \ldots, n\}$). De là, pour tous j, k, on a

$$(A^*)_{k,j} = \widetilde{e_k} A^* e_j = \langle A^* e_j, e_k\rangle = \langle Be_j, e_k\rangle = \widetilde{e_k} B e_j = (B)_{k,j}.$$

■

Les deux corollaires suivants découlent directement de la proposition précédente.

Corollaire XII.2.2. *On a*

$$\langle Ax, y\rangle = \langle x, Ay\rangle, \quad \forall x, y \in \mathbb{C}^n$$

si et seulement si A est hermitien, i.e., $A = A^*$.

Définition XII.2.3. Une matrice $U \in \mathbb{C}_n^n$ est *unitaire* si $U^*U = I$.

Corollaire XII.2.4. *On a*

$$\langle Ax, Ay\rangle = \langle x, y\rangle, \quad \forall x, y \in \mathbb{C}^n$$

si et seulement si A est unitaire, i.e., $A^*A = I$.

Démonstration. En effet, on a $\langle Ax, Ay\rangle = \langle A^*Ax, y\rangle$.

■

La proposition qui suit montre en particulier que le calcul de l'inverse d'une matrice unitaire est particulièrement simple.

Proposition XII.2.5. *Soit U une matrice unitaire, i.e., $U^*U = I$.*

- *Le déterminant de U est de module 1. En particulier, U est inversible.*
- *On a $U^{-1} = U^*$ et dès lors, $UU^* = I$.*
- *Réciproquement, si $T \in \mathbb{C}_n^n$ est tel que $TT^* = I$ ou $T^{-1} = T^*$, alors T est unitaire.*
- *Le produit de deux matrices unitaires est unitaire.*
- *L'inverse d'une matrice unitaire est unitaire.*
- *Une matrice est unitaire si et seulement si ses colonnes sont orthonormées.*

Démonstration. Les trois premiers points sont immédiats. Il suffit d'observer que

$$\det(U^*U) = \overline{\det U} \det U = |\det U|^2 = 1.$$

Soient T et V deux matrices unitaires. On a[2]

$$(TV)^{-1} = V^{-1}T^{-1} = V^*T^* = (TV)^*$$

et

$$(T^{-1})^{-1} = T = (T^*)^* = (T^{-1})^*.$$

Pour le dernier point, si $U = \begin{pmatrix} C_1 & \cdots & C_n \end{pmatrix}$ où les C_i sont les colonnes de U. L'égalité $U^*U = I$ se réécrit

$$\begin{pmatrix} C_1^* \\ \vdots \\ C_n^* \end{pmatrix} \begin{pmatrix} C_1 & \cdots & C_n \end{pmatrix} = I$$

[2]Ceci montre en particulier que l'ensemble des matrices unitaires forment un sous-groupe du groupe $\mathrm{GL}_n(\mathbb{C})$ des matrices inversibles (pour l'opération de multiplication matricielle).

ou encore

$$C_i^* C_j = \delta_{i,j}, \quad \forall i, j \in \{1, \ldots, n\}$$

c'est-à-dire, $\langle C_j, C_i \rangle = \delta_{i,j}$. Ceci signifie que les colonnes de U sont orthonormées si et seulement si $U^*U = I$.

■

Exemple XII.2.6. Voici une matrice unitaire et son inverse (on a repris les vecteurs orthonormés de l'exemple XII.1.7),

$$U = \begin{pmatrix} \sqrt{2}/2 & -i\sqrt{6}/6 & i\sqrt{3}/3 \\ 0 & \sqrt{6}/3 & \sqrt{3}/3 \\ i\sqrt{2}/2 & -\sqrt{6}/6 & \sqrt{3}/3 \end{pmatrix}$$

et

$$U^{-1} = U^* = \begin{pmatrix} \sqrt{2}/2 & 0 & -i\sqrt{2}/2 \\ i\sqrt{6}/6 & \sqrt{6}/3 & -\sqrt{6}/6 \\ -i\sqrt{3}/3 & \sqrt{3}/3 & \sqrt{3}/3 \end{pmatrix}.$$

Nous allons à présent nous intéresser à la question suivante : quelles sont les matrices N diagonalisables par une matrice unitaire ? En d'autres termes quelles sont les matrices N pour lesquelles il existe U unitaire tel que

$$U^{-1} N U = U^* N U = \operatorname{diag}(\lambda_1, \ldots, \lambda_n).$$

En particulier, si N est une telle matrice, cela signifie que N possède n vecteurs propres orthonormés.

Puisque

$$N = U \underbrace{\operatorname{diag}(\lambda_1, \ldots, \lambda_n)}_{:=D} U^*,$$

il vient

$$NN^* = UDU^*(UDU^*)^* = UDU^*UD^*U^* = UDD^*U^*$$

et

$$N^*N = UD^*U^*UDU^* = UD^*DU^*.$$

Or $DD^* = D^*D = \operatorname{diag}(|\lambda_1|^2, \ldots, |\lambda_n|^2)$ et donc, une condition nécessaire pour que N soit diagonalisable par une matrice unitaire est que

$$NN^* = N^*N.$$

En fait, nous allons voir que cette condition est aussi suffisante (cf. théorème XII.2.11). Il est donc naturel d'introduire la définition suivante.

Définition XII.2.7. Une matrice $N \in \mathbb{C}_n^n$ est *normale* si

$$N^*N = NN^*.$$

Remarque XII.2.8. Les matrices hermitiennes et unitaires sont en particulier normales.

Lemme XII.2.9. *Si x est un vecteur propre associé à la valeur propre λ d'une matrice normale $N \in \mathbb{C}_n^n$, alors x est aussi vecteur propre associé à $\overline{\lambda}$ de la matrice N^*.*

Démonstration. On a

$$\begin{aligned}\langle (N-\lambda I)x, (N-\lambda I)x\rangle &= \langle x, (N-\lambda I)^*(N-\lambda I)x\rangle \\ &= \langle x, (N-\lambda I)(N-\lambda I)^* x\rangle \\ &= \langle (N-\lambda I)^* x, (N-\lambda I)^* x\rangle\end{aligned}$$

car, à la première et à la troisième ligne, on a utilisé la proposition XII.2.1 et à la deuxième, le caractère normal de N. Dès lors, $|(N-\lambda I)x| = |(N^*-\overline{\lambda} I)x|$.

■

Proposition XII.2.10. *Des vecteurs propres d'une matrice normale $N \in \mathbb{C}_n^n$ associés à des valeurs propres distinctes sont orthogonaux.*

Démonstration. Soient x et y des vecteurs propres de N de valeur propre λ et μ respectivement. Par la proposition XII.2.1, on a

$$\langle Nx, y\rangle = \langle x, N^* y\rangle$$

et dès lors, par le lemme précédent,

$$\langle \lambda x, y\rangle = \langle x, \overline{\mu} y\rangle = \mu\langle x, y\rangle.$$

De là, $\lambda\langle x, y\rangle = \mu\langle x, y\rangle$. Ceci permet de conclure car λ diffère de μ.

■

Le résultat suivant complète notre constatation initiale et montre qu'une matrice est diagonalisable par une matrice unitaire si et seulement si elle est normale.

Théorème XII.2.11. *Toute matrice normale est diagonalisable par une matrice unitaire.*

Démonstration. Soient $\lambda_1, \ldots, \lambda_p$ les valeurs propres distinctes de la matrice normale N et

$$x_{j,1}, \ldots, x_{j,d_j}, \quad j \in \{1, \ldots, p\}$$

une base de l'espace propre E_{λ_j}. Grâce au procédé d'orthogonalisation de Gram-Schmidt et au vu de la proposition précédente, nous pouvons supposer les $r = d_1 + \cdots + d_p$ vecteurs

$$x_{1,1}, \ldots, x_{1,d_1}, \ldots, x_{p,1}, \ldots, x_{p,d_p}$$

orthonormés. Si $r = n$, le résultat est démontré. La matrice ayant ces vecteurs pour colonnes est unitaire et diagonalise N.

Supposons $r < n$. On peut compléter la famille de vecteurs ci-dessus par des vecteurs $y_{r+1}, \ldots, y_n$ pour obtenir une base orthonormée de $\mathbb{C}^n$. Soit la matrice unitaire $U = \begin{pmatrix} C_1 & \cdots & C_n \end{pmatrix}$ dont les colonnes sont

$$x_{1,1}, \ldots, x_{1,d_1}, \ldots, x_{p,1}, \ldots, x_{p,d_p}, y_{r+1}, \ldots, y_n.$$

Il vient pour $j, k \in \{1, \ldots, n\}$,

$$(U^* N U)_{j,k} = \langle U^* N U\, e_k, e_j\rangle = \langle NU\, e_k, U\, e_j\rangle = \langle NC_k, C_j\rangle.$$

Si $k \in \{1, \dots, r\}$, alors la colonne C_k est de la forme x_{ℓ_k, m_k} avec $1 \leq \ell_k \leq p$ et $1 \leq m_k \leq d_{\ell_k}$. Dès lors, $NC_k = \lambda_{\ell_k} C_k$ et

$$(U^*NU)_{j,k} = \lambda_{\ell_k} \langle C_k, C_j \rangle = \lambda_{\ell_k} \delta_{j,k}.$$

De la même façon, on a aussi $(U^*NU)_{j,k} = \langle NU\, e_k, U\, e_j \rangle = \langle C_k, N^* C_j \rangle$ et si $j \in \{1, \dots, r\}$, alors

$$(U^*NU)_{j,k} = \lambda_{\ell_j} \delta_{j,k}.$$

Par conséquent,

$$U^*NU = \begin{pmatrix} D & 0 \\ 0 & M \end{pmatrix}$$

avec D une matrice carrée diagonale de dimension r et M, une matrice carrée de dimension $n-r$. La matrice M possède[3] au moins un vecteur propre non nul $z \in \mathbb{C}^{n-r}$ de valeur propre μ. Ainsi,

$$U^*NU \begin{pmatrix} 0 \\ z \end{pmatrix} = \mu \begin{pmatrix} 0 \\ z \end{pmatrix}$$

et

$$NU \begin{pmatrix} 0 \\ z \end{pmatrix} = \mu\, U \begin{pmatrix} 0 \\ z \end{pmatrix}.$$

Cette dernière relation montre que le vecteur $U \begin{pmatrix} 0 \\ z \end{pmatrix} = z_1 C_{r+1} + \cdots + z_{n-r} C_n$ est un vecteur propre non nul de N. Par conséquent[4], ce vecteur est aussi combinaison linéaire de $C_1, \dots, C_r$. De là, les vecteurs $C_1, \dots, C_r, C_{r+1}, \dots, C_n$ sont linéairement dépendants. Il s'agit d'une contradiction avec le fait que ces vecteurs forment une base de $\mathbb{C}^n$ d'où $n = r$.

■

Proposition XII.2.12. *On dispose des deux résultats suivants.*

- *Une matrice normale est hermitienne si et seulement si ses valeurs propres sont réelles.*
- *Une matrice normale est unitaire si et seulement si ses valeurs propres sont de module* 1*.*

Démonstration. Soit N une matrice hermitienne (resp. unitaire) et x un vecteur propre non nul de valeur propre λ. On a

$$\langle Nx, x \rangle = \langle x, Nx \rangle \quad (\text{resp. } \langle Nx, x \rangle = \langle x, N^{-1}x \rangle).$$

[3] En vertu du théorème fondamental de l'algèbre, une matrice $T \in \mathbb{C}_n^n$ possède toujours n valeurs propres comptées avec leur multiplicité. Si λ est une de ces valeurs propres, le système $(T - \lambda I)x = 0$ n'est pas de Cramer et possède donc une solution non nulle.

[4] En effet, tout vecteur propre de N appartient à l'un des espaces propres E_{λ_j} (avec $j \in \{1, \dots, p\}$) et s'obtient donc comme combinaison linéaire de $x_{j,1}, \dots, x_{j,d_j}$ qui ne sont autre que certaines colonnes C_k de U pour $k \leq r$.

De là[5],

$$\lambda\langle x,x\rangle = \overline{\lambda}\langle x,x\rangle \quad (\text{resp. } \lambda\langle x,x\rangle = \frac{1}{\overline{\lambda}}\langle x,x\rangle).$$

Puisque x est non nul, $\langle x,x\rangle \neq 0$ et on en tire que $\lambda = \overline{\lambda}$ (resp. $|\lambda|^2 = 1$).

La condition est suffisante. Au vu du théorème précédent, une matrice normale N est diagonalisable par une matrice unitaire U. Ainsi,

$$U^*NU = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$$

où $\lambda_1, \ldots, \lambda_n$ sont les valeurs propres de N répétées suivant leur multiplicité. Dès lors,

$$N = U \operatorname{diag}(\lambda_1, \ldots, \lambda_n)\, U^* \text{ et } N^* = U \operatorname{diag}(\overline{\lambda_1}, \ldots, \overline{\lambda_n})\, U^*.$$

Si les valeurs propres sont réelles, on en tire directement que $N = N^*$, c'est-à-dire que N est hermitienne. Si les valeurs propres sont de module 1, alors

$$N^*N = U \operatorname{diag}(|\lambda_1|^2, \ldots, |\lambda_n|^2)\, U^* = I$$

et N est unitaire.

■

3. Matrices hermitiennes définies positives

Définition XII.3.1. Une matrice hermitienne $H \in \mathbb{C}_n^n$ est *définie positive* (resp. *définie négative*) si pour tout $x \in \mathbb{C}^n \setminus \{0\}$, on a[6]

$$\langle Hx, x\rangle > 0 \quad (\text{resp. } \langle Hx, x\rangle < 0).$$

Remarque XII.3.2. Une application usuelle des matrices hermitiennes définies positives ou négatives, en abrégé hdp ou hdn, réside en la recherche des extrema d'une fonction réelle et dérivable d'un ouvert de $\mathbb{R}^n$. En effet, si Ω est un ouvert de $\mathbb{R}^n$ et si f appartient à $C_2(\Omega)$, alors la *matrice hessienne* de f en $x \in \Omega$ est

$$H_f(x) = ((D_iD_jf)(x))_{1\leq i,j\leq n}.$$

En vertu du théorème d'interversion des dérivées, $H_f(x)$ est une matrice réelle symétrique (et donc en particulier, hermitienne). Le lien avec la recherche des extrema est fourni par le résultat suivant.

Soit $x_0 \in \Omega$ un point stationnaire de f. Si $H_f(x_0)$ est hdp (resp. hdn), alors x_0 est un minimum (resp. maximum) strict local de f dans Ω.

---

[5] Remarquons que si $A \in \mathbb{C}_n^n$ est une matrice inversible ayant un vecteur propre non nul x de valeur propre λ, alors $Ax = \lambda x$ et $A^{-1}Ax = \lambda A^{-1}x$, d'où $A^{-1}x = \frac{1}{\lambda}x$. De plus, λ ne peut être nul car une matrice inversible n'a pas de valeur propre nulle (le déterminant étant égal au produit des valeurs propres).

[6] *A priori* la quantité $\langle Hx, x\rangle$ pourrait être complexe, mais ici on a

$$\overline{\langle x, Hx\rangle} = \langle Hx, x\rangle = \langle x, H^*x\rangle = \langle x, Hx\rangle.$$

Remarque XII.3.3. Si $H \in \mathbb{C}_n^n$ est hdp, toutes ses valeurs propres sont strictement positives. Nous savons déjà que ses valeurs propres sont réelles. Soit x un vecteur propre non nul associé à la valeur propre λ. Il vient

$$\langle Hx, x\rangle > 0$$

car H est hdp. De là,

$$\langle \lambda x, x\rangle = \lambda |x|^2 > 0$$

et $\lambda > 0$.

La détermination du caractère hdp résulte de la proposition suivante.

Proposition XII.3.4. *Une matrice hermitienne $H \in \mathbb{C}_n^n$ est définie positive si et seulement si toutes les sous-matrices diagonales de H occupant le coin supérieur gauche ont un déterminant strictement positif.*

Ce résultat découle du lemme suivant.

Lemme XII.3.5. *Soit $H \in \mathbb{C}_n^n$ une matrice hermitienne. On désigne par $H_k = H_{(1,\dots,k;1,\dots,k)}$ la sous-matrice diagonale de H de dimension k occupant le coin supérieur gauche. Si $\det H_k \neq 0$ pour tout $k \in \{1,\dots,n\}$, alors il existe une matrice triangulaire supérieure S dont les éléments diagonaux sont tous égaux à 1 telle que*

$$S^* H S = \operatorname{diag}\left(\det H_1, \frac{\det H_2}{\det H_1}, \dots, \frac{\det H_n}{\det H_{n-1}}\right).$$

Démonstration. On procède par récurrence sur k en montrant que pour tout k, il existe une matrice triangulaire supérieure S_k dont les éléments diagonaux sont tous égaux à 1 telle que

$$S_k^* H_k S_k = \operatorname{diag}\left(\det H_1, \frac{\det H_2}{\det H_1}, \dots, \frac{\det H_k}{\det H_{k-1}}\right).$$

Le cas de base $k = 1$ est immédiat. Supposons la propriété satisfaite pour k et vérifions-la pour $k+1$. Si S_k effectue la réduction annoncée de H_k, H_{k+1} étant de la forme

$$H_{k+1} = \begin{pmatrix} H_k & v \\ v^* & c \end{pmatrix}$$

avec $v \in \mathbb{C}^k$ et $c \in \mathbb{C}$, alors nous allons montrer que

Le choix du vecteur $-H_k^{-1}v$ peut paraître artificiel mais n'est pas anodin.

$$S_{k+1} = \begin{pmatrix} S_k & -H_k^{-1}v \\ 0 & 1 \end{pmatrix}$$

réalise la réduction de H_{k+1}. Notons dès à présent qu'il s'agit bien d'une matrice triangulaire supérieure dont les éléments diagonaux sont égaux à 1.

Calculons

$$\begin{aligned} S_{k+1}^* H_{k+1} S_{k+1} &= \begin{pmatrix} S_k^* & 0 \\ -v^*(H_k^{-1})^* & 1 \end{pmatrix} \begin{pmatrix} H_k & v \\ v^* & c \end{pmatrix} \begin{pmatrix} S_k & -H_k^{-1}v \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} S_k^* & 0 \\ -v^* H_k^{-1} & 1 \end{pmatrix} \begin{pmatrix} H_k S_k & 0 \\ v^* S_k & c - v^* H_k^{-1} v \end{pmatrix} \\ &= \begin{pmatrix} S_k^* H_k S_k & 0 \\ 0 & c - v^* H_k^{-1} v \end{pmatrix} \end{aligned}$$

où à la deuxième ligne, on a utilisé le fait que H_k était hermitien, $H_k^{-1} = (H_k^*)^{-1} = (H_k^{-1})^*$. Il nous reste à calculer $\det(c - v^* H_k^{-1} v)$. Par les formules de Frobenius-Schur, on conclut que $\det H_{k+1} = \det(c - v^* H_k^{-1} v) \det H_k = (c - v^* H_k^{-1} v) \det H_k$.

■

Nous pouvons à présent démontrer la proposition XII.3.4.

Démonstration. La condition est suffisante. Au vu du lemme précédent, il existe une matrice inversible[7] S telle que $S^* H S = \operatorname{diag}(\alpha_1, \ldots, \alpha_n) := \Delta$ avec les α_i tous strictement positifs. Ainsi, $H = (S^{-1})^* \Delta S^{-1}$ et pour tout $x \in \mathbb{C}^n \setminus \{0\}$, on a

$$\langle Hx, x \rangle = x^* H x = (S^{-1}x)^* \Delta (S^{-1}x) = \sum_{i=1}^{n} \alpha_i \, |(S^{-1}x)_i|^2 > 0.$$

Ceci montre que H est hdp.

La condition est nécessaire. Supposons H hdp et considérons un vecteur non nul $x \in \mathbb{C}^n$ de la forme

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_k \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} x' \\ 0 \end{pmatrix}, \quad k \in \{1, \ldots, n\}, \ x' \in \mathbb{C}^k \setminus \{0\}.$$

Dès lors,

$$\langle Hx, x \rangle = \langle H_k x', x' \rangle > 0.$$

Cela signifie que H_k est hdp. Au vu de la remarque XII.3.3, les valeurs propres de H_k sont strictement positives et dès lors, par la proposition XI.3.11, $\det H_k > 0$. Ceci conclut la preuve.

■

Remarque XII.3.6. Avec des raisonnements semblables à ceux développés ci-dessus, il est facile de se convaincre qu'une matrice hdn a toutes ses valeurs propres strictement négatives et qu'une matrice H est hdn si et seulement si les déterminants des sous-matrices diagonales de H occupant le coin

[7] En effet, S est une matrice triangulaire dont les éléments diagonaux valent 1 et dès lors, $\det S = 1$.

En effet, si $\det H_1 < 0$, pour que $\frac{\det H_2}{\det H_1} < 0$, il est nécessaire que $\det H_2 > 0$ et ainsi de suite...

supérieur gauche sont alternativement strictement négatifs et strictement positifs.

4. Diagonalisation simultanée par des matrices normales

Le résultat démontré dans cette section est le suivant.

Proposition XII.4.1. *Des matrices normales $N_1, \dots, N_s \in \mathbb{C}_n^n$ sont diagonalisables simultanément par une même matrice unitaire si et seulement si elles commutent.*

Citons par exemple, qu'un tel résultat intervient notamment en physique ou en mécanique quantique. En effet, cette dernière discipline fait un usage fréquent des notions d'algèbre vue dans ce cours. Un lemme préalable est nécessaire.

Lemme XII.4.2. *Soit*

$$\Delta = \begin{pmatrix} \lambda_1 I_{d_1} & 0 & \cdots & 0 \\ 0 & \lambda_2 I_{d_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_p I_{d_p} \end{pmatrix}$$

où $\lambda_1, \dots, \lambda_p$ sont des nombres complexes distincts deux à deux. Une matrice $A \in \mathbb{C}_n^n$ commute avec Δ, i.e., $A\Delta = \Delta A$, si et seulement si A est une matrice composée diagonale

$$A = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & A_p \end{pmatrix}$$

où A_i est un bloc carré de dimension d_i, $i = 1, \dots, p$.

Démonstration. Soit A de la forme

$$A = \begin{pmatrix} A_{11} & \cdots & A_{1p} \\ \vdots & & \vdots \\ A_{p1} & \cdots & A_{pp} \end{pmatrix}$$

avec A_{ij} une matrice $d_i \times d_j$. En effectuant les produits matriciels suivants, on trouve

$$A\Delta = \begin{pmatrix} \lambda_1 A_{11} & \cdots & \lambda_p A_{1p} \\ \vdots & & \vdots \\ \lambda_1 A_{p1} & \cdots & \lambda_p A_{pp} \end{pmatrix}$$

et

$$\Delta A = \begin{pmatrix} \lambda_1 A_{11} & \cdots & \lambda_1 A_{1p} \\ \vdots & & \vdots \\ \lambda_p A_{p1} & \cdots & \lambda_p A_{pp} \end{pmatrix}.$$

De là, $A\Delta = \Delta A$ si et seulement si pour tout $i, j \in \{1, \dots, p\}$,

$$\lambda_i A_{ij} = \lambda_j A_{ij}.$$

Si $i \neq j$, alors $\lambda_i \neq \lambda_j$ et on en tire que $A_{ij} = 0$.

■

Nous pouvons passer à la preuve du résultat proprement dit.

Démonstration. Supposons qu'il existe une matrice unitaire U telle que pour tout $j \in \{1, \dots, s\}$,

$$U^* N_j U = \Delta_j$$

où Δ_j est une matrice diagonale. Dans ce cas,

$$N_j N_k = U\Delta_j U^* U \Delta_k U^* = U\Delta_j \Delta_k U^*$$

et

$$N_k N_j = U\Delta_k U^* U \Delta_j U^* = U\Delta_k \Delta_j U^* = U\Delta_j \Delta_k U^*$$

car des matrices diagonales commutent. De là, on en tire que $N_j N_k = N_k Nj$ pour tous $j, k \in \{1, \dots, s\}$.

Pour la réciproque, procédons par récurrence sur s, le cas $s = 1$ étant acquis.

Une seule matrice est toujours simultanément diagonalisable !

Puisque N_1 est une matrice normale, au vu du théorème XII.2.11, il existe une matrice unitaire U_1 telle que

$$U_1^* N_1 U_1 = \begin{pmatrix} \lambda_1 I_{d_1} & 0 & \cdots & 0 \\ 0 & \lambda_2 I_{d_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_p I_{d_p} \end{pmatrix}$$

où $\lambda_1, \dots, \lambda_p$ sont les valeurs propres distinctes de N_1 de multiplicité respective $d_1, \dots, d_p$. Par hypothèse, pour tout $j \in \{2, \dots, s\}$, $N_1 N_j = N_j N_1$ et de là, on en tire que $U_1^* N_1 U_1$ et $U_1^* N_j U_1$ commutent. Dès lors, par le lemme précédent, $U_1^* N_j U_1$ a nécessairement la forme suivante,

$$U_1^* N_j U_1 = \begin{pmatrix} N'_{j,1} & 0 & \cdots & 0 \\ 0 & N'_{j,2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & N'_{j,p} \end{pmatrix}$$

avec $N'_{j,i}$ une matrice normale[8] carrée de dimension d_i. Par hypothèse, pour tous $j, k \in \{2, \dots, s\}$, N_j et N_k commutent. Dès lors, $N'_{j,\ell}$ et $N'_{k,\ell}$ commutent aussi. Pour ℓ fixé dans $\{1, \dots, p\}$, on est en présence de $s - 1$ matrices normales

On se met dans les conditions pour appliquer l'hypothèse de récurrence.

$$N'_{2,\ell}, \dots, N'_{s,\ell}$$

[8]En effet, puisque N_j est normale, $(U_1^* N_j U_1)(U_1^* N_j U_1)^* = (U_1^* N_j U_1)^* (U_1^* N_j U_1)$ et de là, on en tire que $N'^*_{j,i} N'_{j,i} = N'_{j,i} N'^*_{j,i}$. Avec un développement semblable, on montre que, puisque N_j et N_k commutent, il en est de même pour $N'_{j,\ell}$ et $N'_{k,\ell}$.

qui commutent. Par hypothèse de récurrence, il existe une matrice unitaire U'_ℓ telle que

$$U'^*_\ell N'_{j,\ell} U'_\ell$$

soit une matrice diagonale. Vérifions que la matrice unitaire

$$U = U_1 \begin{pmatrix} U'_1 & 0 & \cdots & 0 \\ 0 & U'_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & U'_p \end{pmatrix}$$

Vérifiez-le ! diagonalise N_j pour tout $j \in \{1, \dots, s\}$. Il est clair que

$$U^* N_1 U = U_1^* N_1 U_1.$$

De plus, pour $j \in \{2, \dots, s\}$, il vient

$$U^* N_j U = \begin{pmatrix} U'^*_1 & 0 & \cdots & 0 \\ 0 & U'^*_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & U'^*_p \end{pmatrix} \underbrace{\begin{pmatrix} N'_{j,1} & 0 & \cdots & 0 \\ 0 & N'_{j,2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & N'_{j,p} \end{pmatrix}}_{U_1^* N_j U_1} \begin{pmatrix} U'_1 & 0 & \cdots & 0 \\ 0 & U'_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & U'_p \end{pmatrix}$$

et donc

$$U^* N_j U = \begin{pmatrix} U'^*_1 N'_{j,1} U'_1 & 0 & \cdots & 0 \\ 0 & U'^*_2 N'_{j,2} U'_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & U'^*_p N'_{j,p} U'_p \end{pmatrix}$$

est bien une matrice diagonale.

■

5. Le cas des matrices réelles

Dans cette courte section, nous énonçons simplement quelques faits ayant notamment un intérêt certain en géométrie euclidienne réelle[9].

Définition XII.5.1. Une matrice réelle $A \in \mathbb{R}^n_n$ telle que

$$\widetilde{A} A = I$$

est *orthogonale*.

Puisqu'une matrice orthogonale peut être vue comme un cas particulier de matrice unitaire (réelle), on en tire directement que si A est orthogonale, alors $\det A = \pm 1$, A est inversible et $A^{-1} = \widetilde{A}$. Réciproquement, si $B\widetilde{B} = I$, alors B est orthogonale. Les colonnes de A forment une base orthonormée de $\mathbb{R}^n$ et les valeurs propres de A sont de module 1.

[9] Pensez par exemple aux matrice de changement de bases orthonormées ou aux matrices de rotation.

Exemple XII.5.2. La matrice

$$\frac{1}{3}\begin{pmatrix} 2 & -2 & 1 \\ 1 & 2 & 2 \\ 2 & 1 & -2 \end{pmatrix}$$

est orthogonale et ses valeurs propres sont

$$-1, \frac{5+i\sqrt{11}}{6}, \frac{5-i\sqrt{11}}{6}.$$

Attirons l'attention du lecteur, s'il en était encore nécessaire, qu'une matrice réelle peut posséder des valeurs propres complexes.

Un polynôme réel possède lui aussi éventuellement des zéros complexes.

Exemple XII.5.3. La matrice de rotation

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$$

est aussi une matrice orthogonale.

Remarque XII.5.4. Le produit de deux matrices orthogonales (resp. l'inverse d'une matrice orthogonale) est encore une matrice orthogonale. De plus, la matrice identité étant orthogonale, l'ensemble des matrices orthogonales forment un sous-groupe de $GL_n(\mathbb{R})$, appelé *groupe orthogonal* et généralement noté $O(n)$. Notons encore que l'ensemble des matrices orthogonales de déterminant 1 est noté $SO(n)$, il s'agit encore d'un sous-groupe de $GL_n(\mathbb{R})$. En effet, le produit de deux matrices de déterminant 1 (resp. l'inverse d'une matrice de déterminant 1) est encore de déterminant 1.

Rappelons enfin qu'une matrice réelle $A \in \mathbb{R}_n^n$ *symétrique* est telle que $\widetilde{A} = A$. Puisqu'une matrice réelle symétrique est en particulier hermitienne, on en tire directement que ses valeurs propres sont réelles et que des vecteurs propres associées à des valeurs propres distinctes sont orthogonaux.

Par une démarche analogue à celle effectuée dans la preuve du théorème XII.2.11, on dispose du résultat suivant.

Proposition XII.5.5. *Toute matrice symétrique $A \in \mathbb{R}_n^n$ est diagonalisable par une matrice orthogonale.*

Remarque XII.5.6. La réciproque de cette proposition est également vraie. En effet, si S est une matrice orthogonale telle que $\widetilde{S}AS = \Delta$ où Δ est une matrice diagonale, alors

$$A = S\Delta\widetilde{S} = S\widetilde{\Delta}\widetilde{S} = \widetilde{A}$$

ce qui signifie que A est symétrique.

Exemple XII.5.7. Soit la matrice symétrique

$$A = \begin{pmatrix} 6 & -2 & -1 \\ -2 & 6 & -1 \\ -1 & -1 & 5 \end{pmatrix}.$$

Le polynôme caractéristique de A est

$$\chi_A(\lambda) = -(\lambda - 8)(\lambda - 6)(\lambda - 3).$$

Aux valeurs propres 8, 6 et 3 correspondent respectivement les vecteurs propres

$$\begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} -1 \\ -1 \\ 2 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Il est immédiat de vérifier que ces vecteurs sont orthogonaux. Pour construire une matrice orthogonale qui diagonalise A, il suffit de normer ces vecteurs. Ainsi, la matrice S est orthogonale

$$S = \begin{pmatrix} -\sqrt{2}/2 & -\sqrt{6}/6 & \sqrt{3}/3 \\ \sqrt{2}/2 & -\sqrt{6}/6 & \sqrt{3}/3 \\ 0 & 2\sqrt{6}/6 & \sqrt{3}/3 \end{pmatrix}$$

et telle que

$$\widetilde{S}AS = \operatorname{diag}(8, 6, 3).$$

Lettres grecques

L'écriture mathématique fait un usage fréquent des lettres grecques. Nous avons donc décidé de les rappeler ci-dessous.

minuscule	majuscule	
α		alpha
β		beta
γ	Γ	gamma
δ	Δ	delta
ϵ, ε		epsilon
ζ		zeta
η		eta
θ, ϑ	Θ	theta
ι		iota
κ		kappa
λ	Λ	lambda
μ		mu
ν		nu
ξ	Ξ	xi
o		omicron
π, ϖ	Π	pi
ρ		rho
σ, ς	Σ	sigma
τ		tau
υ	Υ	upsilon
ϕ, φ	Φ	phi
χ		chi
ψ	Ψ	psi
ω	Ω	omega

Bibliographie

[1] H. G. Campbell, *Linear Algebra with Applications*, Appleton-Century-Crofts, 1971.

[2] E. H. Connell, *Elements of Abstract and Linear Algebra*, University of Miami, 1999.

[3] K. J. Devlin, *The Millenium Problems: The Seven Greatest Unsolved Mathematical Puzzles of Our Time*, Basic Books, New-York, 2002.

[4] J. Dorst *et al.*, Encyclopédie des sciences, Vol. XIII, *Mathématiques*, Editions Erasme, 1976.

[5] J. Gilbert, L. Gilbert, *Linear Algebra and Matrix Theory*, Academic Press, 1994.

[6] R. Godement, *Analyse Mathématique I, Convergence, fonctions élémentaires*, 2ème édition corrigée, Springer, 2001.

[7] R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete Mathematics*, second edition, Addison-Wesley, 1994.

[8] P. P. Halmos, *Finite Dimensional Vector Spaces*, second edition, Van Nostrand, 1958.

[9] R. W. Hamming, *Introduction to Applied Numerical Analysis*, Hemisphere Publishing, 1971.

[10] J. Hefferon, *Linear Algebra*, Saint Michael's College, Colchester, Vermont.

[11] B. R. Hodgson, *On some sequences related to the parity of binomial coefficients*, Fibonacci Quart. **30**, 1992, 35–47.

[12] J.-M. De Koninck, A. Mercier, *Introduction à la théorie des nombres*, Modulo, 1994.

[13] S. Lang, *Linear Algebra*, Addison-Wesley, 1966.

[14] P. Laubin, *Algèbre linéaire, première candidature en sciences mathématiques*, Université de Liège, 1991.

[15] D. C. Lay, *Linear Algebra and Its Applications*, second edition, Addison-Wesley, 1997.

[16] F. Liret, D. Martinais, *Algèbre Licence 1ère année MIAS-MASS-SM*, Dunod, 2002.

[17] F. Liret, D. Martinais, *Algèbre et Géométrie 2e année*, Dunod, 2002.

[18] C. D. Meyer, *Matrix Analysis and Applied Linear Algebra*, Siam, Philapeldhia, 2000.

[19] M. Mignotte, *Mathématiques pour le calcul formel*, Presses Universitaires de France, 1989.

[20] M. Mignotte, *Algèbre concrète*, cours et exercices, Ellipses, Paris, 2003.

[21] E. D. Nering, *Linear Algebra and Matrix Theory*, second edition, John Wiley and Sons, 1963.

[22] K. Nomizu, *Fundamentals of Linear Algebra*, McGraw-Hill Book Company, 1966.

[23] V. Pless, *An introduction to the Theory of Error-Correcting Codes*, John Wiley and Sons, 1982.

[24] H. Roudier, *Algèbre linéaire, CAPES & Agrégation*, deuxième édition, Vuibert, 2003.

[25] J.-P. Schneiders, *Algèbre linéaire, première candidature en sciences mathématiques*, Université de Liège, 2001.

[26] V. Voïévodine, *Algèbre Linéaire*, Editions MIR, Moscou, 1976.

[27] T. A. Whitelaw, *Introduction to Abstract Algebra*, second edition, Blackie, 1988.

Liste des figures

Index

Notations

E

F

G

H

I