Structures algébriques
et
algèbre bilinéaire

Introduction

Ce texte est le polycopié du module Algèbre I de deuxième année de licence de mathématiques à Sorbonne Université pour l'année 2025-2026. Il se décompose en deux parties principales, qui correspondent au contenu du cours, et de plusieurs annexes, qui contiennent des compléments de cours facultatifs.

Dans la première partie, on introduit les structures algébriques fondamentales (les groupes, anneaux et corps) et leurs morphismes. En cours de route, on étudie aussi les relations d'équivalence et les quotients. Ensuite, on utilise la division euclidienne pour étudier les propriétés de l'anneau des entiers relatifs et de celui des polynômes sur un corps.

La deuxième partie commence par quelques rappels d'algèbre linéaire (matrices des applications linéaires, déterminants et diagonalisation). Elle se poursuit par l'étude de l'algèbre bilinéaire (formes bilinéaires symétriques, formes quadratiques). Son aboutissement est donné par les théorèmes de diagonalisation des endomorphismes autoadjoints réels et de diagonalisation simultanée. L'analogue complexe de cette théorie se trouve dans l'Annexe C et ne sera traité que si le temps le permet.

La lecture des Annexes A et B est facultative.

La partie I sur les structures algébriques a été rédigée par Frédéric Paugam. Une grande part de la partie algèbre linéaire et bilinéaire est une reprise directe des parties correspondantes du polycopié [2] de Patrick Polo et Laurent Koelblen, repris et revu par Vincent Humilière. Marco Maculan et Jean Roydor ont aussi participé à la relecture de certaines parties de ce polycopié. Tous sont ici remerciés pour leur précieuse contribution à ce texte.

Table des matières

I Structures algébriques et division euclidienne **7**

1 Structures algébriques **9**
1.1 Ensembles et applications . . . 9
1.2 Entiers naturels et principe de récurrence . . . 11
1.3 Opérations binaires et structures algébriques . . . 12
1.4 Relations d'ordre, relations d'équivalence et quotients . . . 16
1.4.1 Relations binaires . . . 16
1.4.2 La relation d'ordre sur les entiers naturels . . . 17
1.4.3 Relations d'équivalence, quotients et classes de nombres . . . 17
1.5 Sous-groupes et groupes quotients . . . 20
1.5.1 Sous-groupes . . . 20
1.5.2 Quotient d'un groupe abélien par un sous-groupe . . . 21
1.6 Idéaux et anneaux quotients . . . 22

2 Division euclidienne **25**
2.1 L'algèbre des polynômes sur un anneau . . . 25
2.2 Anneaux principaux et anneaux euclidiens . . . 27
2.3 Les anneaux $\mathbb{Z}$ et $K[X]$ sont euclidiens . . . 28
2.4 Diviseurs, multiples et algorithme de Bézout . . . 31
2.5 Éléments premiers d'un anneaux euclidien . . . 32
2.6 Polynôme minimal d'un endomorphisme . . . 34

II Algèbre linéaire et bilinéaire **37**

3 Rappels d'algèbre linéaire **39**
3.1 Espaces vectoriels et applications linéaires . . . 39
3.2 Quotients d'espaces vectoriels et théorème du rang . . . 43
3.3 Déterminant . . . 44
3.3.1 Déterminant des matrices 2×2 . . . 44
3.3.2 Déterminant sur un anneau . . . 45
3.3.3 Cas d'un corps . . . 53
3.4 Endomorphismes : déterminant, trace, valeurs propres, etc. . . . 54
3.5 Espaces propres et critères de diagonalisabilité . . . 56

4 Algèbre bilinéaire **61**
4.1 Dualité et équations intrinsèques . . . 61
4.2 Formes bilinéaires symétriques . . . 63
4.2.1 Définition . . . 63
4.2.2 Base duale, matrice d'une forme bilinéaire, adjoint . . . 64

4.2.3 Orthogonalité 66
4.3 Formes quadratiques 67
4.3.1 Définition 67
4.3.2 Bases orthogonales 68
4.3.3 Signature d'une forme quadratique 70
4.3.4 Réduction d'une forme quadratique en somme de carrés 71
4.4 Espaces euclidiens et diagonalisation simultanée 75
4.4.1 Espaces euclidiens. Inégalité de Cauchy-Schwarz. Isométries 75
4.4.2 Endomorphismes auto-adjoints et théorème de diagonalisation simultanée 80
4.5 Orthogonalité. Orthonormalisation de Gram-Schmidt 85

III Annexes **91**

A Les axiomes de Peano pour les entiers naturels **93**

B Catégories, endomorphismes et isomorphismes **97**

C Formes hermitiennes, espaces hilbertiens et groupes unitaires U(n) **101**
C.0 Rappels sur les nombres complexes 101
C.1 Formes hermitiennes 102
C.2 Réduction en sommes de carrés de modules 108
C.3 Espaces hilbertiens. Inégalité de Cauchy-Schwarz. Isométries 112
C.4 Diagonalisation des endomorphismes auto-adjoints et normaux 117
C.5 Forme normale des éléments de O(n) 120
C.6 Appendice (†) : espaces préhilbertiens réels ou complexes 124

Bibliographie **125**

Première partie

Structures algébriques et division euclidienne

Chapitre 1

Structures algébriques

Ce premier chapitre est relativement abstrait, mais les structures introduites et les relations qu'elles entretiennent, encodées par ce que l'on appellera leurs morphismes [1], seront utilisées et illustrées concrètement tout au long de la licence.

L'objectif de cette présentation initiale précoce de toutes ces idées et notions, accompagnée de nombreux exemples, est de permettre à chacun.e de disposer de suffisamment de temps pour les faire mâturer.

1.1 Ensembles et applications

Se donner une application $f : X \to Y$ entre deux ensembles X et Y, c'est se donner pour chaque x dans X un élément $f(x)$ de Y. On peut formaliser cela précisément en termes de sous-ensembles du produit $X \times Y$.

Définition 1.1. *Soient X et Y deux ensembles.*

1. *Une application $f : X \to Y$, appelée aussi un morphisme d'ensembles, est la donnée d'un sous-ensemble $\Gamma_f \subset X \times Y$ appelé son graphe, vérifiant la condition suivante : pour tout $x \in X$, il existe une unique paire de la forme (x, y) dans Γ_f. On écrit alors $y = f(x)$, et la connaissance de $f(x) \in Y$ pour tout $x \in X$ est équivalente à la connaissance de f, puisqu'on a l'égalité*
$$\Gamma_f = \{(x, f(x)), x \in X\} \subset X \times Y.$$
2. *L'application $\mathrm{id}_X : X \to X$ est définie par $\mathrm{id}_X(x) = x$ pour tout $x \in X$.*
3. *Si $f : X \to Y$ et $g : Y \to Z$ sont deux applications, leur composition $g \circ f : X \to Z$ est définie par $(g \circ f)(x) = g(f(x))$ pour tout $x \in X$.*
4. *On dit que deux applications $f, g : X \to Y$ sont égales si leurs graphes sont égaux, ce qui revient à dire que pour tout $x \in X$, on a l'égalité $f(x) = g(x)$.*
5. *Si X et Y sont des ensembles, on note $\mathrm{Hom}_{\mathrm{Ens}}(X, Y)$ ou Y^X l'ensemble des applications $f : X \to Y$.*

Le résultat suivant, bien qu'élémentaire, est fondamental.

Proposition 1.2. *Si $f : X \to Y$ est une application, alors on a les égalités*
$$f \circ \mathrm{id}_X = f \text{ et } \mathrm{id}_Y \circ f = f.$$

1. On pourra facultativement se référer en cours de lecture à l'Appendice B pour disposer d'un formalisme général des structures, morphismes et isomorphismes.

De plus, si $g : Y \to Z$ et $h : Z \to T$ sont deux autres applications, on a l'égalité

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

Démonstration. Si $x \in X$, on a $[f \circ \mathrm{id}_X](x) = f(\mathrm{id}_X(x)) = f(x)$. De même, si $x \in X$, on a $[\mathrm{id}_Y \circ f](x) = \mathrm{id}_Y(f(x)) = f(x)$. Enfin, si $x \in X$, on a

$$[h \circ (g \circ f)](x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = [(h \circ g) \circ f](x).$$

□

Définition 1.3. *Soit $f : X \to Y$ une application entre deux ensembles.*

1. *Pour $P \subset X$ et $Q \subset Y$ des parties, on note $f(P) = \{f(x),\ x \in P\}$ l'image de P et $f^{-1}(Q) = \{y \in X,\ f(y) \in Q\}$ l'image inverse de Q.*
2. *On dit que f est injective si pour tous $x_1, x_2 \in X$, on a l'implication*

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2,$$

   Ceci revient à dire que pour tout $y \in Y$, $f^{-1}(\{y\})$ est vide ou restreint à un point.
3. *On dit que f est surjective si pour tout $y \in Y$, il existe $x \in X$ tel que $f(x) = y$. Ceci revient à dire que $f(X) = Y$.*
4. *On dit que f est une bijection si elle est injective et surjective, i.e., si pour tout $y \in Y$, il existe un unique $x \in X$ tel que $f(x) = y$.*

Exemple 1.4. *Si X est un ensemble, l'application $X \to \{0\}$ qui envoie tout élément $x \in X$ sur 0 est surjective, sauf si X est vide. Si $Y \subset X$ est un sous-ensemble, l'application d'injection $i : Y \to X$ définie par $i(y) = y$ est injective.*

Proposition 1.5. *Une application $f : X \to Y$ entre deux ensembles non vides est :*

1. *surjective si et seulement si elle admet un inverse à droite, i.e., une application $s : Y \to X$ telle que $f \circ s = \mathrm{id}_Y$.*
2. *injective si et seulement si elle admet un inverse à gauche, i.e., une application $p : Y \to X$ telle que $p \circ f = \mathrm{id}_X$.*
3. *bijective si et seulement si elle admet un inverse à gauche et à droite, i.e., une application $g : Y \to X$ telle que $f \circ g = \mathrm{id}_Y$ et $g \circ f = \mathrm{id}_X$.*

Démonstration. Supposons que f est admet un inverse à droite s. Soit $y \in Y$ et posons $x = s(y)$. Alors $f(x) = f(s(y)) = y$ donc f est surjective. Supposons f surjective. On peut choisir[2] pour chaque $y \in Y$ un $x \in X$ tel que $f(x) = y$, ce qui définit une application $s : Y \to X$ par $s(y) = x$ et qui vérifie $f \circ s = \mathrm{id}_Y$. Supposons que f admet un inverse à gauche p. Alors, si $f(x_1) = f(x_2)$, on obtient $x_1 = p(f(x_1)) = p(f(x_2)) = x_2$ donc f est injective. Réciproquement, si f est injective, on peut fixer un élément $x_0 \in X$ et envoyer $y = f(x)$ vers x si $x \in X$ et y vers x_0 si $y \in Y$ n'est pas dans l'image de f. Ceci définit bien, par injectivité de f, une application $p : Y \to X$ telle que $p \circ f = \mathrm{id}_X$. Le cas des bijections se déduit des deux cas précédents. En effet, si f a un inverse à droite et à gauche, alors elle est injective et surjective, donc bijective. Réciproquement, si f est bijective, elle est injective et surjective, donc il existe s et p tels que $f \circ s = \mathrm{id}_X$ et $p \circ f = \mathrm{id}_Y$. L'associativité de la composition des applications donne alors

$$s = \mathrm{id}_Y \circ s = (p \circ f) \circ s = p \circ (f \circ s) = p \circ \mathrm{id}_X = p,$$

2. Ici, on utilise l'axiome du choix.

Ceci signifie que f est a pour inverse à gauche et à droite $g = p = s$. On pourrait aussi plus simplement montrer ce dernier point en construisant directement l'application inverse de f : la bijectivité implique que le transposé

$$\Gamma_{f^{-1}} = \{(y, x) \in Y \times X,\ (x, y) \in \Gamma_f\} \subset Y \times X$$

du graphe de f est bien le graphe d'une application f^{-1}, et on vérifie que c'est bien un inverse de f. □

Définition 1.6. *Une propriété (appelée aussi un prédicat) sur un ensemble X est une application $P : X \to \{\text{vrai}, \text{faux}\}$. On dit que la propriété est vraie en $x \in X$ si $P(x) = \text{vrai}$ et fausse si $P(x) = \text{faux}$.*

Pour X un ensemble, on note $\mathcal{P}(X)$ l'ensemble de ses parties, i.e., l'ensemble de ses sous-ensembles.

Proposition 1.7. *L'ensemble $\{\text{vrai}, \text{faux}\}^X$ des propriétés $P : X \to \{\text{vrai}, \text{faux}\}$ est en bijection naturelle avec l'ensemble des parties de X.*

Démonstration. Une propriété $P : X \to \{\text{vrai}, \text{faux}\}$ définit un sous-ensemble $V(P) \subset X$ par

$$V(P) = P^{-1}(\{\text{vrai}\}) = \{x \in X,\ P(x) = \text{vrai}\}.$$

Un sous-ensemble $V \subset X$ définit une propriété $P_V : X \to \{\text{vrai}, \text{faux}\}$ par $P_V(x) = \text{vrai}$ si $x \in V$ et $P_V(x) = \text{faux}$ si $x \in X - V$. Ces deux constructions sont inverses l'une de l'autre. □

1.2 Entiers naturels et principe de récurrence

La définition de l'ensemble des entiers naturels, possible point de départ pour la définition d'ensembles infinis, peut être abordée en formulant l'axiome suivant, qui est très proche de la définition des entiers utilisée dans les assistants de preuve [3].

Axiome 1.1 (Axiome des entiers naturels)**.** *Il existe un triplet $(\mathbb{N}, S : \mathbb{N} \to \mathbb{N}, 0 \in \mathbb{N})$ formé d'un ensemble $\mathbb{N}$ appelé ensemble des entiers naturels, d'une application $S : \mathbb{N} \to \mathbb{N}$ notée aussi*

$$S(n) = n + 1$$

et appelée application successeur, et d'un élément $0 \in \mathbb{N}$ vérifiant la propriété universelle suivante : pour tout triplet

$$(X, T : X \to X, x \in X)$$

avec X ensemble, il existe une unique application $f : \mathbb{N} \to X$ telle que $f(0) = x$ et $f \circ S = T \circ f$.

La résultat suivant peut être admis [4].

Proposition 1.8 (Axiomes de Peano)**.** *Le triplet $(\mathbb{N}, S : \mathbb{N} \to \mathbb{N}, 0 \in \mathbb{N})$ vérifie les propriétés suivantes :*

1. $1 = S(0) \neq 0$.

3. Les étudiants intéressés pourront consulter l'Annexe A.
4. Sa démonstration est donnée dans l'Annexe A.

2. *(Principe de récurrence) Pour toute partie*[5] $P \subset \mathbb{N}$, *si* $0 \in P$ *et si pour tout* $n \in \mathbb{N}$, *on a l'implication* $[n \in P \Rightarrow n+1 \in P]$, *alors* $P = \mathbb{N}$.
3. *(Principe de récurrence forte) Pour toute partie* $P \subset \mathbb{N}$, *si* $0 \in P$ *et si pour tout* $n \in \mathbb{N}$, *on a l'implication* $[\forall k \in \{0, \dots, n\},\ k \in P \Rightarrow n+1 \in P]$ *alors* $P = \mathbb{N}$.
4. S *est injective.*

Remarque 1.9. *On peut remplacer* 0 *par un entier* n_0 *dans les principes de récurrence. Dans ce cas, on obtient que le sous-ensemble* P *est égal à l'ensemble* $\{n \in \mathbb{N}, n \geq n_0\}$ *des entiers supérieurs ou égaux à* n_0.

1.3 Opérations binaires et structures algébriques

Nous allons maintenant définir et étudier les opérations binaires sur les ensembles, qui jouent un rôle fondamental dans la définition des structures algébriques (groupes, anneaux et corps) que nous allons considérer.

Définition 1.10. *Une opération binaire (ou loi interne) sur un ensemble* X *est une application* $* : X \times X \to X$. *On dit que l'opération* $*$ *sur* X *:*

1. *est associative si pour tous* $(x, y, z) \in X^3$, *on a*
$$(x * y) * z = x * (y * z).$$
2. *possède* $e \in X$ *comme élément neutre si pour tout* $x \in X$,
$$e * x = x * e = x.$$
3. *est commutative si pour tous* $(x, y) \in X^2$, *on a*
$$x * y = y * x.$$
4. *fait de* $x \in X$ *un élément inversible d'inverse* $y \in X$ *pour l'élément neutre* e *si*
$$x * y = e = y * x.$$

On dit qu'une partie $Y \subset X$ *est stable si* $(x, y) \in Y^2$ *implique* $x * y \in Y$.
Si $\times$ *et* $+$ *sont deux opérations binaires sur* X, *on dit que* $\times$ *est distributif par rapport à* $+$ *si pour tous* $(x, y, z) \in X^3$, *on a*
$$x \times (y + z) = x \times y + x \times z \ \text{ et } \ (y + z) \times x = y \times x + z \times x.$$

Proposition 1.11. *Soit* $* : X \times X \to X$ *une opération binaire.*

1. *Si* e *et* f *sont deux éléments neutres pour* $*$, *alors* $e = f$.
2. *Si* $*$ *est associative et si* e *est un élément neutre pour* $*$, *et* y_1 *et* y_2 *sont deux inverses de* x *pour* e, *alors* $y_1 = y_2$.

Démonstration. Les deux résultats sont des applications directes des axiomes.

5. Rappelons que la donnée d'une telle partie est équivalente à la donnée d'une propriété $P : \mathbb{N} \to \{\text{vrai}, \text{faux}\}$. Cette correspondance entre sous-ensembles et propriétés permet de traduire le principe de récurrence en termes de propriétés sur les entiers.

1. On a $e = e * f = f$ car e et f sont des éléments neutres pour $*$.
2. On a par associativité et neutralité

$$y_1 = y_1 e = y_1(xy_2) = (y_1 x)y_2 = ey_2 = y_2.$$

□

Remarque 1.12. *Dans la suite, les opérations binaires seront souvent notées de deux manières :*

1. *Notation additive :* $(x, y) \mapsto x + y$. *L'élément neutre est noté* 0 *et l'inverse pour l'addition, aussi appelé l'opposé, est noté* $-x$.
2. *Notation multiplicative* $(x, y) \mapsto x \times y$ *ou* $(x, y) \mapsto x \cdot y$. *L'élément neutre est noté* 1 *et l'inverse pour la multiplication est noté* x^{-1}.

Le cas général sera noté multiplicativement.

La proposition suivante peut être admise [6].

Proposition 1.13. *On peut munir l'ensemble* $\mathbb{N}$ *de deux opérations binaires* $+$ *et* $\times$. *Ces opérations sont associatives et commutatives, avec pour élément neutre respectifs* 0 *et* 1. *De plus, la multiplication est distributive par rapport à l'addition.*

Nous allons maintenant définir les monoïdes, groupes, anneaux et corps, comme des ensembles munis d'opérations binaires particulières.

Définition 1.14. *Soit* $(M, *, e)$ *un triplet formé d'un ensemble* M, *d'une opération binaire* $*$ *sur* M *et d'un élément* $e \in M$.

1. *On dit que* $(M, *, e)$ *est un monoïde si* $*$ *est associative et* e *est un élément neutre.*
2. *On dit que* $(M, *, e)$ *est un groupe si c'est un monoïde et si tout élément de* M *est inversible.*
3. *On dit que* $(M, *, e)$ *est abélien (ou commutatif) si la loi* $*$ *est commutative.*

Soit $(A, +, \times, 0, 1)$ *un quintuplet formé d'un ensemble* A, *de deux opérations* $+$ *et* $\times$, *et d'une paire d'éléments* $(0, 1) \in A^2$.

4. *On dit que* $(A, +, \times, 0, 1)$ *forme un anneau si* $(A, +, 0)$ *est un groupe commutatif,* $(A, \times, 1)$ *est un monoïde, et* $\times$ *est distributive par rapport a* $+$. *Si* $(A, \times, 1)$ *est de plus commutatif, on dit que l'anneau est commutatif.*
5. *On dit qu'un anneau* $(A, +, \times, 0, 1)$ *est intègre s'il est non nul et s'il vérifie que pour toute paire* $(a, b) \in A^2$, *on a l'implication*

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

6. *On dit qu'un anneau* $(K, +, \times, 0, 1)$ *est un corps si l'ensemble de ses éléments inversibles (pour la multiplication* $\times$*) est* $K - \{0\}$. et si K est non nul.

Exemple 1.15. *Donnons d'abord quelques exemples simples de monoïdes et de groupes.*

1. *On peut munir l'ensemble* $\mathbb{N}$ *des entiers naturels de deux structures de monoides commutatifs : la structure additive* $(\mathbb{N}, +, 0)$ *et la structure multiplicative* $(\mathbb{N}, \cdot, 1)$. *Bien que la multiplication soit distributive par rapport à l'addition, ceci ne donne pas une structure d'anneau car* $(\mathbb{N}, +, 0)$ *n'est pas un groupe puisque* 1 *n'a pas d'opposé.*

6. Le début de sa démonstration à partir de l'Axiome des entiers 1.1 se trouve dans l'Annexe A et on pourra l'approfondir ludiquement en se référant au site interactif [3].

2. *Soit X un ensemble. L'ensemble $\mathrm{End}_{\mathrm{Ens}}(X)$ des application $f : X \to X$ muni de la composition des applications et de l'unité donnée par l'application identique id_X est un monoïde. Le sous-ensemble $\mathrm{Aut}_{\mathrm{Ens}}(X) \subset \mathrm{End}_{\mathrm{Ens}}(X)$ des application inversibles $f : X \to X$ (qui sont les bijections, par la Proposition 1.5) est un groupe appelé le groupe symétrique de X. Si $X = \{1, \ldots, n\}$, on note $S_n = \mathrm{Aut}_{\mathrm{Ens}}(X)$.*
3. *Plus généralement, si $(M, *, e)$ est un monoïde, l'ensemble $M^\times$ de ses éléments inversibles forme un groupe (voir la Proposition 1.19).*
4. *Voici un monoide assez différent qui intervient dans la théorie des langages en informatique. Si A est un ensemble fini de lettres d'un alphabet, on note $M(A)$ l'ensemble dont les éléments sont les mots finis écrits avec des lettres dans l'alphabet A. La loi de composition des mots est simplement donnée par leur juxtaposition, et le mot neutre est le mot vide. On vérifie facilement que $M(A)$ est ainsi muni d'une structure de monoïde, qui n'est pas commutatif dès que A possède plus de deux éléments. Un langage sur l'alphabet A est défini par un sous-ensemble $L \subset M(A)$.*

Exemple 1.16. *Voici maintenant quelques exemples d'anneaux et de corps.*

1. *L'anneau nul est l'ensemble $A = \{0\}$ muni des unités $0_A = 0$ et $1_A = 0$ et des opérations définies par $0 + 0 = 0$ et $0 \cdot 0 = 0$.*
2. *Les opérations d'addition et de multiplication usuelles sur l'ensemble $\mathbb{Z}$ des entiers relatifs font de ce dernier un anneau commutatif intègre qui n'est pas un corps, car les seuls entiers inversibles sont 1 et -1.*
3. *Les opérations d'addition et de multiplication usuelles sur les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ des nombres rationnels, réels et complexes font de ces derniers des corps commutatifs.*
4. *L'ensemble $\mathcal{C}^0([0,1], \mathbb{R})$ des fonctions continues sur l'intervalle $[0, 1]$ muni de ses opérations usuelles forme un anneau commutatif.*
5. *Si A est un anneau commutatif, l'ensemble $(\mathrm{M}_n(A), +, \cdot)$ des matrices à coefficients dans A munies de l'addition usuelle et de la multiplication des matrices, donnée par*

$$(a_{i,j}) \cdot (b_{i,j}) = (c_{i,j}) := \left(\sum_k a_{i,k} b_{k,j} \right)$$

est un anneau (en général non commutatif si $n > 1$). Le groupe de ses inversibles pour la multiplication est noté $\mathrm{GL}_n(A)$.

Nous allons maintenant définir les morphismes entre les structures algébriques précédemment définies.

Définition 1.17. *Un morphisme de monoïdes (resp. morphisme de groupes)*

$$f : (M, *_M, e_M) \to (N, *_N, e_N)$$

est une application $f : M \to N$ telle que

$$f(e_M) = e_N$$

et

$$f(m *_M n) = f(m) *_N f(n)$$

pour tous $(m, n) \in M^2$. Un morphisme d'anneaux (resp. morphisme de corps)

$$f : (A, +_A, \times_A, 0_A, 1_A) \to (B, +_B, \times_B, 0_B, 1_B)$$

est une application $f : A \to B$ qui est un morphisme de groupes additifs

$$f : (A, +_A, 0_A) \to (B, +_B, 0_B)$$

et un morphisme de monoïdes multiplicatifs

$$f : (A, \times_A, 1_A) \to (B, \times_B, 1_B).$$

Définition 1.18. *Un morphisme $f : X \to X$ d'un objet (monoïde, groupe, anneau ou corps) dans lui-même est appelé un endomorphisme. Un morphisme $f : X \to Y$ entre deux objets est appelé un isomorphisme s'il admet un inverse pour la composition, i.e., s'il existe un morphisme $g : Y \to X$ tel que $g \circ f = \mathrm{id}_X$ et $f \circ g = \mathrm{id}_Y$.*

Proposition 1.19. *Soit $(M, *, e)$ un monoïde. Si on note $M^\times \subset M$ l'ensemble des éléments inversibles de M, alors $M^\times$ est un groupe, et tout morphisme de monoïdes $f : M \to N$ induit par restriction un morphisme*

$$f^\times : M^\times \to N^\times$$

entre leurs groupes d'éléments inversibles. On a de plus $f(m^{-1}) = f(m)^{-1}$ pour tout $m \in M^\times$.

Démonstration. Le fait que $M^\times$ soit un groupe découle de l'unicité de l'inverse et des égalités $e^{-1} = e$ et

$$(n *_M m)^{-1} = m^{-1} *_M n^{-1}.$$

Si $m^{-1} \in M$ est l'inverse de m dans M, on a

$$f(m) *_N f(m^{-1}) = f(m *_M m^{-1}) = f(e_M) = e_N$$

et aussi $f(m^{-1}) *_N f(m) = e_N$ donc $f(m^{-1})$ est l'inverse de $f(m)$ dans N. Ceci démontre aussi que $f^\times : M^\times \to N^\times$ est bien définie. □

Exemple 1.20. *Voici quelques exemples de morphismes.*

1. *Soit A un anneau commutatif (par exemple $A = \mathbb{R}$) et $n \geq 1$. Le déterminant* [7]

   $$\det : \mathrm{M}_n(A) \to \mathrm{M}_1(A) = A$$

   est un morphismes de monoïdes mutliplicatifs. Par passage aux inversibles, il induit un morphisme

   $$\det : \mathrm{GL}_n(A) \to \mathrm{GL}_1(A) = A^\times$$

   où $A^\times$ désigne le groupe des inversibles de l'anneau A pour sa multiplication.

2. *Si $f : A \to B$ est un morphisme d'anneaux, le morphisme sous-jacent de monoïdes multiplicatifs induits un morphisme*

   $$f^\times : A^\times \to B^\times$$

   entre les groupes d'éléments inversibles pour les multiplications.

3. *Les inclusions $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sont toutes des morphismes d'anneaux. Elles induisent des inclusions de groupes $\mathbb{Z}^\times \subset \mathbb{Q}^\times \subset \mathbb{R}^\times \subset \mathbb{C}^\times$.*

4. *Si $x \in [0, 1]$, l'application $\mathrm{ev}_x : \mathcal{C}^0([0, 1], \mathbb{R}) \to \mathbb{R}$ d'évaluation des fonctions en x, donnée par $f \mapsto f(x)$, est un morphisme d'anneaux.*

7. Nous reverrons sa définition générale plus loin.

5. *Si A est un anneau commutatif et $n \geq 1$, l'inclusion $A \subset \mathrm{M}_n(A)$ donnée par $a \mapsto a \cdot \mathrm{Id}$ est un morphisme d'anneaux.*

Proposition 1.21. *Une application $f : G \to G'$ entre deux groupes est un morphisme de groupes si et seulement si elle est compatible à la multiplication, i.e., si elle vérifie*

$$f(g_1 * g_2) = f(g_1) * f(g_2)$$

pour tous $g_1, g_2 \in G$. Elle vérifie alors aussi $f(g^{-1}) = f(g)^{-1}$ pour tout $g \in G$.

Démonstration. Une des implications de l'équivalence est évidente. Pour démontrer l'autre, il suffit de multiplier l'égalité

$$f(e_G) * f(e_G) = f(e_G * e_G) = f(e_G)$$

par $f(e_G)^{-1}$ pour obtenir $f(e_G) = e_{G'}$. La deuxième partie de l'énoncé est un corollaire direct de la Proposition 1.19 et du fait que le groupe des inversibles d'un groupe est le groupe lui-même. □

1.4 Relations d'ordre, relations d'équivalence et quotients

1.4.1 Relations binaires

Nous allons maintenant définir les relations d'ordre et les relations d'équivalence, qui jouent toutes deux un rôle important dans la formalisation de l'algèbre et de l'analyse.

Définition 1.22. *Soit X un ensemble.*

1. *Une relation (binaire) sur X est un sous-ensemble $R \subset X \times X$.*
2. *Si R est une relation sur X et $(x, y) \in X^2$, on écrit xRy pour $(x, y) \in R$.*
3. *Un morphisme $f : (X, R) \to (Y, S)$ entre deux relations est une application $f : X \to Y$ vérifiant que pour tous $(x, y) \in X^2$, on a l'implication $xRy \Rightarrow f(x)S\,f(y)$.*

On dit que la relation R sur X est :

1. *réflexive si pour tout $x \in X$, on a xRx.*
2. *transitive si pour tous $(x, y, z) \in X^3$, on a l'implication $[xRy$ et $yRz] \Rightarrow xRz$.*
3. *symétrique si pour tous $(x, y) \in X^2$, on a $xRy \Rightarrow yRx$.*
4. *antisymétrique si pour tous $(x, y) \in X^2$, on a l'implication $[xRy$ et $yRx] \Rightarrow x = y$.*
5. *totale si pour tous $(x, y) \in X^2$, on a $[xRy$ ou $yRx]$.*

Une relation R sur X est appelée :

1. *une relation d'ordre (souvent notée $\leq$) si elle est réflexive, transitive et antisymétrique.*
2. *une relation d'équivalence (souvent notée $\sim$) si elle est réflexive, transitive et symétrique.*

Exemple 1.23. *Voici quelques exemples simples.*

1. *La seule relation sur un ensemble X qui est en même temps une relation d'ordre et une relation d'équivalence est la relation d'égalité, donnée pour tout $(x, y) \in X^2$ par*

$$xRy \Leftrightarrow x = y.$$

2. *La relation $\sim$ sur l'ensemble E des étudiants de ce cours donnée par $x \sim y$ si x et y ont la même marque de chaussures est une relation d'équivalence.*

3. *La relation* $\leq$ *sur l'ensemble* $\{0,1\}$ *donnée par* $0 \leq 0$, $1 \leq 1$ *et* $0 \leq 1$ *est une relation d'ordre total.*
4. *La relation* $\sim$ *sur l'ensemble* $\{0,1\}$ *donnée par* $0 \sim 0$, $0 \sim 1$, $1 \sim 0$ *et* $1 \sim 1$ *est une relation d'équivalence.*
5. *Si* $X = \{0,1\}$*, l'application identique est un morphisme* $\mathrm{id}_X : (X, \leq) \to (X, \sim)$ *entre les deux relations précédemment définies.*

1.4.2 La relation d'ordre sur les entiers naturels

Les entiers naturels sont munis d'une relation d'ordre naturelle définie par le résultat suivant, qui est une conséquence de la Proposition 1.13, et que nous allons aussi admettre.

Proposition 1.24. *La relation définie sur l'ensemble des nombres entiers par* $n \leq m$ *si il existe* $k \in \mathbb{N}$ *tel que* $n + k = m$ *est une relation d'ordre totale dont* 0 *est le plus petit élément.*

Exemple 1.25. *L'application successeur* $S : \mathbb{N} \to \mathbb{N}$ *donnée par* $S(n) = n + 1$ *est un morphisme de relations d'ordre* $S : (\mathbb{N}, \leq) \to (\mathbb{N}, \leq)$*, i.e., une application croissante.*

Nous aurons aussi besoin du résultat suivant concernant cette relation d'ordre.

Proposition 1.26. *Toute partie non vide de* $\mathbb{N}$ *possède un plus petit élément.*

Démonstration. Montrons par récurrence sur $n \in \mathbb{N}$ que la propriété

$$P(n) = \{\text{Si } A \subset \{0, \ldots, n\} \text{ est une partie non vide alors elle a un plus petit élément}\}.$$

est vraie.

1. Le cas de base est $n = 0$. On a alors $A = \{0\}$ et A a 0 comme plus petit élément donc $P(0)$ est vraie.
2. Supposons $P(n)$ vraie et montrons $P(n+1)$. On a deux cas :
   (a) Si $n + 1 \notin A$, alors $A \subset \{0, \ldots, n\}$ et on peut appliquer $P(n)$ pour conclure.
   (b) Si $n + 1 \in A$, on considère $A' = A - \{n + 1\}$. Alors on a deux cas :
      i. Si $A' \neq \emptyset$ alors $A' \subset \{0, \ldots, n\}$ et $P(n)$ s'applique pour conclure.
      ii. Si $A' = \emptyset$ alors $A = \{n + 1\}$ et son plus petit élément est $n + 1$.

Ceci conclut la démonstration par récurrence de $P(n)$. Maintenant, prenons une partie non vide B de $\mathbb{N}$ et soit $n \in B$. Posons $A = \{0, \ldots, n\} \cap B \subset \{0, \ldots, n\}$. On applique $P(n)$ a A pour lui trouver un plus petit élément et c'est aussi par construction un plus petit élément de B. □

1.4.3 Relations d'équivalence, quotients et classes de nombres

Les relations d'équivalence se retrouvent un peu partout en mathématiques parce qu'elles amènent à la notion d'*ensemble quotient*, défini comme étant l'ensemble des classes d'équivalence d'une relation donnée, et que cette notion est à la base de constructions de nombreux objets mathématiques fondamentaux, comme nous le verrons plus loin.

Pour E un ensemble, rappelons qu'on note $\mathcal{P}(E)$ l'ensemble de ses parties, i.e., l'ensemble de ses sous-ensembles.

Définition 1.27. *Soit R une relation d'équivalence sur un ensemble E. La* classe d'équivalence *de $x \in E$ est*

$$cl_R(x) = \{y \in E \mid yRx\}.$$

*L'*ensemble quotient *de R*

$$E/R = \{cl_R(x), x \in E\} \subset \mathcal{P}(E)$$

est l'ensemble des classes d'équivalence de tous les éléments de E. On dispose d'une application surjective naturelle $cl_R : E \to E/R$.

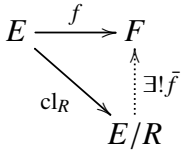
Proposition 1.28. *Soit E un ensemble et R une relation d'équivalence sur E. L'ensemble quotient E/R forme une partition de E.*

Démonstration. Pour montrer que l'ensemble quotient forme une partition de E, il faut montrer que tout élément $x \in E$ appartient à une et une seule classe d'équivalence.
Tout d'abord, pour tout $x \in E$, on a xRx (réflexivité) et donc $x \in cl_R(x)$. En particulier, x appartient à au moins une classe d'équivalence.
Ensuite, si on suppose que $y \in E$ appartient à la fois à $cl_R(x_1)$ et à $cl_R(x_2)$. On veut montrer que $cl_R(x_1) = cl_R(x_2)$ (attention, ce n'est pas vrai en général que $x_1 = x_2$!). Soit donc $z \in cl_R(x_1)$. Alors on a zRx_1 mais aussi x_1Ry et x_2Ry. Par symétrie et transitivité, cela implique que zRy puis que zRx_2. Ainsi, $z \in cl_R(x_2)$ et donc $cl_R(x_1) \subset cl_R(x_2)$. Par symétrie des rôles joués par x_1 et x_2, on a aussi $cl_R(x_2) \subset cl_R(x_1)$, et donc $cl_R(x_1) = cl_R(x_2)$, ce qu'on voulait démontrer. □

Proposition 1.29 (Propriété universelle du quotient ensembliste)**.** *L'application $cl_R : E \to E/R$ vérifie la propriété universelle suivante : pour tout ensemble F, et pour toute application $f : E \to F$ vérifiant la condition* [8]

$$\textit{pour tous } (x, y) \in E^2,\ xRy \textit{ implique } f(x) = f(y),$$

il existe une unique application $\bar{f} : E/R \to F$ telle que $\bar{f} \circ \mathrm{cl}_R = f$, i.e., qui fait commuter le diagramme



Démonstration. On doit forcément définir $\bar{f}$ sur une classe $\mathrm{cl}_R(x)$ par $\bar{f}(\mathrm{cl}_R(x)) = f(x)$ car on veut avoir $\bar{f} \circ \mathrm{cl}_R = f$. Ceci ne dépend pas du choix du représentant x de la classe car xRy implique $f(x) = f(y)$. On a aussi alors clairement $\bar{f} \circ \mathrm{cl}_R = f$. □

Exemple 1.30. *Considérons à nouveau l'exemple de la relation R donnée par "avoir la même marque de chaussure" sur l'ensemble E des étudiants de ce cours. On note M l'ensemble des marque de chaussures représentées dans ce cours. L'application $c : E \to M$ qui associe à un étudiant la marque de ses chaussures est constante sur les classes d'équivalence et factorise en une bijection*

$$\bar{f} : E/R \xrightarrow{\sim} M$$

entre l'ensemble des groupes d'étudiants classés par marques de chaussures et l'ensemble des marques de chaussures représentées dans le cours. Ainsi, ces deux ensembles ne sont pas égaux, mais sont en bijection naturelle. Cette bijection permet de dénombrer les classes d'étudiants par marques de chaussures, i.e., les éléments de l'ensemble quotient.

8. On remarque qu'une application vérifiant cette condition est exactement un morphisme de relations d'équivalences $f : (E, R) \to (F, =)$.

Le corollaire suivant peut-être utile pour définir des applications entre ensembles quotients.

Corollaire 1.31. *Soit $f : (E, R) \to (F, S)$ un morphisme entre relations d'équivalences. Alors f induit une unique application $\bar{f} : E/R \to F/S$ vérifiant $\bar{f} \circ \mathrm{cl}_R = \mathrm{cl}_S \circ f$, i.e., faisant commuter le diagramme*

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ {\scriptstyle \mathrm{cl}_R}\downarrow & & \downarrow{\scriptstyle \mathrm{cl}_S} \\ E/R & \xrightarrow[\exists ! \bar{f}]{} & F/S \end{array}$$

Démonstration. Le résultat découle directement de la Propriété universelle du quotient ensembliste 1.29 appliquée à l'application $\mathrm{cl}_S \circ f$. □

Lorsque l'on introduit de nouveaux objets mathématiques pour résoudre des problèmes, cela se fait très souvent par le choix du quotient d'un ensemble connu par une relation d'équivalence convenable. Une suite notable de telles constructions est donnée par la construction des différents types de nombres utilisés dans ce cours. On suppose donné l'ensemble $(\mathbb{N}, +, 0, \times, 1, \leq)$ des nombres entiers naturels avec ses structures standards, fournies par les Propositions 1.13 et 1.24. C'est un exercice laborieux (basé sur l'utilisation répétée du Corollaire 1.31) de montrer que toutes ces structures se prolongent aux différentes classes de nombres considérées (sauf la relation d'ordre $\leq$, qui n'est pas définie sur $\mathbb{C}$).

Exemple 1.32. *Les entiers relatifs résolvent le problème de donner aux nombres entiers naturels des opposés (inverses pour l'addition). Formellement, on pose*

$$\mathbb{Z} := \mathbb{N} \times \mathbb{N} / \sim,$$

où on note $n - m$ la classe d'une paire d'entiers (n, m) pour la relation $\sim$ qui identifie (n, m) avec (n', m') lorsque $n + m' = m + n'$. On définit l'inclusion naturelle $\mathbb{N} \to \mathbb{Z}$ en envoyant n sur $(n, 0)$. La somme est définie par

$$(n - m) + (n' - m') = (n + n') - (m + m').$$

Le produit est défini par

$$(n - m) \cdot (n' - m') = (nn' + mm') - (nm' + mn').$$

On vérifie que ceci munit $\mathbb{Z}$ d'une structure d'anneau commutatif. La relation d'ordre $\leq$ sur $\mathbb{Z}$ est définie en disant que $n - m \leq n' - m'$ dans $\mathbb{Z}$ si $n + m' \leq n' + m$ dans $\mathbb{N}$.

Exemple 1.33. *Les nombres rationnels résolvent le problème de donner aux nombres entiers naturels non nuls des inverses pour la multiplication dans $\mathbb{Z}$. Formellement, on pose*

$$\mathbb{Q} := \mathbb{Z} \times \mathbb{N} - \{0\} / \sim$$

où on note p/q la classe d'une paire d'entiers (p, q) pour la relation qui identifie (p, q) et (r, s) si $ps = rq$. On définit l'inclusion naturelle $\mathbb{Z} \to \mathbb{Q}$ en envoyant p sur $p/1$. La somme est définie par

$$(p/q) + (r/s) = (ps + qr)/(qs).$$

Le produit est défini par

$$(p/q) \cdot (r/s) = (pr)/(qs).$$

Ceci munit $\mathbb{Q}$ d'une structure de corps commutatif. La relation d'ordre $\leq$ sur $\mathbb{Q}$ est définie en disant que $(p/q) \leq (r/s)$ dans $\mathbb{Q}$ si $ps \leq qr$ dans $\mathbb{Z}$.

Exemple 1.34. *Les nombres réels résolvent le problème de donner aux suites de Cauchy de nombres rationnels des limites. Rappelons qu'une suite de rationnels* $(x_n) \in \mathbb{Q}^{\mathbb{N}}$ *est de Cauchy si ses termes se rapprochent à l'infini, i.e., si, pour tout* $\epsilon \in \mathbb{Q}_+^*$*, il existe un entier* $N > 0$ *tel que* $p, q \geq N$ *implique* $|x_p - x_q| < \epsilon$*. Si on note* $\mathrm{Cauchy}(\mathbb{Q}, |\cdot|)$ *l'ensemble des suites de Cauchy de rationnels, on pose*

$$\mathbb{R} := \mathrm{Cauchy}(\mathbb{Q}, |\cdot|)/\sim$$

où on dit que deux suites de Cauchy sont équivalentes si elles ont formellement la même limite, i.e., si leur différence tend vers 0*. La limite d'une suite de Cauchy* (x_n) *de nombres rationnels est simplement donnée par sa classe* $cl_\sim((x_n))$ *dans* $\mathbb{R}$*. On définit l'application naturelle* $\mathbb{Q} \to \mathbb{R}$ *en envoyant un nombre rationnel* p/q *sur la suite constante correspondante, qui est de Cauchy. On montre enfin que toute suite de Cauchy de nombres réels est convergente. On peut montrer que* $\mathbb{R}$ *est muni d'une addition et d'une multiplication (induites par la somme et le produit terme à terme des suites) qui en font un corps commutatif. La relation d'ordre* $\leq$ *sur* $\mathbb{R}$ *est définie de la manière suivante : on définit* $\mathbb{R}_+$ *comme l'ensemble des classes qui ont un représentant donné par une suite de Cauchy de* $\mathbb{Q}_+ = \{x \in \mathbb{Q},\ x \geq 0\}$*, et on écrit que* $(x_n) \leq (y_n)$ *si* $\mathrm{cl}_\sim(y_n - x_n) \in \mathbb{R}_+$*.*

Exemple 1.35. *Les nombres complexes résolvent le problème de donner une racine au polynôme réel* $x^2 + 1 = 0$*. Plus précisément, on pose*

$$\mathbb{C} := \mathbb{R}[x]/\sim$$

où on dit que deux polynômes réels sont équivalents si leur différence est divisible par le polynôme $x^2 + 1$*. On montrera plus loin que* $\mathbb{C}$ *est un anneau commutatif unitaire (qui est en fait un corps). Par division euclidienne, nous verrons qu'il n'est pas difficile de montrer que l'application de classe*

$$cl_\sim : \mathbb{R}[x]_{\leq 1} \to \mathbb{C}$$

est bijective, où $\mathbb{R}[x]_{\leq 1}$ *désigne les polynômes de degré inférieurs ou égal à* 1*. On note alors i la classe de x.*

1.5 Sous-groupes et groupes quotients

1.5.1 Sous-groupes

Définition 1.36. *Un sous-groupe* H *d'un groupe* $(G, *, e_G)$ *est un sous-ensemble* $H \subset G$ *qui :*

1. *contient* e_G*,*
2. *est stable par l'opération* $*$*, i.e., vérifie que pour tous* $g, h \in H$*, on a* $g * h \in H$*,*
3. *est stable par passage à l'inverse, i.e., vérifie que pour tout* $g \in H$*, on a* $g^{-1} \in H$*.*

Proposition 1.37. *Soit* G *un groupe et* H *un sous-ensemble non vide de* G*. Alors* H *est un sous-groupe si et seulement si pour tous* $x, y \in H$*, on a* $xy^{-1} \in H$*.*

Démonstration. L'une des implications découle directement de la définition de sous-groupe. Montrons l'autre. Supposons H non vide et que pour tous $x, y \in H$, on ait $xy^{-1} \in H$. Soit $x \in H$, alors on a $e_G = xx^{-1} \in H$. De plus, on obtient $y^{-1} = e_G y^{-1} \in H$ pour tout $y \in H$. Enfin, si $y \in H$, on a $(y^{-1})^{-1} = y$ donc pour $x, y \in H$, on obtient

$$xy = x(y^{-1})^{-1} \in H.$$

On a bien montré que H est un sous-groupe. □

Exemple 1.38. *Fixons $n \geq 1$ un entier.*

1. *Pour A un anneau commutatif, Le groupe $(\mathrm{GL}_n(A), \cdot, \mathrm{Id})$ des inversibles du monoide multiplicatif $(\mathrm{M}_n(A), \cdot, \mathrm{Id})$ des matrices est appelé groupe général linéaire. C'est un groupe non commutatif pour $n > 1$.*
2. *Le groupe orthogonal $\mathrm{O}_n(\mathbb{R})$ est le sous-groupe de $\mathrm{GL}_n(\mathbb{R})$ donné par*

$$\mathrm{O}_n(\mathbb{R}) = \{M \in \mathrm{M}_n(\mathbb{R}), {}^tMM = M{}^tM = \mathrm{Id}\}.$$

   Ce groupe joue un rôle important dans la théorie de la diagonalisation des matrices symétriques dans une base orthonormée.
3. *Dans l'analogue complexe de cette théorie, qui est la diagonalisation des endomorphismes autoadjoints d'un espace complexe, l'analogue du groupe orthogonal est le groupe unitaire, défini comme le sous-groupe de $\mathrm{GL}_n(\mathbb{C})$ donné par*

$$\mathrm{U}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{C}), {}^t\overline{M}M = M{}^t\overline{M} = \mathrm{Id}\}.$$

Définition 1.39. *Le noyau d'un morphisme de groupes $f : (G, *_G, 1_G) \to (H, *_H, 1_H)$ est défini par*

$$\mathrm{Ker}(f) = f^{-1}(\{1_H\}) = \{g \in G,\ f(g) = 1_H\}$$

et l'image de f est définie par

$$\mathrm{Im}(f) = f(G) = \{f(g),\ g \in G\}.$$

Proposition 1.40. *Le noyau et l'image d'un morphisme de groupes $f : G \to H$ sont des sous-groupes de la source H et du but G du morphisme. Un morphisme de groupe est injectif si et seulement si $\mathrm{Ker}(f) = \{1_G\}$ et surjectif si et seulement si $\mathrm{Im}(f) = H$.*

Démonstration. La démonstration des propriétés de sous-groupes est laissée en exercice. Si $f : G \to H$ est injectif, comme $f(1_G) = 1_H$, si $f(g) = 1_H$ alors $g = 1_G$, donc on a forcément $\mathrm{Ker}(f) = \{1_G\}$. Réciproquement, si $\mathrm{Ker}(f) = \{1_G\}$ et $f(g_1) = f(g_2)$, alors $1_H = f(g_1) \cdot f(g_2)^{-1} = f(g_1 g_2^{-1})$ donc $g_1 g_2^{-1} = 1_G$ donc $g_1 = g_2$. La condition pour la surjectivité est évidente. □

1.5.2 Quotient d'un groupe abélien par un sous-groupe

Nous allons maintenant définir le quotient par un sous-groupe seulement dans le cas d'un groupe abélien, car ceci est suffisant pour ce qui suit. Les groupes abéliens abstraits sont souvent notés en notation additive.

Proposition 1.41. *Soit $(A, +, 0)$ un groupe abélien et $B \subset A$ un sous-groupe. La relation R_B sur A définie par $a_1 R_B a_2$ si et seulement si $a_1 - a_2 \in B$ est une relation d'équivalence. Le quotient A/B de A par cette relation d'équivalence est muni d'une unique structure de groupe telle que l'application de classe $\mathrm{cl}_B : A \to A/B$ soit un morphisme de groupes.*

Démonstration. Vérifions qu'on a bien une relation d'équivalence.

1. (Réflexivité) On a $a - a = 0 \in B$ donc aR_Ba pour tout $a \in A$.
2. (Symétrie) Si $a_1 - a_2 \in B$, alors $a_2 - a_1 = -(a_1 - a_2) \in B$ car B est un sous-groupe. Ainsi, $a_1 R_B a_2$ implique $a_2 R_B a_1$ pour tous $a_1, a_2 \in A$.
3. (Transitivité) Si $a_1 - a_2 \in B$ et $a_2 - a_3 \in B$ alors $a_1 - a_3 = (a_1 - a_2) + (a_2 - a_3) \in B$. Ceci donne que $a_1 R_B a_2$ et $a_2 R_B a_3$ implique $a_1 R_B a_3$ pour tous $a_1, a_2, a_3 \in A$.

Pour $a \in A$, on note $a + B = \{a + b,\ b \in B\}$ et $B + a = \{b + a,\ b \in B\}$. La classe d'un élément $a \in A$ est donnée par

$$\mathrm{cl}_B(a) = a + B = B + a$$

car le groupe A est commutatif. La structure de groupe sur le quotient est unique, si elle existe. En effet, si on veut que l'application de classe cl_B soit un morphisme de groupes, elle doit vérifier

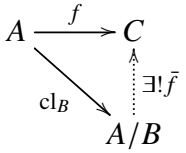
$$\mathrm{cl}_B(a_1) + \mathrm{cl}_B(a_2) = (a_1 + B) + (a_2 + B) = (a_1 + a_2) + B = \mathrm{cl}_B(a_1 + a_2)$$

pour tous $a_1, a_2 \in A$. D'autre part, si $a_1 + B = a_1' + B$ et $a_2 + B = a_2' + B$, on a

$$\mathrm{cl}_B(a_1) + \mathrm{cl}_B(a_2) = a_1 + B + a_2 + B = (a_1 + a_2) + B = a_1' + B + a_2' + B = (a_1' + a_2') + B$$

car le groupe A est commutatif, donc l'addition des classes ne dépend pas du choix du représentant et est bien définie. On obtient aussi, par construction, que l'application de classe est un morphisme de groupe. □

Proposition 1.42 (Propriété universelle du quotient dans les groupes abéliens)**.** *Soit A un groupe abélien et $B \subset A$ un sous-groupe. Le morphisme $\mathrm{cl}_B : A \to A/B$ vérifie la propriété universelle suivante : pour tout groupe abélien C et tout morphisme $f : A \to C$ tel que $f(B) = \{0_C\}$, il existe un unique morphisme $\bar{f} : A/B \to C$ tel que $\bar{f} \circ \mathrm{cl}_B = f$, i.e., qui fait commuter le diagramme*



Démonstration. Ceci découle de la propriété universelle 1.29 du quotient dans les ensembles, car $a_1 R_B a_2$ si et seulement si il existe $b \in B$ tel que $a = c + b$ et alors $f(a_1) = f(a_2) + f(b) = f(a_2)$. On vérifie facilement que $\bar{f}$ est un morphisme de groupe. □

1.6 Idéaux et anneaux quotients

Dans toute cette section, les anneaux sont supposés commutatifs.

Définition 1.43. *Un idéal d'un anneau A est un sous-groupe additif $I \subset A$ qui est stable par multiplication par les éléments de A, i.e, qui vérifie que pour tous $a \in A$ et $x \in I$, on a $ax \in I$.*

Proposition 1.44. *Soit $f : A \to B$ un morphisme d'anneaux. Le noyau $I = \mathrm{Ker}(f)$ du morphisme de groupes additifs sous-jacents est un idéal.*

Démonstration. Par la Proposition 1.40, le noyau I est un sous-groupe de $(A, +, 0)$. Il existe à vérifier qu'il est stable par multiplication externe par les éléments de A. Soit $a \in A$ et $m \in I$. On a

$$f(am) = f(a)f(m) = f(a) \cdot 0 = 0$$

ce qui termine la preuve. □

Théorème 1.45. *Soit A un anneau et $I \subset A$ un idéal. Alors il existe une unique structure d'anneau sur le quotient de groupes additifs commutatifs A/I telle que l'application de classe $\mathrm{cl}_I : A \to A/I$ soit un morphisme d'anneau.*

Démonstration. Pour $a, b \in A$, on a $\mathrm{cl}_I(a) = a + I$ et $\mathrm{cl}_I(b) = b + I$. On va poser

$$(a + I) \cdot (b + I) = (ab) + I$$

pour que le morphisme de groupes additifs

$$\mathrm{cl}_I : A \to A/I$$

donné par la projection naturelle (obtenu par la Proposition 1.41) soit aussi un morphisme de monoïdes multiplicatifs, où A/I est muni de l'unité $\bar{1} := \mathrm{cl}_I(1)$ Pour prouver que c'est possible, on remarque d'abord que l'égalité de deux classes $a + I$ et $a' + I$ est équivalente à $a - a' \in I$. Dire que $a' + I = a + I$ et $b' + I = b + I$ est donc équivalent à dire que $a - a' \in I$ et $b - b' \in I$. Ceci implique alors

$$ab - a'b' = ab + a'b - a'b - a'b' = (a - a')b - a'(b - b') \in I$$

car I est un sous-groupe additif de A stable par multiplication externe. Ainsi, on a bien $ab + I = a'b' + I$, donc la multiplication $A \times A \to A$ passe bien au quotient par le sous-groupe additif I. On montre ensuite que la structure ainsi obtenue fait bien de A/I un anneau (l'associativité et la distributivité découlent de celles de A) tel que le morphisme de projection $\mathrm{cl}_I : A \to A/I$ soit un morphisme d'anneaux (par construction). □

Exemple 1.46. *Si $n \in \mathbb{Z}$ est un entier, l'ensemble $n\mathbb{Z}$ de ses multiples est un idéal de $\mathbb{Z}$. Le quotient $\mathbb{Z}/n\mathbb{Z}$ est appelé l'anneau des entiers modulo n.*

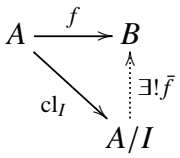
Exemple 1.47. *On peut montrer (avec un travail non négligeable) les résultats suivants :*

1. *l'ensemble* $\mathrm{Cauchy}(\mathbb{Q}, |\cdot|)$ *des suites de Cauchy de nombres rationnels considérées dans l'Exemple 1.34 forme un anneau commutatif unitaire pour les opérations induites par l'addition et le produit des suites termes à termes.*
2. *Le sous-ensemble* $\mathrm{Cauchy}_0(\mathbb{Q}, |\cdot|)$ *des suites tendant vers* 0 *est un idéal de cet anneau.*
3. *Ceci implique que le quotient*

$$\mathbb{R} = \mathrm{Cauchy}(\mathbb{Q}, |\cdot|)/\mathrm{Cauchy}_0(\mathbb{Q}, |\cdot|)$$

est un anneau commutatif unitaire (qui est en fait un corps).

Proposition 1.48 (Propriété universelle du quotient dans les anneaux)**.** *Soit A un anneau et $I \subset A$ un idéal. Le morphisme $\mathrm{cl}_I : A \to A/I$ vérifie la propriété universelle suivante : pour tout anneau B et tout morphisme $f : A \to B$ tel que $f(I) = \{0_B\}$, il existe un unique morphisme $\bar{f} : A/I \to B$ tel que $\bar{f} \circ \mathrm{cl}_H = f$, i.e., qui fait commuter le diagramme*



Démonstration. Ceci découle de la propriété universelle 1.42 du quotient dans les groupes abéliens. On vérifie facilement que $\bar{f}$ est un morphisme d'anneaux. □

Exemple 1.49. *Si n et m sont des entiers tel que n divise m, i.e., si il existe $q \in \mathbb{Z}$ tel que $nq = m$, alors on a l'inclusion $m\mathbb{Z} \subset n\mathbb{Z}$, donc l'image de $m\mathbb{Z}$ par l'application de classe $\mathrm{cl}_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est nulle. Ceci implique, par la propriété universelle du quotient dans les anneaux qu'il existe un unique morphisme d'anneaux $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ tel que $f \circ \mathrm{cl}_m = \mathrm{cl}_n$.*

Chapitre 2

Division euclidienne

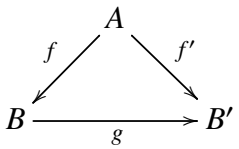
Dans toutes la suite, les anneaux seront supposés commutatif, sauf mention explicite du contraire, et K désigne un corps commutatif.

Dans ce chapitre, nous allons présenter une similitude frappante entre l'anneau des entiers $\mathbb{Z}$ et l'anneau $K[X]$ des polynômes sur un corps : tous deux sont munis d'une division euclidienne. Il peut être utile, à titre culturel, de préciser que l'analogie entre l'anneau des entiers et l'anneaux des polynômes (sur un corps fini), dont c'est un des aspects, est à la source de nombreux problèmes intéressants et encore bien ouverts en théorie des nombres.

2.1 L'algèbre des polynômes sur un anneau

On fixe un anneau commutatif A.

Définition 2.1. *Une algèbre B sur l'anneau A, appelée aussi une A-algèbre, est un anneau B muni d'un morphisme d'anneaux $f : A \to B$ (qui est souvent sous-entendu). Un morphisme de A-algèbres $g : B \to B'$ est un morphisme d'anneaux tel que $g \circ f = f'$, i.e., tel que le diagramme*



commute.

Exemple 2.2. *Le morphisme naturel $A \to \mathrm{M}_n(A)$ donné par $a \mapsto a \cdot I$ fait de l'algèbre des matrices sur l'anneau A une A-algèbre non commutative.*

Définition 2.3. *Un polynôme sur A est une somme formelle*

$$P(X) = \sum_{n \in \mathbb{N}} a_n X^n$$

dont tous les coefficients a_n sont des éléments de A et telle que seul un nombre fini de coefficients a_n soient non nuls. La somme de deux polynômes est définie par linéarité par

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

Le produit de deux polynômes est défini par distributivité par

$$\left(\sum_{n \in \mathbb{N}} a_n X^n \right) \cdot \left(\sum_{n \in \mathbb{N}} b_n X^n \right) = \sum_{n \in \mathbb{N}, m \in \mathbb{N}} a_n b_m X^{n+m} = \sum_{n \in \mathbb{N}} \left(\sum_{p+q=n} a_p b_q \right) X^n.$$

Pour $a \in A$, on note aussi a l'élément correspondant de $A[X]$, donné par $a \cdot X^0$. Si $P = \sum_{n\in N} a_n X^n \in A[X]$ est un polynôme, on définit son degré $\deg(P)$ *comme le plus grand n (valant par convention $-\infty$ si P est nul) tel que le coefficient a_n soit non nul et tous les a_m pour $m > n$ soient nuls. Le coefficient $a_{\deg(P)}$ est appelé coefficient dominant de P.*

Proposition 2.4. *On dispose des inégalités*

$$\deg(PQ) \leq \deg(P) + \deg(Q)$$

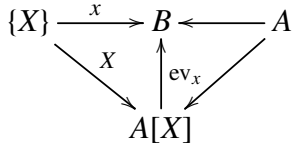
et

$$\deg(P + Q) \leq \max(\deg(P), \deg(Q)).$$

La première inégalité est une égalité si A est un corps.

Démonstration. Si a_n et b_m sont les coefficients dominants de P et Q, le coefficient dominant de PQ est $c_{n+m} = a_n b_m$ s'il n'est pas nul. C'est le cas si A est un corps. S'il est nul, le coefficient dominant c_d de PQ a donc un indice d strictement inférieur à $n+m$. La deuxième inégalité, laissée en exercice, se démontre aussi en raisonnant sur les coefficients dominants. □

Proposition 2.5. *L'ensemble $A[X]$ avec son addition et sa multiplication naturels forme une A-algèbre commutative. Elle vérifie la propriété universelle suivante : si B est une A-algèbre (pas forcément commutative), et $x \in B$ est un élément, il existe un unique morphisme de A-algèbre* $\mathrm{ev}_x : A[X] \to B$ *tel que* $\mathrm{ev}_x(X) = x$*, i.e., faisant commuter le diagramme*



Démonstration. On remarque d'abord que pour tous entiers p et q, on a bien

$$x^p x^q = x^{p+q}$$

dans B, même si elle n'est pas commutative. Posons $\mathrm{ev}_x(P) = P(x) = \sum_{n\in N} a_n x^n$. On a aussi

$$\left(\sum_{n\in\mathbb{N}} a_n x^n\right) \cdot \left(\sum_{n\in\mathbb{N}} b_n x^n\right) = \sum_{n\in\mathbb{N}, m\in\mathbb{N}} a_n b_m x^{n+m} = \sum_{n\in\mathbb{N}} \left(\sum_{p+q=n} a_p b_q\right) x^n$$

et la compatibilité à la somme est évidente. Le fait que ce soit un morphisme de A-algèbre est aussi clair car $\mathrm{ev}_x(a_A X^0) = \mathrm{ev}_x(a_A x^0) = \mathrm{ev}_x(a_A \cdot 1_B) = a_1 \cdot 1_B$. □

Remarque 2.6. *La propriété précédente joue un rôle important dans la diagonalisation des matrices sur un corps K, car elle permet de définir un morphisme* $\mathrm{ev}_M : K[X] \to \mathrm{M}_n(K)$ *associé à chaque matrice M et d'étudier ainsi les polynômes de matrices.*

Proposition 2.7. *Si K est un corps, les éléments inversibles de l'anneau des polynômes $K[X]$ sont les éléments inversibles de K, i.e., on a*

$$K[X]^\times = K^\times = K - \{0\}.$$

Démonstration. L'inclusion $K^\times \subset K[X]^\times$ vient de l'inclusion $K \to K[X]$ par passage aux inversibles. Pour l'autre inclusion, si $P \in K[X]$ est inversible, on a

$$0 = \deg(X^0) = \deg(PP^{-1}) = \deg(P) + \deg(P^{-1})$$

donc $\deg(P) = \deg(P^{-1}) = 0$. □

2.2 Anneaux principaux et anneaux euclidiens

Proposition 2.8. *Soit A un anneau et $X \subset A$ un sous-ensemble. Il existe un plus petit idéal (X) contenant X. Il s'identifie à l'ensemble des combinaisons linéaires (finies) $\sum_{x\in X} a_x \cdot x$ d'éléments de X à coefficients (presque tous nuls) dans A.*

Démonstration. Si $\{I_s\}_{s\in S}$ est une famille non vide d'idéaux, son intersection $I = \cap_{s\in S} I_s$ est un idéal. D'autre part, la famille des idéaux de A contenant X est non vide car elle contient A. On peut donc définir le plus petit idéal contenant X comme l'intersection de tous les idéaux contenant X. Remarquons maintenant que l'ensemble $(X)_\ell$ des combinaisons linéaires finies d'éléments de X à coefficients dans A est clairement un idéal contenant X, ce qui donne l'inclusion $(X) \subset (X)_\ell$. Inversement, tout idéal contenant (X) contient ces combinaisons linéaires finies, ce qui donne l'inclusion $(X)_\ell \subset (X)$, d'où l'égalité $(X) = (X)_\ell$. □

Définition 2.9. *Soit A un anneau et $X \subset A$ un sous-ensemble. Le plus petit idéal (X) contenant X est appelé l'idéal engendré par X. Un idéal I est principal s'il est engendré par un élément $a \in A$, i.e., s'il existe $a \in A$ tel que $I = (a)$.*

Définition 2.10. *Soit A un anneau.*

1. *On dit que A est principal si tout idéal I différent de A est principal.*
2. *Si $a, b \in A$, on dit que a divise b ou que b est un multiple de a, et on note $a|b$ si il existe $q \in A$ tel que $aq = b$.*

Exemple 2.11. *Dans $\mathbb{Z}$, les idéaux principaux sont de la forme $(n) = n\mathbb{Z}$ pour $n \in \mathbb{Z}$. Leurs éléments sont les multiples de n. L'anneau $\mathbb{Z}$ est intègre et on verra plus loin (en utilisant la division euclidienne) qu'il est aussi principal, i.e., que ses idéaux sont tous de la forme $n\mathbb{Z}$ pour $n \in \mathbb{Z}$.*

Définition 2.12. *Un anneau euclidien est un anneau intègre A équipé d'une fonction $\delta : A \to \mathbb{N} \cup \{-\infty\}$ (appelée le stathme) telle qu'on ait :*

1. *$\delta(0) = -\infty$ et $\delta(a) \in \mathbb{N}$ pour tout $a \in A - \{0\}$,*
2. *pour tout $a \in A$ et $b \in A - \{0\}$, il existe $q, r \in A$ tels que $a = bq + r$ et $\delta(r) < \delta(b)$,*
3. *pour tous $a, b \in A - \{0\}$, $\delta(b) \leq \delta(ab)$.*

Remarque 2.13. *Le stathme est uniquement déterminé par sa valeur sur $A-\{0\}$: on peut toujours poser $\delta(0) = -\infty$.*

Proposition 2.14. *Tout anneau euclidien est principal, i.e., si I est un idéal d'un anneau euclidien A, il existe $a \in A$ tel que $A = (a)$.*

Démonstration. Notons $\delta : A-\{0\} \to \mathbb{N}$ le stathme. Si $I = 0$, on a $I = (0)$ et le problème est réglé. Supposons donc $I \neq 0$. On choisit $a \in I - \{0\} \subset A - \{0\}$ tel que $\delta(a)$ soit minimal. On va montrer $I \subset (a)$, puisque l'autre inclusion est évidente par définition de (a). Soit $b \in I$. Alors il existe q et r dans A tels que $b = qa + r$ et $\delta(r) < \delta(a)$. On a $qa \in (a) \subset I$ et $b \in I$ donc $r = b - qa \in I$. Si $r = 0$, on a gagné car alors $b = qa \in (a)$. Si $r \neq 0$, on a $\delta(r) < \delta(a)$ et $r \in I$ ce qui contredit la minimalité de a dans I pour δ. Ceci conclut la démonstration. □

2.3 Les anneaux $\mathbb{Z}$ et $K[X]$ sont euclidiens

Proposition 2.15. *L'anneau des entiers $\mathbb{Z}$ muni du stathme donné par la valeur absolue $\delta = |\cdot| : \mathbb{Z} - \{0\} \to \mathbb{N}$ est euclidien. De plus, dans la division euclidienne, le quotient et le reste sont uniques si on suppose le reste positif ou nul.*

Démonstration. Rappelons qu'on pose $\delta(0) = -\infty$ et $\delta(a) = |a|$ pour $a \in \mathbb{Z} - \{0\}$. Pour a et b des entiers non nuls, on a $|a| \geq 1$ et $|b| \geq 1$. Ceci implique

$$|a| = |a| \cdot 1 \leq |a| \cdot |b| = |ab|$$

donc la dernière condition pour être un stathme est vérifiée. Fixons $b \in \mathbb{Z} - \{0\}$. On a $|b| > 0$. On va démontrer par une récurrence sur $a' \in \mathbb{N}$ que pour tout $a' \in \mathbb{N}$, il existe $q', r' \in \mathbb{Z}$ tels que

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

Le cas de base est $a' = 0$. On pose alors $q' = r' = 0$. On a alors bien $\delta(r') = -\infty < \delta(b) = |b|$. Fixons maintenant $a > 0$, et supposons l'hypothèse vraie pour tout $a' < a$. On procède par une étude de cas.

1. Si $a < |b|$, on pose $q = 0$ et $a = r$ et on a bien $a = bq + r$ avec $|r| = a < |b|$.
2. Si $a \geq |b|$, alors $0 \leq a - |b| < a$ car $|b| > 0$, donc on peut appliquer l'hypothèse de récurrence à $a' = a - |b|$, pour obtenir q' et r' tels que

   $$a' = q'b + r' \text{ et } |r'| < |b|.$$

   Ceci implique
   $$a = (a - |b|) + |b| = q'b + r' + |b|.$$

   (a) Si $b > 0$, on a $|b| = b$ donc
   $$a = b(q' + 1) + r',$$
   et on pose $q = q' + 1$ et $r = r'$. Comme $|r'| < |b|$, on a obtenu ce qu'on cherchait.

   (b) Si $b < 0$, alors $|b| = -b$, donc
   $$a = q'b + r' - b = b(q' - 1) + r'$$
   avec toujours $|r'| < |b|$. On peut donc poser $r = r'$ et $q = q' - 1$.

Il reste à traiter le cas où a est strictement négatif. Par le résultat précédent, on a

$$(-a) = bq + r$$

avec $\delta(r) < \delta(b)$. Mais comme $\delta(-r) = \delta(r)$, on peut utiliser l'identité

$$a = b(-q) - r$$

pour arriver au résultat recherché. □

Proposition 2.16. *Soit K un corps. L'application $\delta : K[X] - \{0\} \to \mathbb{N}$ définie par $\delta(P) = \deg(P)$ munit $K[X]$ d'une structure d'anneau euclidien. De plus, dans la division euclidienne, le quotient et le reste sont uniques.*

Démonstration. La preuve est similaire à celle de l'énoncé 2.15 sur les entiers et se fait par récurrence. D'abord, si $f, g \in K[X] - \{0\}$, on a vu dans la Proposition 2.4 que

$$\deg(fg) = \deg(f) + \deg(g)$$

donc $\deg(f) \leq \deg(fg)$. Fixons maintenant $g \in K[X] - \{0\}$. On va démontrer par récurrence sur le degré de $f \in K[X]$ qu'il existe $q, r \in K[X]$ tels que

$$f = gq + r$$

et $\deg(r) < \deg(g)$. Commençons par initier la récurrence en supposant $\deg(f) = 0$, i.e., $f = c \in K$ est une constante.

1. Si $\deg(g) > 0$, on pose $q(X) = 0$ et $r(X) = f(X)$ et on obtient

   $$f = 0 \cdot g + r$$

   avec $\deg(r) < \deg(g)$.
2. Sinon, g est une constante λ de $K - \{0\}$ qu'on peut inverser dans K pour définir $q(X) = c/\lambda$ et $r(X) = 0$, ce qui donne

   $$f = c = (c/\lambda) \cdot \lambda + 0 = q \cdot g + r.$$

On va supposer l'hypothèse de récurrence vérifiée pour tout $m \leq n$. Notons

$$f(X) = a_n X^n + \cdots + a_0 \text{ et } g(X) = b_m X^m + \cdots + b_0$$

avec $b_m \neq 0$.

1. Si $\deg(f) < \deg(g)$, on pose $q(X) = 0$ et $r(X) = f(X)$ et on obtient

   $$f = 0 \cdot g + r$$

   avec $\deg(r) < \deg(g)$.
2. Sinon, $\deg(f) \geq \deg(g)$. On suppose $a_n \neq 0$, i.e., $n = \deg(f)$ et on a $m = \deg(g)$. Comme K est un corps, $b_m \neq 0$ est inversible, et on pose

   $$c = a_n/b_m \in K$$

   et

   $$f_1(X) = f(X) - cX^{n-m}g(X).$$

   Alors, le coefficient de X^n pour f_1 est

   $$a_n - cb_m = a_n - (a_n/b_m)b_m = 0$$

   donc on a $\deg(f_1) < n$, et on peut appliquer l'hypothèse de récurrence à f_1 pour obtenir q_1 et r_1 tels que

   $$f_1 = q_1 g + r_1$$

   avec $\deg(r_1) < \deg(g)$. On obtient

   $$f(X) = cX^{n-m}g(X) + f_1(X) = (cX^{n-m} + q_1(X))g(X) + r_1(X).$$

   On peut alors poser $q(X) = cX^{n-m} + q_1(X)$ et $r(X) = r_1(X)$, et obtient

   $$f = qg + r$$

   avec $\deg(r) < \deg(g)$.

Il reste à montrer que le quotient et le reste sont uniques. Supposons donc

$$f = gq + r = gq' + r'$$

avec $\deg(r) < \deg(g)$ et $\deg(r') < \deg(g)$. Alors on a

$$r - r' = g(q' - q).$$

Mais on a aussi $\deg(r - r') < \deg(g)$. Supposons $q \neq q'$. Alors

$$\deg(g) \leq \deg(g(q - q')) = \deg(r - r') < \deg(g),$$

ce qui donne une contradiction. On obtient donc $q = q'$ et $r = r'$. □

Corollaire 2.17. *Les idéaux de $\mathbb{Z}$ sont tous de la forme $n\mathbb{Z}$ avec $n \in \mathbb{Z}$. Si K est un corps, les idéaux de $K[X]$ sont tous de la forme (P) avec $P \in K[X]$.*

Nous allons maintenant donner une description ensembliste explicite des quotients de $\mathbb{Z}$ et $K[X]$ par leurs idéaux en utilisant la division euclidienne.

On fixe un entier $n > 0$. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est le quotient de $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$, i.e., par la relation d'équivalence

$$k \sim l \Leftrightarrow n \text{ divise } k - l.$$

Définition 2.18. *Si $k \in \mathbb{Z}$ est un entier, on note $k \mod n$ le reste positif ou nul de sa division euclidienne par n.*

L'application $\mod n : \mathbb{Z} \to \{0, \ldots, n-1\}$ est surjective et vérifie que

$$k \sim l \Leftrightarrow k \mod n = l \mod n.$$

Ceci implique, par la propriété universelle du quotient ensembliste $\mathbb{Z}/n\mathbb{Z}$, qu'on dispose d'une application $\overline{\mod n} : \mathbb{Z}/n\mathbb{Z} \to \{0, \ldots, n-1\}$ telle que si $\mathrm{cl}_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est la projection naturelle du quotient, on ait $\overline{\mod n} \circ \mathrm{cl}_n = \mod n$. L'application

$$\overline{\mod n} : \mathbb{Z}/n\mathbb{Z} \to \{0, \ldots, n-1\}$$

ainsi construite est bijective.

Soit maintenant K un corps. On fixe un polynôme non nul $g \in K[X] - \{0\}$. L'anneau $K[X]/(g)$ est le quotient de $K[X]$ par l'idéal (g), i.e., par la relation d'équivalence

$$p \sim q \Leftrightarrow g \text{ divise } p - q.$$

Définition 2.19. *Si $f \in K[X]$ est un polynôme, on note $f \mod g$ le reste de la division euclidienne de f par g.*

L'application $\mod g : K[X] \to K[X]_{<\deg(g)}$ vers les polynômes de degré inférieur à celui de g est surjective, et envoie la relation d'équivalence induite par (g) sur la relation d'égalité. Ceci permet de construire une application

$$\overline{\mod g} : K[X]/(g) \longrightarrow K[X]_{<\deg(g)}$$

qui est bijective. On peut montrer que c'est en fait un isomorphisme de K-espaces vectoriels.

Exemple 2.20. *Si on considère le polynôme $g(X) = X^2 + 1$ dans $\mathbb{R}[X]$, on obtient une identification ensembliste*

$$\overline{mod\ g} : \mathbb{C} = \mathbb{R}[X]/(X^2 + 1) \xrightarrow{\sim} \mathbb{R}[X]_{\leq 1}$$

qui est en fait un isomorphisme de $\mathbb{R}$-espaces vectoriels.

2.4 Diviseurs, multiples et algorithme de Bézout

L'intersection de deux idéaux I et J est un idéal $I \cap J$. Il est possible de définir aussi la somme de deux idéaux I et J en posant

$$I + J = \{a + b,\ a \in I, b \in J\}.$$

Dans le cas de deux idéaux principaux, ceci donne

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

Définition 2.21. *Soit A un anneau principal et $a, b \in A$. Un plus grand commun diviseur pour a et b est un élément* $\text{pgcd}(a, b)$ *tel que*

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

On dit que a et b sont premiers entre eux si 1 *est un plus grand commun diviseur pour a et b, i.e., si*

$$(a) + (b) = (1) = A.$$

Un plus petit commun multiple pour a et b est un élément $\text{ppcm}(a, b)$ *tel que*

$$(a) \cap (b) = (\text{ppcm}(a, b)).$$

Théorème 2.22 (de Bézout)**.** *Si A est un anneau principal, $a, b \in A$ et d est un diviseur commun de a et b, alors d est un plus grand commun diviseur pour a et b, si et seulement si il existe $u, v \in A$ tels que*

$$au + bv = d.$$

En particulier, a et b sont premiers entre eux si il existe $u, v \in A$ tels que

$$au + bv = 1.$$

Si de plus l'anneau A est euclidien de stathme $\delta : A - \{0\} \to \mathbb{N}$, il existe un algorithme naturel pour calculer le triplet (d, u, v) à partir de la paire (a, b).

Démonstration. Montrons la double implication de la première partie de l'énoncé. Si d est un plus grand diviseur commun pour a et b, c'est à dire si

$$(a, b) = (d),$$

alors $d|a$ et $d|b$ (car $a \in (d)$ et $b \in (d)$) et il existe $u, v \in A$ tels que $d = au + bv$ (car $(d) \subset (a, b)$). Réciproquement, supposons que d est un diviseur commun de a et b et qu'il existe $u, v \in A$ tels que $d = au + bv$. Soit d' un plus grand commun diviseur de a et b, i.e., un élément tel que

$$(a, b) = (d').$$

Alors, comme $d = au + bv \in (a, b) = (d')$, on sait que $d'|d$. On sait aussi que $d|a$ et $d|b$ donc $(d') = (a, b) \subset (d)$ et $d|d'$. On a obtenu en particulier $(d) = (d')$ donc d est un plus grand commun diviseur de a et b. Voyons maintenant l'algorithme de Bézout (aussi appelé algorithme d'Euclide étendu).

1. Initialisation : on prend en entrée la paire $(r_0, r_1) = (a, b)$ et on pose $u_0 = 1$, $v_0 = 0$ et $u_1 = 0$, $v_1 = 1$.

2. Boucle de la division euclidienne : pour $i \geq 1$, tant que $r_i \neq 0$, on fait
   (a) La division euclidienne de r_{i-1} par r_i :

$$r_{i-1} = q_i r_i + r_{i+1}, \delta(r_{i+1}) < \delta(r_i).$$

   (b) Mise à jour des coefficients de Bézout :

$$\begin{aligned} u_{i+1} &= u_{i-1} - q_i u_i \\ v_{i+1} &= v_{i-1} - q_i v_i \end{aligned}$$

   (c) Incrémenter i.

Arrêt : Soit n le plus grand indice tel que $r_n \neq 0$ et $r_{n+1} = 0$. Alors on a l'identité de Bézout

$$r_n = u_n a + v_n b$$

et

$$\text{pgcd}(a, b) = r_n$$

car r_n est un diviseur commun de a et b vérifiant l'identité de Bézout. □

2.5 Éléments premiers d'un anneaux euclidien

Définition 2.23. *Soit A un anneau intègre. Un élément $p \in A$ est dit premier si p est non nul, non inversible, et si $p|ab$ implique $p|a$ ou $p|b$ pour tous $a, b \in A$. Il est dit irréductible si p est non nul, non inversible et si pour toute décomposition $p = ab$, on a que a ou b est inversible.*

Proposition 2.24. *Soit A un anneau euclidien. Si $p \in A$ est un élément premier, alors $A/(p)$ est un corps.*

Démonstration. Soit $\bar{a} \in A/(p)$ tel que $\bar{a} \neq 0$. Alors, on a que $a \notin (p)$, donc

$$p \nmid a.$$

On applique l'algorithme de Bézout pour obtenir u et v tels que

$$au + pv = 1.$$

Quand on passe aux classes modulo p, on obtient

$$\bar{a}\bar{u} = \bar{1}$$

donc $\bar{u}$ est un inverse de $\bar{a}$ dans $A/(p)$. On a bien montré que $A/(p)$ est un corps. □

Corollaire 2.25. *Pour p premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps. Pour tout anneau commutatif A, il existe un unique morphisme $i : \mathbb{Z} \to A$. Pour tout corps commutatif K, on a :*

1. *soit* $\text{Ker}(i) = (0)$*, i.e., i est injectif,*
2. *soit il existe un premier p tel que* $\text{Ker}(i) = (p)$*, i.e., tel que i factorise en une application injective $\bar{i} : \mathbb{Z}/p\mathbb{Z} \to A$.*

Démonstration. Si $i : \mathbb{Z} \to A$ est un morphisme d'anneau alors $i(1) = 1_A$ et $f(0) = 0_A$. Mais dans ce cas, pour tout $n \in \mathbb{N}$, $i(n) = i(n.1) = ni(1) = n \cdot 1_A$. De plus, si $n < 0$, on a $-n > 0$ et $i(n) = i(-(-n)) = -i(-n) = -(-n)1_A$. Ceci définit une unique application $i : \mathbb{Z} \to A$, qui est bien un morphisme d'anneaux. Si K est un corps et $i : \mathbb{Z} \to K$ est l'unique application, alors si n et m sont dans $\mathrm{Ker}(i)$ et $i(nm) = 0$ alors $i(n)i(m) = 0$ donc $i(n) = 0$ ou $i(m) = 0$ car K est un corps. Si $\mathrm{Ker}(i) = (0)$, alors i est injectif. Sinon, $\mathrm{Ker}(i)$ est un idéal engendré principal (p) et la condition précédente montre que p est premier. La propriété universelle du quotient dans les anneaux 1.48 permet dans ce cas de construire une application injective $\bar{i} : \mathbb{Z}/p\mathbb{Z} \to A$. □

Définition 2.26. *Le générateur (soit nul, soit premier) de* $\mathrm{Ker}(i)$ *défini ci-dessus est appelé la caractéristique du corps* K.

Remarque 2.27. *Si* p *est fini, un corps* K *est de caractéristique* p *si et seulement si* $p = 0$ *dans* K. *Un corps est de caractéristique* 0 *si et seulement si aucun premier fini n'est nul dans* K.

Exemple 2.28. *Soit* $p \in \mathbb{Z}$ *un entier premier. On note* $k = \mathbb{Z}/p\mathbb{Z}$ *et soit et* $P \in k[X]$ *un polynôme premier. Alors le quotient* $K = k[X]/(P)$ *est un corps qui est en bijection (par division euclidienne par* P*) avec l'ensemble fini* $k[X]_{<\deg(P)} \cong k^{\deg(P)}$ *des polynômes de degré inférieur au degré de* P. *C'est donc un* corps fini. *On peut montrer que tous les corps finis (à isomorphisme près) sont obtenus par cette construction. Les corps finis sont utilisés de manière très pratique en cryptographie et en théorie des codes correcteurs d'erreurs.*

Proposition 2.29 (Lemme de Gauss)**.** *Soit* A *un anneau euclidien, et soit* $p \in A$ *un élément* Irréductible*. Alors, pour tous* $a, b \in A$*, si* $p|ab$ *et* $p \nmid a$*, alors* $p|b$.

Démonstration. On va utiliser l'identité de Bézout. On a $p \nmid a$, donc $\mathrm{pgcd}(a, p) = 1$. Par l'algorithme d'Euclide, on obtient $u, v \in A$ tels que

$$au + pv = 1.$$

On multiplie cette identité par b pour obtenir

$$aub + bvp = b.$$

Or on sait que $p|ab$ pour il existe $q \in A$ tel que $ab = pq$. Ainsi, on obtient

$$aub = upq.$$

Ainsi, on obtient

$$b = aub + pvb = upq + pvb = p(uq + vb)$$

donc $p|b$. □

Proposition 2.30. *Un élément* p *d'un anneau euclidien est irréductible si et seulement si il est premier.*

Démonstration. Démontrons les deux implications.

1. Supposons p premier et $p = ab$. Comme $p|ab$ et p premier, on a $p|a$ ou $p|b$. Supposons $p|a$. Alors $a = pu$ pour $u \in A$ donc

$$p = ab = pub$$

dont $ub = 1$ et $b \in A^\times$ donc l'un des deux facteurs est inversible et p est irréductible.

2. Inversement, supposons p irréductible et $p|ab$. On veut montrer $p|a$ ou $p|b$. Supposons que $p \nmid a$. Alors, par le Lemme de Gauss 2.29, on obtient que $p|b$ donc on a montré que $p|ab$ implique $p|a$ ou $p|b$. Ainsi, p est premier.

□

Théorème 2.31 (Décomposition en irréductibles)**.** *Soit A un anneau euclidien et $a \in A - \{0\}$ non inversible. Supposons de plus* [1] *que le stathme euclidien $\delta : A - \{0\} \to \mathbb{N}$ vérifie :*

1. *si $a = a_1 a_2$ est une décomposition en facteurs non inversibles, on a $\delta(a_1) < \delta(a)$ et $\delta(a_2) < \delta(a)$.*
2. *les éléments de $A - \{0\}$ de stathme $\delta(a)$ minimal sont les inversibles de A.*

Alors il existe un nombre fini de facteurs irréductibles $p_i \in A$ tels que

$$a = p_1 \cdots p_n.$$

Démonstration. On note $\delta : A - \{0\} \to \mathbb{N}$ le stathme euclidien. On va prouver l'énoncé

$$P(n) = \text{“tout } a \in A - \{0\} \text{ non inversible avec } \delta(a) = n \text{ se factorise en irréductibles”}$$

par récurrence forte sur $\delta(a) \in \mathbb{N}$. Si n_0 est la valeur minimale de δ, $P(n_0)$ est trivialement vraie par l'hypothèse 2), qui garantit que l'ensemble $\{a \in A - \{0\} \text{ non inversibles avec } \delta(a) = n_0\}$ est vide. Si on suppose a irréductible, il n'y a rien à démontrer. Supposons que a est non inversible et non irréductible. Alors, par définition, $a = a_1 a_2$ avec a_1, a_2 non inversibles donc $\delta(a_1) < \delta(a)$ et $\delta(a_2) < \delta(a)$. On peut appliquer l'hypothèse de récurrence aux a_i pour les décomposer en produits de facteurs irréductibles. □

Corollaire 2.32. *Tout nombre entier non nul et non inversible se décompose de manière unique en un produit*

$$n = u \cdot p_1^{n_1} \cdots p_k^{n_k}$$

avec p_i des premiers positifs croissants, $n_i \geq 0$ et $u \in \mathbb{Z}^\times = \{\pm 1\}$.

Corollaire 2.33. *Tout polynôme non nul et non inversible $P \in K[X]$ se décompose en un produit*

$$P = u \cdot P_1^{n_1} \cdots P_k^{n_k}$$

avec P_i des polynômes irréductibles unitaires, $n_i \geq 0$ et $u \in K[X]^\times = K^\times$.

2.6 Polynôme minimal d'un endomorphisme

Comme $K[X]$ est euclidien, il est aussi principal. Ce résultat joue un rôle central dans la diagonalisation des matrices.

Définition 2.34. *Si $A \in \mathrm{M}_n(K)$, on peut définir l'idéal annulateur de A dans $K[X]$ par*

$$\mathrm{Ann}(A) := \{P \in K[X],\ P(A) = 0\}.$$

Un polynôme minimal $M_A(X)$ est un générateur de cet idéal.

Remarque 2.35. *Pour montrer que* Ann(A) *est bien un idéal, on l'identifie à l'idéal noyau* $\mathrm{Ker}(\mathrm{ev}_A : K[X] \to \mathrm{M}_n(K))$ *du morphisme de K-algèbres d'évaluation en M, évoqué dans la Remarque 2.6.*

1. Ces conditions sont vérifiées pour les entiers et les polynômes sur un corps.

Le théorème de diagonalisation, qui sera vu au second semestre, est le suivant :

Théorème 2.36. *La matrice A (supposée non nulle) est diagonalisable si et seulement si son polynôme minimal est scindé à racines simples, i.e., de la forme*

$$M_A(X) = c \prod_{i=1}^{d} (X - \lambda_i)$$

avec c une constante non nulle et les $\lambda_i \in K$ tous distincts.

Deuxième partie

Algèbre linéaire et bilinéaire

Chapitre 3

Rappels d'algèbre linéaire

On fixe un corps commutatif K dans ce chapitre et les suivants. L'algèbre linéaire abstraite peut être vue comme un langage qui permet de parler des équations linéaires d'un point de vue intrinsèque, i.e., qui ne dépend pas du choix des coordonnées.

3.1 Espaces vectoriels et applications linéaires

Définition 3.1. *Un K-espace vectoriel est la donnée d'un quadruplet $(V, +, 0_V, \cdot)$ formé d'un groupe commutatif $(V, +, 0_V)$ et d'une multiplication externe*

$$\cdot : K \times V \to V$$

tels que on ait pour tous $\lambda, \lambda' \in K$ et $v, v' \in V$ les égalités

1. $1 \cdot v = v$ *et* $\lambda \cdot (\lambda' \cdot v) = (\lambda\lambda') \cdot v$.
2. $(\lambda + \lambda') \cdot v = \lambda \cdot v + \lambda' \cdot v$ *et* $\lambda \cdot (v + v') = \lambda \cdot v + \lambda \cdot v'$.

Un morphisme entre deux K-espaces vectoriels V et W, appelé aussi une application linéaire, est un morphisme de groupes additifs $f : V \to W$, i.e., une application qui vérifie $f(0_V) = 0_W$ et

$$f(u + v) = f(u) + f(v)$$

pour tous $u, v \in V$, qui est aussi compatible à la multiplication externe, i.e., qui vérifie

$$f(\lambda \cdot v) = \lambda \cdot f(v)$$

pour tous $\lambda \in K$ et $v \in V$. On note $\mathrm{Hom}_{\mathrm{VECT}_K}(V, W)$ l'ensemble des applications linéaires de V dans W et $\mathrm{End}_{\mathrm{VECT}_K}(V) = \mathrm{Hom}_{\mathrm{VECT}_K}(V, V)$ l'ensemble des endomorphismes linéaires de V.

On déduit de ces axiomes que $v = 1 \cdot v = (1 + 0) \cdot v = 1 \cdot v + 0 \cdot v = v + 0 \cdot v$ donc

$$0 \cdot v = v - v = 0_V.$$

Notation. *Si V et W sont des K-espaces vectoriels, l'ensemble $\mathrm{Hom}_{\mathrm{VECT}_K}(V, W)$ est muni d'une structure naturelle d'espace vectoriel en posant, pour tout $v \in V$ et $\lambda \in K$,*

$$(f + g)(v) = f(v) + g(v) \;\; et \;\; (\lambda f)(v) = \lambda f(v).$$

L'espace vectoriel ainsi obtenu est aussi souvent noté $\mathcal{L}(V, W)$, et on note aussi $\mathcal{L}(V) = \mathcal{L}(V, V)$. L'espace $V^* = \mathcal{L}(V, K)$ est appelé l'espace dual de V. Ses éléments sont appelés les formes linéaires sur V.

Définition 3.2. *Soit V un espace vectoriel et $W \subset V$ un sous-ensemble. On dit que W est un sous-espace vectoriel s'il contient 0_V, est stable par addition et par multiplication par un scalaire.*

Exemple 3.3. *Voici deux exemples simples de K-espaces vectoriels.*

1. *Soit I un ensemble et $K^I = \mathrm{Hom}_{\mathrm{Ens}}(I, K)$ l'ensemble des applications ensemblistes $f : I \to K$. On peut munir K^I d'une structure naturelle d'espace vectoriel en posant, pour tout $x \in I$ et $\lambda \in K$,*

$$(f + g)(x) = f(x) + g(x) \text{ et } (\lambda f)(x) = \lambda f(x).$$

   La donnée d'un élément v de K^I est équivalente à la donnée d'une famille $v = (\lambda_i)_{i\in I}$, avec $\lambda_i \in K$. Si $I = \{1, \dots, n\}$, on obtient l'espace $K^I = K^n$.

2. *Notons maintenant $K^{(I)} \subset K^I$ l'ensemble des applications ensemblistes $f : I \to K$ qui s'annulent en dehors d'un sous ensemble fini I_f de I. Plus précisément, une application $f : I \to K$ est dans $K^{(I)}$ si $I_f = f^{-1}(K - \{0\})$ est fini. C'est un sous-espace vectoriel de K^I et on a $K^{(I)} = K^I$ si et seulement si I est fini. La donnée d'un élément v de $K^{(I)}$ est équivalente à la donnée d'une famille $v = (\lambda_i)_{i\in I}$, avec $\lambda_i \in K$ et telle que tous les λ_i soient nuls sauf un nombre fini d'entre eux.*

Définition 3.4. *Soit V un espace vectoriel et $\mathcal{F}$ une famille de vecteurs de V.*

1. *On note $\mathrm{Vect}(\mathcal{F})$ le sous-espace vectoriel engendré par $\mathcal{F}$, i.e., le plus petit sous-espace de V contenant $\mathcal{F}$. C'est aussi l'ensemble des combinaisons linéaires finies d'éléments de $\mathcal{F}$.*
2. *La famille $\mathcal{F}$ de vecteurs de V est génératrice si $\mathrm{Vect}(\mathcal{F}) = V$.*
3. *La famille $\mathcal{F}$ est libre si pour toute famille finie de vecteurs $(v_i)_{i\in I}$ de $\mathcal{F}$ et de scalaires $(\lambda_i)_{i\in I}$ de K,*

$$\sum_{i\in I} \lambda_i v_i = 0 \Rightarrow \forall i,\ \lambda_i = 0.$$

4. *Une base $\mathfrak{B}$ d'un espace vectoriel V est une famille libre, génératrice* [redacted]
5. *La dimension d'un espace vectoriel V est le cardinal d'une de ses bases* [1].
6. *Un espace vectoriel basé est une paire $(V, \mathfrak{B})$ formé d'un espace vectoriel et d'une base. Un morphisme d'espaces basés est juste une application linéaire.*

totalement ordonnée

Remarque 3.5. *La famille $\mathcal{F} = \{v_i\}_{i\in I}$ de la définition précédente définit une application*

$$f : K^{(I)} \to V$$

par $f((\lambda_i)) = \sum_{i\in I} \lambda_i v_i$ (ces sommes sont bien définies car leurs coefficients non nuls sont toujours en nombre fini, par définition de $K^{(I)}$). Demander que la famille $\mathcal{F}$ soit libre revient à demander que f soit injective. Demander que la famille $\mathcal{F}$ soit génératrice revient à demander que f soit surjective. Le choix d'une base pour un espace vectoriel de dimension finie est donc équivalente au choix d'un isomorphisme linéaire

$$f : K^{\{1,\dots,n\}} \xrightarrow{\sim} V,$$

ou $\{1, \dots, n\}$ est muni de son ordre total usuel.

1. La dimension ne dépend pas du choix de la base.

Remarque 3.6. *On peut aussi donner un exemple simple d'espace vectoriel de dimension infinie tiré de ce cours, donné par la K-algèbre $K[X]$ des polynômes. La famille $\mathfrak{B} = \{X^n, n \in \mathbb{N}\}$ forme une base de $K[X]$, si on munit $\mathbb{N}$ de son ordre usuel, et l'application naturelle*

$$f : K^{(\mathbb{N})} \to K[X]$$

associée à cette base est un isomorphisme linéaire. En effet, un polynôme est une somme formelle $\sum_{n\in\mathbb{N}} a_n X^n$ dont tous les coefficients sont nuls sauf éventuellement un nombre fini d'entre eux.

La démonstration du résultat suivant est admise.

Théorème 3.7. *Soit E un espace vectoriel et $\mathcal{F} = \{e_i\}_{i\in I}$ une famille libre de E. Alors on peut compléter $\mathcal{F}$ en une base de E, i.e., il existe une base $\mathfrak{B}$ de E telle que $\mathcal{F} \subset \mathfrak{B}$.*

Nous allons maintenant principalement nous intéresser aux espaces vectoriels de dimension finie.

Notation. *Si $\mathfrak{B} = \{e_1, \dots, e_n\}$ est une base de V et $v \in V$ est un vecteur, on note*

$$[v]_{\mathfrak{B}} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

la matrice colonne contenant les coordonnées du vecteur v dans la base $\mathfrak{B}$, i.e., vérifiant

$$v = x_1 \cdot e_1 + \cdot + x_n \cdot e_n.$$

Définition 3.8. *Si $f : (V, \mathfrak{B}) \to (W, \mathcal{C})$ est une application linéaire entre deux espaces vectoriels basés, avec $\mathfrak{B} = \{e_i\}_{i=1,\dots,n}$ et $\mathcal{C} = \{f_j\}_{j=1,\dots,m}$, la matrice de f dans les bases considérées est donnée par la matrice dont les colonnes sont les coordonnées*

$$\mathrm{Mat}_{\mathfrak{B},\mathcal{C}}(f) = [[f(e_1)]_{\mathcal{C}}, \dots, [f(e_n)]_{\mathcal{C}}] \in \mathrm{M}_{m,n}(K)$$

des vecteurs $f(e_i)$, images des vecteurs de la base $\mathfrak{B} = \{e_i\}$, dans la base $\mathcal{C} = \{f_j\}$. Si $f : (V, \mathfrak{B}) \to (V, \mathfrak{B})$ est un endomorphisme, on note simplement $\mathrm{Mat}_{\mathfrak{B}}(f) = \mathrm{Mat}_{\mathfrak{B},\mathfrak{B}}(f)$.

Ces applications

$$\mathrm{Mat}_{\mathfrak{B},\mathcal{C}} : \mathcal{L}(V, W) \to \mathrm{M}_{m,n}(K)$$

sont des isomorphismes de K-espace vectoriels. On va aussi voir qu'elles sont aussi compatibles à la composition des applications linéaires (resp. des matrices).

On a que l'application des fonctions linéaires correspond à l'application des matrices aux vecteurs colonnes correspondants :

$$[f(v)]_{\mathcal{C}} = \mathrm{Mat}_{\mathfrak{B},\mathcal{C}}(f) \cdot [v]_{\mathfrak{B}}.$$

Proposition 3.9. *Soient $(V, \mathfrak{B}) \xrightarrow{f} (W, \mathcal{C}) \xrightarrow{g} (U, \mathcal{D})$ deux applications linéaires composables entre des espaces vectoriels basés. La composition des applications linéaires correspond à la multiplication des matrices : on a l'égalité*

$$\mathrm{Mat}_{\mathfrak{B},\mathcal{D}}(g \circ f) = \mathrm{Mat}_{\mathcal{C},\mathcal{D}}(g) \cdot \mathrm{Mat}_{\mathfrak{B},\mathcal{C}}(f).$$

Si $f = \mathrm{id}_V : (V, \mathfrak{B}) \to (V, \mathcal{C})$ est l'application linéaire identité de V considérée entre deux bases différentes, on a

$$[v]_{\mathcal{C}} = [\mathrm{id}_V(v)]_{\mathcal{C}} = \mathrm{Mat}_{\mathfrak{B},\mathcal{C}}(\mathrm{id}_V) \cdot [v]_{\mathfrak{B}}.$$

Définition 3.10. *La matrice $P_{\mathfrak{B},\mathcal{C}} = \mathrm{Mat}_{\mathfrak{B},\mathcal{C}}(\mathrm{id}_V)$ est appelée inverse de la matrice de passage de la base $\mathfrak{B}$ à la base $\mathcal{C}$. Elle est explicitement donnée par*

$$P_{\mathfrak{B},\mathcal{C}} = [[e_1]_{\mathcal{C}}, \ldots, [e_n]_{\mathcal{C}}]$$

avec $\mathfrak{B} = (e_i)_{i=1,\ldots,n}$ et $\mathcal{C} = (f_j)_{j=1,\ldots,n}$. On remarque qu'on a $P_{\mathcal{C},\mathfrak{B}} = P^{-1}_{\mathfrak{B},\mathcal{C}}$ et $P = P_{\mathcal{C},\mathfrak{B}}$ est appelée la matrice de passage de la base $\mathfrak{B}$ à la base $\mathcal{C}$.

Corollaire 3.11. *Soit $f : V \to V$ une application linéaire et $\mathfrak{B}$ et $\mathcal{C}$ deux bases de V. Si on veut passer de la matrice $A = \mathrm{Mat}_{\mathfrak{B}}(f)$ à la matrice $B = \mathrm{Mat}_{\mathcal{C}}(f)$, on écrit le diagramme*

$$(V, \mathcal{C}) \xrightarrow{\mathrm{id}_V} (V, \mathfrak{B}) \xrightarrow{f} (V, \mathfrak{B}) \xrightarrow{\mathrm{id}_V} (V, \mathcal{C})$$

et on obtient la formule

$$\mathrm{Mat}_{\mathcal{C}}(f) = \mathrm{Mat}_{\mathcal{C}}(\mathrm{id}_V \circ f \circ \mathrm{id}_V) = \mathrm{Mat}_{\mathfrak{B},\mathcal{C}}(\mathrm{id}_V) \cdot \mathrm{Mat}_{\mathfrak{B},\mathfrak{B}}(f) \cdot \mathrm{Mat}_{\mathcal{C},\mathfrak{B}}(\mathrm{id}_V)$$

qui se simplifie, si on pose $P = P_{\mathcal{C},\mathfrak{B}} = \mathrm{Mat}_{\mathcal{C},\mathfrak{B}}(\mathrm{id}_V)$, pour donner la formule classique

$$B = P^{-1}AP.$$

Exemple 3.12. *Voyons quelques exemples d'application linéaires simples et des matrices correspondantes.*

1. *Soit V un espace vectoriel muni d'une base $\mathfrak{B}$. Si $v \in V$ est un vecteur, il définit une application $f_v : K \to V$ en envoyant la base $\{1\}$ du K-espace vectoriel K sur v. La matrice de f_v dans cette base est alors simplement donnée par la matrice colonne des coordonnées de v dans la base $\mathfrak{B}$:*

$$\mathrm{Mat}_{\{1\},\mathfrak{B}}(f_v) = [v]_{\mathfrak{B}}.$$

2. *Posons $V = K^2$ et soit $f(x, y) = x + y$. Alors f est une forme linéaire sur V, i.e., un élément de l'espace vectoriel $V^* = \mathcal{L}(V, K)$ qui peut et doit être pensé comme représentant une équation sur V :*

$$f(x, y) = x + y = 0.$$

   L'étude des formes linéaires correspond donc à l'étude (intrinsèque, i.e., sans choix de coordonnées) des équations sur un espace vectoriel V. La matrice de f dans les bases canoniques de K^2 et de K est donnée par une matrice ligne

$$\mathrm{Mat}_{\{e_1,e_2\},\{1\}}(f) = [f(e_1), f(e_2)] = [1, 1].$$

3. *Posons $V = K^2$ et soit $f(x, y) = (x + y, y)$. Alors $f : V \to V$ est une application linéaire de matrice dans la base canonique $\mathfrak{B} = \{e_1, e_2\}$ avec $e_1 = (1, 0)$ et $e_2 = (0, 1)$ donnée par*

$$\mathrm{Mat}_{\mathfrak{B}}(f) = [[f(e_1)_{\mathfrak{B}}, [f(e_2)]_{\mathfrak{B}}] = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

3.2 Quotients d'espaces vectoriels et théorème du rang

Définition 3.13. *Soit $f : V \to W$ une application linéaire. Alors, l'image*

$$\mathrm{Im}(f) = f(V)$$

est un sous-espace vectoriel de W et le noyau

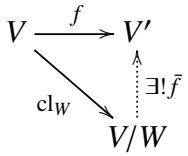
$$\mathrm{Ker}(f) = f^{-1}(\{0\})$$

est un sous-espace vectoriel de V. Le rang de f est défini par

$$\mathrm{rang}(f) = \dim(\mathrm{Im}(f)).$$

Remarque 3.14. *On peut calculer le noyau et l'image d'une application linéaire $f : (V, \mathfrak{B}) \to (W, \mathcal{D})$ entre espaces vectoriels basés (les bases étant de cardinal respectifs m et n) en utilisant le méthode du pivot de Gauss sur les lignes ou sur les colonnes. Si $A = \mathrm{Mat}_{\mathfrak{B},\mathcal{D}}(f)$, les coordonnées des vecteurs de $\mathrm{Im}(f)$ dans la base $\mathcal{C}$ sont données par les matrices colonnes $Y \in K^m$ telles qu'il existe $X \in K^n$ avec $AX = Y$, et les coordonnées des vecteurs de $\mathrm{Ker}(f)$ dans la base $\mathfrak{B}$ sont les matrices colonnes $X \in K^m$ telles que $AX = 0$. Dans un pivot sur les colonnes, on ne change pas la base $\mathcal{D}$ d'arrivée (dans laquelle on exprime les colonnes de la matrice), mais on modifie la base $\mathfrak{B}$ de départ de l'application linéaire. Dans un pivot sur les lignes, on ne change pas la base $\mathcal{D}$ d'arrivée, mais on change la base $\mathfrak{B}$ de départ de l'application linéaire. Le point de vue du pivot sur les colonnes rend donc un peu plus facile l'interprétation des opérations élémentaires du point de vue des applications linéaires. On peut aussi utiliser le point de vue des formes linéaires pour interpréter les opérations sur les lignes dans le calcul du noyau, mais c'est une autre histoire.*

Théorème 3.15 (Propriété universelle du quotient dans les espaces vectoriels)**.** *Soit $W \subset V$ une inclusion d'espace vectoriels. Le groupe abélien quotient V/W est muni d'une structure d'espaces vectoriels telle que l'application de classe $\mathrm{cl}_W : V \to V/W$ vérifie la propriété suivante : pour toute application linéaire $f : V \to V'$ telle que $f(W) = \{0\}$, il existe une unique application linéaire $\bar{f} : V/W \to V'$ telle que $\bar{f} \circ \mathrm{cl}_W = f$, i.e., qui fait commuter le diagramme*



Démonstration. Ceci découle de la propriété universelle du quotient 1.42 dans les groupes abéliens. On munit V/W de la multiplication externe par K donnée, pour $\lambda \in K$ et $v \in V$, par la formule

$$\lambda \cdot (v + W) = (\lambda v) + W.$$

Ceci est bien défini car si $v + W = v' + W$, on a $v - v' \in W$. Comme $W \subset V$ est un sous-espace vectoriel, on en déduit

$$\lambda v - \lambda v' = \lambda(v - v') \in W,$$

ce qui implique $(\lambda v) + W = (\lambda v') + W$. Ceci munit V/W d'une structure d'espace vectoriel naturelle qui fait de $\mathrm{cl}_W : V \to V/W$ une application linéaire. □

Exemple 3.16. *L'ensemble* $\mathrm{Cauchy}(\mathbb{Q}, |\cdot|)$ *des suites de Cauchy de nombres rationnels forme un $\mathbb{Q}$-espace vectoriel. L'espace* $\mathrm{Cauchy}_0(\mathbb{Q}, |\cdot|)$ *des suites tendant vers* 0 *est un sous-espace*

vectoriel de Cauchy$(\mathbb{Q}, |\cdot|)$. *Le $\mathbb{Q}$-espace vectoriel quotient est le $\mathbb{Q}$-espace vectoriel des nombres réels*

$$\mathbb{R} = \text{Cauchy}(\mathbb{Q}, |\cdot|)/\text{Cauchy}_0(\mathbb{Q}, |\cdot|).$$

On peut en fait munir $\mathbb{R}$ d'une multiplication naturelle qui en fait une $\mathbb{Q}$-algèbre.

Corollaire 3.17. *Si $f : V \to V'$ est une application linéaire, elle induit un isomorphisme naturel*

$$\bar{f} : V/\text{Ker}(f) \xrightarrow{\sim} \text{Im}(f).$$

Démonstration. Ceci découle directement de la propriété universelle 3.15 du quotient dans les espaces vectoriels. □

Corollaire 3.18 (Théorème du rang)**.** *Soit $f : V \to V'$ une application linéaire avec V de dimension finie. Alors on a l'égalité*

$$\dim(V) = \dim(\text{Ker}(f)) + \dim(\text{Im}(f)).$$

En particulier, si $\dim(V') = \dim(V)$*, alors f est injective si et seulement si f est surjective si et seulement si f est bijective.*

Démonstration. On utilise les deux résultats précédents pour obtenir

$$\dim(\text{Im}(f)) = \dim(V/\text{Ker}(f)).$$

Soit $\{e_1, \dots, e_r\}$ une base de $\text{Ker}(f)$, qu'on complète en une base $\{e_1, \dots, e_n\}$ de V. On veut montrer que $\{f(e_{r+1}), \dots, f(e_n)\}$ forme une base de $\text{Im}(f)$. C'est bien une famille génératrice car si $x = \sum_{i=1}^{n} x_i e_i$ est dans E, on a

$$f(x) = \sum_{i=r+1}^{n} x_i f(e_i).$$

C'est aussi une famille libre. En effet, si $\sum_{i=r+1}^{n} \lambda_i f(e_i) = 0$ alors $f(\sum_{i=r+1}^{n} \lambda_i e_i) = 0$ donc $\sum_{i=r+1}^{n} \lambda_i e_i \in \text{Ker}(f)$ donc il existe λ_j tels que $\sum_{i=r+1}^{n} \lambda_i e_i = \sum_{j=1}^{r} \lambda_j e_j$, ce qui donne une combinaison linéaire nulle

$$\sum_{j=1}^{r} -\lambda_j e_j + \sum_{i=r+1}^{n} \lambda_i e_i = 0$$

des vecteurs de la base de V, dont les coefficients sont forcément tous nuls. On obtient $\dim(\text{Im}(f)) = \dim(V) - \dim(\text{Ker}(f))$, ce qui est le résultat souhaité. □

3.3 Déterminant

3.3.1 Déterminant des matrices 2×2

Soit k un corps, on rappelle que le déterminant d'une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(k)$ est

$$\det(A) = ad - bc.$$

On sait que A est inversible si et seulement si $\det(A) \neq 0$. En effet, on a

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} = \det(A) \cdot I_2 ;$$

ceci montre que si $\det(A) \neq 0$, alors $\frac{1}{\det(A)}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ est l'inverse de A.

Réciproquement, supposons A inversible, alors le système

$$(S) \qquad \begin{cases} ax + by &= 0 \\ cx + dy &= 0 \end{cases}$$

a $(0, 0)$ comme unique solution. En particulier, a, b ne sont pas simultanément nuls. Si $a \neq 0$ (resp. si $b \neq 0$), (S) est équivalent au système obtenu en remplaçant la ligne L_2 par $aL_2 - cL_1$ (resp. par $bL_2 - dL_1$) :

$$\begin{cases} ax + by &= 0 \\ (ad - bc)y &= 0 \end{cases} \qquad \text{resp.} \qquad \begin{cases} ax + by &= 0 \\ (bc - ad)x &= 0; \end{cases}$$

on en déduit que $ad - bc = 0$ (sinon, l'espace des solutions serait la droite d'équation $ax + by = 0$).

D'autre part, soit X une indéterminée ; on définit le « polynôme caractéristique » de A comme

$$P_A(X) = X^2 - (a + d)X + (ad - bc)$$

c'est-à-dire, c'est le « déterminant » de la matrice $\begin{pmatrix} a - X & b \\ c & d - X \end{pmatrix}$ à coefficients dans l'anneau de polynômes $k[X]$. Ceci conduit à définir, pour *tout anneau commutatif* R le déterminant d'une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R)$ comme $\det(A) = ad - bc$. Notons que le déterminant 2×2 ainsi défini vérifie les trois propriétés suivantes :

(1) C'est une fonction *R-linéaire* de *chacune des colonnes* $\begin{pmatrix} a \\ c \end{pmatrix}$ et $\begin{pmatrix} b \\ d \end{pmatrix}$ de la matrice A, c'est-à-dire, pour tous $t, a, b, c, d, \in R$, on a :

$$\det\begin{pmatrix} ta + a' & b \\ tc + c' & d \end{pmatrix} = (ta + a')d - b(tc + c') = t(ad - bc) + a'd - bc' = t\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \det\begin{pmatrix} a' & b \\ c' & d \end{pmatrix}$$

et

$$\det\begin{pmatrix} a & tb + b' \\ c & td + d' \end{pmatrix} = a(td + d') - (tb + b')c = t(ad - bc) + ad' - b'c = t\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \det\begin{pmatrix} a & b' \\ c & d' \end{pmatrix}$$

(2) Lorsque les deux colonnes sont égales, on a $\det(A) = 0$.

(3) $\det(I_2) = 1$.

On va voir que ces conditions s'étendent de façon naturelle pour les matrices $n \times n$, c'est-à-dire, on a le théorème suivant, où k désigne un *anneau commutatif arbitraire*. (Dans la suite, on s'intéressera uniquement au cas où k est un corps ou un anneau de polynômes sur un corps, mais ça ne coûte pas plus cher de le faire pour un anneau commutatif arbitraire, par exemple $\mathbb{Z}$, ou $\mathbb{Z}/n\mathbb{Z}$, ou $\mathbb{Z}[X]$, etc.)

3.3.2 Déterminant sur un anneau

Théorème 3.19 (Existence et propriétés du déterminant)**.** *Soit k un anneau commutatif et soit $n \in \mathbb{N}^*$.*

(a) *Il existe une unique fonction* det : $M_n(k) \to k$ *vérifiant les trois propriétés suivantes :*

(1) *C'est une fonction* k-linéaire *de* chacune des colonnes $A_1, \dots, A_n$ *de la matrice* A*, c'est-à-dire, pour tout* $i = 1, \dots, n$*, si* $A'_i \in M_{n,1}(k)$ *est une autre matrice colonne à coefficients dans* k *et si* $t \in k$*, on a :*

$$\det(A_1, \dots, tA_i + A'_i, \dots, A_n) = t \det(A_1, \dots, A_i, \dots, A_n) + \det(A_1, \dots, A'_i, \dots, A_n).$$

(2) *Si deux colonnes sont égales,* i.e. *s'il existe* $i \neq j$ *tels que* $A_i = A_j$*, alors* $\det(A) = 0$.

(3) $\det(I_n) = 1$.

Plus précisément, pour toute fonction $D : M_n(k) \to k$ *vérifiant les propriétés* (1) *et* (2)*, on a* $D = D(I_n) \cdot \det$.

(b) *Pour tout* $A, B \in M_n(k)$ *on a*

$$(*) \qquad \boxed{\det(BA) = \det(B) \cdot \det(A)}$$

$$(**) \qquad \boxed{\det({}^tA) = \det(A).}$$

(c) *Enfin, il existe une matrice* $\tilde{A}$ *(appelée la matrice des cofacteurs de* A*) telle que*

$$(***) \qquad \boxed{A \cdot {}^t\tilde{A} = \det(A) I_n = {}^t\tilde{A} \cdot A.}$$

Par conséquent A *est inversible si et seulement si* $\det(A)$ *est un élément inversible de* k*; dans ce cas, on a* $\boxed{\det(A^{-1}) = \det(A)^{-1}.}$

Démonstration. On va montrer d'abord que si une fonction $D : M_n(k) \to k$ vérifie les les propriétés (1) et (2), elle est entièrement déterminée par le scalaire $D(I_n)$. Ceci prouvera l'unicité, et permettra ensuite de construire par récurrence une fonction $\det : M_n(k) \to k$ vérifiant toutes les propriétés ci-dessus.

Soit donc $D : M_n(k) \to k$ vérifiant les propriétés (1) et (2). Notons d'abord que ces conditions entraînent les conditions $(2')$ et (2^-) qui suivent.

a) Pour $i \neq j$ dans $\{1, \dots, n\}$, D *ne change pas* si l'on ajoute à la colonne A_j un multiple tA_i de la colonne A_i, c'est-à-dire, on a :

$$(2') \qquad D(A_1, \dots, A_i, \dots, A_j + tA_i, \dots, A_n) = D(A_1, \dots, A_i, \dots, A_j, \dots, A_n).$$

Par conséquent, si une colonne, disons A_j, est combinaison k-linéaire des autres colonnes, c'est-à-dire, s'il existe des $t_i \in k$, pour $i \neq j$, tels que $A_j = \sum_{i \neq j} t_i A_i$ alors $D(A) = 0$. En effet, d'après (1), $D(A)$ est la somme pour $i \neq j$ des termes

$$D(A_1, \dots, A_i, \dots, t_i A_i, \dots, A_n)$$

(où $t_i A_i$ est à la j-ème place), et d'après $(2')$ chacun de ces termes est nul, d'où $D(A) = 0$.

b) Si l'on échange les colonnes i et j, la valeur de D est multipliée par -1, c'est-à-dire,

$$(2^-) \qquad D(A_1, \dots, A_j, \dots, A_i, \dots, A_n) = -D(A_1, \dots, A_i, \dots, A_j, \dots, A_n)$$

En effet, si l'on place $A_i + A_j$ dans les colonnes i et j, alors les conditions (2) et (1) entraînent que

$$\begin{aligned} 0 = D(\dots, A_i + A_j, \dots, A_i + A_j, \dots) = D(\dots, A_i, \dots, A_i, \dots) + D(\dots, A_j, \dots, A_j, \dots) \\ + D(\dots, A_i, \dots, A_j, \dots) + D(\dots, A_j, \dots, A_i, \dots) \end{aligned}$$

or dans le dernier membre les deux premiers termes sont nuls, par (2) à nouveau, d'où

$$D(\dots, A_i, \dots, A_j, \dots) = -D(\dots, A_j, \dots, A_i, \dots),$$

ce qui prouve (2^-).

Unicité. Montrons maintenant que les conditions (1) et (2) permettent de calculer D en fonction du scalaire $\lambda = D(I_n)$. On procède par récurrence sur n. Si $n = 1$, alors $M_1(k) = \{(a) \mid a \in k\}$ et $I_1 = (1)$, donc toute application linéaire $D : M_1(k) \to k$ est de la forme $(a) \mapsto \lambda a$, où $\lambda = D(I_1)$. Soit donc $n \geq 2$ et supposons avoir établi qu'il existe une application

$$\det_{n-1} : M_{n-1}(k) \to k$$

vérifiant les conditions (1), (2), (3), et que pour toute application $\psi : M_{n-1}(k) \to k$ vérifiant les conditions (1) et (2), on a

$$\psi = \psi(I_{n-1}) \cdot \det_{n-1}$$

(ceci implique, en particulier, que $\det_{n-1}$ est uniquement déterminé).

Soit $A = (a_{ij})$ un élément arbitraire de $M_n(k)$. Considérons les matrices colonnes suivantes :

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad \cdots \qquad e_n = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

alors la première colonne A_1 de A s'écrit $A_1 = a_{11}e_1 + \cdots + a_{n1}e_n$ donc, d'après (1), on a :

$$(\dagger') \qquad D(A) = \sum_{i=1}^{n} a_{i1}\, D(A'(i,1)),$$

où l'on désigne par $A'(i,1)$ la matrice dont les colonnes sont $e_i, A_2, \dots, A_n$, *i.e.*

$$A'(i,1) = \begin{pmatrix} 0 & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

Soit alors $A''(i,1)$ la matrice dont les colonnes sont : $e_i, A_2 - a_{i2}e_i, \dots, A_n - a_{in}e_i$, c'est-à-dire,

$$A''(i,1) = \begin{pmatrix} 0 & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{i-1,2} & \cdots & a_{i-1,n} \\ 1 & 0 & \cdots & 0 \\ 0 & a_{i+1,2} & \cdots & a_{i+1,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

On a $D(A''(i,1)) = D(A'(i,1))$ d'après $(2')$, et donc $(\dagger')$ devient :

$$(\dagger'') \qquad D(A) = \sum_{i=1}^{n} a_{i1}\, D(A''(i,1)).$$

Pour $i = 1, \ldots, n$, notons φ_i la fonction $M_{n-1}(k) \to k$ qui à tout $B \in M_{n-1}(k)$ associe $D(\tilde{B}(i,1))$, où $\tilde{B}(i,1)$ désigne la matrice :

$$\begin{pmatrix} 0 & b_{11} & \cdots & b_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_{i-1,1} & \cdots & b_{i-1,n-1} \\ 1 & 0 & \cdots & 0 \\ 0 & b_{i,1} & \cdots & b_{i,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_{n-1,1} & \cdots & b_{n-1,n-1} \end{pmatrix}.$$

Alors, φ_i vérifie les conditions (1) et (2). De plus, on a

$$\tilde{I_{n-1}}(i,1) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 1 \end{pmatrix}$$

et cette matrice est déduite de la matrice identité I_n en faisant glisser la i-ème colonne à la première place, c'est-à-dire, en faisant $i-1$ échanges de colonnes, d'où

$$\varphi_i(I_{n-1}) = D(\tilde{I_{n-1}}(i,1)) = (-1)^{i-1} D(I_n) = (-1)^{i+1} D(I_n)$$

donc, d'après l'hypothèse de récurrence, on obtient :

$$(\ddagger_i) \qquad \varphi_i = D(I_n)(-1)^{i+1} \det_{n-1}.$$

Notons $A(i,1) = A - L_i - C_1$ l'élément de $M_{n-1}(k)$ obtenu à partir de A en supprimant la i-ème ligne et la première colonne, alors d'après $(\ddagger_i)$ on a

$$D(A''(i,1)) = D(I_n)(-1)^{i+1} \det_{n-1}(A - L_i - C_1)$$

et donc $(\dagger'')$ donne :

$$(\star^1) \qquad D(A) = D(I_n) \sum_{i=1}^{n} (-1)^{i+1} a_{i1} \det_{n-1}(A - L_i - C_1).$$

Donc, si D vérifie (1) et (2), elle est déterminé par le scalaire $D(I_n) \in k$, d'après la formule $(\star^1)$ ci-dessus.

De plus, soit j un indice de colonne arbitraire, faisant glisser la colonne A_j à la première place, on obtient

$$D(A) = (-1)^{j-1} D(A_j, A_1, \ldots, A_{j-1}, A_{j+1}, \ldots, A_n),$$

puis appliquant $(\star^1)$ à la matrice $(A_j, A_1, \ldots, A_{j-1}, A_{j+1}, \ldots, A_n)$, on obtient :

$$(\star^j) \qquad D(A) = D(I_n) \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det_{n-1}(A - L_i - C_j),$$

ce qui montre que si D vérifie (1) et (2), alors elle vérifie les égalités $(\star^j)$ pour tout $j = 1, \ldots, n$.

Remarque 3.20. *1) Pour ceux qui ont déjà rencontré les déterminants, on reconnaît dans* $(\star^j)$ *le développement d'un déterminant selon la* j*-ème colonne.*

2) En répétant le calcul précédent pour $\det_{n-1}$*, puis* $\det_{n-2}$*, etc., on obtiendrait que si* D *vérifie (1) et (2), elle est* nécessairement donnée *par une certaine formule*

$$D(A) = D(I_n) \sum_{\sigma \in S_n} \epsilon(\sigma)\, a_{1\sigma(1)} \cdots a_{n\sigma(n)}\,,$$

où S_n *désigne le groupe des permutations (c'est-à-dire, bijections) de l'ensemble* $\{1, \ldots, n\}$*, et où* $\epsilon(\sigma)$ *est un signe* ± 1*, explicitement déterminé en fonction de* σ*. On pourrait alors montrer* l'existence *de* $\det_n$ *en montrant que la fonction*

$$A \mapsto \sum_{\sigma \in S_n} \epsilon(\sigma)\, a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

vérifie (1), (2) et (3). Toutefois, il est plus simple de montrer l'existence de $\det_n$ *comme suit.*

Existence. Fixons un indice de ligne i arbitraire, et pour $j = 1, \ldots, n$ notons

$$\Delta_{ij}(A) = \det_{n-1}(A - L_i - C_j),$$

où $A - L_i - C_j$ désigne l'élément de $M_{n-1}(k)$ obtenu à partir de A en supprimant la i-ème ligne et la j-ème colonne. Considérons la fonction $D_i : M_n(k) \to k$ définie par

$$(\star_i) \qquad D_i(A) = \sum_{j=1}^{n} (-1)^{j+i} a_{ij}\, \Delta_{ij}(A),$$

et montrons que D_i vérifie les conditions (1), (2) et (3).

Fixons un indice de colonne ℓ. Alors les fonctions $A \mapsto a_{i\ell}$ et $A \mapsto \Delta_{ij}$ pour $j \neq \ell$ sont des fonctions linéaires de C_ℓ, tandis que les fonctions $A \mapsto \Delta_{i\ell}$ et $A \mapsto a_{ij}$ pour $j \neq \ell$ ne dépendent pas de C_ℓ, donc la somme dans $(\star_i)$ est bien une fonction linéaire de chaque colonne C_ℓ, *i.e.* (1) est vérifée.

Lorsque $A = I_n$, la matrice $I_n - L_i - C_j$ a sa i-ème colonne nulle si $j \neq i$, et égale I_{n-1} si $j = i$, donc la somme dans $(\star_i)$ égale $\det_{n-1}(I_{n-1}) = 1$, donc (3) est vérifiée.

Enfin, supposons qu'il existe $p < q$ tels que les colonnes C_p et C_q de A soient égales. Alors, d'une part on a $\Delta_{ij}(A) = 0$ pour $j \neq p, q$. D'autre part, les matrices $A - L_i - C_p$ et $A - L_i - C_q$ se déduisent l'une de l'autre par $q - 1 - p$ échanges de colonnes, car la colonne $C = C_p = C_q$ est à la place p dans $A - L_i - C_q$ et à la place $q - 1$ dans $A - L_i - C_p$. Donc

$$\Delta_{ip}(A) = (-1)^{q-1-p} \Delta_{iq}(A) \qquad \textit{i.e.} \qquad \Delta_{iq}(A) = (-1)^{p+1-q} \Delta_{iq}(A).$$

Posant $\alpha = a_{ip} = a_{iq}$, l'égalité $(\star_i)$ donne alors :

$$D_i(A) = \alpha\, \Delta_{ip}(A)\, \big((-1)^{i+p} + (-1)^{i+q+p+1-q}\big) = (-1)^{i+p} \alpha\, \Delta_{ip}(A)\, (1 - 1) = 0,$$

donc (2) est vérifiée. Compte-tenu de ce qui précède, ceci prouve que $\det_n(A) = D_i(A)$ *ne dépend pas* de i et est l'unique application $M_n(k) \to k$ vérifiant (1), (2) et (3) ; de plus toute application $D : M_n(k) \to k$ vérifiant (1) et (2) égale $D(I_n) \cdot \det_n$.

On a donc démontré le point (a) du théorème 3.19, et l'on a obtenu au passage les formules de développement suivant une ligne $(\star_i)$ ou suivant une colonne $(\star^j)$.

Prouvons le point (b). Fixons $B \in M_n(k)$. Alors, pour tout $A \in M_n(k)$, les colonnes de la matrice BA sont $BA_1, \ldots, BA_n$, où $A_1, \ldots, A_n$ désignent les colonnes de A. Par conséquent, comme chaque application $A_i \mapsto BA_i$ est linéaire, l'application

$$\varphi_B : \quad A \mapsto \det(BA) = \det(BA_1, \ldots, BA_n)$$

vérifie (1) et (2), donc est égale à $\varphi_B(I_n) \cdot \det$; comme $\varphi_B(I_n) = \det(B)$ on obtient

$$(*) \qquad \det(BA) = \det(B) \cdot \det(A).$$

Montrons que $\det({}^tA) = \det(A)$, en procédant par récurrence sur n. Il n'y a rien à montrer si $n = 1$, donc on peut supposer $n \geq 2$ et le résultat établi pour $n - 1$. Soient $A \in M_n(k)$. D'après $(\star_1)$ appliqué à ${}^tA$, on a

$$\det({}^tA) = \sum_{j=1}^{n} (-1)^{j+1} ({}^tA)_{1j} \, \Delta_{1j}({}^tA) \, .$$

Or, $({}^tA)_{1j} = a_{j1}$ et

$$\Delta_{1j}({}^tA) = \det_{n-1}\Big({}^tA - L_1({}^tA) - C_j({}^tA)\Big) = \det_{n-1}\Big({}^t(A - C_1(A) - L_j(A))\Big)$$
$$= \det_{n-1}\Big(A - C_1(A) - L_j(A)\Big) = \Delta_{j1}(A)$$

(l'avant-dernière égalité d'après l'hypothèse de récurrence). On obtient donc

$$\det({}^tA) = \sum_{j=1}^{n} (-1)^{j+1} a_{j1} \, \Delta_{j1}(A) = \det(A),$$

la seconde égalité étant $(\star^1)$. On a donc prouvé le point (b) du théorème 3.19.

Définition 3.21 (Matrice des cofacteurs)**.** *Pour $i, j \in \{1, \ldots, n\}$, $(-1)^{i+j}\Delta_{ij}(A)$ est appelé le* cofacteur *de A d'indice (i, j). On appelle* matrice des cofacteurs *de A la matrice $\tilde{A}$ dont le coefficient d'indice (i, j) est $\tilde{A}_{ij} = (-1)^{i+j}\Delta_{ij}(A)$.*

Démontrons maintenant le point (c) du théorème 3.19. Pour tout $i, \ell \in \{1, \ldots, n\}$, on a :

$$(A \, {}^t\tilde{A})_{i\ell} = \sum_{j=1}^{n} a_{ij} \, ({}^t\tilde{A})_{j\ell} = \sum_{j=1}^{n} (-1)^{j+\ell} a_{ij} \, \Delta_{\ell j}(A)$$

et l'on reconnaît là le développement suivant la ligne ℓ du déterminant de la matrice $B(\ell, i)$ déduite de A en remplaçant la ligne d'indice ℓ par celle d'indice i. Donc $(A \, {}^t\tilde{A})_{i\ell} = 0$ si $\ell \neq i$ (car $B(\ell, i)$ a alors deux lignes égales), et $(A \, {}^t\tilde{A})_{ii} = \det(A)$ si $\ell = i$. Ceci montre que

$$A \, {}^t\tilde{A} = \det(A) \cdot I_n.$$

De même,

$$({}^t\tilde{A} \, A)_{i\ell} = \sum_{j=1}^{n} (-1)^{i+j} \Delta_{ji}(A) \, a_{j\ell}$$

et l'on reconnaît là le développement suivant la colonne i du déterminant de la matrice $B'(i, \ell)$ déduite de A en remplaçant la colonne d'indice i par celle d'indice ℓ. Donc, à nouveau, $({}^t\tilde{A} \, A)_{i\ell} = 0$ si $\ell \neq i$, et $= \det(A)$ si $\ell = i$, d'où

$${}^t\tilde{A} \, A = \det(A) \cdot I_n.$$

On a ainsi montré les égalités (∗∗∗) de 3.19 ; de plus, ceci montre que si $\det(A)$ est inversible dans k (*i.e.* s'il existe $\alpha \in k$ tel que $\alpha \cdot \det(A) = 1$), alors $\det(A)^{-1}\,{}^t\tilde{A}$ est *l'inverse* de A. Réciproquement, si A est inversible, l'égalité $AA^{-1} = I_n$ et la *multiplicativité du déterminant* $(*)$ entraînent $\det(A)\det(A^{-1}) = 1$, donc $\det(A)$ est inversible dans k, son inverse étant

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

Ceci achève la preuve du théorème 3.19. □

Corollaire 3.22. *Soient k un anneau commutatif, $A, P \in M_n(k)$ avec P inversible, alors*

$$\boxed{\det(P^{-1}AP) = \det(P^{-1})\det(A)\det(P) = \det(A).}$$

Remarque 3.23 (Forme explicite du déterminant)**.** *Soit S_n le groupe des permutations (c'est-à-dire, bijections) de $\{1, \dots, n\}$. En procédant par récurrence sur n, on déduit de la formule de développement suivant une ligne (ou bien une colonne) que, pour toute matrice $A = (a_{ij})_{1\le i,j\le n}$ on a une formule explicite :*

$$\det(A) = \sum_{\sigma \in S_n} \epsilon(\sigma)\, a_{1\sigma(1)} \cdots a_{n\sigma(n)}\,, \qquad \text{où} \quad \epsilon(\sigma) = \pm 1$$

c'est-à-dire, c'est la somme, avec certains signes + ou −, de tous les produits de n coefficients de A, en ne prenant dans chaque produit qu'un seul coefficient par ligne et par colonne ; de plus le terme « diagonal »$a_{11}a_{22}\cdots a_{nn}$ (qui correspond à $\sigma = \mathrm{id}$) est précédé du signe « + ». (On verra plus loin comment calculer explicitement le signe $\epsilon(\sigma)$; par exemple si $n = 3$ on a $\det(A) = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{32}a_{21} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32}$.*)*

Proposition 3.24 (Déterminant de matrices triangulaires)**.** 1) *Si A est une matrice triangulaire de termes diagonaux $\lambda_1, \dots, \lambda_n$, alors*

$$\det(A) = \lambda_1 \cdots \lambda_n.$$

2) *Plus généralement, si A est une matrice triangulaire par blocs, c'est-à-dire, de la forme*

$$A = \left(\begin{array}{c|c|c|c} A_1 & * & \cdots & * \\ \hline 0 & A_2 & \ddots & * \\ \hline 0 & \ddots & \ddots & * \\ \hline 0 & \cdots & 0 & A_n \end{array}\right)$$

(où les $*$ désignent des coefficients arbitraires), alors

$$\det(A) = \det(A_1)\cdots\det(A_n).$$

Démonstration. 1) Supposons que A soit une matrice triangulaire supérieure :

$$A = \begin{pmatrix} \lambda_1 & * & \cdots & * \\ 0 & \lambda_2 & \ddots & \vdots \\ 0 & \ddots & \ddots & * \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}$$

alors en développant par rapport à la première colonne, on obtient que

$$\det(A) = \lambda_1 \det\begin{pmatrix} \lambda_2 & * & * \\ 0 & \ddots & * \\ 0 & 0 & \lambda_n \end{pmatrix};$$

le résultat en découle, en répétant l'opération ou en procédant par récurrence sur n.

2) En procédant par récurrence sur n, il suffit de montrer que si

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

où B (resp. D) est une matrice carrée de taille p (resp. q), C est une matrice à p lignes et q colonnes, et 0 désigne la matrice nulle à q lignes et p colonnes, alors

$$\det(A) = \det(B) \cdot \det(D).$$

Fixons C, D et considérons l'application φ qui à une matrice $B' \in M_p(k)$ associe

$$\varphi(B') = \det\begin{pmatrix} B' & C \\ 0 & D \end{pmatrix}.$$

Alors on voit aussitôt que φ vérifie les propriétés (1) et (2), donc d'après le théorème 3.19, on a

$$\varphi(B') = \varphi(I_p) \cdot \det(B') = \det\begin{pmatrix} I_p & C \\ 0 & D \end{pmatrix} \cdot \det(B');$$

de plus, en développant suivant la première colonne, puis suivant la seconde, etc... jusqu'à la p-ème colonne, on obtient que

$$\det\begin{pmatrix} I_p & C \\ 0 & D \end{pmatrix} = \det D,$$

d'où finalement $\det(A) = \varphi(B) = \det(B) \cdot \det(D)$. □

Remarque 3.25. *Attention ! Si on décompose une matrice M sous la forme*

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

où A, B, C, D sont toutes des matrices carrées (nécessairement de même taille p, de sorte que M est de taille $2p$), il n'est pas vrai en général que $\det(M)$ *égale* $\det(A)\det(D) - \det(B)\det(C)$. *Par exemple si*

$$M = \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right)$$

alors $\det(A) = 0 = \det(B) = \det(C) = \det(D)$ *mais* $\det(M) = -1$.

3.3.3 Cas d'un corps

Supposons dans ce paragraphe que l'anneau de base k soit un corps. Alors, en plus des propriétés (1), (2) et (2′), (2⁻) de 3.19, le déterminant vérifie la propriété suivante :

(2″) Si les colonnes $A_1, \dots, A_n$ sont liées, alors $\det(A_1, \dots, A_n) = 0$.

En effet, si les colonnes $A_1, \dots, A_n$ sont liées, il existe $t_1, \dots, t_n \in k$ non tous nuls tels que $t_1A_1 + \cdots + t_nA_n = 0$. Soit j tel que $t_j \neq 0$, alors

$$A_j = -\sum_{i \neq j} t_i t_j^{-1} A_i.$$

Donc, d'après (1), $\det(A)$ est la somme pour $i \neq j$ des termes

$$-t_i t_j^{-1} \det(\dots, A_i, \dots, A_i, \dots)$$

(où A_i apparaît aux places i et j), et d'après (2) chacun de ces termes est nul, d'où $\det(A) = 0$. Ceci prouve (2″).

D'autre part, et c'est le plus important, pour calculer pratiquement un déterminant, on ne procède pas véritablement en développant suivant les lignes ou les colonnes (ce qui serait trop fastidieux, et couteux en temps de calcul), mais on essaie de faire des opérations élémentaires sur les lignes ou les colonnes, pour rendre la matrice triangulaire.

C'est-à-dire, soit $A = (a_{ij})$ un élément arbitraire de $M_n(k)$. Si la première ligne de A est nulle, alors $\det(A) = 0$ (en développant suivant la première ligne, ou bien en utilisant $\det(A) = \det({}^tA)$), et il n'y a rien à calculer. Supposons donc qu'il existe au moins une colonne C_j telle que $a_{1j} \neq 0$. Faisons glisser la colonne C_j au-dessus de $C_1, \dots, C_{j-1}$ pour l'amener à la première place ; ceci introduit le signe $(-1)^{j-1}$, puis mettons a_{1j} en facteur, ceci donne :

$$\det(A) = (-1)^{j-1} a_{1j} \det(a_{1j}^{-1} C_j, C_1, \dots, C_{j-1}, C_{j+1}, \cdots, C_n).$$

Soustrayons alors $a_{1\ell} a_{1j}^{-1} C_j$ de C_ℓ, pour $\ell \neq j$, pour annuler les coefficients de la première ligne autres que le premier ; ceci ne change pas la valeur du déterminant et l'on obtient donc que

$$(\dagger) \qquad \det(A) = (-1)^{j-1} a_{1j} \det \begin{pmatrix} 1 & 0 \\ v & A' \end{pmatrix} = (-1)^{j-1} a_{1j} \det(A')$$

où A' est la matrice carrée de taille $n-1$ formée des lignes d'indice 2 à n des vecteurs $C_\ell - a_{1\ell} a_{1j}^{-1} C_j$, pour $\ell \in \{1, \dots, n\} - \{j\}$ (ces vecteurs ont tous leur première ligne nulle). On répète ensuite l'opération pour A', etc. Illustrons ceci par un :

Exemple 3.26. *Calculons le déterminant suivant (où $n \in \mathbb{Z}$) :*

$$D = \begin{vmatrix} 2 & 3 & 4 & 5 \\ 7 & 6 & 9 & 8 \\ 10 & 11 & 12 & 13 \\ 14 & 15 & 16 & n \end{vmatrix}$$

Mettant $a_{11} = 2$ en facteur dans la première colonne et remplaçant C_2, C_3 et C_4 par $C_2 - (3/2)C_1$, $C_3 - 2C_1$ et $C_4 - (5/2)C_1$ on obtient :

$$D = 2 \begin{vmatrix} 1 & 0 & 0 & 0 \\ 7/2 & -9/2 & -5 & -19/2 \\ 5 & -4 & -8 & -12 \\ 7 & -6 & -12 & n-35 \end{vmatrix} = 2 \begin{vmatrix} -9/2 & -5 & -19/2 \\ -4 & -8 & -12 \\ -6 & -12 & n-35 \end{vmatrix}$$

puis remplaçant chaque colonne par son opposé (ce qui introduit un signe $(-1)^3$), mettant 4 en facteur dans la 2ème ligne, puis échangeant L_1 et L_2 (ce qui introduit un signe -1), on obtient :

$$D = 2 \cdot 4 \cdot (-1)^4 \begin{vmatrix} 1 & 2 & 3 \\ 9/2 & 5 & 19/2 \\ 6 & 12 & 35-n \end{vmatrix} = 8 \begin{vmatrix} 1 & 2 & 3 \\ 9/2 & 5 & 19/2 \\ 6 & 12 & 35-n \end{vmatrix}$$

puis remplaçant C_2 et C_3 par $C_2 - 2C_1$ et $C_2 - 3C_1$ on obtient :

$$D = 8 \begin{vmatrix} 1 & 0 & 0 \\ 9/2 & -4 & -4 \\ 6 & 0 & 17-n \end{vmatrix} = 8 \begin{vmatrix} -4 & -4 \\ 0 & 17-n \end{vmatrix} = 32(n-17).$$

3.4 Endomorphismes : déterminant, trace, valeurs propres, etc.

Soit V un espace vectoriel de dimension n. En raison de son importance, répétons encore ici le théorème de changement de base pour un endomorphisme u de V (étant entendu qu'on exprime la matrice de u dans une même base au départ et à l'arrivée) :

Théorème 3.27 (Changement de base pour un endomorphisme)**.** *Soit A la matrice d'un endomorphisme u de V relativement à une base $\mathfrak{B}$ de V. Si $\mathfrak{B}'$ est une seconde base, et si P est la matrice de passage de $\mathfrak{B}$ à $\mathfrak{B}'$, alors la matrice de u dans la base B' est :*

$$\mathrm{Mat}_{\mathfrak{B}'}(u) = P^{-1}AP.$$

Ceci permet de définir le déterminant et le polynôme caractéristique de u comme suit.

Théorème/Définition 3.1 (Déterminant, polynôme caractéristique et trace d'un endomorphisme)**.** *Soit $u \in \mathrm{End}_k(V)$ et soit A sa matrice dans une base $\mathfrak{B}$ de V. On définit le déterminant et le polynôme caractéristique de u par :*

$$\det(u) = \det(A), \qquad P_u(X) = \det(A - XI_n) \in k[X];$$

ceci ne dépend pas du choix de la base $\mathfrak{B}$. De plus, $P_u(X)$ est de degré $n = \dim_k(V)$ et est de la forme

$$P_u(X) = (-1)^n X^n + (-1)^{n-1}\mathrm{tr}(u)X^{n-1} + \cdots + \det(u).$$

Le coefficient $\mathrm{tr}(u)$ *s'appelle la* trace *de u, il est égal à la somme des coefficients diagonaux a_{ii} de A (et ceci ne dépend pas de la base choisie).*

Démonstration. En effet, soient $\mathfrak{B}'$ une autre base, P la matrice de passage, et A' la matrice de u dans la base $\mathfrak{B}'$. Alors on a $A' = P^{-1}AP$ et donc aussi

$$A' - XI_n = P^{-1}(A - XI_n)P$$

(égalité dans l'anneau $M_n(k[X])$ des matrices à coefficients dans $k[X]$). Donc, d'après la multiplicativité du déterminant (*cf.* 3.22), on a

$$\det(A') = \det(A), \qquad \det(A' - XI_n) = \det(A - XI_n)$$

ce qui prouve que $\det(u)$ et $P_u(X)$ sont bien définis. De plus, notons b_{ij} les coefficients de la matrice $A - XI_n$, *i.e.* $b_{ij} = a_{ij}$ si $i \neq j$ et $b_{ii} = a_{ii} - X$. D'après la formule 3.23, on a

$$P_u(X) = \sum_{\sigma \in S_n} \epsilon(\sigma)\, b_{1\sigma(1)} \cdots b_{n\sigma(n)}$$

c'est-à-dire, c'est la somme, avec certains signes + ou −, de tous les produits de n coefficients de $B = A - XI_n$, en ne prenant dans chaque produit qu'un seul coefficient dans chaque ligne et chaque colonne, et de plus on a $\epsilon(\mathrm{id}) = 1$, *i.e.* le terme $b_{11}b_{22}\cdots b_{nn}$ apparaît avec le signe +.

Donc, le terme de degré maximal en X est $(-X)^n$, qui s'obtient en développant le produit des termes diagonaux :

$$b_{11}b_{22}\cdots b_{nn} = (a_{11} - X)\cdots(a_{nn} - X).$$

Pour avoir un terme en X^{n-1}, il faut prendre $n-1$ fois $(-X)$ sur la diagonale, mais alors, comme chaque produit de n coefficients n'a qu'un seul coefficient par ligne et par colonne, le dernier terme du produit est le coefficient diagonal restant, dans lequel on prend le terme a_{ii}. Ceci montre que le coefficient de $(-X)^{n-1}$ est

$$a_{11} + \cdots + a_{nn},$$

qu'on appelle la trace de A. Comme $P_u(X)$ ne dépend pas de la base choisie, ce coefficient n'en dépend pas non plus ; on l'appelle la trace de u et on le note $\mathrm{tr}(u)$. □

Remarque 3.28. *On peut aussi montrer directement que, pour tout $A, B \in M_n(k)$, on a* $\mathrm{tr}(AB) = \mathrm{tr}(BA)$*, d'où* $\mathrm{tr}(P^{-1}AP) = \mathrm{tr}(APP^{-1}) = \mathrm{tr}(A)$.

D'après le théorème 3.19, on a :

Proposition 3.29. *Soit $u \in \mathrm{End}_k(V)$ ($\dim_k(V) = n$). Les conditions suivante sont équivalentes :*

1. *u est injectif ;*
2. *u est surjectif ;*
3. *u est bijectif ;*
4. $\det(u) \neq 0$.

Définition 3.30 (Valeurs, vecteurs et sous-espaces propres)**.** *1) Soit $u \in \mathrm{End}_k(V)$. On dit que $\lambda \in k$ est une* valeur propre *de u si* $\mathrm{Ker}(u - \lambda\mathrm{id}_V) \neq 0$ *(*i.e. *s'il existe $v \in V - \{0\}$ tel que $u(v) = \lambda v$). Dans ce cas, $V_\lambda = \mathrm{Ker}(u - \lambda\mathrm{id}_V)$ est appelé* l'espace propre *associé à λ, et tout vecteur $v \in V_\lambda - \{0\}$ est appelé un* vecteur propre *de u, associé à la valeur propre λ.*

2) Pour $A \in M_n(k)$, on définit ses valeurs, vecteurs et sous-espaces propres comme étant ceux de l'endomorphisme u de k^n défini par A, c'est-à-dire, λ est valeur propre de A si et seulement si $V_\lambda = \mathrm{Ker}(A - \lambda I_n)$ est non nul.

Proposition 3.31. *Soient $u \in \mathrm{End}_k(V)$ et $\lambda \in k$, alors λ est une valeur propre de u si et seulement si $P_u(\lambda) = 0$.*

Démonstration. D'après la proposition 3.29, λ est valeur propre de u si et seulement si $\det(u - \lambda\mathrm{id}_V) = 0$. D'autre part, d'après la formule explicite exprimant le déterminant d'une matrice A en fonction des coefficients a_{ij} de A (*cf.* Remarque 3.23), on voit que :

$$\det(u - \lambda\mathrm{id}_V) = P_u(\lambda)$$

c'est-à-dire, calculer le polynôme $P_u(X) = \det(A - XI_n)$, où $A = \mathrm{Mat}_{\mathfrak{B}}(u)$, puis l'évaluer en $X = \lambda$ « est la même chose » que de calculer $\det(A - \lambda I_n)$. Ceci démontre la proposition. □

Signalons aussi le lemme utile suivant :

Lemme 3.32. *Soient $u \in \mathrm{End}_k(V)$ et $v \in V$ un vecteur propre pour une valeur propre $\lambda \in k$. Alors, pour tout $Q \in k[X]$ on a $Q(u)(v) = Q(\lambda)\, v$.*

Démonstration. En effet, on a $u(v) = \lambda v$, donc $u^2(v) = u(u(v)) = u(\lambda v) = \lambda u(v) = \lambda^2 v$, et l'on montre par récurrence sur n que $u^n(v) = \lambda^n v$ pour tout $n \in \mathbb{N}$. Alors, pour tout polynôme $Q = a_0 + a_1 X + \cdots + a_d X^d$, on a :

$$Q(u)(v) = (a_0 \mathrm{id}_V + a_1 u + \cdots + a_d u^d)(v) = a_0 v + a_1 u(v) + \cdots + a_d u^d(v) = a_0 v + a_1 \lambda v + \cdots + a_d \lambda^d v = Q(\lambda)\, v.$$

□

3.5 Espaces propres et critères de diagonalisabilité

Définition 3.33 (Sous-espaces en somme directe)**.** *Soient V un k-espace vectoriel, $E_1, \ldots, E_n$ des sous-espaces de V. (Ni V ni les E_i ne sont supposés de dimension finie.)*

1. *D'abord, on note $E_1 + \cdots + E_n$ (ou $\sum_{i=1}^n E_i$) le sous-espace de V engendré par $E_1 \cup \cdots \cup E_n$; c'est l'ensemble de toutes les sommes*

   $$(*) \qquad x_1 + \cdots + x_n, \qquad \text{avec } x_i \in E_i.$$

2. *On dit que les E_i* sont en somme directe *si pour tous $x_1 \in E_1$, …, $x_n \in E_n$, l'égalité $x_1 + \cdots + x_n = 0$ entraîne $x_1 = 0 = \cdots = x_n$. Ceci équivaut à dire que tout élément x de $E_1 + \cdots + E_n$ s'écrit* de façon unique *$x = x_1 + \cdots + x_n$ avec $x_i \in E_i$. Dans ce cas, $E_1 + \cdots + E_n$ est noté $E_1 \oplus \cdots \oplus E_n$ ou $\bigoplus_{i=1}^n E_i$.*

3. *Si chaque E_i est de dimension finie d_i, et si $\mathfrak{B}_1 = (e_1, \ldots, e_{d_1})$ est une base de E_1, et $\mathfrak{B}_2 = (e_{d_1+1}, \ldots, e_{d_1+d_2})$ une base de E_2, …puis $\mathfrak{B}_n = (e_{d_1+\cdots+d_{n-1}+1}, \ldots, e_{d_1+\cdots+d_n})$ une base de E_n, la condition précédente équivaut à dire que la famille $\mathcal{F} = (e_1, \ldots, e_{d_1+\cdots+d_n})$ est une base de $E_1 + \cdots + E_n$, et comme $\mathcal{F}$ engendre de toute façon $E_1 + \cdots + E_n$, ceci équivaut aussi à dire que*

   $$(\star) \qquad \dim(E_1 + \cdots + E_n) = \dim(E_1) + \cdots + \dim(E_n).$$

Terminologie. *Si $E_1, \ldots, E_n$ sont en somme directe et si de plus $E_1 \oplus \cdots \oplus E_n$ égale V, alors on dit que V est la somme directe des E_i.*

Remarque 3.34. *(1) Il résulte de la définition que $E_1, \ldots, E_n$ sont en somme directe si et seulement si, pour tout $i = 1, \ldots, n$, on a : $E_i \cap \sum_{j \neq i} E_j = 0$.*

(2) En particulier, si $n = 2$, alors E_1 et E_2 sont en somme directe si et seulement si $E_1 \cap E_2 = (0)$.

(3) **Attention !** *Si des sous-espaces sont en somme directe, leur somme n'est pas nécessairement égale à l'espace tout entier : par exemple si E_1, E_2 sont deux droites distinctes dans $\mathbb{R}^3$, leur somme est directe, et c'est un plan de $\mathbb{R}^3$, et non $\mathbb{R}^3$ tout entier !*

(4) **Attention !** *Si $n \geq 3$, la condition $E_i \cap E_j = \{0\}$ pour $i \neq j$* n'entraîne pas *que la somme des E_i soit directe : par exemple si E_1, E_2, E_3 sont trois droites distinctes dans $\mathbb{R}^2$, elles vérifient $E_i \cap E_j = \{0\}$ pour $i \neq j$, mais leur somme n'est pas directe (car $E_1 + E_2$ égale $\mathbb{R}^2$ donc contient E_3).*

Définition 3.35 (Sous-espaces supplémentaires)**.** *Soient V un espace vectoriel, E, F deux sous-espaces de V. On dit que E et F sont des sous-espaces* supplémentaires *si $V = E \oplus F$, c'est-à-dire, si $E \cap F = (0)$ et $E + F = V$.*

Si V est de dimension finie, ceci équivaut à dire que $E \cap F = (0)$ et $\dim(E) + \dim(F) = \dim(V)$.

Proposition 3.36. *Soit V un k-espace vectoriel de dimension finie n. Tout sous-espace E de V admet un supplémentaire.*

Démonstration. Soit $(e_1, \dots, e_r)$ une base de E, complétons-la en une base $(e_1, \dots, e_n)$ de V et soit F le sous-espace de V engendré par $e_{r+1}, \dots, e_n$. Alors $E \cap F = \{0\}$ et $E + F = V$, donc $V = E \oplus F$.

Exercice 3.37. *Soient V un espace vectoriel, E (resp. F) un sous-espace de dimension finie m (resp. n). Soit $(v_1, \dots, v_r)$ une base de $E \cap F$, complétons-la en une base $(e_1, \dots, e_{m-r}, v_1, \dots, v_r)$ de E (resp. $(v_1, \dots, v_r, f_1, \dots, f_{n-r})$ de F). Montrer que $(e_1, \dots, e_{m-r}, v_1, \dots, v_r, f_1, \dots, f_{n-r})$ est une base de $E + F$. En déduire l'égalité $\dim(E + F) = \dim(E) + \dim(F) - \dim(E \cap F)$.*

Remarque 3.38. *Soient V un k-espace vectoriel et $f : V \to k$ une forme linéaire sur V. Supposons $f \neq 0$ et notons $H = \mathrm{Ker}(f)$. Comme $f \neq 0$, il existe $v \in V$ tel que $f(v) \neq 0$, et remplaçant v par $f(v)^{-1} v$, on peut supposer $f(v) = 1$. Alors, pour tout $w \in V$, on a $f(w - f(w)v) = 0$, donc $w - f(w)v \in \mathrm{Ker}(f) = H$ et donc w s'écrit*

$$w = h + f(w)v \qquad \text{avec} \quad h = w - f(w)v \in H,$$

d'où $V = H + kv$. D'autre part, si $tv \in H$ alors $0 = f(tv) = t$; on a donc $H \cap kv = (0)$ et donc $V = H \oplus kv$, i.e. *H et la droite kv sont supplémentaires. On dit que H est un* hyperplan *de V; si V est de dimension finie n, alors H est de dimension $n - 1$.*

Un exemple très important de sous-espaces en somme directe est celui des sous-espaces propres d'un endomorphisme de V ; rappelons-le ici.

Théorème 3.39. *Soient V un k-espace vectoriel (pas nécessairement de dimension finie), u un k-endomorphisme de V, et $\lambda_1, \dots, \lambda_r$ des valeurs propres, deux à deux distinctes, de u. Pour $i = 1, \dots, r$, on note*

$$E_i = V_{\lambda_i} = \{v \in V \mid u(v) = \lambda_i v\}$$

le sous-espace propre associé. Alors les V_{λ_i} sont en somme directe. (Mais bien sûr, leur somme $\bigoplus_{i=1}^{r} V_{\lambda_i}$ n'est pas nécessairement égale à V; si $\dim(V) < \infty$, c'est le cas si et seulement si u est diagonalisable.)

Démonstration. On va montrer par récurrence sur r l'assertion : $(\star_r)$ si l'on a une égalité $x_1 + \cdots + x_r = 0$, avec $x_i \in V_{\lambda_i}$, alors $x_1 = 0 = \cdots = x_r$. C'est évident si $r = 1$, donc on peut supposer $r \geq 2$ et l'assertion établie pour $r - 1$. Supposons qu'on ait une égalité $x_1 + \cdots + x_r = 0$, avec $x_i \in V_{\lambda_i}$. En appliquant l'endomorphisme u, d'une part, et en multipliant par λ_r, d'autre part, on obtient les égalités :

$$\begin{cases} \lambda_1 x_1 + \cdots + \lambda_{r-1} x_{r-1} + \lambda_r x_r = 0 \\ \lambda_r x_1 + \cdots + \lambda_r x_{r-1} + \lambda_r x_r = 0 \end{cases}$$

d'où par soustraction l'égalité

$$(*) \qquad (\lambda_1 - \lambda_r)x_1 + \cdots + (\lambda_{r-1} - \lambda_r)x_{r-1} = 0.$$

Chaque vecteur $y_i = (\lambda_i - \lambda_r)x_i$ appartient à V_{λ_i} donc, d'après l'hypothèse de récurrence $(\star_{r-1})$, l'égalité $(*)$ entraîne $y_i = 0$ pour tout $i = 1, \dots, r - 1$, et comme $\lambda_i - \lambda_r \neq 0$ ceci entraîne $x_i = 0$ pour tout $i = 1, \dots, r - 1$. Enfin, reportant ceci dans l'égalité initiale $x_1 + \cdots + x_r = 0$, on obtient $x_r = 0$. Ceci montre que $(\star_r)$ est vérifiée, et la proposition est démontrée.

Exemple 3.40. *(1) Soit $V = \mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$ le $\mathbb{R}$-espace vectoriel des fonctions $f : \mathbb{R} \to \mathbb{R}$ de classe C^∞. Alors les fonctions $f_\lambda : t \mapsto \exp(\lambda t)$, pour $\lambda \in \mathbb{R}$ sont linéairement indépendantes, c'est-à-dire, quelques soient $n \in \mathbb{N}^*$ et $\lambda_1, \dots, \lambda_n$ des réels deux à deux distincts, les fonctions $f_{\lambda_1}, \dots, f_{\lambda_n}$ sont linéairement indépendantes. En effet, l'opérateur de dérivation $d : f \mapsto f'$ est un endomorphisme de V (car f' est C^∞ si f l'est), et chaque f_λ est un vecteur propre de d pour la valeur propre λ.*

*(2) Soit $V = \mathbb{R}^{\mathbb{N}}$ le $\mathbb{R}$-espace vectoriel des suites réelles $(u_n)_{n\in\mathbb{N}}$. Alors, pour $\lambda \in \mathbb{R}$, les suites géométrique $u(\lambda)$, définies par $u(\lambda)_n = \lambda^n$, sont linéairement indépendantes, c'est-à-dire, quelques soient $n \in \mathbb{N}^*$ et $\lambda_1, \dots, \lambda_n$ des réels deux à deux distincts, les suites $u(\lambda_1), \dots, u(\lambda_n)$ sont linéairement indépendantes. En effet, soit $D : V \to V$ l'opérateur de décalage, défini par $(D(u))_n = u_{n+1}$ (*i.e. *l'image par D de la suite $(u_0, u_1, u_2, \dots)$ est la suite $(u_1, u_2, u_3, \dots)$); alors chaque $u(\lambda)$ est un vecteur propre de D pour la valeur propre λ.*

Définition 3.41 (Endomorphismes diagonalisables)**.** *Soient V un k-espace vectoriel de dimension finie et $u \in \mathrm{End}_k(V)$. Les conditions suivantes sont équivalentes :*

1. *V admet une base formée de vecteurs propres de u ;*
2. *les vecteurs propres de u engendrent V ;*
3. *la somme des espaces propres de u égale V ;*
4. *V est la somme directe des espaces propres de u.*

Si ces conditions sont vérifiées, on dit que u est diagonalisable.

Démonstration. En effet, il est clair que (iv) $\Rightarrow$ (iii) $\Leftrightarrow$ (ii) $\Leftarrow$ (i), et (ii) $\Rightarrow$ (i) car d'un système de générateurs on peut extraire une base. Enfin (iii) $\Rightarrow$ (iv) d'après le théorème précédent. □

Une condition *suffisante* de diagonalisabilité est donnée par la proposition ci-dessous. (Bien entendu, cette condition n'est **pas nécessaire** : par exemple la matrice identité I_n (≥ 2) est diagonale et a toutes ses valeurs propres égales à 1 !)

Proposition 3.42 (Valeurs propres distinctes)**.** *Soit $u \in \mathrm{End}_k(V)$ ($\dim_k(V) = n$). Si $P_u(X)$ a n valeurs propres distinctes, alors u est diagonalisable.*

Démonstration. En effet, u possède alors n espaces propres distincts $V_1, \dots, V_n$, qui sont en somme directe d'après le théorème précédent. Alors le sous-espace $E = V_1 \oplus \cdots \oplus V_n$ de V est de dimension

$$\sum_{i=1}^{n} \dim V_i \geq n = \dim V$$

donc égale V (et de plus chaque V_i est de dimension 1). □

Enfin, une CNS (condition nécessaire et suffisante) de diagonalisabilité est donnée par la :

Proposition/Définition 3.1 (Multiplicités algébrique et géométrique d'une valeur propre)**.** *Soient V un $\mathbb{C}$-espace vectoriel de dimension n, $u \in \mathrm{End}_{\mathbb{C}}(V)$, $\lambda_1, \dots, \lambda_r$ les racines (deux à deux distinctes) de $P_u(X)$ dans $\mathbb{C}$. D'une part, $P_u(X)$ se factorise*

$$P_u(X) = (-1)^n (X - \lambda_1)^{m_1} \cdots (X - \lambda_r)^{m_r}$$

où m_i est la multiplicité de λ_i comme racine de $P_u(X)$. D'autre part, d'après 3.31, $\lambda_1, \dots, \lambda_r$ sont les valeurs propres de u.

1. *On appelle multiplicité* algébrique *(resp.* géométrique*) de la valeur propre λ_i sa multiplicité m_i comme racine de $P_u(X)$ (resp. la dimension n_i de l'espace propre V_{λ_i}).*
2. *On a* $\dim V_{\lambda_i} \leq m_i$ *pour tout* i.
3. *u est diagonalisable si et seulement si* $\dim V_{\lambda_i} = m_i$ *pour tout* i.

Démonstration. (2) Pour tout i, soit $\mathcal{C}^i$ une base de V_{λ_i}. Comme les espaces propres sont en somme directe, la famille $\mathcal{C} = \mathcal{C}^1 \cup \cdots \cup \mathcal{C}^r$ est une famille libre, donc on peut la compléter en une base $\mathfrak{B}$ de V. Alors $A = \mathrm{Mat}_{\mathfrak{B}}(u)$ est de la forme suivante :

$$A = \left(\begin{array}{c|c|c|c|c} \lambda_1 I_{n_1} & 0 & \cdots & 0 & * \\ \hline 0 & \lambda_2 I_{n_2} & \ddots & \vdots & * \\ \hline 0 & \ddots & \ddots & 0 & * \\ \hline \vdots & \ddots & 0 & \lambda_r I_{n_r} & * \\ \hline 0 & \cdots & 0 & 0 & B \end{array}\right)$$

où B est une matrice carrée de taille $p = n - (n_1 + \cdots + n_r)$. En particulier, A est triangulaire par blocs. Donc, d'après 3.24, on a

$$P_u(X) = \det(A - XI_n) = P_B(X) \prod_{i=1}^{r} (\lambda_i - X)^{n_i}.$$

Donc $\prod_{i=1}^{r} (\lambda_i - X)^{n_i}$ divise $P_u(X)$, d'où $n_i \leq m_i$ pour tout i, ce qui prouve (2).

Si $n_i = m_i$ pour tout i, alors le sous-espace $E = \bigoplus_{i=1}^{r} V_{\lambda_i}$ est de dimension $\sum_{i=1}^{r} m_i = n$, donc égale V, donc u est diagonalisable. Réciproquement, si u est diagonalisable, il existe une base $\mathfrak{B}$ de V telle que

$$A = \mathrm{Mat}_{\mathfrak{B}}(u) = \left(\begin{array}{c|c|c|c} \lambda_1 I_{n_1} & 0 & \cdots & 0 \\ \hline 0 & \lambda_2 I_{n_2} & \ddots & \vdots \\ \hline \vdots & \ddots & \ddots & \vdots \\ \hline 0 & \cdots & 0 & \lambda_r I_{n_r} \end{array}\right)$$

alors $P_u(X) = \det(A - XI_n) = \prod_{i=1}^{r} (\lambda_i - X)^{n_i} = (-1)^n \prod_{i=1}^{r} (X - \lambda_i)^{n_i}$, d'où $n_i = m_i$ pour tout i. □

Donnons de plus une propriété remarquable des endomorphismes diagonalisables, qui sera utile par la suite. Commençons par une définition :

Définition 3.43 (Restriction de u à un sous-espace stable)**.** *Soit $u \in \mathrm{End}_k(V)$. On dit qu'un sous-espace E de V est stable par u si $u(E) \subseteq E$. Dans ce cas, la restriction de u à E induit un endomorphisme de E, que l'on notera u_E.*

Théorème 3.44 (Restriction d'un endomorphisme diagonalisable)**.** *Soient V un k-espace vectoriel de dimension finie, u un endomorphisme diagonalisable de V, et E un sous-espace de V stable par u. Alors E admet une base formée de vecteurs propres de u,* i.e. *la restriction u_E de u à E est diagonalisable.*

Démonstration. D'après la proposition précédente, il suffit de montrer que E est engendré par des vecteurs propres de u. Comme u est diagonalisable, tout $x \in E$ s'écrit dans V comme une somme de vecteurs propres :

$$(\dagger) \qquad x = x_1 + \cdots + x_r, \qquad \text{avec} \quad x_i \in V_{\mu_i} \quad \text{et} \quad \mu_i \neq \mu_j \text{ si } i \neq j.$$

Montrons par récurrence sur r que pour tout $x \in E$ et toute écriture (†) comme ci-dessus, chaque x_i appartient à E (ce qui prouvera le théorème). C'est OK pour $r = 1$, donc on peut supposer $r \geq 2$ et le résultat démontré pour $r - 1$. Appliquant $u - \mu_r \mathrm{id}_V$ à (†) on obtient

$$x' = (u - \mu_r \mathrm{id}_V)(x) = \sum_{i=1}^{r-1} (\mu_i - \mu_r) x_i$$

et $x' \in E$ puisque E est stable par u. Donc par hypothèse de récurrence, $(\mu_i - \mu_r)x_i$ appartient à E pour $i = 1, \ldots, r-1$, donc x_i y appartient aussi (puisque $\mu_i - \mu_r \neq 0$), et reportant ceci dans (†) on obtient aussi $x_r \in E$. Ceci prouve le théorème. □

Pour terminer ce paragraphe, donnons encore l'exemple ci-dessous d'endomorphismes diagonalisables.

Rappels. *Soit k un corps. Si $n \cdot 1_k = 1_k + \cdots + 1_k$ (n termes) est $\neq 0$ pour tout entier $n > 0$, on dit que k est de caractéristique 0; c'est le cas par exemple pour $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Sinon, le plus petit entier $p > 0$ tel que $p \cdot 1_k = 0$ est nécessairement un nombre premier (car si $p = rs$ avec $r, s \geq 1$, l'égalité $0 = (r \cdot 1_k)(s \cdot 1_k)$ entraîne que $r \cdot 1_k = 0$ ou $s \cdot 1_k = 0$, disons $r \cdot 1_k = 0$, mais alors la minimalité de p entraîne que $r = p$); dans ce cas on dit que k est de caractéristique p. D'autre part, si V est un k-espace vectoriel et $p \in \mathrm{End}_k(V)$, rappelons qu'on dit que p est un* **projecteur** *si $p^2 = p \circ p$ est égal à p.*

Proposition 3.45 (Symétries)**.** *Soient k un corps de caractéristique $\neq 2$ (par exemple, $k = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$), V un k-espace vectoriel de dimension n, et $s \in \mathrm{End}_k(V)$ tel que $s^2 = \mathrm{id}_V$. Alors s est diagonalisable; plus précisément, soient*

$$p_+ = \frac{\mathrm{id}_V + s}{2}, \qquad p_- = \frac{\mathrm{id}_V - s}{2}, \qquad V_\pm = \mathrm{Im}(p_\pm).$$

Alors p_+ et p_- sont des projecteurs et l'on a :

$$V = V_+ \oplus V_- \qquad \text{et} \qquad \forall x \in V_\pm, \quad s(x) = \pm x.$$

Donc, si $s \neq \pm \mathrm{id}_V$, alors V_+ et V_- sont non nuls, et $V_\pm$ est l'espace propre associé à la valeur propre ± 1; dans ce cas, s est la symétrie par rapport à V_+ parallèlement à V_-.

Démonstration. On a $p_+^2 = p_+$, $p_-^2 = p_-$ et $p_- = \mathrm{id}_V - p_+$ d'où $p_+ p_- = 0 = p_- p_+$, donc p_+ et p_- sont des projecteurs et l'on a $V = V_+ \oplus V_-$. De plus, si $x \in V_\pm$, on voit aussitôt que $s(x) = \pm x$, d'où la proposition. □

Remarque 3.46. *Attention, si k est de caractéristique 2, c'est-à-dire, si $2 = 0$ dans k (par exemple, si k est le corps à deux éléments $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$), la matrice $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in M_2(k)$ vérifie $A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = I_2$ mais A n'est pas diagonalisable : en effet sa seule valeur propre est 1, donc si A était diagonalisable on aurait $A = I_2$, ce qui n'est pas le cas.*

Chapitre 4

Algèbre bilinéaire

4.1 Dualité et équations intrinsèques

Le langage de la dualité est un moyen de parler d'équations pour des sous-espaces vectoriels d'un espace vectoriel d'un point de vue intrinsèque, i.e., qui ne dépend pas du choix des coordonnées.

Définition 4.1. *Soit V un espace vectoriel. Son dual V^* est l'espace $\mathcal{L}(V, K)$ des formes linéaires sur V.*

1. *Si $f : V \to W$ est une application linéaire, elle induit une application linéaire*

$$f^\vee : W^* \to V^*,$$

appelée son adjoint formel, définie, si $\varphi : W \to K$ est une forme linéaire, par

$$f^\vee(\varphi) = \varphi \circ f : V \to K.$$

2. *Si $X \subset V$ est un sous-ensemble, il définit un sous-espace orthogonal formel $X^\perp \subset V^*$ (des équations de $\text{Vect}(X)$) par*

$$X^\perp = \{\varphi \in V^*,\ \forall v \in X,\ \varphi(v) = 0\}.$$

3. *Si $Y \subset V^*$ est un sous-ensemble, il définit un sous-espace pré-orthogonal formel $Y^\top$ (des solutions de $Y = 0$) par*

$$Y^\top = \{v \in V,\ \forall \varphi \in Y,\ \varphi(v) = 0\}.$$

Remarque 4.2. *On doit penser à l'espace dual comme un espace dans lequel se trouvent les équations linéaires pour les sous-espaces vectoriels (i.e., les formes linéaires) et dans lequel on peut étudier les propriétés de ces équations : sont elles libres ou génératrices ? L'espace $X^\perp$ est ainsi l'espace de toutes les équations qui s'annulent sur X, et $Y^\top$ est l'espace des solutions du système donné par $Y = 0$.*

Exercice 4.3. *Montrer les résultats suivants :*

1. *Si $Y_1 \subset Y_2$, on a $Y_2^\top \subset Y_1^\top$ et si $X_1 \subset X_2$, on a $X_2^\perp \subset X_1^\perp$.*
2. *$X^\perp$ et $Y^\top$ sont des sous-espaces vectoriels.*
3. *On a $(X^\perp)^\top = \text{Vect}(X)$, i.e., le sous-espace sur lequel les équations nulles sur un sous-ensemble s'annulent est le sous-espace engendré par ce sous-ensemble.*

Remarque 4.4. *La matrice d'une forme linéaire f dans une base $\mathfrak{B} = \{e_1, \dots, e_n\}$ (et dans la base $\{1\}$ de K) est une matrice ligne*

$$\mathrm{Mat}_{\mathfrak{B},\{1\}}(f) = [f(e_1), \dots, f(e_n)].$$

Lorsqu'on fait des opérations élémentaires sur les lignes d'une matrice M ayant m lignes et n colonnes, on calcule donc des formes linéaires à partir des formes linéaires qui forment les lignes de la matrice donnée. La résolution d'un système d'équations $Y = 0$ pour $Y \subset V^*$ est donc souvent faite en utilisant des opérations sur les lignes de la matrice M (qui sont données par les matrices lignes des formes linéaires de Y), i.e., des opérations sur les formes linéaires. Si on veut raisonner en termes des images des vecteurs de base pour calculer l'image et le noyau d'une application linéaire de matrice M, on fait plutôt des opérations élémentaires sur les colonnes. Les deux approches ont donc des interprétations différentes mais compatibles en termes d'applications linéaires.

Exemple 4.5.

1. *Un système d'équations linéaires sur $E = K^2$ comme*

$$\begin{cases} x + y &= 0 \\ x - y &= 0 \end{cases}$$

peut être encodé dans le couple de forme linéaires $(f_1, f_2) \in (E^*)^2$ donné par $f_1(x, y) = x + y$ et $f_2(x, y) = x - y$. Si 2 n'est pas nul dans K, ces deux formes linéaires sont libres (et génératrices) dans E^*. Le sous-espace W des solutions de ce système est réduit à $W = \{0\}$ et $W^\perp = \mathrm{Vect}(f_1, f_2) = E^*$.

2. *Si on ne prend qu'une des deux équations sur $E = K^2$, on obtient le système*

$$x + y = 0.$$

Il peut être encodé par la forme linéaire $f_1(x, y) = x + y$. En résolvant le système avec le paramètre x, on obtient $x = x$ et $y = -x$, ce qui donne $W = \mathrm{Vect}((1, -1))$. On a bien $W^\perp = \mathrm{Vect}(f_1)$ et chacun de ces espaces est de dimension 1 : il faut une équation pour définir un espace vectoriel de dimension 1 en dimension 2.

Voyons maintenant un exemple plus analytique d'utilisation de la dualité en dimension infinie.

Exemple 4.6 (Dualité et mesures)**.** *Considérons le $\mathbb{R}$-espace vectoriel $V = \mathcal{C}_c^0(\mathbb{R})$ des fonctions continues sur $\mathbb{R}$ nulles en dehors d'un invervalle fermé borné variable $[a, b]$. Une mesure naïve* [1] *est un élément*

$$T : \mathcal{C}_c^0(\mathbb{R}) \to \mathbb{R}$$

du dual de V. On vérifie facilement que la mesure de Dirac, définie par $\delta_0(\varphi) = \varphi(0)$ est une mesure naïve. L'intégrale de Riemann définit elle aussi une mesure naïve

$$\begin{array}{rccc} \int_{\mathbb{R}} : & \mathcal{C}_c^0(\mathbb{R}) & \to & \mathbb{R} \\ & \varphi & \mapsto & \int_{\mathbb{R}} \varphi(x)dx \end{array}$$

Plus généralement, elle permet aussi d'associer à chaque fonction continue $f : \mathbb{R} \to \mathbb{R}$ une mesure naïve définie par

$$[f](\varphi) = \int_{\mathbb{R}} f(x)\varphi(x)dx$$

1. Une vraie mesure vérifie une condition supplémentaire de continuité.

(l'intégrale se faisant en fait sur le domaine $[a, b]$ en dehors duquel φ est nulle). On a alors $\int_{\mathbb{R}} = [1]$. On peut montrer que cette application

$$\mathcal{C}^0(\mathbb{R}) \to \mathcal{C}_c^0(\mathbb{R})^*$$

donnée par $f \mapsto [f]$ est injective, ce qui permet de voir les mesures naïves comme des fonctions continues généralisées. Dans cette analogie, on peut penser la mesure de Dirac comme le faisait Dirac au début du siècle précédent : c'est une sorte de fonction généralisée qui est nulle partout sauf en 0, qui vaut l'infini en 0 et dont l'intégrale sur $\mathbb{R}$ vaut 1. Cette construction utilisant la dualité est le point de départ de la théorie des distributions, qui est un outil clef en analyse.

4.2 Formes bilinéaires symétriques

4.2.1 Définition

Définition 4.7. *Soit V un espace vectoriel. Une application $\varphi : V \times V \to K$ est appelée une forme bilinéaire si elle est linéaire en chacun de ses arguments, i.e., si*

$$\varphi(\lambda u + v, w) = \lambda\varphi(u, w) + \varphi(v, w) \text{ et } \varphi(w, \lambda u + v) = \lambda\varphi(w, u) + \varphi(w, v)$$

pour tous $u, v, w \in V$ et $\lambda \in K$. Elle est symétrique si

$$\varphi(u, v) = \varphi(v, u)$$

pour tous $u, v \in V$. On note $c(\varphi) : V \to V^*$ l'application linéaire donnée par

$$c(\varphi)(u) = [v \mapsto \varphi(u, v)].$$

On dit que φ est parfaite si $c(\varphi)$ est un isomorphisme et non dégénérée si $c(\varphi)$ est injective.

Remarque 4.8. *Le théorème du rang 3.18 implique qu'une forme bilinéaire φ sur un espace vectoriel de dimension finie est parfaite si et seulement si elle est non dégénérée.*

Exemple 4.9. *Voici trois exemples très importants, en mathématiques comme en physique, de formes bilinéaires.*

1. *La forme euclidienne standard sur $V = K^n$ est donnée par $\varphi((x_i), (y_i)) = \sum_{i=1}^n x_i y_i$. Elle est symétrique et non dégénérée. Elle intervient dans la description de la géométrie euclidienne, qui est aussi un outil clef de la mécanique newtonienne dans $\mathbb{R}^3$ dans $K = \mathbb{R}$.*
2. *La forme de Minkowski sur l'espace temps $\mathbb{R}^4$ de coordonnées (x, y, z, t) est donnée par $\varphi((x, y, z, t), (x', y', z', t')) = xx' + yy' + zz' - c^2tt'$ avec $c = 3 \cdot 10^8 m/s$. Elle est non dégénérée et permet de formaliser la relativité restreinte : la "distance" donnée par la forme quadratique correspondante correspond au temps propre que l'observateur peut lire sur sa montre personnelle pendant un déplacement rapide uniforme. Pour les déplacements accélérés, c'est la forme bilinéaire φ elle même qui devient la quantité variable pour décrire la géométrie des déplacements accélérés dans l'espace temps. Cet exemple montre que les formes bilinéaires jouent un rôle fondamental autant dans la description des déplacements aux très petites échelles (particules élémentaires) qu'aux très grandes échelles (objets celestes) en mécanique.*

3. *La forme bilinéaire d'intégration de Riemann*

$$\int_{\mathbb{R}} : \mathcal{C}_c^0(\mathbb{R}) \times \mathcal{C}_c^0(\mathbb{R}) \to \mathbb{R}$$

donnée par $\int_{\mathbb{R}}(f,g) = \int_{\mathbb{R}} f(x)g(x)dx$ *est symétrique. Elle est non dégénérée et il est possible de la rendre "continuement parfaite" (nous ne préciserons pas cette notion), mais ceci nécessite de la prolonger, par un procédé de complétion, à l'espace de Lebesgue* $L^2(\mathbb{R})$ *des fonctions de carré intégrable. Cette construction est un des points de départs possible pour la théorie des espaces de Hilbert, qui intervient en mécanique quantique.*

4.2.2 Base duale, matrice d'une forme bilinéaire, adjoint

Un intérêt important des formes bilinéaires non dégénérées est qu'elles permettent d'identifier un espace à son dual, et donc des équations à des vecteurs, et inversement. Nous allons maintenant voir comment cela se traduit en termes de bases.

Soit $(V, \mathfrak{B})$ un espace vectoriel basé de dimension finie. On peut le munir de la forme bilinéaire euclidienne $\varphi_e : V \times V \to K$ donnée par

$$\varphi_e((x_i),(y_i)) = \sum_i x_i y_i.$$

Cette forme bilinéaire est parfaite et induit donc un isomorphisme

$$c(\varphi_e) : V \xrightarrow{\sim} V^*.$$

Cet isomorphisme permet de relier les bases de V aux bases de V^*.

Définition 4.10. *Soit* $\varphi : V \times V \to K$ *une forme bilinéaire.*

1. *Si* $\mathfrak{B} = \{e_i\}$ *est une base de* V*, la base duale* $\mathfrak{B}^* = \{e_i^*\}$ *de* $\mathfrak{B}$ *est définie comme l'image par* $c(\varphi_e)$ *de la base* $\mathfrak{B}$*, i.e., par*
$$e_i^* = c(\varphi_e)(e_i) : V \to K,$$
ou encore par $e_i^*(e_j) = \delta_{i,j}$ *qui vaut* 1 *pour* $i = j$ *et* 0 *sinon.*
2. *Si* $\mathcal{D}$ *est une base de* V^**, il existe une unique base* $\mathcal{C}$ *de* V *telle que* $\mathcal{C}^* = \mathcal{D}$ *et cette base est appelée la base pré-duale de* $\mathcal{D}$*.*
3. *La matrice de la forme bilinéaire* φ *dans la base* $\mathfrak{B}$ *est définie comme la matrice*
$$\mathrm{Mat}_{\mathfrak{B}}(\varphi) = \mathrm{Mat}_{\mathfrak{B},\mathfrak{B}^*}(c(\varphi)) = [\varphi(e_i, e_j)]_{i,j}.$$
4. *Le noyau de la forme bilinéaire est le noyau de* $c(\varphi)$ *et son rang est le rang de* $c(\varphi)$*.*

Proposition 4.11. *Si* $f : (V, \mathfrak{B}) \to (W, \mathcal{C})$ *est une application linéaire entre espaces vectoriels basés, la matrice de l'application linéaire basée adjointe formelle* $f^\vee : (V^*, \mathcal{C}^*) \to (W^*, \mathfrak{B}^*)$ *est donnée par*

$$\mathrm{Mat}_{\mathcal{C}^*,\mathfrak{B}^*}(f^\vee) = {}^t\mathrm{Mat}_{\mathfrak{B},\mathcal{C}}(f).$$

Démonstration. Notons $\mathfrak{B} = (e_1, \ldots, e_n)$ et $\mathcal{C} = (f_1, \ldots, f_m)$. On a $\mathfrak{B}^* = (e_1^*, \ldots, e_n^*)$ et $\mathcal{C}^* = (f_1^*, \ldots, f_m^*)$. Soit $A = \mathrm{Mat}_{\mathfrak{B},\mathcal{C}}(f) = (a_{i,j}) \in M_{m,n}(K)$. Par définition, on a

$$f(e_j) = \sum_{k=1}^{m} a_{k,j} f_k \in W,$$

et

$$f^\vee(f_i^*) = f_i^* \circ f \in V^*.$$

On veut exprimer explicitement $f_i^* \circ f$ dans la base $\mathfrak{B}^* = (e_i^*)$. Soit $j \in \{1, \dots, n\}$, on a

$$f^\vee(f_i^*)(e_j) = f_i^*(f(e_j)) = \sum_{k=1}^{m} a_{k,j} f_i^*(f_k) = \sum_{k=1}^{m} a_{k,j}\delta_{i,k} = a_{i,j}.$$

Ceci donne

$$f^\vee(f_i^*) = \sum_{j=1}^{n} a_{i,j} e_j^*$$

donc on obtient l'égalité recherchée

$$\mathrm{Mat}_{\mathcal{C}^*,\mathfrak{B}^*}(f^\vee) = {}^t\mathrm{Mat}_{\mathfrak{B},\mathcal{C}}(f).$$

□

Définition 4.12. *Soit $\varphi : V \times V \to K$ une forme bilinéaire parfaite. Soit $f : V \to V$ un endomorphisme. L'endomorphisme adjoint $f_\varphi^* : V \to V$ de f pour la forme φ est obtenu en complétant le carré commutatif*

$$\begin{array}{ccc} V^* & \xrightarrow{f^\vee} & V^* \\ {\scriptstyle c(\varphi)}\uparrow & & \downarrow{\scriptstyle c(\varphi)^{-1}} \\ V & \xrightarrow{f_\varphi^*} & V \end{array}$$

i.e., en posant $f_\varphi^* = c(\varphi)^{-1} \circ f^\vee \circ c(\varphi)$. On dit que f est autoadjoint pour φ si $f_\varphi^* = f$.

Corollaire 4.13. *Soit $\varphi : V \times V \to K$ une forme bilinéaire parfaite sur un espace vectoriel de dimension finie. Si $f : (V, \mathfrak{B}) \to (V, \mathfrak{B})$ est une application linéaire entre espaces vectoriels basés, la matrice de l'application adjointe f_φ^* est*

$$\mathrm{Mat}_{\mathfrak{B}}(f^*) = \mathrm{Mat}_{\mathfrak{B}}(\varphi)^{-1\,t}\mathrm{Mat}_{\mathfrak{B}}(f)\mathrm{Mat}_{\mathfrak{B}}(\varphi).$$

Ainsi, la matrice d'un endomorphisme autoadjoint pour la forme euclidienne $\varphi = \varphi_e$ est symétrique.

Démonstration. Il suffit de prendre les matrices des applications linéaires du carré commutatif

$$\begin{array}{ccc} (V^*, \mathfrak{B}^*) & \xrightarrow{f^\vee} & (V^*, \mathfrak{B}^*) \\ {\scriptstyle c(\varphi)}\uparrow & & \downarrow{\scriptstyle c(\varphi)^{-1}} \\ (V, \mathfrak{B}) & \xrightarrow{f_\varphi^*} & (V, \mathfrak{B}) \end{array}$$

et d'appliquer la Proposition 4.11 et la Définition 4.10 pour conclure que

$$\mathrm{Mat}_{\mathfrak{B}}(f_\varphi^*) = \mathrm{Mat}_{\mathfrak{B}}(\varphi)^{-1\,t}\mathrm{Mat}_{\mathfrak{B}}(f)\mathrm{Mat}_{\mathfrak{B}}(\varphi).$$

La deuxième partie de l'énoncé se démontre en remarquant que, par définition de la base duale, on a

$$\mathrm{Mat}_{\mathfrak{B},\mathfrak{B}^*}(c(\varphi_e)) = \mathrm{Id} \;\text{ et }\; \mathrm{Mat}_{\mathfrak{B},\mathfrak{B}^*}(c(\varphi_e)^{-1}) = \mathrm{Id}.$$

□

On énonce maintenant une proposition qui permet de calculer les valeurs de la forme bilinéaire en utilisant sa matrice.

Proposition 4.14. *Pour $v, w \in V$ des vecteurs, on a l'égalité*

$$\varphi(v, w) = {}^t[w]_{\mathfrak{B}}\mathrm{Mat}_{\mathfrak{B}}(\varphi)[v]_{\mathfrak{B}}.$$

Démonstration. Rappelons que si v est un vecteur, on lui associe une application $f_v : K \to V$ donnée par $f_v(1) = v$. Son adjoint formel donne une application $f_v^\vee : V^* \to K^*$. Remarquons que la multiplication sur K donne une forme bilinéaire m qui identifie K à K^* en envoyant $1 \in K$ sur $\mathrm{id}_K \in K^*$. On note $c(m) : K \to K^*$ cette identification. Le lien entre la forme bilinéaire φ et l'application $c(\varphi)$ peut alors être écrit en disant que la multiplication $m_{\varphi(v,w)} : K \to K$ par le scalaire $\varphi(v, w)$ vaut

$$c(m)^{-1} \circ f_w^\vee \circ c(\varphi) \circ f_v = m_{\varphi(v,w)},$$

ce qui peut se traduire par la commutation du rectangle suivant :

$$\begin{array}{ccccccccc} K & \xrightarrow{f_v} & V & \xrightarrow{c(\varphi)} & V^* & \xrightarrow{f_w^\vee} & K^* & \xrightarrow{c(m)^{-1}} & K \\ \| & & & & & & & & \| \\ K & & & & \xrightarrow{\qquad m_{\varphi(u,v)} \qquad} & & & & K \end{array}$$

En passant aux matrices associées, on obtient le résultat recherché. □

Voyons ce qui se passe lorsqu'on veut changer de base.

Proposition 4.15. *Soit $\mathfrak{B}$ et $\mathcal{C}$ deux bases de V. Soit $P = \mathrm{Mat}_{\mathcal{C},\mathfrak{B}}(\mathrm{id}_V)$ la matrice de passage. Alors, on a l'égalité*

$$\mathrm{Mat}_{\mathcal{C}}(\varphi) = {}^tP\mathrm{Mat}_{\mathfrak{B}}(\varphi)P.$$

Démonstration. Le diagramme

$$(V, \mathcal{C}) \xrightarrow{\mathrm{id}_V} (V, \mathfrak{B}) \xrightarrow{c(\varphi)} (V^*, \mathfrak{B}^*) \xrightarrow{\mathrm{id}_V^\vee} (V^*, \mathcal{C}^*)$$

d'espaces vectoriels basés nous permet d'écrire l'égalité recherchée simplement par passage aux matrices de la composition de ces applications, en utilisant que la matrice de l'adjoint formel est donnée par la transposée. □

4.2.3 Orthogonalité

Définition 4.16. *Soit V un espace vectoriel et $\varphi : V \times V \to K$ une forme bilinéaire symétrique.*

1. *On dit que deux sous-ensembles X et Y de V sont orthogonaux si $\varphi(x, y) = 0$ pour tout $x \in X$ et $y \in Y$. On note cette situation $X \perp_\varphi Y$ ou simplement $X \perp Y$ si la forme bilinéaire est entendue.*
2. *L'orthogonal d'un sous-ensemble $X \subset V$ est l'espace vectoriel*

$$X^\perp = \{v \in V, \forall x \in X,\ \varphi(v, x) = 0\}.$$

Proposition 4.17. *Soit V un espace vectoriel et $\varphi : V \times V \to K$ une forme bilinéaire symétrique. Si $X \subset V$ est un sous-ensemble, on a $X^\perp = \mathrm{Vect}(X)^\perp$. Si $X \subset Y \subset V$, on a $Y^\perp \subset X^\perp$. On a aussi $\mathrm{Ker}(\varphi) = E^\perp$.*

Théorème 4.18 (Orthogonal d'un sous-espace)**.** *Soit $F \subset V$ un sous-espace vectoriel.*

1. *On a $F \subset (F^\perp)^\perp$ et $\dim(F^\perp) \geq \dim(E) - \dim(F)$.*
2. *Si φ est non dégénérée, on a $\dim(F^\perp) = \dim(E) - \dim(F)$ et $F = (F^\perp)^\perp$.*
3. *Si $F \cap F^\perp = \{0\}$, alors $E = F \oplus F^\perp$.*

Démonstration. Soit $f \in F$, pour tout $x \in F^\perp$ on a $\varphi(f, x) = 0$, d'où $f \in (F^\perp)^\perp$. Ceci montre la première assertion de (1). Prouvons la seconde.

Soit $(f_1, \ldots, f_r)$ une base de F, complétons-la en une base $\mathfrak{B} = (f_1, \ldots, f_n)$ de E, et soit $A = (a_{ij})_{1 \leq i,j \leq n}$ la matrice de φ dans la base $\mathfrak{B}$, *i.e.* $a_{ij} = \varphi(f_i, f_j)$ pour $i, j = 1, \ldots, n$.

On a que $F^\perp$ est formé des vecteurs $v = x_1 f_1 + \cdots + x_n f_n \in E$ tels que $\varphi(f_i, v) = 0$ pour $i = 1, \ldots, r$. Comme $\varphi(f_i, x_1 f_1 + \cdots + x_n f_n) = \sum_{j=1}^n x_j \varphi(f_i, f_j) = \sum_{j=1}^n a_{ij} x_j$, ceci équivaut à dire que le vecteur colonne $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ est solution du système linéaire homogène :

$$(\Sigma) \qquad \begin{cases} a_{11} x_1 & + \cdots + & a_{1n} x_n & = 0 \\ \vdots & & \vdots & \vdots \\ a_{1r} x_1 & + \cdots + & a_{rn} x_n & = 0 \end{cases}$$

dont la matrice B est formée des r premières lignes de A. Comme l'espace des solutions du système est de dimension $n - \operatorname{rang}(B)$, on obtient :

$$\dim F^\perp = n - \operatorname{rang}(B) \geq n - r,$$

ce qui prouve la seconde assertion de (1). De plus, dans le cas particulier où $F = E$, on a $B = A$ et l'on obtient que $\dim E^\perp = n - \operatorname{rang}(A)$. Donc $N(\varphi) = E^\perp$ est nul si et seulement si $\operatorname{rang}(A) = n$. Ceci prouve (2).

Supposons φ non dégénérée. Alors A est de rang n, *i.e.* ses lignes sont linéairement indépendantes, en particulier les r premières lignes le sont, donc la matrice B est de rang r, et donc $\dim F^\perp = n - r$. Remplaçant alors F par $F^\perp$, on obtient l'égalité $\dim(F^\perp)^\perp = n - (n - r) = r$, et par conséquent l'inclusion $F \subseteq (F^\perp)^\perp$ est une égalité. Ceci prouve (3).

Enfin, supposons $F \cap F^\perp = \{0\}$ (sans supposer φ non dégénérée). Alors F et $F^\perp$ sont en somme directe, et le sous-espace $F \oplus F^\perp$ de E est de dimension $d = r + \dim F^\perp$. D'après (1), on a $d \geq n$, d'où $E = F \oplus F^\perp$ (et $\dim F^\perp = n - r$). Ceci prouve (4). Le théorème est démontré. □

Définition 4.19 (Restriction à un sous-espace)**.** *Soit $F \subset V$ un sous-espace vectoriel. On note $\varphi_F : F \times F \to K$ la restriction de φ au sous-espace F.*

4.3 Formes quadratiques

On suppose que 2 n'est pas nul dans le corps K.

4.3.1 Définition

Soit V un K-espace vectoriel.

Définition 4.20. *Une forme quadratique $q : V \to K$ est une fonction de la forme $q(v) = \varphi(v, v)$ avec $\varphi : V \times V \to K$ une forme bilinéaire symétrique.*

Proposition 4.21. *On peut retrouver*[2] *la forme bilinéaire qui a permis de construire une forme quadratique q en posant*

$$\varphi_q(u,v) = \frac{1}{2}(q(u+v) - q(u) - q(v)).$$

La forme φ_q s'appelle alors la forme polaire de q.

Proposition 4.22. *On suppose V de dimension finie et on se fixe une base $\mathfrak{B}$ de V. Soit $A = [a_{i,j}] = \mathrm{Mat}_{\mathfrak{B}}(\varphi)$. Alors la forme quadratique q peut s'écrire*

$$q((x_i)) = \sum_{i=1}^{n} a_{i,i}x_i^2 + \sum_{1\le i<j\le n} 2a_{i,j}x_ix_j.$$

Définition 4.23. *Le rang et le noyau d'une forme quadratique sont définis comme le rang et le noyau de la forme bilinéaire correspondante. Le cône isotrope est défini par*

$$C(q) = \{x \in V,\ q(x) = 0\},$$

et si $K = \mathbb{R}$, le cône positif est défini par

$$C^+(q) = \{x \in V,\ q(x) \ge 0\}.$$

On a une suite évident d'inclusions (en général strictes)

$$N(q) \subset C(q) \subset C^+(q).$$

Remarque 4.24. *Si $K = \mathbb{R}$, la forme quadratique euclidienne $q_e(x,y,z) = x^2 + y^2 + z^2$ permet de définir la norme euclidienne de vecteurs*

$$\|(x,y,z)\|_e = \sqrt{q_e(x,y,z)},$$

et donc la distance euclidienne entre deux points de l'espace. Sa généralisation en dimension supérieure joue un rôle important en sciences des données, ou on doit calculer des distances euclidiennes entre points de $\mathbb{R}^N$ pour N très grand, points qui représentent les données à considérer.

Remarque 4.25. *Dans le cas de la forme de Minkowski $q_m(x,y,z,t) = x^2 + y^2 + z^2 - c^2t^2$ utilisée pour formaliser la relativité restreinte, le cône positif, appelé cône de lumière, est la zône dans laquelle l'observateur peut se déplacer en partant de l'origine et la valeur*

$$\tau(x,y,z,t) = \sqrt{q_m(x,y,z,t)}$$

bien définie dans ce cône positif correspond au temps propre (à la montre) de l'observateur lorsqu'il arrive à la position (x,y,z,t) s'il est parti de la position 0 au temps propre $\tau = 0$.

4.3.2 Bases orthogonales

Définition 4.26 (Bases orthogonales)**.** *Soit E un k-espace vectoriel de dimension n et soient φ une forme bilinéaire symétrique sur E, et q la forme quadratique associée. Soit $\mathfrak{B} = (e_1, \dots, e_n)$ une base de E*

1. *On dit que $\mathfrak{B}$ est une base orthogonale pour φ (ou pour q) si l'on $\varphi(e_i, e_j) = 0$ pour $i \neq j$.*

2. C'est ici qu'on utilise que 2 n'est pas nul dans K, donc y est inversible.

2. *Ceci équivaut à dire que la matrice* $A = \mathrm{Mat}_{\mathfrak{B}}(\varphi)$ *est diagonale ; si l'on note* $\lambda_1, \dots, \lambda_n$ *ses coefficients diagonaux et* $(x_1, \dots, x_n)$ *les coordonnées dans la base* $\mathfrak{B}$*, ceci équivaut encore à dire que* $q(x_1, \dots, x_n) = \lambda_1 x_1^2 + \cdots + \lambda_n x_n^2$.

Théorème 4.27 (Existence de bases orthogonales pour une fbs)**.** *Soit* φ *une forme bilinéaire symétrique sur un k-espace vectoriel E de dimension n, et soit q la forme quadratique associée.*

1. *Il existe une base* $\mathfrak{B}$ *de E orthogonale pour* φ.
2. *Soient* $\mathfrak{B} = (e_1, \dots, e_n)$ *une base orthogonale pour* φ *et D la matrice diagonale* $\mathrm{Mat}_{\mathfrak{B}}(\varphi)$*. Quitte à renuméroter les* e_i*, on peut supposer que les coefficients diagonaux* $\lambda_1, \dots, \lambda_r$ *sont non nuls, et que* $\lambda_i = 0$ *pour* $i > r$*. Notons* $(x_1, \dots, x_n)$ *les coordonnées dans la base* $\mathfrak{B}$*, alors :*
   (a) *On a* $q(x_1, \dots, x_n) = \lambda_1 x_1^2 + \cdots + \lambda_r x_r^2$. $(*)$
   (b) *On a* $r = \mathrm{rang}(\varphi)$*, plus précisément,* $N(\varphi)$ *est le sous-espace* $\textsc{Vect}(e_{r+1}, \dots, e_n)$*, donné par les équations* $x_1 = 0 = \cdots = x_r$.

Démonstration. (1) Montrons l'existence d'une base orthogonale en procèdant par récurrence sur $n = \dim E$. Il n'y a rien à montrer si $n = 0$ ou si $\varphi = 0$. On peut donc supposer $n \geq 1$ et le résultat établi pour $n - 1$, et $\varphi \neq 0$. Alors, la forme quadratique q est non nulle, donc il existe $e_1 \in E$ tel que $q(e_1) \neq 0$. Posons $F = ke_1$, comme $\varphi(e_1, e_1) \neq 0$, alors $F \cap F^\perp = \{0\}$ donc, d'après le théorème 4.18, on a

$$E = F \oplus F^\perp.$$

Par hypothèse de récurrence, il existe une base $(e_2, \dots, e_n)$ de $F^\perp$ telle que $\varphi(e_i, e_j) = 0$ pour $i \neq j$. Alors $(e_1, e_2, \dots, e_n)$ est une base de E orthogonale pour φ. Ceci prouve l'assertion (1).

Puis, (2.a) et la première assertion de (2.b) découlent aussitôt des définitions ; prouvons la dernière assertion. D'après la *démonstration* du théorème 4.18, on sait que $N(\varphi)$ est égal au noyau de D, qui est bien le sous-espace $F = \textsc{Vect}(e_{r+1}, \dots, e_n)$, donné par les équations $x_1 = 0 = \cdots = x_r$. Mais ceci peut se voir directement ici, de la façon suivante. D'après $(*)$, φ est donnée dans la base $\mathfrak{B}$ par :

$$(*') \qquad \forall u = \sum_{i=1}^{n} x_i e_i,\ \forall v = \sum_{j=1}^{n} y_j e_j, \qquad \varphi(u, v) = \lambda_1 x_1 y_1 + \cdots + \lambda_r x_r y_r.$$

Supposons $u \in N(\varphi)$, alors pour tout $i = 1, \dots, r$, prenant $v = e_i$ (c'est-à-dire, $y_i = 1$ et $y_j = 0$ pour $j \neq i$), on obtient $x_i = 0$, d'où $u \in F = \textsc{Vect}(e_{r+1}, \dots, e_n)$. Réciproquement, $(*')$ montre aussi que tout $u \in F$ (*i.e.* tel que $x_1 = 0 = \cdots = x_r$) appartient à $N(\varphi)$, d'où l'égalité désirée. Le théorème est démontré. □

Le théorème précédent est valable pour tout corps k de caractéristique $\neq 2$. La possibilité d'effectuer des réductions supplémentaires dépend de propriétés « arithmétiques » de k, c'est-à-dire, de quels éléments de k sont des carrés. Lorsque $k = \mathbb{C}$ ou $\mathbb{R}$, on peut donner des versions plus précises.

Théorème 4.28 (Formes quadratiques sur $\mathbb{C}$)**.** *Soient E un* $\mathbb{C}$*-espace vectoriel de dimension finie, Q une forme quadratique sur E et* φ *sa forme polaire. Il existe une base* $\mathfrak{B}$ *de E pour laquelle* $\mathrm{Mat}_{\mathfrak{B}}(\varphi)$ *est la matrice diagonale de termes diagonaux* $(1, \dots, 1, 0, \dots, 0)$*, le nombre de* 1 *étant égal à* $r = \mathrm{rang}(\varphi)$*; si l'on note* $(x_1, \dots, x_n)$ *les coordonnées dans la base* $\mathfrak{B}$*, on a alors* $q(x_1, \dots, x_n) = x_1^2 + \cdots + x_r^2$.

Démonstration. Soit $r = \mathrm{rang}(\varphi)$. D'après le théorème 4.27, il existe une base orthogonale $(e_1, \dots, e_n)$ telle que $q(e_i) \neq 0$ pour $i \leq r$, et $q(e_i) = 0$ pour $i > r$. Pour tout $i = 1, \dots, r$, soit $\lambda_i \in \mathbb{C}$ tel que $\lambda_i^2 = q(e_i)$. Remplaçant e_i par e_i/λ_i, pour $i \leq r$, on obtient une base $\mathfrak{B}$ ayant la propriété énoncée dans le théorème. □

4.3.3 Signature d'une forme quadratique

Théorème 4.29 (Théorème d'inertie de Sylvester)**.** *Soient E un $\mathbb{R}$-espace vectoriel de dimension n, q une forme quadratique sur E et φ sa forme polaire.*

1. *Soit $\mathfrak{B} = (e_1, \dots, e_n)$ une base orthogonale pour φ et soient s (resp. t) le nombre d'indices i tels que $q(e_i) > 0$ (resp. < 0). Alors s et t ne dépendent pas de la base orthogonale choisie.*
2. *Le couple (s, t) s'appelle la* **signature** *de q (ou de φ) ; on a $r = \operatorname{rang}(\varphi) = s + t$.*
3. *De plus, on peut choisir $\mathfrak{B}$ de sorte que la matrice diagonale $D = \operatorname{Mat}_{\mathfrak{B}}(\varphi)$ ait pour termes diagonaux $(1, \dots, 1, -1, \dots, -1, 0, \dots, 0)$, le nombre de 1 (resp. -1) étant s (resp. t).*

Démonstration. Posons $r = \operatorname{rang}(\varphi)$. Soient $\mathfrak{B} = (e_1, \dots, e_n)$ et $\mathcal{C} = (f_1, \dots, f_n)$ deux bases de E orthogonales pour φ. Notons s (resp. s') le nombre d'indices i tels que $q(e_i) > 0$ (resp. $q(f_i) > 0$) et t (resp. t') le nombre d'indices i tels que $q(e_i) < 0$ (resp. $q(f_i) < 0$). Alors

$$r = s + t = s' + t'$$

et il s'agit de montrer que $s = s'$ et $t = t'$. Quitte à renuméroter les éléments de $\mathfrak{B}$ et $\mathcal{C}$, on peut supposer que

$$(\star) \quad \begin{cases} q(e_i) > 0 & \text{pour } i = 1, \dots, s \\ q(e_i) < 0 & \text{pour } i = s+1, \dots, s+t \\ q(e_i) = 0 & \text{pour } i > s + t = r\,; \end{cases} \qquad \begin{cases} q(f_i) > 0 & \text{pour } i = 1, \dots, s' \\ q(f_i) < 0 & \text{pour } i = s'+1, \dots, s'+t' \\ q(f_i) = 0 & \text{pour } i > s' + t' = r\,. \end{cases}$$

Notons P_+ le sous-espace de E engendré par les vecteurs e_i tels que $q(e_i) \geq 0$. Ces vecteurs sont au nombre de $n - t$, donc $\dim P_+ = n - t$. Soit x un élément arbitraire de P_+, écrivons $x = \sum_{i \in I} x_i e_i$, avec $I = \{1, \dots, s\} \cup \{r+1, \dots, n\}$; alors, d'après $(\star)$, on obtient

$$q(x) = \sum_{i=1}^{s} x_i^2 \, q(e_i) \geq 0. \tag{1}$$

D'autre part, soit P'_- le sous-espace de E engendré par les vecteurs f_j tels que $q(f_j) < 0$. Ces vecteurs sont au nombre de t', donc $\dim P'_- = t'$. Soit y un élément non nul de P'_-, on peut écrire $y = \sum_{j=s'+1}^{s'+t'} y_j f_j$, avec au moins l'un des y_j non nul (car $y \neq 0$). Alors, d'après $(\star)$ à nouveau, on obtient

$$q(y) = \sum_{j=s'+1}^{s'+t'} y_j^2 \, q(f_j) < 0. \tag{2}$$

Par conséquent, on a $P_+ \cap P'_- = \{0\}$ et donc

$$n = \dim E \geq \dim P_+ + \dim P'_- = n - t + t'$$

d'où $t \geq t'$. Échangeant les rôles des bases $\mathfrak{B}$ et $\mathcal{C}$, on obtient de même $t' \geq t$, d'où $t = t'$, et de même $s = s'$. Ceci prouve la première assertion du théorème.

Voyons la deuxième assertion. Soit $\mathfrak{B} = (e_1, \dots, e_n)$ comme ci-dessus ; pour $i = 1, \dots, s+t$, notons $|q(e_i)| > 0$ la valeur absolue de $q(e_i)$. En remplaçant e_i par $e_i / \sqrt{|q(e_i)|}$, pour $i = 1, \dots, s+t$, on obtient une base orthogonale ayant la propriété énoncée dans le théorème. □

4.3.4 Réduction d'une forme quadratique en somme de carrés

On suppose que le corps de base est $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

Remarque 4.30. *Soit E un k-espace vectoriel de dimension n. D'après la Proposition 4.21,* il revient au même *de se donner sur E une forme quadratique q ou sa forme polaire φ.*

Le langage des formes quadratiques permet d'être plus concis : si E est muni d'une base $\mathfrak{B}$, et donc de coordonnées $(x_1, \dots, x_n)$ relativement à cette base (par exemple, si $E = k^n$), on dira simplement, disons pour $n = 3$: « soit q la forme quadratique $ax_1^2 + bx_2^2 + cx_3^2 + dx_1x_2 + ex_1x_3 + fx_2x_3$ », ce qui est plus rapide que d'écrire : soit φ la forme bilinéaire symétrique définie par :

$$\varphi(x_1e_1 + x_2e_2 + x_3e_3, y_1e_1 + y_2e_2 + y_3e_3) = \\ ax_1y_1 + bx_2y_2 + cx_3y_3 + \frac{d}{2}(x_1y_2 + x_2y_1) + \frac{e}{2}(x_1y_3 + x_3y_1) + \frac{f}{2}(x_2y_3 + x_3y_2).$$

De même, le fait d'écrire une forme quadratique comme un polynôme (homogène) de degré 2 en les coordonnées x_i, i.e.

$$q(x_1, \dots, x_n) = \sum_{i=1}^{n} a_i x_i^2 + \sum_{1 \le i < j \le n} a_{ij}\, x_i x_j$$

permet d'effectuer sur ce polynôme des opérations algébriques simples, qui équivalent à trouver une base orthogonale pour φ : c'est ce qu'on explique ci-dessous.

Définition 4.31. *Soient E un k-espace vectoriel de dimension n, q une forme quadratique sur E et φ sa forme polaire. Soit $\mathfrak{B} = (e_1, \dots, e_n)$ une base de E, notons $(x_1, \dots, x_n)$ les coordonnées dans cette base,* i.e. *x_i désigne en fait la forme linéaire $f_i = e_i^*$ sur E.*

1. *On dit que q s'écrit dans la base $\mathfrak{B}$ comme* **somme de carrés de formes linéaires indépendantes** *si l'expression de q en fonction des coordonnées x_i est de la forme*

$$q = q_1\, x_1^2 + \cdots + q_n\, x_n^2.$$

   Ceci équivaut à dire que la matrice de φ dans la base $\mathfrak{B}$ est **diagonale***, avec les q_i pour coefficients diagonaux.*

2. *Les formes linéaires $f_i = e_i^*$ sont linéairement indépendantes ($\mathfrak{B}^* = (e_1^*, \dots, e_n^*)$ est la base duale de $\mathfrak{B}$), d'où la terminologie « somme de carrés de* **formes linéaires indépendantes** *». En pratique, pour abréger on écrira souvent « somme de carrés », mais il est essentiel de s'assurer que les formes linéaires en question sont bien linéairement indépendantes (voir plus bas).*

Théorème 4.32 (Réduction d'une forme quadratique en somme de carrés)**.** *Soient E un k-espace vectoriel de dimension n, et q une forme quadratique sur E, donnée dans une base $\mathfrak{B} = (e_1, \dots, e_n)$ par*

$$(*) \qquad \forall (x_1, \dots, x_n) \in k^n, \qquad q(x_1e_1 + \cdots + x_ne_n) = \sum_i b_i x_i^2 + \sum_{i<j} b_{ij} x_i x_j.$$

1. *Par une suite d'opérations « élémentaires » (décrites dans la démonstration), on peut trouver un nouveau système de coordonnées $(y_1, \dots, y_n)$ sur E, dans lequel q s'écrit comme une somme de carrés,* i.e. *:*

$$(**) \qquad q(y_1, \dots, y_n) = a_1y_1^2 + \cdots + a_ny_n^2.$$

2. *Le nombre de coefficients a_i non nuls est égal à $r = \mathrm{rang}(q)$, et si $k = \mathbb{R}$, la signature de q est (s,t), où s (resp. t) est le nombre de coefficients a_i qui sont > 0 (resp. < 0).*
3. *De plus, $N(\varphi)$ est le sous-espace vectoriel de E défini par les équations $y_i = 0$, pour i parcourant l'ensemble des $i \in \{1,\dots,n\}$ tels que $a_i \neq 0$.*

Démonstration. Remarquons d'abord que si q s'écrit sous la forme $(**)$ dans une base $\mathfrak{B}'$, alors la matrice de sa forme polaire y est diagonale, avec les a_i pour coefficients diagonaux, d'où les assertions (2) et (3) du théorème, compte-tenu des théorèmes 4.27 et 4.29.

Il reste à donner une démonstration « algorithmique » de l'assertion (1). On procède par récurrence sur le nombre n de variables. Si $n = 1$ on a $q(x_1e_1) = b_1x_1^2$, et $(**)$ est vérifié. On peut donc supposer $n > 1$ et le résultat démontré pour $n-1$. Distinguons deux cas.

(a) Si dans l'écriture $(*)$ plus haut, il existe un coefficient « diagonal » b_i non nul, on peut supposer, quitte à changer l'ordre des coordonnées, que $b_1 \neq 0$. On considère alors la somme de **tous** les termes contenant la variable x_1 et on l'écrit comme suit :

$$S = b_1\,x_1^2 + \sum_{j=2}^{n} b_{1j}\,x_1x_j = b_1\Big(x_1^2 + 2x_1(\underbrace{\sum_{j=2}^{n}\frac{b_{1j}}{2b_1}x_j}_{=L(x_2,\dots,x_n)})\Big)$$

alors L est une forme linéaire ne contenant plus la variable x_1 (*i.e.* L est une combinaison linéaire des formes linéaires $e_2^*,\dots,e_n^*$). Puis, en utilisant que

$$(x_1+L)^2 = x_1^2 + 2x_1L + L^2, \qquad \text{d'où} \qquad x_1^2 + 2x_1L = (x_1+L)^2 - L^2,$$

on récrit ceci sous la forme :

$$S = b_1\,(x_1+L)^2 - b_1L^2 = b_1\Big(x_1 + \sum_{j=2}^{n}\frac{b_{1j}}{2b_1}x_j\Big)^2 - \sum_{j=2}^{n}\frac{b_{1j}^2}{4b_1}\,x_j^2 - \sum_{2\le i<j\le n}\frac{b_{1i}b_{1j}}{2b_1}\,x_ix_j\,.$$

Donc, en posant $y_1 = x_1 + \sum_{j=2}^{n}\frac{b_{1j}}{2b_1}\,x_j$ (et $b'_j = b_j - b_{1j}^2/4b_1$ pour $j = 2,\dots,n$, et $b'_{ij} = b_{ij} - b_{1i}b_{1j}/2b_1$ pour $2 \le i < j \le n$), on obtient une écriture :

$$(\dagger) \qquad q(y_1,x_2,\dots,x_n) = b_1{y_1}^2 + \underbrace{\sum_{j=2}^{n} b'_j\,x_j^2 + \sum_{2\le i<j\le n} b'_{ij}\,x_ix_j}_{q_1(x_2,\dots,x_n)}$$

où la forme quadratique $q_1(x_2,\dots,x_n)$ ne dépend que des variables $x_2,\dots,x_n$.

L'opération $y_1 = x_1 + L(x_2,\dots,x_n)$ et $x_j = x_j$ pour $j \ge 2$, est bien un changement de coordonnées, car la matrice exprimant $(y_1,x_2,\dots,x_n)$ en fonction de $(x_1,\dots,x_n)$ est triangulaire avec des 1 sur la diagonale, donc inversible ; explicitement le changement de coordonnées inverse est donné par $x_j = x_j$ pour $j \ge 2$ et $x_1 = y_1 - L(x_2,\dots,x_n)$.

Par hypothèse de récurrence on peut faire un changement de coordonnées $(x_2,\dots,x_n) \to (y_2,\dots,y_n)$ tel que $q_1(x_2,\dots,x_n) = a_2\,y_2^2 + \cdots + a_n\,y_n^2$ d'où, d'après $(\dagger)$:

$$q(y_1,\dots,y_n) = a_1\,y_1^2 + \cdots + a_n\,y_n^2$$

(avec $a_1 = b_1$), ce qui prouve le résultat voulu dans ce cas.

(b) Supposons au contraire que **tous** les coefficients « diagonaux » b_i soient nuls. Si $q = 0$, il n'y a rien à montrer ; sinon on peut supposer, quitte à changer l'ordre des coordonnées, que $b_{12} \neq 0$. Le plus simple est alors de procéder comme suit : faisons le changement de coordonnées

$$x_1 = x'_1 + x'_2, \qquad x_2 = x'_1 - x'_2, \qquad x_j = x'_j \quad \text{pour } j > 2$$

(c'est bien un changement de coordonnés, dont l'inverse est donné par $x'_1 = (x_1 + x_2)/2$, $x'_2 = (x_1 - x_2)/2$, $x'_j = x_j$ pour $j > 2$). Alors les termes $b_{ij}\, x_i x_j$ (avec $i < j$) se transforment comme suit :

$$\begin{cases} b_{12}\, x_1 x_2 \to b_{12}\,({x'_1}^2 - {x'_2}^2) \\ b_{ij}\, x_i x_j \to b_{ij}\, x_i x_j \qquad \text{si } i, j \geq 3 \end{cases} \qquad \begin{cases} b_{1j}\, x_1 x_j \to b_{1j}\,(x'_1 + x'_2) x_j \quad \text{pour } j \geq 3 \\ b_{2j}\, x_2 x_j \to b_{2j}\,(x'_1 - x'_2) x_j \quad \text{pour } j \geq 3 \end{cases}$$

donc on obtient

$$q(x'_1, \dots, x'_n) = b_{12}\,({x'_1}^2 - {x'_2}^2) + \sum_{j=3}^{n} \Big((b_{1j} + b_{2j})\, x'_1 x_j + (b_{1j} - b_{2j})\, x'_2 x_j \Big) + \sum_{3 \leq i < j \leq n} b_{ij}\, x'_i x'_j$$

et l'on est ramené au cas **(a)**, c'est-à-dire, on peut éliminer la variable x'_1 et se ramener, à nouveau, au cas de $n - 1$ variables. Le théorème est démontré. □

Remarque 4.33. *Dans le cas* **(b)***, une méthode plus sophistiquée, qui permet d'éliminer en même temps les variables x_1 et x_2, est la suivante. On la désignera par* **(b′)***. On considère la somme de* **tous** *les termes contenant x_1* **ou** *x_2 et on l'écrit comme suit :*

$$\begin{aligned} S &= b_{12}\, x_1 x_2 + \sum_{j=3}^{n} b_{1j}\, x_1 x_j + \sum_{j=3}^{n} b_{2j}\, x_2 x_j = b_{12}\Big(x_1 + \sum_{j=3}^{n} \frac{b_{2j}}{b_{12}}\, x_j\Big)\Big(x_2 + \sum_{j=3}^{n} \frac{b_{1j}}{b_{12}}\, x_j\Big) - \sum_{3 \leq j, \ell \leq n} \frac{b_{1j} b_{2\ell}}{b_{12}} x_j x_\ell \\ &= b_{12}\underbrace{\Big(x_1 + \sum_{j=3}^{n} \frac{b_{2j}}{b_{12}}\, x_j \Big)}_{=X} \underbrace{\Big(x_2 + \sum_{j=3}^{n} \frac{b_{1j}}{b_{12}}\, x_j \Big)}_{=Y} - \sum_{j=3}^{n} \frac{b_{1j} b_{2j}}{b_{12}} x_j^2 - \sum_{3 \leq j < \ell \leq n} \frac{2 b_{1j} b_{2\ell}}{b_{12}} x_j x_\ell \end{aligned}$$

Puis, en utilisant l'égalité

$$(\star) \qquad \boxed{XY = \frac{1}{4}\Big((X+Y)^2 - (X-Y)^2\Big)}$$

et en posant

$$x'_1 = \frac{1}{2}(X+Y) = \frac{1}{2}(x_1 + x_2 + \sum_{j=3}^{n} \frac{b_{1j} + b_{2j}}{b_{12}}\, x_j), \qquad x'_2 = \frac{1}{2}(X-Y) = \frac{1}{2}(x_1 - x_2 + \sum_{j=3}^{n} \frac{b_{1j} - b_{2j}}{b_{12}}\, x_j),$$

on obtient :

$$q(x'_1, x'_2, x_3, \dots, x_n) = b_{12}\,({x'_1}^2 - {x'_2}^2) - \sum_{j=3}^{n} \frac{b_{1j} b_{2j}}{b_{12}} x_j^2 + \sum_{3 \leq j < \ell \leq n} c_{j\ell}\, x_j x_\ell$$

où $c_{j\ell} = b_{j\ell} - 2 b_{1j} b_{2\ell}/b_{12}$ pour tout $j < \ell$ dans $\{3, \dots, n\}$.

Illustrons ceci par deux exemples : dans le premier n'apparaissent que des changements de coordonnées du type **(a)**.

Exemple 4.34. *Considérons dans* $\mathbb{R}^4$ *la forme quadratique*

$$q = x_1^2 - 2x_1x_2 + 4x_1x_3 + 2x_1x_4 + x_2^2 + 4x_3^2 + 5x_4^2 - 4x_2x_3 + 6x_2x_4 - 4x_3x_4.$$

Considérant les termes contenant x_1*, on écrit d'abord :*

$$q = (\underbrace{x_1 - x_2 + 2x_3 + x_4}_{y_1})^2 + 4x_4^2 + 8x_2x_4 - 8x_3x_4$$

puis

$$4x_4^2 + 8x_2x_4 - 8x_3x_4 = 4(\underbrace{x_4 + x_2 - x_3}_{y_4})^2 - 4x_2^2 + 8x_2x_3 - 4x_3^2$$

puis $-4x_2^2 + 8x_2x_3 - 4x_3^2 = -4(\underbrace{x_2 - x_3}_{y_2})^2$*. Donc en faisant successivement les changements de coordonnées :*

$$y_1 = x_1 - x_2 + 2x_3 + x_4, \qquad y_4 = x_4 + x_2 - x_3, \qquad y_2 = x_2 - x_3, \qquad y_3 = x_3,$$

on obtient que $q(y_1, y_4, y_2, y_3) = y_1^2 + 4y_4^2 - 4y_2^2$*. Donc* q *est de signature* $(2, 1)$ *et de rang* $2 + 1 = 3$*. Son noyau* $N(q)$ *est la droite définie par les équations* $y_2 = 0 = y_4 = y_1$*, donc, dans les coordonnées initiales, par les équations* $x_2 = x_3$*,* $x_4 = 0$*,* $x_1 + x_3 = 0$*.*

Exemple 4.35. *Considérons dans* $\mathbb{R}^4$ *la forme quadratique :*

$$q(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + 2x_1x_2 + 2x_1x_3 - 3x_2x_4 - 4x_3x_4 + 5x_3x_4.$$

Considérant les termes contenant x_1*, écrivons d'abord :*

$$q(x_1, x_2, x_3, x_4) = (x_1 + x_2 + x_3)^2 - 5x_2x_3 - 4x_2x_4 + 5x_3x_4 = y_1^2 - 5x_2x_3 - 4x_2x_4 + 5x_3x_4.$$

1ère méthode : transformons le terme x_2x_3 *en posant* $x_2 = y_2 + y_3$ *et* $x_3 = y_2 - y_3$*, on obtient :*

$$q(y_1, y_2, y_3, x_4) = y_1^2 - 5(y_2^2 - y_3^2) + y_2x_4 - 9y_3x_4 = y_1^2 - 5y_2^2 + y_2x_4 + 5y_3^2 - 9y_3x_4.$$

Puis $-5y_2^2 + y_2x_4 = -5(y_2 - \frac{1}{10}x_4)^2 + \frac{1}{20}x_4^2$ *donne, en posant* $z_2 = y_2 - \frac{1}{10}x_4$ *:*

$$q(y_1, z_2, y_3, x_4) = y_1^2 - 5z_2^2 + 5y_3^2 - 9y_3x_4 + \frac{1}{20}x_4^2$$

Puis $5y_3^2 - 9y_3x_4 = 5(y_3 - \frac{9}{10}x_4)^2 - \frac{81}{20}x_4^2$ *donne, en posant* $z_3 = y_3 - \frac{9}{10}x_4$ *:*

$$q(y_1, z_2, z_3, x_4) = y_1^2 - 5z_2^2 + 5z_3^2 - 4x_4^2.$$

Donc la signature de q *est* $(2, 2)$ *et son rang est* $2 + 2 = 4$*,* i.e. q *est non dégénérée.*
2ème méthode : considérons tous les termes contenant x_2 *ou* x_3 *et écrivons :*

$$-5x_2x_3 - 4x_2x_4 + 5x_3x_4 = -5(\underbrace{x_2 - x_4}_{=X})(\underbrace{x_3 + \frac{4}{5}x_4}_{=Y}) - 4x_4^2$$

alors, posant $z_2 = \frac{1}{2}(X + Y) = \frac{1}{2}(x_2 + x_3 - \frac{4}{5}x_4)$ *et* $z_3 = \frac{1}{2}(X - Y) = \frac{1}{2}(x_2 - x_3 - \frac{9}{5}x_4)$*, on obtient que*

$$q(y_1, z_2, z_3, x_4) = y_1^2 - 5z_2^2 + 5z_3^2 - 4x_4^2$$

et l'on retrouve le résultat précédent.

Exemple 4.36 (Erreur à ne pas commettre !)**.** *Reprenons le calcul précédent, au moment où l'on obtient les termes* $q_1(x_2, x_3, x_4) = -5x_2x_3 - 4x_2x_4 + 5x_3x_4$*. Il ne faut* **pas** *écrire que*

$$-5x_2x_3-4x_2x_4+5x_3x_4 = -\frac{5}{4}\Big((x_2+x_3)^2-(x_2-x_3)^2\Big)-\Big((x_2+x_4)^2-(x_2-x_4)^2\Big)+\frac{5}{4}\Big((x_3+x_4)^2-(x_3-x_4)^2\Big)$$
$$= -\frac{5}{4}y_1^2 + \frac{5}{4}y_2^2 - y_3^2 + y_4^2 + \frac{5}{4}y_5^2 - \frac{5}{4}y_6^2$$

où l'on a posé $y_1 = x_2 + x_3$, $y_2 = x_2 - x_3$, $y_3 = x_2 + x_4$, $y_4 = x_2 - x_4$, $y_5 = x_3 + x_4$, $y_6 = x_3 - x_4$, *et conclure que la signature est (3,3) et le rang 6. Ceci est erroné (et la conclusion absurde !) : comme on part ici d'une forme quadratique* q_1 *en 3 variables, son rang est* $r \leq 3$ *et donc on doit obtenir à la fin une somme ayant* **au plus** *3 termes, or ici on en a écrit 6. L'erreur est que l'on n'a pas fait un vrai « changement de coordonnées », car on a introduit trop de formes linéaires, qui ne sont plus linéairement indépendantes : par exemple, on a* $y_4 = -y_3 + y_1 + y_2$, $y_5 = y_3 - y_2$, $y_6 = y_1 - y_3$.

Donc, pour ne pas se tromper dans ces calculs, il vaut mieux procéder pas à pas, en effectuant à chaque pas une transformation de type **(a), (b)** *ou* **(b′)**. *Il ne faut pas effectuer plusieurs opérations en même temps !*

4.4 Espaces euclidiens et diagonalisation simultanée

4.4.1 Espaces euclidiens. Inégalité de Cauchy-Schwarz. Isométries

Définition 4.37 (Produits scalaires et espaces euclidiens)**.** *Soit* E *un* $\mathbb{R}$*-espace vectoriel, pas nécessairement de dimension finie.*

1. *Soient* φ *une forme bilinéaire symétrique sur* E *et* Q *la forme quadratique associée (*i.e. $Q(x) = \varphi(x, x)$ *pour tout* $x \in E$*). On dit que* Q *(ou* φ*) est* **définie positive** *si l'on a :*

$$\forall x \in E - \{0\}, \qquad Q(x) = \varphi(x, x) > 0.$$

Dans ce cas, on dit que φ *est un* **produit scalaire** *et on note souvent* $\varphi(x, y) = (x \mid y)$.

Remarquons que si Q *(ou* φ*) est définie positive, elle est* non-dégénérée *: en effet, si* $x \in N(\varphi)$*, on a* $0 = \varphi(x, y)$ *pour tout* $y \in E$*, en particulier* $\varphi(x, x) = 0$*, d'où* $x = 0$.

2. *Dans ce cas, on dit que : « E,* muni de (|) *» (ou que : «* le couple (E, φ) *») est un* **espace euclidien**. [3] *Pour abréger, on écrira souvent : « Soit E un espace euclidien », sans préciser le produit scalaire (|), celui-ci étant sous-entendu.*

Exemple 4.38. *(1)* $\mathbb{R}^n$ *muni du produit scalaire euclidien standard :*

$$(x \mid y) = x_1y_1 + \cdots + x_ny_n \qquad si\ x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

et de la forme quadratique associée $Q(x) = x_1^2 + \cdots + x_n^2$*, est un espace euclidien de dimension n. Pour ce produit scalaire, la base canonique* $(e_1, \ldots, e_n)$ *de* $\mathbb{R}^n$ *est* orthonormée, i.e. *on a* $(e_i \mid e_j) = 1$ *si* $i = j$ *et* $= 0$ *sinon.*

3. En fait, on réserve d'habitude cette terminologie au cas où E est de dimension finie ; sinon on dit que E est un espace *préhilbertien réel* (voir l'explication de cette terminologie dans l'Appendice C.6 à la fin du dernier chapitre). Nous n'utiliserons pas cette terminologie.

(2) L'espace vectoriel $E = \mathcal{C}^0([0,1],\mathbb{R})$ *des fonctions continues* $f : [0,1] \to \mathbb{R}$*, muni du produit scalaire*

$$(f \mid g) = \int_0^1 f(t)g(t)dt\,,$$

est un espace euclidien, qui n'est pas de dimension finie.

Proposition 4.39 (Familles et bases orthonormées)**.** *Soit E, muni de* (|)*, un espace euclidien.*

1. *Une famille* $(e_i)_{i\in I}$ *de vecteurs est dite* **orthonormée** *si* $(e_i \mid e_i) = 1$ *et* $(e_i \mid e_j) = 0$ *pour tout* $i \neq j$*.*
2. *Supposons E de dimension n. Une* **base orthonormée** *est une base* $(e_1,\dots,e_n)$ *de E qui est une famille orthonormée,* i.e. *qui vérifie* $(e_i \mid e_i) = 1$ *et* $(e_i \mid e_j) = 0$ *pour tout* $i \neq j$*.*
3. *Toute famille orthonormée est* libre*. En particulier, si* $\dim E = n$*, toute famille orthonormée* $(f_1,\dots,f_n)$ *de cardinal n est une base orthonormée de E.*
4. *Dans la suite, on abrégera souvent « base orthonormée » en : b.o.n. ou BON.*

Démonstration. Prouvons (3). Supposons qu'on ait une relation $0 = t_1 e_{i_1} + \cdots + t_p e_{i_p}$, avec $i_1,\dots,i_p \in I$ deux à deux distincts, et $t_1,\dots,t_p \in \mathbb{R}$. Fixons un indice $r \in \{1,\dots,p\}$ et appliquons $(e_{i_r} \mid\ )$ à l'égalité précédente. Comme $(e_{i_r} \mid e_{i_s}) = 0$ pour $s \neq r$, on obtient $0 = t_r(e_{i_r} \mid e_{i_r}) = t_r$, d'où $t_r = 0$. Ceci prouve que la famille $(e_i)_{i\in I}$ est libre. □

Théorème 4.40 (Existence de b.o.n.)**.** *Soit E un espace euclidien de dimension n. Alors E admet une base orthonormée.*

Démonstration. D'après le théorème d'inertie de Sylvester 4.29, il existe une base $(e_1,\dots,e_n)$ orthogonale (*i.e.* $(e_i \mid e_j) = 0$ pour $i \neq j$) et telle que $(e_i \mid e_i) \in \{1,-1,0\}$; or comme (|) est défini positif on a nécessairement $(e_i \mid e_i) = 1$, donc $(e_1,\dots,e_n)$ est une b.o.n. □

Définition 4.41 (Normes)**.** *Soit E un* $\mathbb{R}$*-espace vectoriel. Une* **norme** $\|\cdot\|$ *sur E est une application* $E \to \mathbb{R}_+$*,* $x \mapsto \|x\|$ *vérifiant les trois propriétés suivantes :*

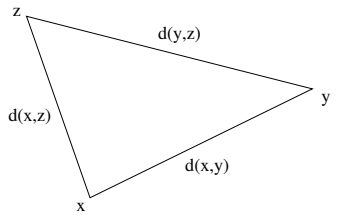
1. $\|x\| = 0 \Leftrightarrow x = 0$*.*
2. *Pour tout* $t \in \mathbb{R}$*,* $x \in E$*, on a* $\|tx\| = |t| \cdot \|x\|$ *(où* $|t|$ *est la valeur absolue de t).*
3. $\|u+v\| \leq \|u\| + \|v\|$*, pour tout* $u, v \in E$*.*

Remarque. L'inégalité précédente est nommée **Inégalité triangulaire***, pour la raison suivante. Si on pose* $d(x,y) = \|y - x\|$*, pour tout* $x, y \in E$*, alors, compte-tenu de (1) et (2) ci-dessus, (3) équivaut à dire (en posant* $u = y - x$*,* $v = z - y$*) que l'application* $d : E \times E \to \mathbb{R}_+$ *est une* **distance** *sur E,* i.e. *vérifie :*

(1′) $d(x,y) = 0 \Leftrightarrow x = y$.

(2′) $d(x,y) = d(y,x)$.

(3′) Inégalité triangulaire *: pour tout* $x, y, z \in E$*, on a :* $d(x,z) \leq d(x,y) + d(y,z)$



Théorème 4.42 (Inégalité de Cauchy-Schwarz et norme euclidienne)**.** *Soit E, muni de* (|)*, un espace euclidien et soit* $Q(x) = (x \mid x)$ *la forme quadratique associée.*

1. *On a l'inégalité de Cauchy-Schwarz :*

   (CS) $$\boxed{\forall x, y \in E \qquad (x \mid y)^2 \leq Q(x)Q(y)}$$

   avec égalité si et seulement si x et y sont liés.

2. *Par conséquent, l'application $x \mapsto \|x\| = \sqrt{(x \mid x)}$ est une norme sur E, appelée la* **norme euclidienne** *associée à $(\ \mid\ )$, et l'inégalité de Cauchy-Schwarz se récrit comme suit (où dans le terme de gauche $|\cdot|$ désigne la valeur absolue dans $\mathbb{R}$) :*

   (CS) $$\boxed{\forall x, y \in E \qquad |(x \mid y)| \leq \|x\| \cdot \|y\|.}$$

Démonstration. Si $y = \lambda x$, on a $Q(y) = \lambda^2 Q(x)$ et $(x \mid y)^2 = \lambda^2 (x \mid x)^2 = Q(y)Q(x)$, et de même si $x = \lambda y$. Donc on a l'égalité si x, y sont liés, en particulier si $x = 0$ ou $y = 0$. Supposons donc x et y non nuls ; pour tout $t \in \mathbb{R}$, on a :

$$0 \leq Q(tx + y) = t^2 Q(x) + 2t\,(x \mid y) + Q(y)$$

donc le discriminant réduit $\Delta' = (x \mid y)^2 - Q(x)Q(y)$ de ce trinôme[4] en t est ≤ 0, ce qui prouve l'inégalité (CS). De plus, si $\Delta' = 0$ le trinôme ci-dessus a une racine double réelle $t_0 = -(x \mid y)/Q(x)$, et l'égalité $Q(t_0 x + y) = 0$ entraîne, puisque Q est définie positive, $t_0 x + y = 0$, *i.e.*

$$y = \frac{(x \mid y)}{(x \mid x)}\, x.$$

Ceci prouve (1).

Prouvons que $x \mapsto \|x\| = \sqrt{(x \mid x)}$ est une norme sur E. Comme $(\ \mid\ )$ est défini positif, on a $\|x\| = 0 \Leftrightarrow x = 0$. D'autre part, pour tout $t \in \mathbb{R}$ et $x \in E$, on a $|t| = \sqrt{t^2}$ et donc

$$\|t\,x\| = \sqrt{t^2\,(x \mid x)} = |t| \cdot \|x\|.$$

Enfin, soient $x, y \in E$. D'abord, l'inégalité de Cauchy-Schwarz équivaut (en prenant la racine carrée) à :

$$|(x \mid y)| \leq \|x\| \cdot \|y\|\,;$$

alors, multipliant par 2 et ajoutant $\|x\|^2 + \|y\|^2$ aux deux membres, on obtient

$$\begin{aligned}\|x + y\|^2 = \|x\|^2 + \|y\|^2 + 2(x \mid y) &\leq \|x\|^2 + \|y\|^2 + 2|(x \mid y)| \\ &\leq \|x\|^2 + \|y\|^2 + 2\|x\| \cdot \|y\| = (\|x\| + \|y\|)^2.\end{aligned}$$

Prenant la racine carrée, ceci entraîne (et équivaut à) l'inégalité triangulaire. Le théorème est démontré. □

Récrivons certaines conséquences de l'égalité $(x + y \mid x + y) = (x \mid x) + (y \mid y) + 2(x \mid y)$ en utilisant la norme $\|\cdot\|$ (ou plutôt son carré) :

Proposition 4.43 (Pythagore, parallélogramme et médiane, polarisation)**.** *Soit E un espace euclidien, et soit $\|\cdot\|$ la norme associée au produit scalaire $(\ \mid\ )$. On a les égalités suivantes :*

(Pythagore) $$\|x_1 + \cdots + x_n\|^2 = \|x_1\|^2 + \cdots + \|x_n\|^2 \qquad \text{si } x_1, \ldots, x_n \text{ sont orthogonaux}$$

(Parallélogramme/Médiane) $$\|x + y\|^2 + \|x - y\|^2 = 2\|x\|^2 + 2\|y\|^2$$

(Polarisation) $$4(x \mid y) = \|x + y\|^2 - \|x - y\|^2$$

4. Pour un trinôme $aX^2 + 2bX + c$ dont le coefficient de X est *pair*, il est commode de considérer le discriminant réduit $\Delta' = b^2 - ac$ (au lieu du discriminant usuel $\Delta = (2b)^2 - 4ac = 4\Delta'$).

Démonstration. L'égalité de Pythagore est immédiate si $n = 2$, et dans ce cas on a même la réciproque : si $\|x_1+x_2\|^2 = \|x_1\|^2+\|x_2\|^2$ alors $(x_1 \mid x_2) = 0$. L'égalité pour n vecteurs orthogonaux s'obtient par récurrence sur n. On prendra garde que la réciproque est fausse pour $n \geq 3$: prendre par exemple dans $\mathbb{R}^2$ euclidien les vecteurs $x_1 = e_1$, $x_2 = e_1 + e_2$, $x_3 = e_2 - e_1$.

Les deux autres égalités s'obtiennent en ajoutant (resp. soustrayant) les égalités :

$$\|x + y\|^2 = (x + y \mid x + y) = \|x\|^2 + \|y\|^2 + 2(x \mid y)$$
$$\|x - y\|^2 = (x - y \mid x - y) = \|x\|^2 + \|y\|^2 - 2(x \mid y)$$

□

Remarque 4.44. *La deuxième égalité s'appelle «* identité du parallélogramme *», car elle exprime que dans le parallélograme construit sur les vecteurs x et y, la somme des carrés des longueurs des quatre côtés égale la somme des carrés des longueurs des deux diagonales (qui sont $x + y$ et $x - y$). Elle s'appelle aussi «* identité de la médiane *», car dans le triangle construit sur les vecteurs x et y, la « médiane » joignant* 0 *au milieu du côté $x - y$ est $(x + y)/2$, et l'on a donc une formule exprimant (le carré de) la longueur de la médiane en fonction de la longeur des côtés :*

$$\left\|\frac{x+y}{2}\right\|^2 = \frac{\|x\|^2}{2} + \frac{\|y\|^2}{2} - \frac{\|x-y\|^2}{4} .$$

Enfin, la dernière égalité est appelée « identité de polarisation *», car elle exprime en fonction de la forme quadratique $Q(x) = \|x\|^2$ le produit scalaire, qui est la « forme polaire » de Q. On l'a déjà rencontrée dans le Chap. 4 sous la forme $4\varphi(x, y) = Q(x + y) - Q(x - y)$.*

Avant d'introduire la définition suivante, rappelons que la fonction cosinus induit une **bijection de** $[0, \pi]$ **sur** $[-1, 1]$ (on a $\cos(0) = 1$, $\cos(\pi) = -1$, et cos est strictement décroissante sur l'intervalle $[0, \pi]$).

Définition 4.45 (Angle non orienté de deux vecteurs non nuls)**.** *Soit E, muni de $(\ \mid\ )$, un espace euclidien et soit $\|\cdot\|$ la norme euclidienne. Soient u, v deux vecteurs non nuls. D'après l'inégalité de Cauchy-Schwarz, on a*

$$|(u \mid v)| \leq \|u\| \cdot \|v\| \qquad d'où \qquad -1 \leq \frac{(u \mid v)}{\|u\| \cdot \|v\|} \leq 1$$

donc il existe un unique $\theta \in [0, \pi]$ tel que $\boxed{\cos(\theta) = \dfrac{(u \mid v)}{\|u\| \cdot \|v\|}}$ i.e. $\boxed{(u \mid v) = \cos(\theta)\, \|u\| \cdot \|v\|.}$ *On appelle θ* **l'angle non-orienté** *des vecteurs u et v, il ne change pas si l'on échange u et v.*

Proposition 4.46 (Isométries vectorielles)**.** *Soient E, F deux espaces euclidiens de même dimension n, notons $(\ \mid\ )_E$ et $\|\cdot\|_E$ (resp. $(\ \mid\ )_F$ et $\|\cdot\|_F$) le produit scalaire et la norme euclidienne sur E (resp. F). Soit $f : E \to F$ une application linéaire.*

1. *Les conditions suivantes sont équivalentes :*
   (a) *f* préserve la norme *:* $\boxed{\forall x \in E, \quad \|x\|_E = \|f(x)\|_F}$
   (b) *f* préserve le produit scalaire *:* $\boxed{\forall x, y \in E, \quad (x \mid y)_E = (f(x) \mid f(y))_F}$
   (c) *Pour toute b.o.n. $\mathfrak{B} = (e_1, \ldots, e_n)$ de E, la famille $(f(e_1), \ldots, f(e_n))$ est une b.o.n. de F.*
   (d) *Il existe une b.o.n. $\mathfrak{B} = (e_1, \ldots, e_n)$ de E telle que $(f(e_1), \ldots, f(e_n))$ soit une b.o.n. de F.*

2. *Sous ces conditions, on dit que f est une* **isométrie** *vectorielle de E sur F*

3. *Dans ce cas, f est bijective, et son inverse f^{-1} est aussi une isométrie.*

Démonstration. Supposons que f préserve la norme, et soient $x, y \in E$. Alors $\|x+y\|_E^2 = \|f(x+y)\|_F^2 = \|f(x)+f(y)\|_F^2$, et le premier (resp. dernier) membre égale :

$$\|x\|_E^2 + \|y\|_E^2 + 2(x \mid y)_E, \qquad \text{resp.} \qquad \|f(x)\|_F^2 + \|f(y)\|_F^2 + 2(f(x) \mid f(y))_F$$

et comme $\|x\|_E^2 = \|f(x)\|_F^2$ et $\|y\|_E^2 = \|f(y)\|_F^2$, on obtient que $(x \mid y)_E = (f(x) \mid f(y))_F$. Ceci prouve que (a) $\implies$ (b).

Les implications (b) $\implies$ (c) $\implies$ (d) sont évidentes, montrons que (d) $\implies$ (a). Supposons (d) vérifiée. Pour tout $x = x_1e_1 + \cdots + x_ne_n$ dans E, on a $f(x) = \sum_i x_i f(e_i)$ et, comme $(e_1, \ldots, e_n)$ et $(f(e_1), \ldots, f(e_n))$ sont des b.o.n., on obtient

$$\|x\|_E^2 = \sum_{i=1}^{n} x_i^2 = \|f(x)\|_F^2$$

donc (a) est vérifiée. Ceci prouve l'assertion (1).

Prouvons (3). Soit $f : E \to F$ une isométrie, et soit $\mathfrak{B} = (e_1, \ldots, e_n)$ de E. Comme $f(\mathfrak{B})$ est une b.o.n. (donc une base) de F, alors f est bijective. Son inverse f^{-1} envoie la b.o.n. $f(\mathfrak{B}) = (f(e_1), \ldots, f(e_n))$ de F sur la b.o.n. $\mathfrak{B}$ de E, donc f^{-1} est une isométrie. Ceci prouve (3). La proposition est démontrée. □

Terminologie. *On a introduit la terminologie isométrie « vectorielle » pour pouvoir faire plus tard la distinction avec la notion d'isométrie « affine », qu'on introduira lorsqu'on étudiera les espaces et applications affines.*

Dans la suite de ce chapitre, comme on ne considère que des applications linéaires, on dira simplement « isométrie »au lieu de « isométrie vectorielle ».

Corollaire 4.47. (1) *On dit que deux espaces euclidiens E et E' sont* **isométriques** *s'il existe une isométrie $f : E \xrightarrow{\sim} E'$.*

(2) *Tout espace euclidien E de dimension n est isométrique à $\mathbb{R}^n$ muni du produit scalaire euclidien standard.*

Démonstration. Soit $\mathfrak{B} = (e_1, \ldots, e_n)$ la base canonique de $\mathbb{R}^n$, qui est orthonormée pour le produit scalaire standard. D'après le théorème 4.40, E admet une b.o.n. $\mathcal{C} = (f_1, \ldots, f_n)$. Alors l'application linéaire $u : \mathbb{R}^n \to E$ définie par $u(e_i) = f_i$, pour $i = 1, \ldots, n$, est une isométrie de $\mathbb{R}^n$ sur E. □

Définition 4.48. *On note* $\mathrm{O}(n) = \{A \in M_n(\mathbb{R}) \mid {}^tAA = I_n\}$. *Rappelons que l'égalité ${}^tAA = I_n$ entraîne que A est inversible et $A^{-1} = {}^tA$. Donc* $\mathrm{O}(n) \subset \mathrm{GL}_n(\mathbb{R})$ *et, si* $A \in \mathrm{O}(n)$, *son inverse $B = A^{-1} = {}^tA$ vérifie $B^{-1} = A = {}^tB$, donc appartient aussi à* $\mathrm{O}(n)$. *De plus, pour tout $A, B \in \mathrm{O}(n)$, on a l'égalité ${}^t(AB)AB = {}^tB\,{}^tAAB = {}^tBB = I_n$, donc $AB \in \mathrm{O}(n)$. Donc* $\mathrm{O}(n)$ *est un* sous-groupe *de* $\mathrm{GL}_n(\mathbb{R})$, *appelé le* **groupe orthogonal**.

Munissons $\mathbb{R}^n$ du produit scalaire euclidien standard $(\ \mid\ )$. Pour tout $X, Y \in \mathbb{R}^n$ on a $(X \mid Y) = {}^tXY$, *i.e.* la matrice de $(\ \mid\ )$ dans la base canonique $\mathfrak{B}_0 = (e_1, \ldots, e_n)$ est la matrice identité I_n. Donc une matrice arbitraire $A \in M_n(\mathbb{R})$ préserve le produit scalaire si et seulement si, on a, pour tout $X, Y \in \mathbb{R}^n$:

$${}^tXY = (X \mid Y) = (AX \mid AY) = {}^tX\,({}^tAA)\,Y$$

ce qui équivaut à dire que ${}^tAA = I_n$ Ceci montre que $\mathrm{O}(n)$ est le groupe des isométries de $\mathbb{R}^n$ muni du produit scalaire euclidien standard $(\ |\ )$.

De plus, notons $C_1, \dots, C_n$ les colonnes de A (*i.e.* C_i est le vecteur $Ae_i \in \mathbb{R}^n$). Remarquons que, pour tout $i, j \in \{1, \dots, n\}$, le coefficient d'indice (i, j) de ${}^tAA$ est le produit matriciel de la i-ème ligne de ${}^tA$, *i.e.* de ${}^tC_i$, par la colonne C_j, c'est-à-dire, on a $({}^tAA)_{ij} = (Ae_i \mid Ae_j)$, donc la condition ${}^tAA = I_n$ équivaut aussi à dire que les colonnes de A sont de norme 1 et deux à deux orthogonales. Tenant compte de la proposition 4.46, on obtient donc les caractérisations suivantes de $\mathrm{O}(n)$, chacune étant utile :

Proposition 4.49 (Groupe orthogonal $\mathrm{O}(n)$)**.** *On munit $\mathbb{R}^n$ du produit scalaire euclidien standard $(\ |\ )$ et l'on note $\|\cdot\|$ la norme euclidienne associée. Alors $\mathrm{O}(n)$ est le groupe des isométries de $\mathbb{R}^n$; il est caractérisé par* chacune *des égalités suivantes :*

$$\begin{aligned}
\mathrm{O}(n) &= \{A \in M_n(\mathbb{R}) \mid {}^tAA = I_n\} \\
&= \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^{-1} = {}^tA\} \\
&= \{A \in M_n(\mathbb{R}) \mid (AX \mid AY) = (X \mid Y), \quad \forall X, Y \in \mathbb{R}^n\} \\
&= \{A \in M_n(\mathbb{R}) \mid \|AX\| = \|X\|, \quad \forall X \in \mathbb{R}^n\} \\
&= \{A \in M_n(\mathbb{R}) \mid (Af_1, \dots, Af_n) \text{ est une b.o.n., pour toute b.o.n. } (f_1, \dots, f_n)\} \\
&= \{A \in M_n(\mathbb{R}) \mid (Ae_1, \dots, Ae_n) \text{ est une b.o.n., où } (e_1, \dots, e_n) \text{ est la base canonique de } \mathbb{R}^n\} \\
&= \{A \in M_n(\mathbb{R}) \mid \text{les colonnes de } A \text{ sont de norme } 1 \text{ et deux à deux orthogonales}\}
\end{aligned}$$

Les éléments de $\mathrm{O}(n)$ sont parfois appelés « endomorphismes orthogonaux *» (mais voir la remarque 4.67 plus bas).*

Remarque 4.50. *Il existe* d'autres *groupes orthogonaux (qui ne sont isomorphes à aucun $\mathrm{O}(n)$). Soient p, q des entiers ≥ 1 et soit φ la forme bilinéaire symétrique sur $\mathbb{R}^{p+q}$ définie par $\varphi(X, Y) = \sum_{i=1}^{p} x_i y_i - \sum_{i=p+1}^{q} x_i y_i$,* i.e. *la matrice de φ dans la base canonique de $\mathbb{R}^{p+q}$ est $J = \left(\begin{array}{c|c} I_p & \mathbf{0}_{p,q} \\ \hline \mathbf{0}_{q,p} & -I_q \end{array}\right)$. Alors*

$$\{A \in M_n(\mathbb{R}) \mid {}^tAJA = J\} = \{A \in M_n(\mathbb{R}) \mid \varphi(AX, AY) = \varphi(X, Y), \quad \forall X, Y \in \mathbb{R}^n\}$$

est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$, noté $\mathrm{O}(p, q)$. On ne considérera pas ces groupes dans ce cours.

4.4.2 Endomorphismes auto-adjoints et théorème de diagonalisation simultanée

Commençons par introduire l'adjoint dans le cas général d'une forme bilinéaire symétrique non dégénérée, même si on se limitera dans la suite au cas euclidien.

Théorème 4.51 (Adjoint d'un endomorphisme)**.** *Soient E un $\mathbb{R}$-espace vectoriel de dimension n, φ une forme bilinéaire symétrique sur E,* **non dégénérée***. Pour tout $u \in \mathrm{End}(E)$, il existe un unique endomorphisme u^* de E, appelé* **l'adjoint** *de u, vérifiant :*

(1) $$\forall x, y \in E, \qquad \boxed{\varphi(u(x), y) = \varphi(x, u^*(y)).}$$

Pour toute base $\mathfrak{B}$ de E, si l'on note $J = \mathrm{Mat}_{\mathfrak{B}}(\varphi)$ et $A = \mathrm{Mat}_{\mathfrak{B}}(u)$, on a

(2) $$\boxed{A^* = \mathrm{Mat}_{\mathfrak{B}}(u^*) = J^{-1}\,{}^tA\,J.}$$

Démonstration. Supposons qu'il existe u^* vérifiant (1) et soient $\mathfrak{B}$ une base de E, $J = \mathrm{Mat}_{\mathfrak{B}}(\varphi)$, $A = \mathrm{Mat}_{\mathfrak{B}}(u)$ et $A^* = \mathrm{Mat}_{\mathfrak{B}}(u^*)$. Soient $x, y \in E$ arbitraires, et notons $X, Y \in \mathbb{R}^n$ les vecteurs colonnes des coordonnées dans la base $\mathfrak{B}$. Alors on a

$$ {}^tX\,{}^tAJY = \varphi(u(x), y) = \varphi(x, u^*(y)) = {}^tXJA^*Y $$

d'où ${}^tAJ = JA^*$ et donc, puisque J est inversible (car φ non-dégénérée), $A^* = J^{-1}\,{}^tA\,J$. Ceci montre que u^*, s'il existe, vérifie (2) et est donc unique.

Réciproquement, si l'on note u^* l'endomorphisme de E dont la matrice dans la base $\mathfrak{B}$ est $A^* = J^{-1}\,{}^tA\,J$, alors pour tout x, y on a :

$$ \varphi(x, u^*(y)) = {}^tXJA^*Y = {}^tX\,{}^tA\,JY = \varphi(u(x), y) $$

donc u^* vérifie (1). Ceci prouve l'existence, et le théorème est démontré. □

Remarque 4.52. *Il résulte de la formule (2) (ou directement de la définition (1)) que, pour tout $u, v \in \mathrm{End}(E)$ et $s, t \in \mathbb{R}$, on a $(su + tv)^* = su^* + tv^*$,* i.e. *l'application $\mathrm{End}(E) \to \mathrm{End}(E)$, $u \mapsto u^*$ est linéaire.*

Remarquons aussi que si φ est un produit scalaire et si $\mathfrak{B}$ est une b.o.n., alors la matrice de φ dans $\mathfrak{B}$ est $J = I_n$. On peut donc énoncer le théorème dans le cas euclidien sous la forme suivante.

Théorème 4.53 (Adjoint d'un endomorphisme dans le cas euclidien)**.** *Soit E muni de $(\ |\ )$ un espace* **euclidien** *de dimension n. Pour tout $u \in \mathrm{End}(E)$, il existe un unique endomorphisme u^* de E, appelé* **l'adjoint** *de u, vérifiant :*

$$ (*) \qquad \forall x, y \in E, \qquad \boxed{(u(x) \mid y) = (x \mid u^*(y)).} $$

Pour toute **b.o.n.** *$\mathfrak{B}$ de E, si l'on note $A = \mathrm{Mat}_{\mathfrak{B}}(u)$, on a*

$$ (**) \qquad \boxed{A^* = \mathrm{Mat}_{\mathfrak{B}}(u^*) = {}^tA.} $$

Définition 4.54 (Endomorphismes auto-adjoints)**.** *Soit E un espace* **euclidien** *de dimension n. On dit qu'un endomorphisme $u \in \mathrm{End}(E)$ est* **auto-adjoint** *(ou symétrique) s'il vérifie $u^* = u$. Ceci équivaut à dire que, pour toute b.o.n. $\mathfrak{B}$ de E, la matrice $S = \mathrm{Mat}_{\mathfrak{B}}(u)$ est* **symétrique**.

Proposition 4.55 (Endomorphismes auto-adjoints et formes bilinéaires symétriques)**.** *Soit E muni de $(\ |\ )$ un espace* **euclidien** *de dimension n et soit φ une autre forme bilinéaire symétrique (arbitraire) sur E. Alors il existe un unique $u \in \mathrm{End}(E)$ auto-adjoint pour $(\ |\ )$ tel que :*

$$ (\dagger) \qquad \forall x, y \in E, \qquad \boxed{\varphi(x, y) = (u(x) \mid y) = (x \mid u(y)).} $$

Pour toute **b.o.n.** *$\mathfrak{B}$ de E, on a*

$$ (\ddagger) \qquad \boxed{\mathrm{Mat}_{\mathfrak{B}}(u) = \mathrm{Mat}_{\mathfrak{B}}(\varphi).} $$

Démonstration. Soient $\mathfrak{B}$ une b.o.n. de E et $S = \mathrm{Mat}_{\mathfrak{B}}(\varphi)$, on a ${}^tS = S$. Pour $x, y \in E$, notons $X, Y \in \mathbb{R}^n$ les coordonnées dans la base $\mathfrak{B}$. S'il existe u vérifiant (†), soit $A = \mathrm{Mat}_{\mathfrak{B}}(u)$, alors l'égalité

$$ {}^tXS\,Y = \varphi(x, y) = (x \mid u(y)) = {}^tXAY $$

entraîne $A = S$. Ceci montre que u, s'il existe, vérifie (‡) et est donc unique.

Réciproquement, si l'on note u l'endomorphisme de E dont la matrice dans la base $\mathfrak{B}$ est S, alors pour tout x, y on a :

$$ \begin{aligned} \varphi(x, y) &= {}^tXS\ Y = (x \mid u(y)) \\ &= {}^tX\,{}^tS\ Y = (u(x) \mid y) \end{aligned} $$

donc u vérifie (†). Ceci prouve l'existence, et la proposition est démontrée. □

On a maintenant le théorème important et utile suivant.

Théorème 4.56 (Diagonalisation des endomorphismes auto-adjoints)**.** *Soient E muni de $(\ |\ )$ un espace euclidien de dimension n, et u un endomorphisme auto-adjoint. Alors, u est diagonalisable et ses espaces propres sont deux à deux orthogonaux. Par conséquent, il existe une b.o.n. de E formée de vecteurs propres de u.*

Corollaire 4.57 (Diagonalisation des matrices symétriques réelles)**.** *Soit $S \in M_n(\mathbb{R})$ une matrice symétrique réelle. Alors S est diagonalisable dans une base orthonormée : il existe $P \in \mathrm{O}(n)$ telle que $P^{-1}SP$ soit diagonale.*

Le point le plus difficile de la démonstration est la proposition suivante :

Proposition 4.58 (Existence d'une valeur propre réelle)**.** *Soit $A \in M_n(\mathbb{R})$* **symétrique**. *Alors A admet au moins une valeur propre réelle.*

Admettons pour le moment cette proposition et démontrons le théorème, par récurrence sur $n = \dim E$. C'est ok si $n = 1$, donc on peut supposer $n \geq 2$ et le résultat établi pour $n-1$. D'après la proposition, u admet au moins une valeur propre réelle λ_1, soit f_1 un vecteur propre associé, qu'on peut supposer de norme 1 (quitte à remplacer f_1 par $\dfrac{1}{\|f_1\|} f_1$). Montrons que $E_1 = (\mathbb{R}f_1)^\perp$ est stable par u : pour tout $x \in E_1$, on a :

$$(u(x) \mid f_1) = (x \mid u^*(f_1)) = (x \mid u(f_1)) = (x \mid \lambda_1 f_1) = \lambda_1 (x \mid f_1) = 0,$$

donc $u(x) \in E_1$. La restriction u_1 de u à E_1 est encore auto-adjointe, puisque pour tout $x, y \in E_1$ on a :

$$(u_1(x) \mid y) = (u(x) \mid y) = (x \mid u(y)) = (x \mid u_1(y)).$$

Donc, par hypothèse de récurrence, il existe une b.o.n. $\mathcal{C} = (f_2, \ldots, f_n)$ de E_1 formée de vecteurs propres de u_1, donc de u. Alors, $\mathfrak{B} = \{f_1\} \cup \mathcal{C}$ est une b.o.n. de E formée de vecteurs propres de u. Ceci prouve la première assertion du théorème.

Le fait que les espaces propres soient deux à deux orthogonaux peut se déduire de la démonstration précédente, mais il est plus simple de le voir directement. Soient $\lambda \neq \mu$ deux valeurs propres distinctes de u et soient $x \in V_\lambda$ et $y \in V_\mu$; alors

$$\lambda(x \mid y) = (u(x) \mid y) = (x \mid u(y)) = \mu(x \mid y)$$

et comme $\lambda \neq \mu$ ceci entraîne $(x \mid y) = 0$. Ceci prouve le théorème, modulo la démonstration de la proposition 4.58. □

Démonstration de la proposition 4.58. On munit $\mathbb{R}^n$ de la norme euclidienne usuelle et l'on considère la **sphère unité** :

$$S^{n-1} = \{x \in \mathbb{R}^n \mid \|x\|^2 = x_1^2 + \cdots + x_n^2 = 1\};$$

celle-ci est **compacte**. D'autre part, la fonction

$$f : \mathbb{R}^n \to \mathbb{R}, \qquad x \mapsto (Ax \mid x)$$

est **continue**, car c'est un polynôme de degré 2 en les coordonnées $x_1, \ldots, x_n$. Par conséquent, f atteint un maximum λ en un point x_0 de S^{n-1}, *i.e.* on a :

$$\forall x \in S^{n-1}, \qquad (Ax \mid x) \leq \lambda = (Ax_0 \mid x_0).$$

Alors, pour tout $x \neq 0$ dans $\mathbb{R}^n$, on a $\dfrac{1}{\|x\|}x \in S^{n-1}$, d'où

$$\left(\frac{Ax}{\|x\|} \mid \frac{x}{\|x\|}\right) \leq \lambda$$

et donc :

$$\forall x \in \mathbb{R}^n - \{0\}, \qquad (Ax \mid x) \leq \lambda\,(x \mid x). \tag{1}$$

Fixons $v \in \mathbb{R}^n$ et soit $t \in \mathbb{R}$ variable. On a, d'une part :

$$f(x_0 + tv) = \big(A(x_0 + tv) \mid A(x_0 + tv)\big) = (Ax_0 \mid x_0) + t(Ax_0 \mid v) + t(Av \mid x_0) + t^2(Av \mid v)$$

et comme $(Av \mid x_0) = (v \mid {}^tAx_0) = (v \mid Ax_0) = (Ax_0 \mid v)$, ceci se récrit :

$$f(x_0 + tv) = (Ax_0 \mid x_0) + 2t(Ax_0 \mid v) + t^2(Av \mid v). \tag{2}$$

D'autre part, on a :

$$\lambda\,(x_0 + tv \mid x_0 + tv) = \lambda \underbrace{(x_0 \mid x_0)}_{=1} + 2t(\lambda x_0 \mid v) + t^2(\lambda v \mid v).$$

D'après (1), et tenant compte de l'égalité $\lambda = (Ax_0 \mid x_0)$, on obtient :

$$\forall t \in \mathbb{R}, \qquad 2t(Ax_0 - \lambda x_0 \mid v) + t^2(Av - \lambda v \mid v) \leq 0.$$

On a donc un trinôme du second degré en t, toujours négatif et qui s'annule pour $t = 0$. On en déduit que son discriminant réduit $\Delta' = (Ax_0 - \lambda x_0 \mid v)^2$ est nul, donc :

$$\forall v \in \mathbb{R}^n, \qquad (Ax_0 - \lambda x_0 \mid v) = 0$$

et donc $Ax_0 - \lambda x_0 = 0$, *i.e.* $Ax_0 = \lambda x_0$. Ceci prouve que x_0 est un vecteur propre pour λ. Ceci achève la démonstration de la proposition 4.58 et du théorème 4.56. □

Nous allons proposer une démonstration de la proposition 4.58 qui utilise le théorème suivant de d'Alembert-Gauss.

Théorème 4.59 (d'Alembert-Gauss)**.** *Tout polynôme non constant de $\mathbb{C}[X]$ a une racine complexe.*

Démonstration. On procède par l'absurde. Soit $P(X)$ un polynôme complexe non constant sans racine. Comme $|P(z)|$ tend vers l'infini quand $|z|$ tend vers l'infini et que $|P(z)|$ ne s'annule pas, il possède un minimum non nul atteint en un point $z_0 \in \mathbb{C}$. On peut le supposer égal à 1 et atteint en 0, en remplaçant $P(z)$ par $P(z + z_0)/P(z_0)$. On peut écrire, par développement de Taylor, le polynôme $P(z)$ sous la forme

$$P(z) = 1 + cz^{n_0} + cz^{n_0}Q(z)$$

pour un entier $n_0 > 0$, un coefficient $c \neq 0$ et un polynôme $Q(z)$ qui s'annule en 0. Soit $\alpha \in \mathbb{C}$ tel que $\alpha^{n_0} = -1/c$. Il suffit de se déplacer dans la direction α pour faire décroitre le module de P et obtenir une contradiction. Soit $t \in]0, 1[$ tel que $|Q(\alpha t)| \leq 1/2$. Alors

$$P(\alpha t) = 1 - t^{n_0} - t^{n_0}Q(\alpha t),$$

donc

$$|P(\alpha t)| \leq 1 - t^{n_0} + t^{n_0}|Q(\alpha t)| \leq 1 - t^{n_0}/2 < 1$$

ce qui contredit la minimalité de $P(0)$. On obtient donc le résultat recherché. □

Deuxième démonstration de la proposition 4.58. Soit $A \in \mathrm{M}_n(\mathbb{R})$ une matrice symétrique de dimension $n > 1$. On sait, par le théorème de d'Alembert-Gauss, que son polynôme caractéristique $P_A(X)$, qui est de degré n, a au moins une racine complexe λ. Il s'agit de montrer que λ est forcément réelle. On sait qu'il existe un vecteur propre $v \in \mathbb{C}^n$ tel que $Av = \lambda v$. Notons $\bar{v}$ le vecteur dont les coordonnées sont les conjuguées de celles de v. La matrice étant à coefficients réels, on obtient par conjugaison

$$A\bar{v} = \bar{\lambda}\bar{v}.$$

Le produit scalaire euclidien est étendu à $\mathbb{C}$ par la formule usuelle $\langle x, y\rangle = \sum_i x_i y_i$. Comme A est autoadjointe, on a

$$\langle Av, w\rangle = \langle v, Aw\rangle$$

pour tous vecteurs à coefficients réels et cette égalité s'étend aux vecteurs complexes par bilinéarité. On obtient

$$\lambda\langle v, \bar{v}\rangle = \langle Av, \bar{v}\rangle = \langle v, A\bar{v}\rangle = \bar{\lambda}\langle v, \bar{v}\rangle.$$

On conclut que $\lambda = \bar{\lambda}$ car $\langle v, \bar{v}\rangle = \sum_i |v_i|^2$ est non nul. □

Théorème 4.60 (Réduction simultanée)**.** *Soient E muni de $(\ |\ )$ un espace euclidien de dimension n, Q une forme quadratique arbitraire sur E, φ sa forme polaire, $\mathfrak{B}_0 = (e_1, \dots, e_n)$ une base orthonormée de E, et u l'endomorphisme de E tel que* $\mathrm{Mat}_{\mathfrak{B}_0}(u) = \mathrm{Mat}_{\mathfrak{B}_0}(\varphi) = A$.

Alors il existe une base $\mathfrak{B} = (f_1, \dots, f_n)$ **orthonormée** *pour $(\ |\ )$ et formée de vecteurs propres de u,* i.e. *$u(f_i) = \lambda_i f_i$ pour $i = 1, \dots, n$, et l'on a*

$$\mathrm{Mat}_{\mathfrak{B}}(\varphi) = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}$$

où $\lambda_1, \dots, \lambda_n$ sont les valeurs propres de u; plus précisément, la matrice de passage $P = \mathrm{Mat}_{\mathfrak{B}_0}(\mathfrak{B})$ est orthogonale, i.e. *${}^tP = P^{-1}$, donc la matrice ci-dessus égale à la fois ${}^tPAP = \mathrm{Mat}_{\mathfrak{B}}(\varphi)$ et $P^{-1}AP = \mathrm{Mat}_{\mathfrak{B}}(u)$.*

Remarque 4.61. *Ce théorème est appelé « théorème de* **réduction simultanée** *» ou « de* **diagonalisation simultanée** *» car la base $\mathfrak{B}$ donnée par l'énoncé est à la fois* **orthonormée** *pour $(\ |\ )$ et* **orthogonale** *pour φ. En d'autres termes, si l'on note $(x_1, \dots, x_n)$ les coordonnées dans $\mathfrak{B}$ d'un vecteur x arbitraire, la base $\mathfrak{B}$* **réduit simultanément** *la forme $x \mapsto (x \mid x)$ à la forme standard $x_1^2 + \cdots + x_n^2$, et la forme Q en la somme de carrés $\lambda_1 x_1^2 + \cdots + \lambda_n x_n^2$.*

Démonstration. Notons u l'endomorphisme auto-adjoint tel que

$$\forall x, y \in E, \qquad \varphi(x, y) = (u(x) \mid y) = (x \mid (u(y)),$$

cf. Proposition 4.55. D'après le théorème 4.56, il existe une base $\mathfrak{B} = (f_1, \dots, f_n)$ **orthonormée** pour $(\ |\ )$ et formée de vecteurs propres de u, *i.e.* $u(f_i) = \lambda_i f_i$, pour tout i. Alors, pour tout i, j on a :

$$\varphi(f_i, f_j) = \lambda_i(f_i \mid f_j) = \lambda_j(f_i \mid f_j) = \begin{cases} 0 & \text{si } i \neq j, \\ \lambda_i & \text{si } i = j, \end{cases}$$

ce qui montre que $\mathfrak{B}$ est une base **orthogonale** pour φ. De plus, comme $\mathfrak{B}_0$ et $\mathfrak{B}$ sont orthonormées, la matrice de passage $P = \mathrm{Mat}_{\mathfrak{B}_0}(\mathfrak{B})$ est orthogonale, *i.e.* ${}^tP = P^{-1}$, donc la matrice diagonale de l'énoncé égale à la fois ${}^tPAP = \mathrm{Mat}_{\mathfrak{B}}(\varphi)$ et $P^{-1}AP = \mathrm{Mat}_{\mathfrak{B}}(u)$. □

Répétons la version matricielle du théorème précédent :

Corollaire 4.62 (Réduction simultanée des matrices symétriques réelles)**.** *Soit $S \in M_n(\mathbb{R})$ telle que ${}^tS = S$. Il existe $P \in O(n)$ telle que $P^{-1}SP = {}^tPSP$ soit diagonale.*

Corollaire 4.63 (Calculs de signature)**.** *Soient Q une forme quadratique sur $\mathbb{R}^n$, φ sa forme polaire, A la matrice de φ dans la base canonique. Alors la signature de Q est donnée par le nombre de valeurs propres de A qui sont > 0 (resp. < 0).*

Exemple 4.64. *Illustrons ce qui précède par l'exemple suivant. Soient $n \geq 2$ et Q la forme quadratique sur $\mathbb{R}^n$ définie par*

$$Q(x_1, \ldots, x_n) = 2\sum_{i<j} x_i x_j = \sum_{i \neq j} x_i x_j.$$

La matrice de sa forme polaire est

$$A = \begin{pmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \cdots & 1 & 0 \end{pmatrix}$$

(tous les coefficients valent 1 sauf ceux de la diagonale qui sont nuls). On remarque que la matrice $A + I_n$ est de rang 1, donc l'espace propre $V_{-1} = \mathrm{Ker}(A + I_n)$ est de dimension $n - 1$. Donc -1 est une racine de multiplicité $\geq n - 1$ du polynôme caractéristique $P_A(X)$. Comme $0 = \mathrm{tr}(A)$ est la somme des racines (dans $\mathbb{C}$) de $P_A(X)$, la dernière racine λ vérifie $\lambda + (n-1)(-1) = 0$, d'où $\lambda = n - 1$. Donc, d'après le théorème 4.60, il existe $P \in O(n)$ tel que

$$P^{-1}AP = {}^tPAP = \begin{pmatrix} -1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & -1 & 0 \\ 0 & \cdots & 0 & n-1 \end{pmatrix}$$

il y a donc $n - 1$ valeurs propres égales à -1, et une seule valeur propre > 0 (égale à $n - 1$), donc la signature de Q est $(1, n - 1)$.

4.5 Orthogonalité. Orthonormalisation de Gram-Schmidt

Définition 4.65 (Sous-espaces d'un espace euclidien)**.** *Soit E, muni de $(\ |\ )$, un espace euclidien et soit F un sous-espace vectoriel de E. Alors la restriction $(\ |\ )_F$ de $(\ |\ )$ à F est un produit scalaire sur F, puisque $(x \mid x)_F = (x \mid x) > 0$ pour tout $x \in F - \{0\}$. Donc F muni de $(\ |\ )_F$ est un espace euclidien.*

Théorème/Définition 4.1 (Projection orthogonale sur un sous-espace)**.** *Soit E, muni de $(\ |\ )$, un espace euclidien (pas nécessairement de dimension finie). Soit F un sous-espace de dimension finie r et soit $F^\perp$ son orthogonal pour $(\ |\ )$.*

1. *On a* $\boxed{E = F \oplus F^\perp}$. *Cette décomposition en somme directe permet de définir le projecteur* $\pi_F : E \to E$, *d'image* F *et de noyau* $F^\perp$, *et le projecteur* $\pi_{F^\perp} : E \to E$, *d'image* $F^\perp$ *et de noyau* F. *Alors, pour tout* $x \in E$, *on a*

$$\boxed{x = \pi_F(x) + \pi_{F^\perp}(x)}$$

et π_F *(resp.* $\pi_{F^\perp}$*) s'appelle la* **projection orthogonale** *sur* F *(resp. sur* $F^\perp$*).*

2. *Soit* $(e_1, \dots, e_r)$ *une base* **orthonormée** *de* F. *Alors* $\boxed{\pi_F(v) = (v \mid e_1)e_1 + \cdots + (v \mid e_r)e_r}$ *pour tout* $v \in E$.

3. *On a* $\boxed{(F^\perp)^\perp = F}$.

Remarque 4.66. *(a) On a toujours* $F \cap F^\perp = \{0\}$ *car si* $x \in F \cap F^\perp$ *alors* $(x \mid x) = 0$ *d'où* $x = 0$.

(b) Par conséquent, si E *est de dimension finie* n, *l'égalité* $E = F \oplus F^\perp$ *découle de 4.18. Toutefois, la démonstration donnée ci-dessous ne suppose pas* E *de dimension finie et permet, par exemple, de démontrer l'inégalité de Bessel pour les coefficients de Fourier d'une fonction continue* $f : [0, 2\pi] \to \mathbb{R}$ *(voir par exemple le Devoir du 6/4/2012 et son corrigé).*

Démonstration. On va démontrer en même temps les assertions (1) et (2). Comme $(\ \mid\ )_F$ est définie positive et comme $\dim(F) = r < \infty$, alors F possède une base orthonormée $(e_1, \dots, e_r)$, d'après le théorème 4.40. Pour tout $v \in E$, posons provisoirement

$$p(v) = (v \mid e_1)\, e_1 + \cdots + (v \mid e_r)\, e_r \in F$$

et $q(v) = v - p(v)$. Alors, $v = p(v) + q(v)$. D'autre part, pour $j = 1, \dots, r$, on a

$$(q(v) \mid e_j) = (v \mid e_j) - \sum_{i=1}^{r} (v \mid e_i) \underbrace{(e_i \mid e_j)}_{\substack{=1 \text{ si } i=j \\ =0 \text{ si } i\neq j}} = 0,$$

d'où $q(v) \in F^\perp$. Comme $v = p(v) + q(v)$, ceci montre que $E = F + F^\perp$.

De plus, comme on l'a déjà remarqué plus haut, si $x \in F \cap F^\perp$, alors $(x \mid x) = 0$, d'où $x = 0$. On a donc $F \cap F^\perp = \{0\}$ et $E = F + F^\perp$, d'où $E = F \oplus F^\perp$. Ceci prouve (1).

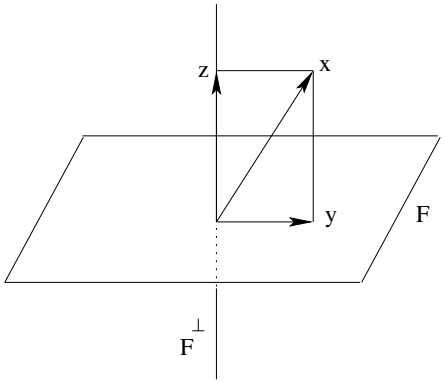
Alors tout $v \in E$ s'écrit de façon unique $v = x + y$ avec $x \in F$ et $y \in F^\perp$, et l'on a $x = \pi_F(v)$ et $y = \pi_{F^\perp}(v)$. Comme $v = p(v) + q(v)$, on a donc

$$\pi_F(v) = p(v) = \sum_{i=1}^{r} (v \mid e_i) e_i,$$

ce qui prouve (2).

Prouvons (3). Pour tout $x \in F$ et $y \in F^\perp$, on a $0 = (x \mid y) = (y \mid x)$. Fixant $x \in F$ et faisant varier y dans $G = F^\perp$, ceci montre que $x \in G^\perp$, d'où l'inclusion $F \subset G^\perp$. Réciproquement, soit $v \in G^\perp$. Comme $E = F \oplus F^\perp$, on peut écrire $v = x + y$ avec $y \in G = F^\perp$ et $x \in F$. Alors $y = v - x \in G \cap G^\perp$, donc $0 = (y \mid y)$ d'où $y = 0$ et donc $v = x \in F$. Ceci montre que $F = G^\perp = (F^\perp)^\perp$. Le théorème est démontré. □

Dans la figure qui suit, on a $y = \pi_F(x)$ et $z = \pi_{F^\perp}(x)$:



Remarque 4.67. *Attention à la terminologie ! Si $F \neq E$, la projection orthogonale π_F n'est* **pas une isométrie** *(car une isométrie est injective, or* $\mathrm{Ker}(\pi_F) = F^\perp$ *est non nul, sauf si $F = E$), donc n'est* **pas** *un « endomorphisme orthogonal » de E (*cf. *4.49).*

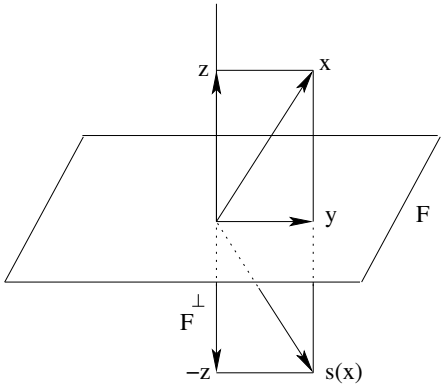
Proposition/Définition 4.1 (Symétries orthogonales)**.** *Soient E un espace euclidien de dimension n et F un sous-espace de dimension r.*

1. *La* **symétrie orthogonale** *s_F par rapport à F est définie comme suit : pour tout $v \in E$, on a $v = \pi_F(v) + \pi_{F^\perp}(v)$ et l'on pose :*

   $$(\star) \qquad \boxed{s_F(v) = \pi_F(v) - \pi_{F^\perp}(v) = v - 2\pi_{F^\perp}(v).}$$

   Alors $s_F^2 = \mathrm{id}_E$ et s_F est une isométrie de E.

2. *Si $\mathcal{C}_+$ est une base de F et $\mathcal{C}_-$ une base de $F^\perp$, la matrice de s_F dans la base $\mathfrak{B} = \mathcal{C}_+ \cup \mathcal{C}_-$ de E est* $\mathrm{Mat}_{\mathfrak{B}}(s_F) = \left(\begin{array}{c|c} I_r & \mathbf{0}_{r,n-r} \\ \hline \mathbf{0}_{n-r,r} & -I_{n-r} \end{array}\right)$*. En particulier, on a* $\boxed{\det s_F = (-1)^{n-r}.}$



Démonstration. D'après la définition, il est clair que $s_F^2 = \mathrm{id}_E$, donc s_F est bijective et égale à son inverse (*i.e.* s_F est **involutive**). Montrons que s_F est une isométrie. Comme $(\pi_F(v) \mid \pi_{F^\perp}(v)) = 0$, on a d'après l'égalité de Pythagore (*cf.* 4.43) :

$$\|v\|^2 = \|\pi_F(v)\|^2 + \|\pi_{F^\perp}(v)\|^2 = \|s_F(v)\|^2$$

et ceci prouve que s_F est une isométrie. Enfin, si si $\mathfrak{B} = \mathcal{C}_+ \cup \mathcal{C}_-$ est comme dans la proposition, il est clair que $\mathrm{Mat}_{\mathfrak{B}}(s_F)$ est comme indiquée. □

Définition 4.68 (Réflexions orthogonales)**.** *Un cas particulier important de symétrie orthogonale est le suivant. Soit $v_0 \in E$, $v_0 \neq 0$, alors $H = (\mathbb{R}v_0)^\perp$ est appelé un* **hyperplan** *de E ; d'après le théorème 4.1 on a*

$$E = \mathbb{R}v_0 \oplus H\,,$$

explicitement, si l'on pose $u_0 = \dfrac{1}{\|v_0\|} v_0$ *alors* $\|u_0\| = 1$ *et tout* $x \in E$ *s'écrit de façon unique*

$$x = (x \mid u_0)u_0 + \pi_H(x), \qquad \text{où} \qquad \pi_H(x) = x - (x \mid u_0)u_0\,,$$

donc

$$\boxed{\pi_{\mathbb{R}v_0}(x) = (x \mid u_0)u_0 = \frac{(x \mid v_0)}{(v_0 \mid v_0)}\, v_0.}$$

La symétrie orthogonale s_H *par rapport à* H *s'appelle la* **réflexion orthogonale** *par rapport à l'hyperplan* H *; d'après ce qui précède elle est donnée par la formule :*

(*4.68*.1)
$$\boxed{\forall x \in E, \qquad s_H(x) = x - 2\frac{(x \mid v_0)}{(v_0 \mid v_0)}\, v_0.}$$

Si $\dim E = n$ *alors* $\dim H = n-1$*, et si* $\mathcal{C}_+$ *est une base de* H*, alors* $\mathfrak{B} = \mathcal{C}_+ \cup \{v_0\}$ *est une base de* E *et* $\mathrm{Mat}_{\mathfrak{B}}(s_H) = \left(\begin{array}{c|c} I_{n-1} & \mathbf{0}_{n-1,1} \\ \hline \mathbf{0}_{1,n-1} & -1 \end{array}\right)$*, d'où en particulier* $\boxed{\det s_H = -1.}$

Théorème 4.69 (Orthonormalisation de Gram-Schmidt)**.** *Soit* E *un espace euclidien et soient* $v_1, \ldots, v_n$ *linéairement indépendants dans* E*. Alors il existe une* unique *famille* $(e_1, \ldots, e_n)$ *vérifiant les deux propriétés suivantes :*

1. *Pour tout* $i = 1, \ldots, n$*,* $(e_1, \ldots, e_i)$ *est une base orthonormée de* $V_i = \textsc{Vect}(v_1, \ldots, v_i)$*.*
2. *Pour tout* $j = 1, \ldots, n$*, on a* $(e_j \mid v_j) > 0$*.*

Démonstration. Pour $j = 1$, on cherche $e_1 = t_1 v_1$ tel que $1 = (e_1 \mid e_1) = t_1^2(v_1 \mid v_1)$ et $0 < (e_1 \mid v_1) = t_1(v_1 \mid v_1)$; la 1ère condition donne $t_1^2 = 1/(v_1 \mid v_1)$, et la 2ème condition, qui implique $t_1 > 0$, donne alors :

(1)
$$t_1 = \frac{1}{\|v_1\|} \qquad \text{d'où} \qquad \boxed{e_1 = \frac{1}{\|v_1\|}\, v_1.}$$

Pour $j = 2$, on cherche d'abord un vecteur $e_2' \in \textsc{Vect}(v_1, v_2) = \textsc{Vect}(e_1, v_2)$, donc de la forme $e_2' = v_2 + \lambda e_1$, vérifiant la condition :

$$0 = (e_2' \mid e_1) = (v_2 \mid e_1) + \lambda \underbrace{(e_1 \mid e_1)}_{=1} = (v_2 \mid e_1) + \lambda,$$

ce qui impose $\lambda = -(v_2 \mid e_1)$. Alors le vecteur

$$\boxed{e_2' = v_2 - (v_2 \mid e_1)e_1}$$

est orthogonal à e_1, et est $\neq 0$ puisque $v_2 \notin \mathbb{R}v_1 = \mathbb{R}e_1$, donc la famille (e_1, e_2') est libre et forme une base de $V_2 = \textsc{Vect}(v_1, v_2)$.

On a $v_2 = e_2' + (v_2 \mid e_1)e_1$ et, puisque $(e_2' \mid e_1) = 0$, l'égalité de Pythagore donne

$$\|v_2\|^2 = \|e_2'\|^2 + (v_2 \mid e_1)^2 \qquad \text{d'où} \qquad \boxed{\|e_2'\|^2 = \|v_2\|^2 - (v_2 \mid e_1)^2.}$$

Pour rendre e_2' unitaire (*i.e.* de norme 1), on le divise par sa norme, c'est-à-dire, on pose

(2)
$$\boxed{e_2 = \frac{1}{\|e_2'\|} e_2' = \frac{1}{\|e_2'\|}\,(v_2 - (v_2 \mid e_1)e_1)}$$

alors (e_1, e_2) est une b.o.n. de V_2, et d'après (2) ci-dessus on a $1 = (e_2 \mid e_2) = (e_2 \mid v_2)/\|e_2'\|$ donc $(e_2 \mid v_2) = \|e_2'\| > 0$. C'est bien le seul choix possible, car si $f_2 \in V_2$ est orthogonal à e_1 et unitaire, alors $f_2 = \pm e_2$, et la condition $(f_2 \mid v_2) > 0$ entraîne $f_2 = e_2$.

Pour $j = 3$, on cherche d'abord un vecteur $e_3' \in V_3 = \text{Vect}(e_1, e_2, v_3)$, donc de la forme $e_3' = v_3 + \mu_2 e_2 + \mu_1 e_1$, vérifiant les relations linéaires :

$$\begin{cases} 0 = (e_3' \mid e_1) = (v_3 \mid e_1) + \mu_1 \,, \\ 0 = (e_3' \mid e_2) = (v_3 \mid e_2) + \mu_2 \end{cases}$$

(on a utilisé le fait que e_1, e_2 sont orthogonaux et unitaires), qui donnent $\mu_i = -(v_3 \mid e_i)$ pour $i = 1, 2$. Alors le vecteur

$$\boxed{e_3' = v_3 - (v_3 \mid e_2)e_2 - (v_3 \mid e_1)e_1}$$

est orthogonal à $V_2 = \text{Vect}(e_1, e_2) = \text{Vect}(v_1, v_2)$, et est $\neq 0$ puisque $v_3 \notin V_2$, donc la famille (e_1, e_2, e_3') est libre et forme une base de V_3. Comme e_1, e_2 et e_3' sont orthogonaux, l'égalité de Pythagore donne

$$\|v_3\|^2 = \|e_3'\|^2 + (v_3 \mid e_2)^2 + (v_3 \mid e_1)^2 \qquad \text{d'où} \qquad \boxed{\|e_3'\|^2 = \|v_3\|^2 - (v_3 \mid e_2)^2 - (v_3 \mid e_1)^2.}$$

Pour rendre e_3' unitaire, on le divise par sa norme, c'est-à-dire, on pose

$$\boxed{e_3 = \frac{1}{\|e_3'\|} e_3' = \frac{1}{\|e_3'\|} \left(v_3 - (v_3 \mid e_2)e_2 - (v_3 \mid e_1)e_1\right)} \tag{3}$$

alors (e_1, e_2, e_3) est une b.o.n. de V_3, et d'après (3) ci-dessus on a $1 = (e_3 \mid e_3) = (e_3 \mid v_3)/\|e_3'\|$ donc $(e_3 \mid v_3) = \|e_3'\| > 0$. C'est bien le seul choix possible, car si $f_3 \in V_3$ est orthogonal à V_2 et unitaire, alors $f_3 = \pm e_3$, et la condition $(f_3 \mid v_3) > 0$ entraîne $f_3 = e_3$.

En répétant ce processus on construit par récurrence, de façon unique, la famille $(e_1, \ldots, e_n)$; les formules explicites pour e_n' et e_n étant :

$$\boxed{e_n' = v_n - \sum_{i=1}^{n-1} (v_n \mid e_i)\, e_i} \qquad \boxed{\|e_n'\|^2 = \|v_n\|^2 - \sum_{i=1}^{n-1} (v_n \mid e_i)^2} \qquad \text{et} \qquad \boxed{e_n = \frac{1}{\|e_n'\|}\, e_n'}$$

□

Remarque 4.70. *(1) Ce qui précède peut aussi s'exprimer, de façon abstraite, comme suit : l'orthogonal G_n de V_{n-1} dans V_n,* i.e. *$G_n = \{x \in V_n \mid (x \mid e_i) = 0$ pour $i = 1, \ldots, n-1\}$, est de dimension $n - (n-1) = 1$, et $\sum_{i=1}^{n-1} (v_n \mid e_i)\, e_i$ est la projection orthogonale de v_n sur V_{n-1} tandis que e_n' est la projection orthogonale de v_n sur G_n ; la droite $G_n = \mathbb{R}e_n'$ contient deux vecteurs de norme 1, à savoir $\pm e_n$, et e_n est déterminé par la condition $(e_n \mid v_n) = \|e_n'\| > 0$.*

(2) La démonstration précédente fournit un algorithme pour calculer explicitement $e_1, \ldots, e_n$. Illustrons ceci par l'exemple suivant.

Exemple 4.71. *On munit $E = \mathbb{R}[X]$ du produit scalaire défini par $(P \mid Q) = \int_{-1}^{1} P(t)Q(t)dt$. Appliquons le procédé d'orthonormalisation de Gram-Schmidt aux vecteurs $1, X, X^2 \in \mathbb{R}_2[X]$. On va noter (e_0, e_1, e_2) au lieu de (e_1, e_2, e_3) la base orthonormée obtenue, afin d'avoir l'égalité $\deg(e_i) = i$. On a $(1 \mid 1) = 2$ donc on prend $e_0 = \dfrac{1}{\sqrt{2}}$. Alors $(X \mid e_0) = \dfrac{1}{\sqrt{2}} \int_{-1}^{1} t\,dt = 0$ et $(X \mid X) = \int_{-1}^{1} t^2\,dt = \dfrac{2}{3}$, d'où $e_1 = \dfrac{\sqrt{3}}{\sqrt{2}}\, X$.*

$$\textit{Puis } (X^2 \mid e_0) = \frac{1}{\sqrt{2}} \int_{-1}^{1} t^2\, dt = \frac{\sqrt{2}}{3} \textit{ et } (X^2 \mid e_1) = \frac{\sqrt{3}}{\sqrt{2}} \int_{-1}^{1} t^3\, dt = 0, \textit{ d'où } e_2' = X^2 - \frac{\sqrt{2}}{3} e_0,$$

$$\|e_2'\|^2 = \int_{-1}^{1} t^4\, dt - \frac{2}{9} = \frac{2 \cdot 4}{5 \cdot 9} \qquad \textit{et} \qquad e_2 = \frac{3\sqrt{5}}{2\sqrt{2}}(X^2 - \frac{1}{3}) = \frac{\sqrt{5}}{\sqrt{2}}\left(\frac{3X^2 - 1}{2}\right).$$

Troisième partie

Annexes

Annexe A

Les axiomes de Peano pour les entiers naturels

Dans cet appendice, nous allons démontrer les propriétés des entiers naturels appelées axiomes de Peano, à partir de leur propriété universelle, donnée par l'axiome des entiers. On pourra se référer au jeu en ligne [3], ainsi qu'au Chapitre 9 du livre [4] pour plus de détails sur cette axiomatique.

Axiome A.1 (Axiome des entiers naturels)**.** *Il existe un triplet* $(\mathbb{N}, S : \mathbb{N} \to \mathbb{N}, 0 \in \mathbb{N})$ *formé d'un ensemble* $\mathbb{N}$ *appelé ensemble des entiers naturels, d'une application* $S : \mathbb{N} \to \mathbb{N}$ *notée aussi*

$$S(n) = n + 1$$

et appelée application successeur, et d'un élément $0 \in \mathbb{N}$ *vérifiant la propriété universelle suivante : pour tout triplet*

$$(X, T : X \to X, x \in X)$$

avec X ensemble, il existe une unique application $f : \mathbb{N} \to X$ *telle que* $f(0) = x$ *et* $f \circ S = T \circ f$.

Proposition A.1 (Axiomes de Peano)**.** *Le triplet* $(\mathbb{N}, S : \mathbb{N} \to \mathbb{N}, 0 \in \mathbb{N})$ *vérifie les propriétés suivantes :*

1. $1 = S(0) \neq 0$.
2. *(Principe de récurrence) Pour toute partie* [1] $P \subset \mathbb{N}$*, si* $0 \in P$ *et si pour tout* $n \in P$*, on a l'implication* $[n \in P \Rightarrow S(n) = n + 1 \in P]$*, alors* $P = \mathbb{N}$.
3. *(Principe de récurrence forte) Pour toute partie* $P \subset \mathbb{N}$*, si* $0 \in P$ *et si pour tout* $n \in P$*, on a l'implication* $[\forall k \in \{0, \ldots, n\},\ k \in P \Rightarrow S(n) = n + 1 \in P]$ *alors* $P = \mathbb{N}$.
4. S *est injective.*

Démonstration. On va appliquer la propriété universelle de $(\mathbb{N}, S, 0)$ avec des (X, T, x) convenables pour obtenir les résultats recherchés.

1. Supposons $S(0) = 0$. On applique la propriété universelle de $\mathbb{N}$ au triplet donné par $X = \{0, 1\}$, $T(0) = T(1) = 1$ et $x = 0$. Ceci donne une unique application $f : \mathbb{N} \to \{0, 1\}$ telle que $f(0) = 0$ et $f \circ S = T \circ f$. On obtient donc

$$0 = f(0) = f(S(0)) = T(f(0)) = T(0) = 1,$$

ce qui donne une contradiction. On a obtenu $S(0) \neq 0$.

1. Rappelons que la donnée d'une telle partie est équivalente à la donnée d'une propriété $P : \mathbb{N} \to \{\text{vrai}, \text{faux}\}$. Cette correspondance entre sous-ensembles et propriétés permet de traduire le principe de récurrence en termes de propriétés.

2. On dispose déjà d'une application injective $i : A \to \mathbb{N}$ donnée par l'inclusion $A \subset \mathbb{N}$. On va montrer qu'elle est aussi surjective en lui définissant un inverse à droite $s : \mathbb{N} \to A$. Comme $0 \in A$ et $n \in A \Rightarrow S(n) \in A$, on peut définir $S : A \to A$, et il existe une unique application $s : \mathbb{N} \to A$ telle que $s(0) = 0$ et $s(Sn) = Sn$. L'application $i \circ s : \mathbb{N} \to \mathbb{N}$ envoie 0 sur 0 et Sn sur Sn, donc est égale à l'identité, par unicité dans la propriété universelle de $\mathbb{N}$. On a ainsi montré que $A = \mathbb{N}$.

3. On va traduire le principe de récurrence sur les parties en termes équivalents de propriétés sur les entiers. Soit $P : \mathbb{N} \to \{\text{vrai}, \text{faux}\}$ une propriété vérifiant que $P(0)$ est vraie et que l'implication
$$[\forall k \in \{0, \dots, n\}, P(k) \Rightarrow P(n+1)]$$
est aussi vraie. On note $Q(n)$ la proposition $[\forall k \in \{0, \dots, n\},\ P(k)]$. Alors, on a $Q(0) = P(0)$ vraie et $[Q(n) \Rightarrow Q(n+1)]$ pour tout n, grâce à l'hypothèse. Ceci permet de conclure que $Q(n)$ est vraie pour tout n par récurrence classique, et on en déduit que $P(n)$ est aussi vraie pour tout n.

4. On va montrer que S est injective en définissant une fonction prédécesseur $P : \mathbb{N} \to \mathbb{N}$, inverse à droite de S. On définit P à partir d'une fonction $G : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ dont l'image est son graphe, donnée moralement par $G(0) = (0, 0)$ et $G(Sn) = (Sn, n)$. Pour être plus précis, on peut utiliser la propriété universelle de $\mathbb{N}$ pour définir G : on pose $X = \mathbb{N} \times \mathbb{N}$ et on se donne $T : X \to X$ par $T(n, m) = (Sn, n)$ et on fixe $x = (0, 0) \in X$. Ceci donne une unique application $G : \mathbb{N} \to X$ telle que
$$G(Sn) = T(G(n))$$
pour tout $n \in \mathbb{N}$ et $G(0) = (0, 0)$. Montrons par récurrence que $G(Sn) = (Sn, n)$ pour tout $n \in \mathbb{N}$. Ceci est vrai pour $n = 0$ car $G(S0) = T(G(0)) = T(0, 0) = (S0, 0)$. Supposons cette propriété $G(Sn) = (Sn, n)$ vérifiée pour un certain n. Alors, on a
$$G(SSn) = T(G(Sn)) = (SSn, Sn)$$
et le résultat recherché est obtenu par récurrence. On définit alors la fonction prédécesseur par $P = p_2 \circ G$ avec $p_2 : \mathbb{N}^2 \to \mathbb{N}$ la projection sur le second membre, et on a bien $P(0) = 0$ et $P(Sn) = n$ pour tout $n \in \mathbb{N}$, ce qui montre que P est un inverse à droite de S.

□

Nous donnerons ici seulement une preuve partielle du corollaire suivant. On pourra approfondir ludiquement sa démonstration en se référant en ligne au "natural number game" [3].

Corollaire A.2. *On peut munir l'ensemble $\mathbb{N}$ de deux opérations binaires $+$ et $\cdot$ appelées son addition et sa multiplication. Ces opérations sont associatives, avec pour élément neutre respectifs 0 et 1. De plus, la multiplication $\cdot$ est distributive par rapport à l'addition $+$. On peut aussi munir $\mathbb{N}$ d'une relation d'ordre total $\leq$ pour laquelle 0 est le plus petit élément.*

Démonstration. Commençons par définir l'addition. Pour chaque entier n, on doit définir une fonction $S_n : \mathbb{N} \to \mathbb{N}$ d'addition de n, moralement donnée par $S_n(m) = n + m$. Cette opération doit vérifier
$$n + (m + 1) = (n + m) + 1.$$
Pour cela, on pose $X = \mathbb{N}$, $x = n$ et $T = S : \mathbb{N} \to \mathbb{N}$ et on applique la propriété universelle de $\mathbb{N}$ pour définir l'application correspondante $S_n : \mathbb{N} \to \mathbb{N}$. Ceci permet de définir l'opération

d'addition $+ : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ par $n+m = S_n(m)$. Pour chaque entier n, on veut définir la multiplication $M_n : \mathbb{N} \to \mathbb{N}$ par n, moralement donnée par $M_n(m) = n \cdot m$. Cette opération doit vérifier

$$n \cdot (m + 1) = n \cdot m + n.$$

Pour cela, on pose $X = \mathbb{N}$, $x = 0$ et on définit $T_n : \mathbb{N} \to \mathbb{N}$ par $T_n(m) = m + n$. Ceci donne donc $M_n(0) = 0$ et $M_n(Sm) = T_n(M_n(m)) = M_n(m) + n$ qui est l'équation souhaitée. L'ordre est défini par $n \leq m$ si et seulement si il existe $k \in \mathbb{N}$ tel que $m = S_n(k)$. □

Annexe B

Catégories, endomorphismes et isomorphismes

Les structures que vous allez rencontrer en algèbre sont souvent reliées entre elles par des morphismes (applications qui respectent la forme [morphê, en grec], i.e., la structure qu'on s'est donnée), morphismes que l'on peut aussi composer. On formalise une telle situation par la notion de catégorie, qui permet de définir les notions d'endomorphisme et d'isomorphisme pour tous les types de structures rencontrés de manière uniforme. C'est aussi un cadre naturel pour les notions de diagramme commutatif et de propriété universelle, que nous avons rencontrées à plusieurs reprises dans ce cours, et qui jouent un rôle fondamental dans la compréhension des aspects structurels des mathématiques.

L'intérêt principal de la notion de catégorie est son champ d'application : elle pourra aussi être utilisée en troisième année de mathématiques en analyse, avec les différentes catégories d'espaces vectoriels normés et d'espaces métriques de la topologie et du calcul différentiel, d'espaces mesurables de la théorie de l'intégration et des probabilités, ainsi qu'en géométrie (on peut rappeler qu'historiquement, les constructions de la topologie algébrique sont à l'origine de l'introduction de la théorie des catégories). C'est aussi un outil clef en informatique théorique (théorie des types).

Pour rendre ce formalisme vraiment utile, il faut définir les morphismes de catégories, appelés les foncteurs, et les morphismes de foncteurs, appelés les transformations naturelles. Nous n'irons pas jusque là dans cet appendice mais invitons les lecteurices intéressé.e.s à entamer une discussion sur le sujet "à quoi servent les catégories" avec leur grand modèle de language préféré.

Définition B.1. *Une catégorie $\mathcal{C}$ est la donnée :*

1. *d'une collection* $\mathrm{Ob}(\mathcal{C})$*, appelée la collection des objets de* $\mathcal{C}$*,*
2. *pour chaque paire* (X, Y) *d'objets de* $\mathcal{C}$ *d'un ensemble* $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ *appelé ensemble des morphismes entre* X *et* Y *et dont les éléments sont notés* $f : X \to Y$ *ou* $X \xrightarrow{f} Y$*,*
3. *pour chaque objet* X *de* $\mathcal{C}$*, d'un morphisme identique* $\mathrm{id}_X : X \to X$*,*
4. *pour chaque triplet* (X, Y, Z) *d'objets de* $\mathcal{C}$ *d'une application*

$$\circ : \mathrm{Hom}_{\mathcal{C}}(X, Y) \times \mathrm{Hom}_{\mathcal{C}}(Y, Z) \to \mathrm{Hom}_{\mathcal{C}}(X, Z)$$

appelée composition des morphismes qui envoie (f, g) *sur* $g \circ f$*,*

vérifiant les deux axiomes suivant :

1. *La composition des morphismes est associative, au sens ou*

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

dès que cela fait sens, i.e., pour tous (f, g, h) composables :

$$X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} T.$$

2. *Les morphismes identiques sont des unités à gauche et à droite pour cette composition, au sens ou*
$$f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f.$$
pour tout X et Y et tout $f : X \to Y$.

Exemple B.2. *Commençons par illustrer cette notion par plusieurs exemples tirés de ce cours. On démontre que chacun de ces exemples forme bien une catégorie en utilisant la Proposition 1.2, qui permet de traiter le cas des applications entre ensembles, et en montrant que la composée de deux morphismes est un morphisme et que l'application identique définit aussi un morphisme.*

1. *La catégorie* Ens *des ensembles a été définie dans la Section 1.1. Elle a pour objets la collection* Ob(Ens) *de tous les ensembles et pour morphismes $f : X \to Y$ les applications. Il découle directement de la Proposition 1.2 que ceci définit bien une catégorie. On notera aussi $Y^X = \mathrm{Hom}_{\mathrm{Ens}}(X, Y)$ l'ensemble des applications $f : X \to Y$ et si $X = \{1, \ldots, n\}$, on écrit $Y^X = Y^n$.*
2. *La catégorie* Rel *des relations binaires a été définie dans la Section 1.4. Elle a pour objets la collection* Ob(Rel) *des paires (X, R) formé d'un ensemble et d'une relation binaire, et pour morphismes $f : (X, R) \to (Y, S)$ les morphismes de relations.*
3. *Les catégories* Mon *et* Grp *des monoïdes et des groupes ont été définies dans la Section 1.3. La catégorie* Mon *des monoïdes (resp. des groupes) a pour objets la collection* Ob(Mon) *des monoïdes (resp. la collection* Ob(Grp) *des groupes) et pour morphismes $f : M \to N$ les morphismes de monoïdes.*
4. *Les catégories* Anneaux *et* Corps *des anneaux et corps ont aussi été définies dans la Section 1.3.*
5. *La catégorie Alg_A des algèbres sur un anneau commutatif A a été définie dans la Section 2.1.*
6. *La catégorie Vect_K des espaces vectoriels sur un corps commutatif K a été définie dans la Section 3.1.*

L'objet principal de cette section est d'arriver à formuler la définition suivante dans un cadre suffisamment général pour qu'il s'applique a tous les types de structures rencontrées en licence de mathématiques.

Définition B.3. *On se fixe une catégorie $\mathcal{C}$.*

1. *Un morphisme $f : X \to X$ est appelé un endomorphisme de X.*
2. *Un morphisme $f : X \to Y$ est un isomorphisme s'il admet un inverse à gauche et à droite, i.e., si il existe $g : Y \to X$ tel que*
$$g \circ f = \mathrm{id}_X \ \text{ et } \ f \circ g = \mathrm{id}_Y.$$
On notera parfois un isomorphisme par $f : X \xrightarrow{\sim} Y$. L'inverse g d'un isomorphisme f est noté f^{-1}.
3. *Un isomorphisme qui est aussi un endomorphisme $f : X \to X$ est appelé un automorphisme de X.*

On note $\mathrm{End}_{\mathcal{C}}(X) = \mathrm{Hom}_{\mathcal{C}}(X, X)$ *l'ensemble des endomorphismes de* X *et* $\mathrm{Aut}_{\mathcal{C}}(X) \subset \mathrm{End}_{\mathcal{C}}(X)$ *l'ensemble de ses automorphismes.*

Remarque B.4. *On montre facilement que l'inverse d'un isomorphisme est unique, ce qui justifie la notation* f^{-1} *pour cet inverse. En effet, si* g_1 *et* g_2 *sont deux inverses, l'associativité de la composition et la propriété d'unité des identités donnent*

$$g_1 = g_1 \circ \mathrm{id}_Y = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = \mathrm{id}_X \circ g_2 = g_2.$$

Remarque B.5. *On a démontré dans la Proposition 1.5 que les isomorphismes d'ensembles sont les bijections. On étudiera en exercice les isomorphismes de monoïdes, de groupes et d'anneaux.*

Remarque B.6. *On remarque une similitude qui n'est pas fortuite entre les axiomes d'associativité et d'unitalité des monoïdes et des catégories. Nous allons maintenant la préciser.*

1. *Soit* $\mathcal{C}$ *une catégorie et* X *est un object de* $\mathcal{C}$*. L'ensemble* $\mathrm{End}_{\mathcal{C}}(X)$ *de ses endomorphismes est muni d'une structure de monoïde pour l'opération* $\circ$ *de composition des morphismes, dont l'unité est le morphisme identique* id_X*. Le sous-ensemble* $\mathrm{Aut}_{\mathcal{C}}(X) \subset \mathrm{End}_{\mathcal{C}}(X)$ *est le groupe des inversibles de ce monoïde.*
2. *Inversement, si* $(M, *, e)$ *un monoïde, on peut lui associer une catégorie* BM *définie de la manière suivante : on pose* $\mathrm{Ob}(BM) = \{e\}$ *et* $\mathrm{Hom}_{BM}(e, e) = M$*. La loi de composition des morphismes est donnée par* $*$ *et l'identité par* $\mathrm{id}_e = e$*. L'associativité et l'unitalité du monoïde nous garantissent que* BM *forme bien une catégorie. On a de plus* $\mathrm{End}_{BM}(e) = M$ *et* $\mathrm{Aut}_{BM}(e) = M^{\times}$*.*

Remarque B.7. *Il existe aussi un lien, un peu moins évident, entre les axiomes des catégories et ceux des relations binaires. Plus précisément, on peut aussi encoder les relations binaires réflexives et transitives de la Section 1.4 (et en particulier, les relations d'équivalence et les relations d'ordre) dans des catégories particulières. Soit* X *un ensemble et* $R \subset X \times X$ *une relation réflexive et transitive. On peut lui associer une catégorie* BR *définie de la manière suivante : on pose* $\mathrm{Ob}(BR) = X$ *et pour* $(x, y) \in X$*, on pose*

$$\mathrm{Hom}_{BR}(x, y) = R \cap \{(x, y)\} \subset X \times X.$$

Cet ensemble vaut $\{(x, y)\}$ *si* $(x, y) \in R$ *(i.e., si* xRy*) et est vide sinon. La réflexivité de* R *permet de définir les morphismes identiques : si* $x \in X$*, on a* xRx*, ce qui permet de poser* $\mathrm{id}_x = (x, x)$*. La transitivité permet de définir la composition des morphismes : si on a un morphisme entre* x *et* y *et un morphisme entre* y *et* z*, cela signifie que* xRy *et* yRz*, ce qui implique* xRz *et définit donc un morphisme de* x *vers* z *donné par* $(x, z) \in R$*. On retrouve* R *à partir de* BR *en prenant l'ensemble de tous les morphismes.*

Annexe C

Formes hermitiennes, espaces hilbertiens et groupes unitaires U(n)

Résumé : Ce chapitre est l'analogue du Chapitre sur les formes bilinéaires symétriques quand on remplace le corps $\mathbb{R}$ par $\mathbb{C}$. De façon simplifiée : « on remplace le carré x^2 d'un nombre réel par le module au carré $|z|^2 = z\bar{z}$ d'un nombre complexe ». Ceci conduit à la notion de *forme hermitienne* (analogue de la notion de forme bilinéaire symétrique), puis de *produit scalaire hilbertien* sur $\mathbb{C}^n$ (analogue du produit scalaire euclidien sur $\mathbb{R}^n$). On introduit alors le groupe U(n) des isométries de l'espace hilbertien $\mathbb{C}^n$, puis la notion d'endomorphisme *auto-adjoint* et, plus généralement, d'endomorphisme *normal*. Un des avantages de se placer sur le corps $\mathbb{C}$ est l'existence de valeurs propres et vecteurs propres ; on obtient ainsi les importants théorèmes de diagonalisation C.36 et C.37.

On a indiqué par des symboles  les définitions, exemples et résultats fondamentaux. Par ailleurs, des *compléments de cours*, pour les étudiants intéressés, sont donnés dans un appendice à la fin du chapitre (on y esquisse brièvement l'utilisation des « espaces de Hilbert » (de dimension infinie) en Analyse). Ces passages n'interviendront pas dans les évaluations.

C.0 Rappels sur les nombres complexes

Dans tout ce chapitre, le corps de base est $\mathbb{C}$. On note i une racine carrée de -1, choisie une fois pour toutes. On rappelle les points suivants.

Définition C.1 (Parties réelle et imaginaire, conjugaison complexe, module et argument)**.**

1. *Tout $z \in \mathbb{C}$ s'écrit de façon unique $z = a + ib$, avec $a, b \in \mathbb{R}$; a s'appelle la* partie réelle *de z et se note* $\mathrm{Re}(z)$*, b s'appelle la* partie imaginaire *de z et se note* $\mathrm{Im}(z)$*. Remarquons que, comme $-iz = b - ia$, on a* $\boxed{\mathrm{Re}(-iz) = \mathrm{Im}(z)}$ *et* $\boxed{\mathrm{Im}(iz) = \mathrm{Re}(z).}$
2. *La* conjugaison complexe *est l'application qui à tout $z = a + ib$ associe $\bar{z} = a - ib$. Remarquons que :* $\boxed{z + \bar{z} = 2\mathrm{Re}(z),}$ $\boxed{z - \bar{z} = 2i\mathrm{Im}(z)}$ *et* $\boxed{z = \bar{z} \Leftrightarrow z \in \mathbb{R}}$ *D'autre part, on a* $\boxed{z + \bar{z'} = \bar{z} + \bar{z'}}$ *et* $\boxed{z\bar{z'} = \bar{z}\,\bar{z'}.}$
3. *Si $z = a + ib$, on a $z\bar{z} = a^2 + b^2$ et $|z| = \sqrt{z\bar{z}}$ s'appelle le* module *(ou la* norme*) de z. D'après la dernière égalité ci-dessus, la norme est* multiplicative, i.e. *on a* $\boxed{|z_1 z_2| = |z_1| \cdot |z_2|.}$
4. *Enfin, si $z \neq 0$, alors $z/|z|$ est de module 1, donc de la forme $e^{i\theta}$, avec $\theta \in \mathbb{R}/2\pi\mathbb{Z}$ (*cf. *Chap. 5, Appendice* **??***). Donc tout $z \neq 0$ s'écrit de façon unique :*

$$\boxed{z = \rho e^{i\theta}, \quad \text{avec } \rho = |z| \in \mathbb{R}_+^* \text{ et } \theta \in \mathbb{R} \text{ défini modulo } 2\pi\mathbb{Z}}$$

(par exemple, on peut prendre θ dans $[0, 2\pi[$ ou bien dans $]-\pi, \pi]$); on dit que θ est l'argument *de z.*

C.1 Formes hermitiennes

Exemple C.2. *Le carré de la norme d'un nombre complexe z est la valeur en $x = y = z$ de la fonction de deux variables $\varphi(x, y) = x\,\bar{y}$. Cette fonction $\varphi : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ est linéaire en la 1ère variable :*

$$\varphi(\lambda x + \mu x', y) = (\lambda x + \mu x')\,\bar{y} = \lambda x\,\bar{y} + \mu x'\,\bar{y} = \lambda\varphi(x, y) + \mu\varphi(x', y)$$

mais pas tout-à-fait linéaire en la 2ème variable, puisqu'on a :

$$\varphi(x, \lambda y + \mu y') = x\,\overline{\lambda y + \mu y'} = x\,\bar{\lambda}\bar{y} + x\,\bar{\mu}\bar{y'} = \bar{\lambda}\varphi(x, y) + \bar{\mu}\varphi(x', y).$$

D'autre part, on a $\varphi(y, x) = y\,\bar{x} = x\bar{\bar{y}} = \varphi(\bar{x}, y)$. Ceci conduit aux définitions suivantes.

Définition C.3 (Applications semi-linéaires)**.** *Soient E, F deux $\mathbb{C}$-espaces vectoriels. Une application $f : E \to F$ est dite* **semi-linéaire** *si elle vérifie :*

$$\forall u, v \in E, \quad \forall z \in \mathbb{C}, \qquad \boxed{f(u + v) = f(u) + f(v)} \qquad \boxed{f(zu) = \bar{z} f(u).}$$

Ces deux conditions équivalent bien sûr à la condition : $\boxed{f(zu + v) = \bar{z} f(u) + f(v).}$

Définition C.4 (Formes hermitiennes)**.** *Soit E un $\mathbb{C}$-espace vectoriel.*

1. *Une* **forme hermitienne** *sur E est une application $\varphi : E \times E \to \mathbb{C}$ qui vérifie les deux conditions suivantes :*
   (a) *φ est linéaire en la 1ère variable et semi-linéaire en la 2ème variable,* i.e. *:*

$$\forall x, x', y, y' \in E, \quad \forall \lambda \in \mathbb{C}, \qquad \begin{cases} \varphi(\lambda x + x', y) = \lambda\varphi(x, y) + \varphi(x', y), \\ \varphi(x, \lambda y + y') = \bar{\lambda}\varphi(x, y) + \varphi(x, y') \end{cases}$$

   (b) *φ a la propriété de «* symétrie hermitienne *» ci-dessous :*

$$(*) \qquad \forall x, y \in E, \qquad \varphi(y, x) = \varphi(\bar{x}, y).$$

2. *Observons que, pour tout $x \in E$, $(*)$ entraîne $\varphi(x, x) = \varphi(\bar{x}, x)$ d'où* $\boxed{\varphi(x, x) \in \mathbb{R}.}$
3. *On note* $\boxed{\mathcal{H}(E)}$ *l'ensemble des formes hermitiennes sur E ; si $\varphi, \psi \in \mathcal{H}(E)$ et $s, t \in \mathbb{R}$, on voit facilement que l'application $s\varphi + t\psi : E \times E \to \mathbb{C}$ définie par $(s\varphi + t\psi)(u, v) = s\varphi(u, v) + t\psi(u, v)$ est encore une forme hermitienne. Par conséquent, $\mathcal{H}(E)$ est un* $\boxed{\mathbb{R}\text{-espace vectoriel}}$ *(mais* **pas** *un $\mathbb{C}$-espace vectoriel, car si $\lambda \in \mathbb{C} - \mathbb{R}$, alors $\lambda\varphi$ ne vérifie plus $(*)$).*
4. *Remarquons enfin que, pour vérifier qu'une application $\varphi : E \times E \to \mathbb{C}$ est une forme hermitienne, il suffit de voir que φ vérifie $(*)$ et est linéaire en la 1ère variable ; ces deux conditions impliquent en effet la semi-linéarité en la 2ème variable, car :*

$$\varphi(x, \lambda y + y') = \varphi(\overline{\lambda y + y'}, x) = \bar{\lambda}\varphi(y, x) + \varphi(y', x) = \bar{\lambda}\,\varphi(\bar{y}, x) + \varphi(\bar{y'}, x) = \bar{\lambda}\,\varphi(x, y) + \varphi(x, y').$$

Remarque C.5. *La notion de forme hermitienne sur un $\mathbb{C}$-espace vectoriel est une « variante » de la notion de forme bilinéaire sur un $\mathbb{R}$-espace vectoriel.*

Définition C.6 (Formes quadratiques hermitiennes)**.** *Soit φ une forme hermitienne sur un $\mathbb{C}$-espace vectoriel E. On dit que l'application $Q : E \to \mathbb{R}$, $x \mapsto \varphi(x,x)$ est une* **forme quadratique hermitienne** *sur E. D'après le lemme qui suit, φ est entièrement déterminée par Q, et l'on dit que φ est la* **forme polaire** *de Q. Notons aussi que pour tout $\lambda \in \mathbb{C}$, on a*

$$Q(\lambda x) = \varphi(\lambda x, \lambda x) = \lambda\bar{\lambda}\varphi(x,x) = \lambda\bar{\lambda}Q(x) = |\lambda|^2\, Q(x).$$

Lemme C.7 (Polarisation)**.** *Soient E un $\mathbb{C}$-espace vectoriel, $\varphi \in \mathcal{H}(E)$ et Q l'application $E \to \mathbb{R}$, $x \mapsto \varphi(x,x)$. Alors, pour tout $x, y \in E$, on a :*

$$\mathrm{Re}(\varphi(x,y)) = \frac{1}{2}(Q(x+y) - Q(x) - Q(y)) = \frac{1}{4}(Q(x+y) - Q(x-y)) \tag{1}$$

$$\mathrm{Im}(\varphi(x,y)) = \frac{1}{2}(Q(x+iy) - Q(x) - Q(y)) = \frac{1}{4}(Q(x+iy) - Q(x-iy)) \tag{2}$$

$$4\varphi(x,y) = Q(x+y) - Q(x-y) + iQ(x+iy) - iQ(x-iy). \tag{3}$$

Démonstration. On a

$$Q(x+y) = \varphi(x+y, x+y) = Q(x) + Q(y) + \varphi(x,y) + \varphi(y,x)$$
$$Q(x-y) = \varphi(x-y, x-y) = Q(x) + Q(y) - \varphi(x,y) - \varphi(y,x)$$

et comme $\varphi(x,y) + \varphi(y,x) = \varphi(x,y) + \varphi(\bar{x},y) = 2\mathrm{Re}(\varphi(x,y))$, on obtient (1). Comme $\mathrm{Im}(z) = \mathrm{Re}(-iz)$ pour tout $z \in \mathbb{C}$, on obtient

$$\mathrm{Im}(\varphi(x,y)) = \mathrm{Re}(-i\varphi(x,y)) = \mathrm{Re}(\varphi(x,iy))$$

et donc (2) s'obtient en remplaçant y par iy dans (1) et en utilisant que $Q(iy) = |i|^2\, Q(y) = Q(y)$. Enfin, (3) découle de (1) et (2). □

Désormais, on suppose E de dimension finie n.

Définition C.8 (Matrices hermitiennes)**.** *Une matrice $A \in M_n(\mathbb{C})$ est* **hermitienne** *si $\boxed{{}^tA = \bar{A}.}$ On note $\mathrm{MH}_n(\mathbb{C})$ l'ensemble de ces matrices, si $A, B \in \mathrm{MH}_n(\mathbb{C})$ et $s, t \in \mathbb{R}$, alors $sA + tB \in \mathrm{MH}_n(\mathbb{C})$, donc $\mathrm{MH}_n(\mathbb{C})$ est un $\mathbb{R}$-espace vectoriel (mais pas un $\mathbb{C}$-espace vectoriel). Observons que si $A \in \mathrm{MH}_n(\mathbb{C})$, ses coefficients diagonaux a_{ii} vérifient $a_{ii} = \bar{a_{ii}}$ donc $\boxed{a_{ii} \in \mathbb{R}.}$*

Remarque C.9. *On a $\boxed{\dim_{\mathbb{R}} \mathrm{MH}_n(\mathbb{C}) = n^2.}$ En effet, notons N le nombre de coefficients qui sont strictement au-dessus de la diagonale. C'est aussi le nombre de coefficients qui sont strictement en-dessous de la diagonale, et il y a n coefficients diagonaux. Donc $2N + n = n^2$, d'où $\boxed{2N = n^2 - n = n(n-1).}$ Puis, une matrice hermitienne est déterminée par le choix de n coefficients réels sur la diagonale et de N coefficients complexes au-dessus (ceux en-dessous en étant les conjugués), pour chaque coefficient complexe, il faut choisir sa partie réelle et sa partie imaginaire, d'où au total $n + 2N = n^2$ coefficients réels.*

Théorème/Définition C.10 (Matrice d'une forme hermitienne et changement de base)**.** *Soit φ une forme hermitienne sur un $\mathbb{C}$-espace vectoriel E de dimension n et soit $\mathfrak{B} = (e_1, \ldots, e_n)$ une base de E.*

1. *La matrice $\mathrm{Mat}_{\mathfrak{B}}(\varphi)$ de φ dans la base $\mathfrak{B}$ est la matrice $A = (a_{ij})_{i,j=1}^n \in M_n(\mathbb{C})$, où $a_{ij} = \varphi(e_i, e_j)$. Comme $\varphi(e_j, e_i) = \varphi(\bar{e_i}, e_j)$, on a $a_{ji} = \bar{a_{ij}}$, donc ${}^tA = \bar{A}$,* i.e. *$A \in \mathrm{MH}_n(\mathbb{C})$.*

2. *φ est entièrement déterminée par sa matrice A : en effet, d'après la linéarité (resp. semi-linéarité) en la* 1*ère (resp.* 2*ème) variable, on a l'égalité :*

$$(*) \qquad \forall \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbb{C}^n, \qquad \varphi\left(\sum_{i=1}^n x_i e_i, \sum_{j=1}^n y_j e_j\right) = \sum_{i,j=1}^n x_i \bar{y_j}\, \varphi(e_i, e_j) = \sum_{i,j=1}^n a_{ij}\, x_i \bar{y_j}.$$

Donc, si l'on note X, Y les vecteurs colonnes ci-dessus, on a la formule matricielle $\boxed{\varphi(X, Y) = {}^t X\, A\, \bar{Y}.}$

3. *Réciproquement, pour tout $A = (a_{ij})_{i,j=1}^n \in \mathrm{MH}_n(\mathbb{C})$, l'application $\varphi_A : E \times E \to \mathbb{C}$ définie par $\varphi_A(\sum_{i=1}^n x_i e_i, \sum_{j=1}^n y_j e_j) = \sum_{i,j=1}^n a_{ij}\, x_i \bar{y_j}$ est une forme hermitienne sur E, et* $\mathrm{Mat}_{\mathfrak{B}}(\varphi_A) = A$. *Donc,* se donner une forme hermitienne sur E « est la même chose » que se donner une matrice hermitienne *: de façon précise, l'application $\mu_{\mathfrak{B}} : \mathcal{H}(E) \to \mathrm{MH}_n(\mathbb{C})$, $\varphi \mapsto \mathrm{Mat}_{\mathfrak{B}}(\varphi)$ est un isomorphisme de $\mathbb{R}$-espaces vectoriels.*

4. *Soient $\mathfrak{B}'$ une autre base de E et P la matrice de passage* $\mathrm{Mat}_{\mathfrak{B}}(\mathfrak{B}')$. *Alors*

$$(**) \qquad \boxed{A' = \mathrm{Mat}_{\mathfrak{B}'}(\varphi) = {}^t P\, A\, \bar{P}.}$$

Démonstration. (2) Comme φ est linéaire (resp. semi-linéaire) en la 1ère (resp. 2ème) variable, on a bien l'égalité $(*)$, qui montre que φ est déterminée par sa matrice, donc que l'application $\mu_{\mathfrak{B}} : \mathcal{H}(E) \to \mathrm{MH}_n(\mathbb{C})$, $\varphi \mapsto \mathrm{Mat}_{\mathfrak{B}}(\varphi)$ est *injective*. D'autre part, on voit que le scalaire $\sum_{i,j=1}^n a_{ij}\, x_i \bar{y_j} \in \mathbb{C}$ est égal au produit matriciel

$${}^t X\, A\, \bar{Y} = (x_1, \ldots, x_n) A \begin{pmatrix} \bar{y_1} \\ \vdots \\ \bar{y_n} \end{pmatrix}.$$

Ceci prouve (2). Avant de prouver (3), remarquons déjà que l'application $\mu_{\mathfrak{B}}$ est $\mathbb{R}$-*linéaire*. En effet, si $\varphi, \psi \in \mathcal{H}(E)$ et $s \in \mathbb{R}$, alors $s\varphi + \psi$ est la forme hermitienne définie par $(s\varphi + \psi)(u, v) = s\varphi(u, v) + \psi(u, v)$ pour *tout* $u, v \in E$, donc *a fortiori* on a $(s\varphi + \psi)(e_i, e_j) = s\varphi(e_i, e_j) + \psi(e_i, e_j)$ pour tout i, j, d'où $\mu_{\mathfrak{B}}(s\varphi + \psi) = s\,\mu_{\mathfrak{B}}(\varphi) + \mu_{\mathfrak{B}}(\psi)$.

Prouvons (3). Pour tout $A = (a_{ij})_{i,j=1}^n \in \mathrm{MH}_n(\mathbb{C})$, l'application $\varphi_A : E \times E \to \mathbb{C}$ définie par

$$\varphi_A\left(\sum_{i=1}^n x_i e_i, \sum_{j=1}^n y_j e_j\right) = \sum_{i,j=1}^n a_{ij}\, x_i \bar{y_j}$$

est linéaire en les x_i, et vérifie :

$$\varphi_A(y, x) = \varphi_A\left(\sum_{j=1}^n y_j e_j, \sum_{i=1}^n x_i e_i\right) = \sum_{i,j=1}^n \underbrace{a_{ji}}_{=\bar{a_{ij}}}\, y_j \bar{x_i} = \sum_{i,j=1}^n a_{ij}\, \bar{x_i}\, \bar{y_j} = \varphi_A(\bar{x}, y)$$

donc est une forme hermitienne sur E ; de plus, prenant $x_{i_0} = 1 = y_{j_0}$ et $x_i = 0 = y_j$ pour $i \neq i_0$ et $j \neq j_0$, on obtient que $\varphi_A(e_{i_0}, e_{j_0}) = a_{i_0, j_0}$ pour tout $i_0, j_0 = 1, \ldots, n$, d'où $\mathrm{Mat}_{\mathfrak{B}}(\varphi_A) = A$. Ceci montre que l'application $\mathbb{R}$-linéaire injective $\mu_{\mathfrak{B}} : \mathcal{H}(E) \to \mathrm{MH}_n(\mathbb{C})$, $\varphi \mapsto \mathrm{Mat}_{\mathfrak{B}}(\varphi)$ est aussi *surjective*, donc c'est un isomorphisme de $\mathbb{R}$-espaces vectoriels. En particulier, *se donner une forme hermitienne sur E « est la même chose » que se donner une matrice hermitienne*.

Enfin, démontrons (4). Soient $x, y \in E$, ils correspondent dans la base $\mathfrak{B}$ (resp. $\mathfrak{B}'$) à des vecteurs colonnes X, Y (resp. X', Y'). D'après la formule de changement de coordonnées, on a $X = PX'$ et $Y = PY'$, d'où ${}^tX = {}^tX'\,{}^tP$ et $\bar{Y} = \bar{P}\,\bar{Y}'$, et donc :

$$\varphi(x,y) = {}^tX\,A\,\bar{Y} = {}^tX'\,{}^tPA\bar{P}\,\bar{Y}'$$

ce qui entraîne $A' = {}^tP\,A\,\bar{P}$. Le théorème est démontré. □

Définition C.11 (Carrés de modules et « doubles produits »)**.** *En séparant, d'une part, les termes $x_i\,\bar{y}_i$ et, d'autre part, les termes $x_i\,\bar{y}_j$ avec $i \neq j$, la formule $(*)$ de C.10 se récrit de la façon suivante (puisque $a_{ji} = \bar{a_{ij}}$ pour tout $i \neq j$) :*

$$(*') \qquad \forall \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in k^n, \qquad \varphi\left(\sum_{i=1}^n x_i e_i, \sum_{j=1}^n y_j e_j\right) = \sum_{i=1}^n a_{ii}\,x_i\,\bar{y}_i + \sum_{1\leq i<j\leq n} (a_{ij}\,x_i\,\bar{y}_j + \bar{a_{ij}}\,x_j\,\bar{y}_i).$$

*En particulier, prenant $Y = X$ (*i.e. *$y_i = x_i$ pour tout i), on voit que la forme quadratique hermitienne Q associée à φ est donnée par la formule suivante (noter que $x_i\,\bar{x}_i = |x_i|^2$) :*

$$(*') \quad Q(x_1,\ldots,x_n) = \sum_{i=1}^n a_{ii}\,|x_i|^2 + \sum_{1\leq i<j\leq n} (a_{ij}\,x_i\,\bar{x}_j + \bar{a_{ij}}\,\bar{x}_i\,x_j) = \sum_{i=1}^n a_{ii}\,|x_i|^2 + \sum_{1\leq i<j\leq n} 2\mathrm{Re}(a_{ij}\,x_i\,\bar{x}_j).$$

On voit donc apparaître les carrés des modules *des x_i, et les parties réelles des doubles produits $x_i\,\bar{x}_j$. Pour abréger, on parlera de « carrés de modules » et de « doubles produits ».*

Proposition/Définition C.1 (Rang d'une forme hermitienne)**.** *Soit φ une forme hermitienne sur un $\mathbb{C}$-espace vectoriel E de dimension n et soit $\mathfrak{B} = (e_1,\ldots,e_n)$ une base de E.*

1. *On définit le* **rang** *de φ par* $\mathrm{rang}(\varphi) = \mathrm{rang}(A)$*, où $A = \mathrm{Mat}_{\mathfrak{B}}(\varphi)$; ceci ne dépend pas du choix de la base $\mathfrak{B}$.*
2. *On dit que φ est* **non-dégénérée** *si* $\mathrm{rang}(\varphi) = \dim E$, i.e. *si sa matrice dans une (et donc dans* toute*) base de E est inversible.*

Démonstration. Soient $\mathfrak{B}'$ une autre base de E et $P = \mathrm{Mat}_{\mathfrak{B}}(\mathfrak{B}')$. Comme ${}^tP$ et $\bar{P}$ sont inversibles (on a $({}^tP)^{-1} = {}^t(P^{-1})$ et $(\bar{P})^{-1} = \bar{P^{-1}}$), alors la matrice $A' = \mathrm{Mat}_{\mathfrak{B}'}(\varphi) = {}^tPA\bar{P}$ a même rang que A. □

Proposition/Définition C.2 (Orthogonalité)**.** *Soit φ une forme hermitienne sur un $\mathbb{C}$-espace vectoriel E.*

1. *On dit que deux vecteurs $x, y \in E$ sont* **orthogonaux** *(pour φ) si $\varphi(x,y) = 0$; ceci équivaut à dire que $\varphi(y,x) = 0$ (puisque $\varphi(y,x) = \overline{\varphi(x,y)}$ et vice-versa). Plus généralement, on dit que deux sous-ensembles X, Y de E sont orthogonaux si l'on a $\varphi(x,y) = 0$ pour tout $x \in X$ et $y \in Y$. On notera $X \perp Y$ pour signifier que X et Y sont orthogonaux.*
2. *Pour tout sous-ensemble Y de E, on définit son orthogonal (relativement à φ), noté $Y^{\perp\varphi}$ ou simplement $Y^\perp$, par :*

   $(\star)$ $$\boxed{Y^\perp = \{x \in E \mid \varphi(x,y) = 0, \quad \forall y \in Y\}}$$

   c'est un **sous-espace vectoriel** *de E (même si Y n'en est pas un); de plus, on a les propriétés suivantes :*

   $(\star\star)$ $$\boxed{Y \subseteq Z \Rightarrow Z^\perp \subseteq Y^\perp} \qquad \boxed{Y^\perp = \mathrm{Vect}(Y)^\perp}$$

en particulier, si Y est un sous-espace vectoriel F de E et si $(f_1, \dots, f_p)$ est une famille génératrice de F, alors

$$\boxed{F^\perp = \{f_1, \dots, f_p\}^\perp = \{x \in E \mid \varphi(x, f_i) = 0, \quad \forall i = 1, \dots, p\}.}$$

3. *On pose* $\boxed{N(\varphi) = E^\perp = \{x \in E \mid \varphi(x, y) = 0, \quad \forall y \in Y\}}$ *et on l'appelle le* **noyau** *de φ.*

Démonstration. Soient $x, x' \in Y^\perp$ et $\lambda \in \mathbb{C}$, alors on a, pour tout $y \in Y$, $\varphi(\lambda x + x', y) = \lambda\varphi(x, y) + \varphi(x', y) = 0$, ce qui montre que $\lambda x + x' \in Y^\perp$. Donc $Y^\perp$ est un sous-espace vectoriel de E.

Il est immédiat que si $Y \subseteq Z$, alors $Z^\perp \subseteq Y^\perp$ car si $x \in Z^\perp$ alors x est orthogonal à tout élément de Z, donc x est *a fortiori* orthogonal à tout élément de Y (puisque $Y \subseteq Z$), donc $x \in Y^\perp$.

Comme $Y \subseteq \text{Vect}(Y)$, ceci donne déjà l'inclusion $\text{Vect}(Y)^\perp \subseteq Y^\perp$. Montrons l'inclusion réciproque. Soit $x \in Y^\perp$ et soit v un élément arbitraire de $\text{Vect}(Y)$, par définition, v s'écrit comme une combinaison linéaire finie $v = \lambda_1 y_1 + \cdots + \lambda_r y_r$, avec $y_i \in Y$ et $\lambda_i \in \mathbb{C}$; alors on a

$$\varphi(x, v) = \sum_{i=1}^{r} \bar{\lambda}_i \underbrace{\varphi(x, y_i)}_{=0} = 0$$

et donc $x \in \text{Vect}(Y)^\perp$. Ceci montre l'inclusion $Y^\perp \subseteq \text{Vect}(Y)^\perp$, d'où l'égalité $\text{Vect}(Y)^\perp = Y^\perp$. L'assertion (2) est démontrée. □

Théorème C.12 (Orthogonal d'un sous-espace)**.** *Soit φ une forme hermitienne sur un $\mathbb{C}$-espace vectoriel E de dimension n et soit F un sous-espace vectoriel de E, de dimension r.*

1. *On a* $\boxed{F \subseteq (F^\perp)^\perp}$ *et* $\boxed{\dim F^\perp \geq \dim E - \dim F.}$
2. $\boxed{N(\varphi) = \{0\} \text{ si et seulement si } \varphi \text{ est non-dégénérée.}}$
3. *Si φ est non-dégénérée, on a* $\boxed{\dim F^\perp = \dim E - \dim F}$ *et* $\boxed{F = (F^\perp)^\perp.}$
4. *Si $F \cap F^\perp = \{0\}$, alors* $\boxed{E = F \oplus F^\perp.}$

Démonstration. Soit $f \in F$, pour tout $x \in F^\perp$ on a $\varphi(f, x) = \varphi(\bar{x}, f) = 0$, d'où $f \in (F^\perp)^\perp$. Ceci montre la première assertion de (1). Prouvons la seconde.

Soit $(f_1, \dots, f_r)$ une base de F, complétons-la en une base $\mathfrak{B} = (f_1, \dots, f_n)$ de E, et soit $A = (a_{ij})_{1 \leq i,j \leq n}$ la matrice de φ dans la base $\mathfrak{B}$, *i.e.* $a_{ij} = \varphi(f_i, f_j)$ pour $i, j = 1, \dots, n$.

D'après le point (2) de C.2, $F^\perp$ est formé des vecteurs $v = x_1 f_1 + \cdots + x_n f_n \in E$ tels que $\varphi(v, f_i) = 0$ pour $i = 1, \dots, r$. Comme $\varphi(x_1 f_1 + \cdots + x_n f_n, f_i) = \sum_{j=1}^n x_j \varphi(f_j, f_i) = \sum_{j=1}^n a_{ji} x_j$, ceci équivaut à dire que le vecteur colonne $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ est solution du système linéaire homogène :

$$(\Sigma) \qquad \begin{cases} a_{11} x_1 & + \cdots + & a_{n1} x_n & = 0 \\ \vdots & & \vdots & \vdots \\ a_{1r} x_1 & + \cdots + & a_{nr} x_n & = 0 \end{cases}$$

dont la matrice B est formée des r premières lignes de la matrice ${}^tA$. Comme l'espace des solutions du système est de dimension $n - \text{rang}(B)$, on obtient :

$$\dim F^\perp = n - \text{rang}(B) \geq n - r,$$

ce qui prouve la seconde assertion de (1). De plus, dans le cas particulier où $F = E$, on a $B = {}^tA$ et, comme $\operatorname{rang}({}^tA) = \operatorname{rang}(A)$, on obtient que $\dim E^\perp = n - \operatorname{rang}(A)$. Donc $N(\varphi) = E^\perp$ est nul si et seulement si $\operatorname{rang}(A) = n$. Ceci prouve (2).

Supposons φ non-dégénérée. Alors A est de rang n, *i.e.* ses colonnes sont linéairement indépendantes, en particulier les r premières colonnes le sont, donc la matrice B est de rang r, et donc $\dim F^\perp = n - r$. Remplaçant alors F par $F^\perp$, on obtient l'égalité $\dim(F^\perp)^\perp = n - (n - r) = r$, et par conséquent l'inclusion $F \subseteq (F^\perp)^\perp$ est une égalité. Ceci prouve (3).

Enfin, supposons $F \cap F^\perp = \{0\}$ (sans supposer φ non-dégénérée). Alors F et $F^\perp$ sont en somme directe, et le sous-espace $F \oplus F^\perp$ de E est de dimension $d = r + \dim F^\perp$. D'après (1), on a $d \geq n$, d'où $E = F \oplus F^\perp$ (et $\dim F^\perp = n - r$). Ceci prouve (4). Le théorème est démontré. □

Définition C.13 (Bases orthogonales)**.** *Soit E un $\mathbb{C}$-espace vectoriel de dimension n et soient φ une forme hermitienne sur E, et Q la forme quadratique hermitienne associée. Soit $\mathfrak{B} = (e_1, \ldots, e_n)$ une base de E*

1. *On dit que $\mathfrak{B}$ est une base* **orthogonale** *pour φ (ou pour Q) si l'on $\varphi(e_i, e_j) = 0$ pour $i \neq j$.*
2. *Ceci équivaut à dire que la matrice $A = \operatorname{Mat}_{\mathfrak{B}}(\varphi)$ est* **diagonale***; si l'on note $\lambda_1, \ldots, \lambda_n$ ses coefficients diagonaux (qui sont* **réels***) et $(z_1, \ldots, z_n)$ les coordonnées dans la base $\mathfrak{B}$, ceci équivaut encore à dire que $Q(z_1, \ldots, z_n) = \lambda_1 |z_1|^2 + \cdots + \lambda_n |z_n|^2$.*

Théorème C.14 (de Sylvester dans le cas hermitien)**.** *Soit φ une forme hermitienne sur un $\mathbb{C}$-espace vectoriel E de dimension n, et soit Q la forme quadratique hermitienne associée.*

1. *Il existe une base $\mathfrak{B}$ de E orthogonale pour φ.*
2. *Soient $\mathfrak{B} = (e_1, \ldots, e_n)$ une base orthogonale pour φ et D la matrice diagonale $\operatorname{Mat}_{\mathfrak{B}}(\varphi)$. Quitte à renuméroter les e_i, on peut supposer que les coefficients diagonaux $\lambda_1, \ldots, \lambda_r \in \mathbb{R}$ sont $\neq 0$, et que $\lambda_i = 0$ pour $i > r$. Notons $(z_1, \ldots, z_n)$ les coordonnées dans la base $\mathfrak{B}$, alors :*
   (a) *On a* $\boxed{Q(z_1, \ldots, z_n) = \lambda_1 |z_1|^2 + \cdots + \lambda_r |z_r|^2.}$ $(*)$
   (b) *Soit p (resp. q) le nombre d'indices i tels que $Q(e_i) > 0$ (resp. < 0). Alors p et q ne dépendent pas de la base orthogonale choisie.*
   (c) *Le couple (p, q) s'appelle la* **signature** *de φ; on a $p + q = r = \operatorname{rang}(\varphi)$.*
   (d) *$N(\varphi)$ est le sous-espace $\textsc{Vect}(e_{r+1}, \ldots, e_n)$, donné par les équations $z_1 = 0 = \cdots = z_r$.*
3. *De plus, on peut choisir $\mathfrak{B}$ de sorte que la matrice diagonale $D = \operatorname{Mat}_{\mathfrak{B}}(\varphi)$ ait pour termes diagonaux $(1, \ldots, 1, -1, \ldots, -1, 0, \ldots, 0)$, le nombre de 1 (resp. -1) étant p (resp. q).*

Démonstration. (1) Montrons l'existence d'une base orthogonale en procèdant par récurrence sur $n = \dim E$. Il n'y a rien à montrer si $n = 0$ ou si $\varphi = 0$. On peut donc supposer $n \geq 1$, le résultat établi pour $n - 1$, et $\varphi \neq 0$. Alors, d'après C.7, la forme quadratique hermitienne Q est non nulle, donc il existe $e_1 \in E$ tel que $Q(e_1) \neq 0$. Posons $F = ke_1$, comme $\varphi(e_1, e_1) \neq 0$, alors $F \cap F^\perp = \{0\}$ donc, d'après le théorème C.12, on a

$$E = F \oplus F^\perp.$$

Par hypothèse de récurrence, il existe une base $(e_2, \ldots, e_n)$ de $F^\perp$ telle que $\varphi(e_i, e_j) = 0$ pour $i \neq j$. Alors $(e_1, e_2, \ldots, e_n)$ est une base de E orthogonale pour φ. Ceci prouve l'assertion (1).

Puis, (2.a) et l'égalité $p + q = r = \operatorname{rang}(\varphi)$ dans (2.c) découlent aussitôt des définitions. Prouvons maintenant (2.d). D'après $(*)$, φ est donnée dans la base $\mathfrak{B}$ par :

$$(*') \qquad \forall u = \sum_{i=1}^{n} x_i e_i,\ \forall v = \sum_{j=1}^{n} y_j e_j, \qquad \varphi(u, v) = \lambda_1 x_1 \bar{y_1} + \cdots + \lambda_r x_r \bar{y_r}.$$

Supposons $u \in N(\varphi)$, alors pour tout $i = 1, \dots, r$, prenant $v = e_i$ (c'est-à-dire, $y_i = 1$ et $y_j = 0$ pour $j \neq i$), on obtient $x_i = 0$, d'où $u \in F = \text{Vect}(e_{r+1}, \dots, e_n)$. Réciproquement, $(*')$ montre aussi que tout $u \in F$ (*i.e.* tel que $x_1 = 0 = \cdots = x_r$) appartient à $N(\varphi)$, d'où l'égalité désirée. Ceci prouve (2.d).

Prouvons (2.b). On note $r = \text{rang}(\varphi)$. Soient $\mathfrak{B} = (e_1, \dots, e_n)$ et $\mathcal{C} = (f_1, \dots, f_n)$ deux bases de E orthogonales pour φ. Notons p (resp. p') le nombre d'indices i tels que $Q(e_i) > 0$ (resp. $Q(f_i) > 0$) et q (resp. q') le nombre d'indices i tels que $Q(e_i) < 0$ (resp. $Q(f_i) < 0$). Alors

$$p + q = r = p' + q'$$

et il s'agit de montrer que $q = q'$ et $p = p'$. Quitte à renuméroter les éléments de $\mathfrak{B}$ et $\mathcal{C}$, on peut supposer que

$(\star)$

$$\begin{cases} Q(e_i) > 0 & \text{pour } i = 1, \dots, p \\ Q(e_i) < 0 & \text{pour } i = p+1, \dots, p+q \\ Q(e_i) = 0 & \text{pour } i > p + q = r\,; \end{cases} \qquad \begin{cases} Q(f_i) > 0 & \text{pour } i = 1, \dots, p' \\ Q(f_i) < 0 & \text{pour } i = p'+1, \dots, p'+q' \\ Q(f_i) = 0 & \text{pour } i > p' + q' = r\,. \end{cases}$$

Notons P_+ le sous-espace de E engendré par les vecteurs e_i tels que $Q(e_i) \geq 0$. Ces vecteurs sont au nombre de $n - q$, donc $\dim P_+ = n - q$. Soit x un élément arbitraire de P_+, écrivons $x = \sum_{i \in I} x_i e_i$, avec $I = \{1, \dots, p\} \cup \{r+1, \dots, n\}$; alors, d'après $(\star)$, on obtient

$$Q(x) = \sum_{i=1}^{p} |x_i|^2 \, Q(e_i) \geq 0. \tag{1}$$

D'autre part, soit P'_- le sous-espace de E engendré par les vecteurs f_j tels que $Q(f_j) < 0$. Ces vecteurs sont au nombre de q', donc $\dim P'_- = q'$. Soit y un élément non nul de P'_-, on peut écrire $y = \sum_{j=p'+1}^{p'+q'} y_j f_j$, avec au moins l'un des y_j non nul (car $y \neq 0$). Alors, d'après $(\star)$ à nouveau, on obtient

$$Q(y) = \sum_{j=p'+1}^{p'+q'} |y_j|^2 \, Q(f_j) < 0. \tag{2}$$

Par conséquent, on a $P_+ \cap P'_- = \{0\}$ et donc

$$n = \dim E \geq \dim P_+ + \dim P'_- = n - q + q'$$

d'où $q \geq q'$. Échangeant les rôles des bases $\mathfrak{B}$ et $\mathcal{C}$, on obtient de même $q' \geq q$, d'où $q = q'$, et de même $p = p'$. Ceci prouve (2.b).

Voyons l'assertion (3). Soit $\mathfrak{B} = (e_1, \dots, e_n)$ comme ci-dessus ; pour $i = 1, \dots, p + q$, notons $|Q(e_i)| > 0$ la valeur absolue du réel $Q(e_i) \neq 0$. En remplaçant e_i par $e_i / \sqrt{|Q(e_i)|}$, pour $i = 1, \dots, p + q$, on obtient une base orthogonale ayant la propriété énoncée dans (3). Ceci achève la démonstration du théorème. □

C.2 Réduction en sommes de carrés de modules

Définition C.15. *Soient E un $\mathbb{C}$-espace vectoriel de dimension n, Q une forme quadratique hermitienne sur E et φ sa forme polaire. Soit $\mathfrak{B} = (e_1, \dots, e_n)$ une base de E, notons $(x_1, \dots, x_n)$ les coordonnées dans cette base,* i.e. *x_i désigne en fait la forme linéaire $f_i = e_i^*$ sur E.*

1. *On dit que Q s'écrit dans la base $\mathfrak{B}$ comme* **somme de carrés de modules de formes linéaires indépendantes** *si l'expression de Q en fonction des coordonnées x_i est de la forme*
$$Q = q_1\,|x_1|^2 + \cdots + q_n\,|x_n|^2, \qquad (\text{avec } q_1, \ldots, q_n \in \mathbb{R}).$$
D'après C.13, ceci équivaut à dire que la matrice de φ dans la base $\mathfrak{B}$ est **diagonale**, *avec les q_i pour coefficients diagonaux.*
2. *Les formes linéaires $f_i = e_i^*$ sont linéairement indépendantes ($\mathfrak{B}^* = (e_1^*, \ldots, e_n^*)$ est la base duale de $\mathfrak{B}$), d'où la terminologie « somme de carrés demodules de* **formes linéaires indépendantes** *». En pratique, pour abréger on écrira souvent « somme de carrés de modules », mais il est essentiel de s'assurer que les formes linéaires en question sont bien linéairement indépendantes (*cf. *l'exemple 4.36 pour les formes bilinéaires symétriques).*

Comme dans le cas des formes bilinéaires symétriques, on dispose d'un procédé algorithmique simple pour réduire une forme quadratique hermitienne en « somme de carrés de modules » (de formes linéaires indépendantes) ; au lieu des égalités $x^2 + 2xL = (x+L)^2 - L^2$ et $4x_1x_2 = (x_1+x_2)^2 - (x_1-x_2)^2$, on va utiliser les égalités :

$$|z|^2 + 2\mathrm{Re}(z\bar{L}) = |z+L|^2 - |L|^2, \qquad 4\mathrm{Re}(z_1\,\bar{z_2}) = |z_1 + \bar{z_2}|^2 - |z_1 - \bar{z_2}|^2.$$

Théorème C.16 (Réduction d'une forme hermitienne en somme de carrés de modules)**.** *Soient E un $\mathbb{C}$-espace vectoriel de dimension n, et Q une forme quadratique hermitienne sur E, donnée en fonctions des coordonnés $(x_1, \ldots, x)$ dans une base $\mathfrak{B}$ par :*

$$(*) \qquad Q(x_1, \ldots, x_n) = \sum_i b_i\,|x_i|^2 + \sum_{1\le i<j\le n} (b_{ij}\,x_i\,\bar{x}_j + \bar{b_{ij}}\,x_j\,\bar{x}_i) \qquad (b_i \in \mathbb{R}, \quad b_{ij} \in \mathbb{C}).$$

1. *Par une suite d'opérations « élémentaires » (décrites dans la démonstration), on peut trouver un nouveau système de coordonnées $(y_1, \ldots, y_n)$ sur E, dans lequel Q s'écrit comme une somme de carrés de modules,* i.e. *:*
$$(**) \qquad Q(y_1, \ldots, y_n) = a_1\,|y_1|^2 + \cdots + a_n|y_n|^2.$$
2. *La signature de Q est (p, q), où p (resp. q) est le nombre de coefficients a_i qui sont > 0 (resp. < 0), et* $\mathrm{rang}(Q) = p + q$.
3. *De plus, $N(Q)$ est le sous-espace vectoriel de E défini par les équations $y_i = 0$, pour i parcourant l'ensemble des $i \in \{1, \ldots, n\}$ tels que $a_i \neq 0$.*

Démonstration. Remarquons d'abord que si Q s'écrit sous la forme $(**)$ dans une base $\mathfrak{B}'$, alors la matrice de sa forme polaire y est diagonale, avec les a_i pour coefficients diagonaux, d'où les assertions (2) et (3) du théorème, compte-tenu du théorème C.14.

Il reste à donner une démonstration « algorithmique » de l'assertion (1). On procède par récurrence sur le nombre n de variables. Si $n = 1$ on a $Q(x_1) = b_1|x_1|^2$, et $(**)$ est vérifié. On peut donc supposer $n > 1$ et le résultat démontré pour $n-1$. Distinguons deux cas.

(a) Si dans l'écriture $(*)$ plus haut, il existe un coefficient « diagonal » b_i non nul, on peut supposer, quitte à changer l'ordre des coordonnées, que $b_1 \neq 0$. On considère alors la somme de **tous** les termes contenant x_1 ou $\bar{x_1}$ et on l'écrit comme suit :

$$S = b_1\,|x_1|^2 + \sum_{j=2}^{n} 2\mathrm{Re}(\bar{b_{j1}}\,x_1\,\bar{x}_j) = b_1\Big(|x_1|^2 + 2\mathrm{Re}\left(x_1 L(x_2, \bar{\ldots}, x_n)\right)\Big)$$

où $L(x_2,\dots,x_n)=\sum_{j=2}^n (b_{j1}/b_1)x_j$. Puis, en utilisant que

$$|x_1+L|^2=|x_1|^2+2\mathrm{Re}(x_1\bar{L})+|L|^2,\qquad \text{d'où}\qquad |x_1|^2+2\mathrm{Re}(x_1\bar{L})=|x_1+L|^2-|L|^2,$$

on récrit ceci sous la forme :

$$S=b_1\,|x_1+L|^2-b_1|L|^2=b_1\Big|x_1+\sum_{j=2}^n\frac{b_{j1}}{b_1}x_j\Big|^2-\frac{1}{b_1}\sum_{j=2}^n|b_{j1}|^2\,|x_j|^2-\frac{2}{b_1}\sum_{2\le i<j\le n}\mathrm{Re}(b_{i1}\,\bar{b_{j1}}\,x_i\,\bar{x}_j).$$

Donc, en posant $y_1=x_1+\sum_{j=2}^n\frac{b_{j1}}{b_1}\,x_j$ (et $b'_j=b_j-|b_{j1}|^2/b_1$ pour $j=2,\dots,n$, et $b'_{ij}=b_{ij}-b_{i1}\,\bar{b_{j1}}/b_1$ pour $2\le i<j\le n$), on obtient une écriture :

$$(\dagger)\qquad Q(y_1,x_2,\dots,x_n)=b_1\,|y_1|^2+\underbrace{\sum_{j=2}^n b'_j\,|x_j|^2+\sum_{2\le i<j\le n}2\mathrm{Re}(b'_{ij}\,x_i\,\bar{x}_j)}_{Q_1(x_2,\dots,x_n)}$$

où la forme quadratique hermitienne $Q_1(x_2,\dots,x_n)$ ne dépend que des variables $x_2,\dots,x_n$.

L'opération $y_1=x_1+L(x_2,\dots,x_n)$ et $x_j=x_j$ pour $j\ge 2$, est bien un changement de coordonnées, car la matrice exprimant $(y_1,x_2,\dots,x_n)$ en fonction de $(x_1,\dots,x_n)$ est triangulaire avec des 1 sur la diagonale, donc inversible ; explicitement le changement de coordonnées inverse est donné par $x_j=x_j$ pour $j\ge 2$ et $x_1=y_1-L(x_2,\dots,x_n)$.

Par hypothèse de récurrence on peut faire un changement de coordonnées $(x_2,\dots,x_n)\to(y_2,\dots,y_n)$ tel que $Q_1(x_2,\dots,x_n)=a_2\,|y_2|^2+\cdots+a_n\,|y_n|^2$ d'où, d'après (†) :

$$Q(y_1,\dots,y_n)=a_1\,|y_1|^2+\cdots+a_n\,|y_n|^2$$

(avec $a_1=b_1$), ce qui prouve le résultat voulu dans ce cas.

(b) Supposons au contraire que **tous** les coefficients « diagonaux » b_i soient nuls. Si $Q=0$, il n'y a rien à montrer ; sinon on peut supposer, quitte à changer l'ordre des coordonnées, que $b_{12}\neq 0$. Comme

$$\mathrm{Re}(b_{12}\,x_1\,\bar{x_2})=\frac{1}{4}(|b_{12}\,x_1+x_2|^2-|b_{12}\,x_1-x_2|^2),$$

posons $y_1=\frac{1}{2}(b_{12}\,x_1+x_2)$ et $y_2=\frac{1}{2}(b_{12}\,x_1+x_2)$; c'est bien un changement de variable, dont l'inverse est donné par

$$x_1=b_{12}^{-1}(y_1+y_2)\qquad\qquad x_2=y_1-y_2.$$

Alors : $2\mathrm{Re}(b_{12}\,x_1\,\bar{x_2})=2(|y_1|^2-|y_2|^2)$, les termes $2\mathrm{Re}(b_{ij}\,x_i\,\bar{x}_j)$ sont inchangés pour $i<j$ dans $\{3,\dots,n\}$, et l'on a :

$$\begin{cases}2\mathrm{Re}(b_{1j}\,x_1\,\bar{x}_j)=2\mathrm{Re}(b_{1j}b_{12}^{-1}\,(y_1+y_2)\,\bar{x}_j) & \text{pour } j\ge 3\\ 2\mathrm{Re}(b_{2j}\,x_2\,\bar{x}_j)=2\mathrm{Re}(b_{2j}\,(y_1-y_2)\,\bar{x}_j) & \text{pour } j\ge 3\end{cases}$$

donc $Q(y_1,y_2,x_3,\dots,x_n)$ égale :

$$2|y_1|^2-2|y_2|^2+\sum_{j=3}^n 2\mathrm{Re}\Big((b_{1j}b_{12}^{-1}+b_{2j})\,y_1\,\bar{x}_j+(b_{1j}b_{12}^{-1}-b_{2j})\,y_2\,\bar{x}_j\Big)+\sum_{3\le i<j\le n}2\mathrm{Re}(b_{ij}\,x_i\,\bar{x}_j)$$

et l'on est ramené au cas **(a)**, c'est-à-dire, on peut maintenant éliminer la variable y_1 et se ramener, à nouveau, au cas de $n-1$ variables. Le théorème est démontré. □

Illustrons ceci par deux exemples : dans le premier n'apparaissent que des changements de coordonnées du type **(a)**.

Exemple C.17. *Considérons dans* $\mathbb{C}^3$ *la forme quadratique hermitienne*

$$q(x_1, x_2, x_3) = x_1\bar{x_1} - 2ix_1\bar{x_2} + 2ix_2\bar{x_1} + ix_1\bar{x_3} - ix_3\bar{x_1} + 2x_2\bar{x_2} + 2x_3\bar{x_3} - 2ix_2\bar{x_3} + 2ix_3\bar{x_2}.$$

Alors q contient le terme $x_1\bar{x_1} = |x_1|^2$*, et les termes contenant* x_1 *ou* $\bar{x_1}$ *sont :*

$$\begin{aligned} x_1\bar{x_1} - 2ix_1\bar{x_2} + 2ix_2\bar{x_1} + ix_1\bar{x_3} - ix_3\bar{x_1} &= |x_1|^2 + 2\mathrm{Re}(x_1\,(2i\bar{x_2} - i\bar{x_3})\,) \\ &= |x_1 + 2ix_2 - ix_3|^2 - |2ix_2 - ix_3|^2 \\ &= |x_1 + 2ix_2 - ix_3|^2 - 4\,|x_2|^2 - |x_3|^2 + 4\mathrm{Re}(x_2\,\bar{x_3}) \end{aligned}$$

donc, posant $y_1 = x_1 + 2ix_2 - ix_3$*, on obtient*

$$\begin{aligned} q(y_1, x_2, x_3) &= |y_1|^2 - 4\,|x_2|^2 - |x_3|^2 + 4\mathrm{Re}(x_2\,\bar{x_3}) + 2|x_2|^2 + 2|x_3|^2 - 4\mathrm{Re}(ix_2\,\bar{x_3}) \\ &= |y_1|^2 - 2|x_2|^2 + |x_3|^2 + 4\mathrm{Re}(x_2\,(1+\bar{i})x_3\,). \end{aligned}$$

Puis

$$\begin{aligned} -2\Big(|x_2|^2 - 2\mathrm{Re}(x_2\,(1+\bar{i})x_3\,)\Big) &= -2\Big(|x_2 - (1+i)x_3|^2 - |(1+i)x_3|^2\Big) \\ &= -2\Big(|x_2 - (1+i)x_3|^2 - 2\,|x_3|^2\Big) \end{aligned}$$

donc, posant $y_2 = x_2 - (1+i)x_3$ *on obtient :* $\boxed{q(y_1, y_2, x_3) = |y_1|^2 - 2|y_2|^2 + 5|x_3|^2.}$ *Donc la signature de q est* $(2, 1)$ *et son rang est* $2 + 1 = 3$*,* i.e. *h est non-dégénérée.*

Exemple C.18. *Considérons dans* $\mathbb{C}^3$ *la forme quadratique hermitienne*

$$Q(x_1, x_2, x_3) = x_1\bar{x_2} + x_2\bar{x_1} + ix_1\bar{x_3} - ix_3\bar{x_1} + (1+i)x_2\bar{x_3} + (1-i)x_3\bar{x_2}.$$

Ici, il n'y a pas de « termes carrés » $|x_i|^2$*, donc on va considérer le terme* $x_1\,\bar{x_2}$*. On a* $b_{12} = 1$*, faisons le changement de coordonnées :*

$$y_1 = \frac{1}{2}(x_1 + x_2), \quad y_2 = \frac{1}{2}(x_1 - x_2), \qquad \textit{d'où} \qquad x_1 = y_1 + y_2, \quad x_2 = y_1 - y_2.$$

On a $2\mathrm{Re}(x_1\,\bar{x_2}) = 2(|y_1|^2 - |y_2|^2)$*, et*

$$\begin{cases} 2\mathrm{Re}(ix_1\bar{x_3}) &= 2\mathrm{Re}(iy_1\bar{x_3}) + 2\mathrm{Re}(iy_2\bar{x_3}) \\ 2\mathrm{Re}((1+i)x_2\bar{x_3}) &= 2\mathrm{Re}((1+i)y_1\bar{x_3}) - 2\mathrm{Re}((1+i)y_2\bar{x_3}) \end{cases}$$

d'où

$$Q(y_1, y_2, x_3) = 2\,|y_1|^2 - 2\,|y_2|^2 + 2\mathrm{Re}((1+2i)y_1\bar{x_3}) - 2\mathrm{Re}(y_2\bar{x_3}).$$

Puis $2\Big(|y_1|^2 + 2\mathrm{Re}(\frac{1+2i}{2}y_1\bar{x_3})\Big) = 2\Big(|y_1 + \frac{1-2i}{2}x_3|^2 - |\frac{1-2i}{2}x_3|^2\Big)$ *donc, posant* $z_1 = y_1 + \frac{1-2i}{2}x_3$*, on obtient*

$$Q(z_1, y_2, x_3) = 2\,|z_1|^2 - \frac{5}{2}|x_3|^2 - 2\,|y_2|^2 - 2\mathrm{Re}(y_2\bar{x_3}).$$

Puis $-2\Big(|y_2|^2 + \mathrm{Re}(y_2\bar{x_3})\Big) = -2\Big(|y_2 + \frac{1}{2}x_3|^2 - \frac{1}{4}|x_3|^2\Big)$ *donc, posant* $2_1 = y_2 + \frac{1}{2}x_3$*, on obtient*

$$\boxed{Q(z_1, z_2, x_3) = 2\,|z_1|^2 - 2\,|z_2|^2 - 2\,|x_3|^2.}$$

Donc la signature de Q est $(1, 2)$ *et son rang est* $1 + 2 = 3$*,* i.e. *Q est non-dégénérée.*

C.3 Espaces hilbertiens. Inégalité de Cauchy-Schwarz. Isométries

Définition C.19 (Produits scalaires et espaces hilbertiens)**.** *Soit E un $\mathbb{C}$-espace vectoriel de dimension finie.*

1. *Soient φ une forme hermitienne sur E et Q la forme quadratique hermitienne associée (*i.e. *$Q(x) = \varphi(x,x)$ pour tout $x \in E$). On dit que Q (ou φ) est* **définie positive** *si l'on a :*

   (*Déf. Pos.*) $\boxed{\forall x \in E - \{0\}, \qquad Q(x) = \varphi(x,x) > 0.}$

   Dans ce cas, on dit que φ est un produit scalaire **hilbertien** *et on note souvent $\varphi(x,y) = (x \mid y)$.*

   Remarquons que si Q (ou φ) est définie positive, elle est non-dégénérée *: en effet, si $x \in N(\varphi)$, on a $0 = \varphi(x,y)$ pour tout $y \in E$, en particulier $\varphi(x,x) = 0$, d'où $x = 0$.*

2. *Dans ce cas, on dit que : « E,* muni de $(\ \mid\ )$ *» (ou que : «* le couple (E, φ) *») est un* **espace hilbertien***. Pour abréger, on écrira souvent : « Soit E un espace hilbertien », sans préciser le produit scalaire $(\ \mid\ )$, celui-ci étant sous-entendu.*

Exemple C.20. *Le produit scalaire hilbertien standard sur $\mathbb{C}^n$ est défini par :*

$$(x \mid y) = x_1\bar{y_1} + \cdots + x_n\bar{y_n} \qquad si\ x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Pour ce produit scalaire, la base canonique $(e_1, \ldots, e_n)$ de $\mathbb{R}^n$ est orthonormée, i.e. *on a $(e_i \mid e_j) = 1$ si $i = j$ et $= 0$ sinon, et la forme quadratique hermitienne associée est $Q(x) = |x_1|^2 + \cdots + |x_n|^2$.*

Proposition/Définition C.3 (Familles et bases orthonormées)**.** *Soit E, muni de $(\ \mid\ )$, un espace hilbertien.*

1. *Une famille $(e_i)_{i \in I}$ de vecteurs est dite* **orthonormée** *si $(e_i \mid e_i) = 1$ et $(e_i \mid e_j) = 0$ pour tout $i \neq j$.*
2. *Supposons E de dimension n. Une* **base orthonormée** *est une base $(e_1, \ldots, e_n)$ de E qui est une famille orthonormée,* i.e. *qui vérifie $(e_i \mid e_i) = 1$ et $(e_i \mid e_j) = 0$ pour tout $i \neq j$.*
3. *Toute famille orthonormée est* libre*. En particulier, si* $\dim E = n$*, toute famille orthonormée $(f_1, \ldots, f_n)$ de cardinal n est une base orthonormée de E.*
4. *Dans la suite, on abrégera souvent « base orthonormée » en : b.o.n.*

Démonstration. Prouvons (3). Supposons qu'on ait une relation $0 = t_1 e_{i_1} + \cdots + t_p e_{i_p}$, avec $i_1, \ldots, i_p \in I$ deux à deux distincts, et $t_1, \ldots, t_p \in \mathbb{R}$. Fixons un indice $r \in \{1, \ldots, p\}$ et appliquons $(e_{i_r} \mid\ )$ à l'égalité précédente. Comme $(e_{i_r} \mid e_{i_s}) = 0$ pour $s \neq r$, on obtient $0 = t_r(e_{i_r} \mid e_{i_r}) = t_r$, d'où $t_r = 0$. Ceci prouve que la famille $(e_i)_{i \in I}$ est libre. □

Théorème C.21 (Existence de b.o.n.)**.** *Soit E un espace hilbertien de dimension n. Alors E admet une base orthonormée*

Démonstration. D'après le théorème C.14, il existe une base $(e_1, \ldots, e_n)$ orthogonale (*i.e.* $(e_i \mid e_j) = 0$ pour $i \neq j$) et telle que $(e_i \mid e_i) \in \{1, -1, 0\}$; or comme $(\ \mid\ )$ est défini positif on a nécessairement $(e_i \mid e_i) = 1$, donc $(e_1, \ldots, e_n)$ est une b.o.n. □

Définition C.22 (Sous-espaces d'un espace hilbertien)**.** *Soit E, muni de $(\ |\ )$, un espace hilbertien et soit F un sous-espace vectoriel de E. Alors la restriction $(\ |\ )_F$ de $(\ |\ )$ à F est un produit scalaire hilbertien sur F, puisque $(x \mid x)_F = (x \mid x) > 0$ pour tout $x \in F - \{0\}$. Donc F muni de $(\ |\ )_F$ est un espace hilbertien.*

Théorème/Définition C.1 (Projection orthogonale sur un sous-espace)**.** *Soit E, muni de $(\ |\ )$, un espace hilbertien et soient F un sous-espace et $F^\perp$ son orthogonal pour $(\ |\ )$.*

1. *On a* $\boxed{E = F \oplus F^\perp.}$ *Le projecteur $\pi_F : E \to E$, d'image F et de noyau $F^\perp$, défini par cette décomposition s'appelle la* **projection orthogonale** *sur F.*
2. *Soit $(e_1, \dots, e_r)$ une base* **orthonormée** *de F. Alors* $\boxed{\pi_F(v) = (v \mid e_1)e_1 + \cdots + (v \mid e_r)e_r}$ *pour tout $v \in E$.*
3. *On a* $\boxed{(F^\perp)^\perp = F}$ *donc la projection orthogonale $\pi_{F^\perp}$ sur $F^\perp$ n'est autre que* $\mathrm{id}_E - \pi_F$, i.e. *on a* $\boxed{\mathrm{id}_E = \pi_F + \pi_{F^\perp}.}$

Démonstration. Comme les formes hermitiennes $(\ |\ )$ et $(\ |\ )_F$ sont définies positives, donc non-dégénérées, on a $(F^\perp)^\perp = F$ et $E = F \oplus F^\perp$ d'après C.12. Alors, tout $x \in E$ s'écrit de façon unique $x = f + g$ avec $f \in F$ et $g \in F^\perp$, et le projecteur π_F sur F parallèlement à $F^\perp$ (*i.e.* de noyau $F^\perp$) est défini par $\pi_F(x) = f$. De plus, comme $(F^\perp)^\perp = F$, alors le projecteur $\pi_{F^\perp}$ sur $F^\perp$ parallèlement à $(F^\perp)^\perp = F$ (*i.e.* de noyau F) est défini par $\pi_{F^\perp}(x) = g$, donc on a bien $\mathrm{id}_E = \pi_F + \pi_{F^\perp}$. Ceci prouve (1) et (3).

Prouvons (2). Soit $r = \dim F$ et soit $(e_1, \dots, e_r)$ une b.o.n. de F. Pour tout $v \in E$, notons provisoirement

$$\pi(v) = (v \mid e_1)\, e_1 + \cdots + (v \mid e_r)\, e_r \in F.$$

Alors, pour $j = 1, \dots, r$, on a $(v - \pi(v) \mid e_j) = (v \mid e_j) - \sum_{i=1}^r (v \mid e_i) \underbrace{(e_i \mid e_j)}_{\substack{=1 \text{ si } i=j \\ =0 \text{ si } i \neq j}} = 0$, d'où $v - \pi(v) \in F^\perp$, et donc $v = \pi(v) + v - \pi(v)$, avec $\pi(v) \in F$ et $v - \pi(v) \in F^\perp$. Comme $E = F \oplus F^\perp$, ceci entraîne que $\pi(v) = \pi_F(v)$, d'où l'assertion (2). □

Définition C.23 (Normes)**.** *Soit E un $\mathbb{C}$-espace vectoriel. Une* **norme** $\|\cdot\|$ *sur E est une application $E \to \mathbb{R}_+$, $v \mapsto \|v\|$ vérifiant les trois propriétés suivantes :*

1. *$\|v\| = 0 \Leftrightarrow v = 0$.*
2. *Pour tout $z \in \mathbb{C}$, $v \in E$, on a $\|zv\| = |z| \cdot \|v\|$ (où $|z|$ est le module de z).*
3. *(Inégalité triangulaire) $\|u + v\| \leq \|u\| + \|v\|$, pour tout $u, v \in E$.*

Théorème C.24 (Inégalité de Cauchy-Schwarz et norme hilbertienne)**.** *Soit E, muni de $(\ |\ )$, un espace hilbertien et soit $Q(x) = (x \mid x)$ la forme quadratique hermitienne associée.*

1. *On a l'inégalité de Cauchy-Schwarz :*

   (CS) $\qquad \boxed{\forall x, y \in E \qquad |(x \mid y)|^2 \leq Q(x)Q(y)}$

   avec égalité si et seulement si x et y sont liés.

2. *Par conséquent, l'application $x \mapsto \|x\| = \sqrt{(x \mid x)}$ est une norme sur E, appelée la* **norme hilbertienne** *associée à $(\ |\ )$, et l'inégalité de Cauchy-Schwarz se récrit comme suit :*

   (CS) $\qquad \boxed{\forall x, y \in E \qquad |(x \mid y)| \leq \|x\| \cdot \|y\|.}$

Démonstration. (1) Soient $x, y \in E$. L'inégalité est trivialement vérifiée si $x = 0$, donc on peut supposer $x \neq 0$. Considérons alors le vecteur

$$v = y - \frac{(y \mid x)}{(x \mid x)} x$$

(c'est la projection orthogonale de y sur l'hyperplan $(\mathbb{C}x)^\perp$. Comme $(y \mid x) = (x \mid y)$, on a :

$$0 \leq (v \mid v) = (y \mid y) - \frac{(y \mid x)}{(x \mid x)}(x \mid y) \underbrace{- \frac{(x \mid y)}{(x \mid x)}(y \mid x) + \frac{(y \mid x)(x \mid y)}{(x \mid x)^2}(x \mid x)}_{=0}$$

donc, multipliant par $(x \mid x) > 0$, on obtient que $0 \leq (x \mid x)\,(v \mid v) = (y \mid y)\,(x \mid x) - |(x \mid y)|^2$. Ceci prouve l'inégalité voulue, et montre que l'on a égalité si et seulement $(v \mid v) = 0$, c'est-à-dire, si $v = 0$, *i.e.* si $y = \dfrac{(y \mid x)}{(x \mid x)} x$. Ceci prouve l'assertion (1).

Prouvons que $v \mapsto \|v\| = \sqrt{(v \mid v)}$ est une norme sur E. Comme $(\ \mid\ )$ est défini positif, on a $\|v\| = 0 \Leftrightarrow v = 0$. D'autre part, pour tout $z \in \mathbb{C}$ et $x \in E$, on a $|z| = \sqrt{z\bar{z}}$ et donc

$$\|z\, v\| = \sqrt{z\bar{z}\,(v \mid v)} = |z| \cdot \|v\|.$$

Enfin, soient $x, y \in E$. D'abord, l'inégalité de Cauchy-Schwarz équivaut (en prenant la racine carrée) à :

$$|(x \mid y)| \leq \|x\| \cdot \|y\|\,;$$

alors, multipliant par 2 et ajoutant $\|x\|^2 + \|y\|^2$ aux deux membres, on obtient

$$(\dagger) \qquad \|x\|^2 + \|y\|^2 + 2|(x \mid y)| \leq \|x\|^2 + \|y\|^2 + 2\|x\| \cdot \|y\| = (\|x\| + \|y\|)^2.$$

D'autre part, d'après les égalités de polarisations C.7, on a :

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2 + 2\mathrm{Re}((x \mid y)).$$

Or, pour tout nombre complexe $z = a + ib$, on a : $\mathrm{Re}(z) = a \leq \sqrt{a^2 + b^2} = |z|$. On obtient donc

$$\|x + y\|^2 \leq \|x\|^2 + \|y\|^2 + 2|(x \mid y)|$$

ce qui, combiné avec (†), entraîne :

$$\|x + y\|^2 \leq (\|x\| + \|y\|)^2.$$

Prenant la racine carrée, ceci entraîne (et équivaut à) l'inégalité triangulaire. Le théorème est démontré. □

Récrivons les égalités de polarisation C.7 en utilisant la norme $\|\cdot\|$, et ajoutons-y l'égalité de Pythagore :

Proposition C.25 (Polarisation)**.** *Soit E, muni de $(\ \mid\ )$, un espace hilbertien et soit $\|\cdot\|$ la norme hilbertienne associée.*

1. *Pour tout $x, y \in E$, on a :*

$$\mathrm{Re}((x \mid y)) = \frac{1}{2}(\|x + y\|^2 - \|x\|^2 - \|y\|^2) = \frac{1}{4}(\|x + y\|^2 - \|x - y\|^2) \tag{1}$$

$$\mathrm{Im}((x \mid y)) = \frac{1}{2}(\|x + iy\|^2 - \|x\|^2 - \|y\|^2) = \frac{1}{4}(\|x + iy\|^2 - \|x - iy\|^2) \tag{2}$$

$$4\,(x \mid y) = \|x + y\|^2 - \|x - y\|^2 + i\|x + iy\|^2 - i\|x - iy\|^2. \tag{3}$$

2. Égalité de Pythagore) *Si $x_1, \dots, x_n$ sont orthogonaux, on a $\|x_1 + \cdots + x_n\|^2 = \|x_1\|^2 + \cdots + \|x_n\|^2$.*

Démonstration. La première assertion n'est qu'une reformulation de C.7. L'égalité de Pythagore est immédiate si $n = 2$, et dans ce cas on a même la réciproque : si $\|x_1 + x_2\|^2 = \|x_1\|^2 + \|x_2\|^2$ alors $(x_1 \mid x_2) = 0$. L'égalité pour n vecteurs orthogonaux s'obtient par récurrence sur n. On prendra garde que la réciproque est fausse pour $n \geq 3$: prendre par exemple dans $\mathbb{C}^2$ hilbertien les vecteurs $x_1 = e_1$, $x_2 = e_1 + e_2$, $x_3 = e_2 - e_1$. □

Proposition/Définition C.4 (Isométries vectorielles)**.** *Soient E, F deux espaces hilbertiens de même dimension n, notons $(\ |\ )_E$ et $\|\cdot\|_E$ (resp. $(\ |\ )_F$ et $\|\cdot\|_F$) le produit scalaire et la norme hilbertienne sur E (resp. F). Soit $f : E \to F$ une application linéaire.*

1. *Les conditions suivantes sont équivalentes :*
   (a) f préserve la norme *:* $\boxed{\forall x \in E, \quad \|x\|_E = \|f(x)\|_F}$
   (b) f préserve le produit scalaire *:* $\boxed{\forall x, y \in E, \quad (x \mid y)_E = (f(x) \mid f(y))_F}$
   (c) *Pour toute b.o.n. $\mathfrak{B} = (e_1, \dots, e_n)$ de E, la famille $(f(e_1), \dots, f(e_n))$ est une b.o.n. de F.*
   (d) *Il existe une b.o.n. $\mathfrak{B} = (e_1, \dots, e_n)$ de E telle que $(f(e_1), \dots, f(e_n))$ soit une b.o.n. de F.*
2. *Sous ces conditions, on dit que f est une* **isométrie** *vectorielle de E sur F*
3. *Dans ce cas, f est bijective, et son inverse f^{-1} est aussi une isométrie.*

Démonstration. Supposons que f préserve la norme, et soient $x, y \in E$. Alors $\|x + y\|_E^2 = \|f(x + y)\|_F^2 = \|f(x) + f(y)\|_F^2$, et le premier (resp. dernier) membre égale :

$$\|x\|_E^2 + \|y\|_E^2 + 2\mathrm{Re}((x \mid y)_E), \qquad \text{resp.} \qquad \|f(x)\|_F^2 + \|f(y)\|_F^2 + 2\mathrm{Re}((f(x) \mid f(y))_F)$$

et comme $\|x\|_E^2 = \|f(x)\|_F^2$ et $\|y\|_E^2 = \|f(y)\|_F^2$, on obtient que $\mathrm{Re}((x \mid y)_E) = \mathrm{Re}((f(x) \mid f(y))_F)$.

D'autre part, pour tout $z \in \mathbb{C}$, on a $\mathrm{Im}(z) = \mathrm{Re}(-iz)$. Donc, appliquant ce qui précède à iy au lieu de y, on obtient aussi l'égalité :

$$\mathrm{Im}((x \mid y)_E) = \mathrm{Re}((x \mid iy)_E) = \mathrm{Re}((f(x) \mid f(iy))_F) = \mathrm{Re}((f(x) \mid if(y))_F) = \mathrm{Im}((f(x) \mid f(y))_F),$$

d'où finalement $(x \mid y)_E = (f(x) \mid f(y))_F$. Ceci prouve que (a) $\implies$ (b).

Les implications (b) $\implies$ (c) $\implies$ (d) sont évidentes, montrons que (d) $\implies$ (a). Supposons (d) vérifiée. Pour tout $x = x_1 e_1 + \cdots + x_n e_n$ dans E, on a $f(x) = \sum_i x_i f(e_i)$ et, comme $(e_1, \dots, e_n)$ et $(f(e_1), \dots, f(e_n))$ sont des b.o.n., on obtient

$$\|x\|_E^2 = \sum_{i=1}^{n} |x_i|^2 = \|f(x)\|_F^2$$

donc (a) est vérifiée. Ceci prouve l'assertion (1).

Prouvons (3). Soit $f : E \to F$ une isométrie, et soit $\mathfrak{B} = (e_1, \dots, e_n)$ de E. Comme $f(\mathfrak{B})$ est un b.o.n. (donc une base) de F, alors f est bijective. Son inverse f^{-1} envoie la b.o.n. $f(\mathfrak{B}) = (f(e_1), \dots, f(e_n))$ de F sur la b.o.n. $\mathfrak{B}$ de E, donc f^{-1} est une isométrie. Ceci prouve (3). La proposition est démontrée. □

Terminologie. *On a introduit la terminologie isométrie « vectorielle » pour faire la distinction avec la notion d'isométrie « affine », étudiée au Chap. 6. Dans la suite de ce chapitre, comme on ne considère que des applications linéaires, on dira simplement « isométrie »au lieu de « isométrie vectorielle ».*

Corollaire/Définition C.26. (1) *On dit que deux espaces hilbertiens E et E' sont* **isométriques** *s'il existe une isométrie $f : E \xrightarrow{\sim} E'$.*

(2) *Tout espace hilbertien E de dimension n est isométrique à $\mathbb{C}^n$ muni du produit scalaire hilbertien standard.*

Démonstration. Soit $\mathfrak{B} = (e_1, \dots, e_n)$ la base canonique de $\mathbb{C}^n$, qui est orthonormée pour le produit scalaire standard. D'après le théorème C.21, E admet une b.o.n. $\mathcal{C} = (f_1, \dots, f_n)$. Alors l'application linéaire $u : \mathbb{C}^n \to E$ définie par $u(e_i) = f_i$, pour $i = 1, \dots, n$, est une isométrie de $\mathbb{C}^n$ sur E. □

Définition C.27. *On note* $\mathrm{U}(n) = \{A \in M_n(\mathbb{C}) \mid {}^tA\,\bar{A} = I_n\}$. *Remarquons que l'égalité* ${}^tA\,\bar{A} = I_n$ *équivaut à l'égalité* ${}^t\bar{A}\,A = I_n$, *qui entraîne que A est inversible et* $A^{-1} = {}^t\bar{A}$. *Donc* $\mathrm{U}(n) \subset \mathrm{GL}_n(\mathbb{C})$ *et, si* $A \in \mathrm{U}(n)$, *son inverse* $B = A^{-1} = {}^t\bar{A}$ *vérifie* $B^{-1} = A = {}^t\bar{B}$, *donc appartient aussi à* $\mathrm{U}(n)$. *De plus, pour tout* $A, B \in \mathrm{U}(n)$, *on a l'égalité* ${}^t(AB)\bar{AB} = {}^tB\,{}^tA\,\bar{A}\,\bar{B} = {}^tB\,\bar{B} = I_n$, *donc* $AB \in \mathrm{U}(n)$. *Donc* $\mathrm{U}(n)$ *est un* sous-groupe *de* $\mathrm{GL}_n(\mathbb{C})$, *appelé le* **groupe unitaire**.

Munissons $\mathbb{C}^n$ du produit scalaire hilbertien standard $(\ |\ )$. Pour tout $X, Y \in \mathbb{C}^n$ on a $(X \mid Y) = {}^tX\bar{Y}$, *i.e.* la matrice de $(\ |\ )$ dans la base canonique $\mathfrak{B}_0 = (e_1, \dots, e_n)$ est la matrice identité I_n. Donc une matrice arbitraire $A \in M_n(\mathbb{C})$ préserve le produit scalaire si et seulement si, on a, pour tout $X, Y \in \mathbb{C}^n$:

$$ {}^tX\bar{Y} = (X \mid Y) = (AX \mid AY) = {}^tX\,({}^tA\bar{A})\,Y $$

ce qui équivaut à dire que ${}^tA\bar{A} = I_n$ (*cf.* C.10). Ceci montre que $\mathrm{U}(n)$ est le groupe des isométries de $\mathbb{C}^n$ muni produit scalaire hilbertien standard $(\ |\ )$.

De plus, notons $C_1, \dots, C_n$ les colonnes de A (*i.e.* C_i est le vecteur $Ae_i \in \mathbb{C}^n$). Remarquons que, pour tout $i, j \in \{1, \dots, n\}$, le coefficient d'indice (i, j) de ${}^tA\bar{A}$ est le produit matriciel de la i-ème ligne de ${}^tA$, *i.e.* de ${}^tC_i$, par la colonne $\bar{C}_j$, c'est-à-dire, on a $({}^tA\bar{A})_{ij} = (Ae_i \mid Ae_j)$, donc la condition ${}^tA\bar{A} = I_n$ équivaut aussi à dire que les colonnes de A sont de norme 1 et deux à deux orthogonales. Tenant compte de la proposition C.4, on obtient donc les caractérisations suivantes de $\mathrm{U}(n)$, chacune étant utile :

Proposition C.28 (Groupe unitaire $\mathrm{U}(n)$)**.** *On munit $\mathbb{C}^n$ du produit scalaire hilbertien standard $(\ |\ )$ et l'on note $\|\cdot\|$ la norme hilbertienne associée. Alors* $\mathrm{U}(n)$ *est le groupe des isométries de $\mathbb{C}^n$; il est caractérisé par* chacune *des égalités suivantes :*

$$
\begin{aligned}
\mathrm{U}(n) &= \{A \in M_n(\mathbb{C}) \mid {}^tA\bar{A} = I_n\} \\
&= \{A \in \mathrm{GL}_n(\mathbb{C}) \mid A^{-1} = {}^t\bar{A}\} \\
&= \{A \in M_n(\mathbb{C}) \mid (AX \mid AY) = (X \mid Y), \quad \forall X, Y \in \mathbb{C}^n\} \\
&= \{A \in M_n(\mathbb{C}) \mid \|AX\| = \|X\|, \quad \forall X \in \mathbb{C}^n\} \\
&= \{A \in M_n(\mathbb{C}) \mid (Af_1, \dots, Af_n) \textit{ est une b.o.n., pour } \text{toute } \textit{b.o.n.} \ (f_1, \dots, f_n)\} \\
&= \{A \in M_n(\mathbb{C}) \mid (Ae_1, \dots, Ae_n) \textit{ est une b.o.n., où } (e_1, \dots, e_n) \textit{ est la base canonique de } \mathbb{C}^n\} \\
&= \{A \in M_n(\mathbb{C}) \mid \textit{les colonnes de } A \textit{ sont de norme } 1 \textit{ et deux à deux orthogonales}\}
\end{aligned}
$$

Les éléments de $\mathrm{U}(n)$ *sont appelés «* endomorphismes unitaires *».*

Remarque C.29. *Il existe* d'autres *groupes unitaires (qui ne sont isomorphes à aucun* $\mathrm{U}(n)$*). Soient* p, q *des entiers* ≥ 1 *et soit* φ *la forme hermitienne sur* $\mathbb{C}^{p+q}$ *définie par* $\varphi(X,Y) = \sum_{i=1}^{p} x_i y_i - \sum_{i=p+1}^{q} x_i y_i$, i.e. *la matrice de* φ *dans la base canonique de* $\mathbb{C}^{p+q}$ *est* $J = \left(\begin{array}{c|c} I_p & \mathbf{0}_{p,q} \\ \hline \mathbf{0}_{q,p} & -I_q \end{array}\right)$*. Alors*

$$\{A \in M_n(\mathbb{C}) \mid {}^tAJA = J\} = \{A \in M_n(\mathbb{C}) \mid \varphi(AX, AY) = \varphi(X,Y), \quad \forall X, Y \in \mathbb{C}^n\}$$

est un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$*, noté* $\mathrm{U}(p,q)$*. On ne considérera pas ces groupes dans ce cours.*

C.4 Diagonalisation des endomorphismes auto-adjoints et normaux

Commençons par introduire l'adjoint dans le cas général d'une forme hermitienne non dégénérée, même si on se limitera dans la suite au cas hilbertien.

Théorème/Définition C.30 (Adjoint d'un endomorphisme)**.** *Soient* E *un* $\mathbb{C}$*-espace vectoriel de dimension* n*, et* φ *une forme hermitienne sur* E*,* **non dégénérée***.*

1. *Pour tout* $u \in \mathrm{End}(E)$*, il existe un unique endomorphisme* u^* *de* E*, appelé* **l'adjoint** *de* u*, vérifiant :*

   $$(*) \qquad \forall x, y \in E, \qquad \boxed{\varphi(u(x), y) = \varphi(x, u^*(y)).}$$

2. *Pour toute base* $\mathfrak{B}$ *de* E*, si l'on note* $J = \mathrm{Mat}_{\mathfrak{B}}(\varphi)$ *et* $A = \mathrm{Mat}_{\mathfrak{B}}(u)$*, on a*

   $$(**) \qquad \boxed{A^* = \mathrm{Mat}_{\mathfrak{B}}(u^*) = \bar{J}^{-1}\, {}^t\bar{A}\, \bar{J}.}$$

3. *On a* $(u^*)^* = u$*.*

Démonstration. Supposons qu'il existe u^* vérifiant $(*)$ et soient $\mathfrak{B}$ une base de E, $J = \mathrm{Mat}_{\mathfrak{B}}(\varphi)$, $A = \mathrm{Mat}_{\mathfrak{B}}(u)$ et $A^* = \mathrm{Mat}_{\mathfrak{B}}(u^*)$. Soient $x, y \in E$ arbitraires, et notons $X, Y \in \mathbb{C}^n$ les vecteurs colonnes associés (coordonnées dans la base $\mathfrak{B}$). Alors on a

$${}^tX\, {}^tAJ\bar{Y} = \varphi(u(x), y) = \varphi(x, u^*(y)) = {}^tXJA^{\bar{*}}Y = {}^tXJ\bar{A^*}\,\bar{Y}$$

d'où ${}^tAJ = J\bar{A^*}$ et donc, puisque J est inversible (car φ non-dégénérée), $A^* = \bar{J}^{-1}\, {}^t\bar{A}\, \bar{J}$. Ceci montre que u^*, s'il existe, vérifie $(**)$ et est donc unique.

Réciproquement, si l'on note u^* l'endomorphisme de E dont la matrice dans la base $\mathfrak{B}$ est $A^* = \bar{J}^{-1}\, {}^t\bar{A}\, \bar{J}$, alors pour tout x, y on a :

$$\varphi(x, u^*(y)) = {}^tXJA^{\bar{*}}Y = {}^tX\, {}^tA\, J\bar{Y} = \varphi(u(x), y)$$

donc u^* vérifie $(*)$. Ceci prouve les assertions (1) et (2).

Prouvons l'assertion (3). Pour tout $x, y \in E$, on a :

$$(u^*(x) \mid y) = (y \mid \bar{u^*}(x)) = (u(\bar{y}) \mid x) = (x \mid u(y))$$

et ceci montre que u est l'adjoint de u^*, *i.e.* $u = (u^*)^*$. Le théorème est démontré. □

Remarque C.31. *Il résulte de la formule* $(**)$ *(ou directement de la définition* $(*)$*) que, pour tout* $u, v \in \mathrm{End}(E)$ *et* $s, t \in \mathbb{C}$*, on a* $(s\,u + t\,v)^* = \bar{s}\,u^* + \bar{t}\,v^*$*,* i.e. *l'application* $\mathrm{End}(E) \to \mathrm{End}(E)$*,* $u \mapsto u^*$ *est semi-linéaire.*

Remarquons aussi que si φ est un produit scalaire hilbertien et si $\mathfrak{B}$ est une b.o.n., alors la matrice de φ dans $\mathfrak{B}$ est $J = I_n$. On peut donc énoncer le théorème dans le cas hilbertien sous la forme suivante.

Théorème C.32 (Adjoint d'un endomorphisme dans le cas hilbertien)**.** *Soit E muni de $(\ |\ )$ un espace* **hilbertien** *de dimension n. Pour tout $u \in \mathrm{End}(E)$, il existe un unique endomorphisme u^* de E, appelé* **l'adjoint** *de u, vérifiant :*

$$(*) \qquad \forall x, y \in E, \qquad \boxed{(u(x) \mid y) = (x \mid u^*(y)).}$$

Pour toute **b.o.n.** *$\mathfrak{B}$ de E, si l'on note $A = \mathrm{Mat}_{\mathfrak{B}}(u)$, on a*

$$(**) \qquad \boxed{A^* = \mathrm{Mat}_{\mathfrak{B}}(u^*) = {}^t\bar{A}.}$$

Lemme C.33 (Stabilité par u ou u^*)**.** *Soient E muni de $(\ |\ )$ un espace* **hilbertien** *de dimension n, $u \in \mathrm{End}(E)$, F un sous-espace vectoriel de E, et $F^\perp$ son orthogonal pour $(\ |\ )$. Alors : F est stable par u (*i.e. *$u(F) \subseteq F$) si et seulement si $F^\perp$ est stable par u^*.*

Démonstration. Supposons $u(F) \subseteq F$, et soit $y \in F^\perp$. Pour tout $x \in F$, on a :

$$(x \mid u^*(y)) = (u(x) \mid y) = 0$$

(la dernière égalité puisque $u(x) \in F$ et $y \in F^\perp$), et ceci montre que $u^*(y) \in F^\perp$. On a donc $u^*(F^\perp) \subseteq F^\perp$.

Réciproquement, supposons $u^*(F^\perp) \subseteq F^\perp$. Comme $(F^\perp)^\perp = F$ et $(u^*)^* = u$, d'après C.1 et C.30, on obtient que $u(F) \subseteq F$, d'après ce qui précède. □

Définition C.34 (Endomorphismes normaux et auto-adjoints)**.** *Soit E un espace* **hilbertien** *de dimension n et soit $u \in \mathrm{End}(E)$.*

1. *On dit que u est* **auto-adjoint** *(ou* hermitien*) si $u^* = u$.*
2. *On dit que u est un endomorphisme* **unitaire** *s'il est inversible et $u^{-1} = u^*$ (*cf. *C.28).*
3. *On dit que u est un endomorphisme* **anti-hermitien** *si $u^* = -u$.*
4. *Enfin, on dit que u est un endomorphisme* **normal** *s'il* **commute à son adjoint** *u^*,* i.e. *si l'on a $u\,u^* = u^*\,u$. Ceci englobe les trois cas précédents.*

Rappelons et complétons la définition C.8 :

Définition C.35 (Matrices hermitiennes ou anti-hermitiennes)**.** *Une matrice $A \in M_n(\mathbb{C})$ est dite* **anti-hermitienne** *(resp.* hermitienne*,* cf. *C.8) si $\boxed{{}^t\bar{A} = -A}$ (resp. si ${}^t\bar{A} = A$).*

Observons que si A est une matrice anti-hermitienne *(resp. hermitienne), ses coefficients diagonaux a_{ii} vérifient $\bar{a_{ii}} = -a_{ii}$ (resp. $\bar{a_{ii}} = a_{ii}$) donc sont* imaginaires purs *(resp. réels).*

Théorème C.36 (Diagonalisation des endomorphismes normaux)**.** *Soient E muni de $(\ |\ )$ un espace hilbertien de dimension n, et u un endomorphisme normal. Alors, u est diagonalisable et les espaces propres sont deux à deux orthogonaux. Par conséquent, il existe une b.o.n. de E formée de vecteurs propres de u.*

Démonstration. On procède par récurrence sur $n = \dim E$. C'est ok si $n = 1$, donc on peut supposer $n \geq 2$ et le résultat établi pour $n - 1$. Comme $\mathbb{C}$ est algébriquement clos, le polynôme caractéristique $P_u(X)$ admet au moins une racine λ dans $\mathbb{C}$, et λ est valeur propre de u. Soit V_λ

l'espace propre associé, il est **stable par** u^* : en effet, comme u et u^* commutent, on a, pour tout $x \in V_\lambda$:

$$u(u^*(x)) = u^*(u(x)) = u^*(\lambda x) = \lambda\, u^*(x), \qquad \text{d'où} \qquad u^*(x) \in V_\lambda.$$

Donc, d'après le lemme C.33, l'orthogonal $G = V_\lambda^\perp$ est stable par u et par u^*. D'autre part, d'après C.12, on a $E = V_\lambda \oplus G$ et $\dim G = \dim E - \dim V_\lambda < \dim E$.

Notons u_G (resp. u_G^*) la restriction de u (resp. u^*) à G, alors pour tout $x, y \in G$, on a $u_G(x) = u(x)$ et $u_G^*(y) = u^*(y)$ et donc :

$$(u_G(x) \mid y) = (u(x) \mid y) = (x \mid u^*(y)) = (x \mid u_G^*(y))$$

ce qui montre que l'adjoint de u_G est la restriction de u^* à G. Comme u et u^* commutent, il en est de même de leurs restrictions à G, *i.e.* u_G est un endomorphisme normal de $G = V_\lambda^\perp$. Alors, par hypothèse de récurrence, $u_{V_\lambda^\perp}$ est diagonalisable, et ses espaces propres sont deux à deux orthogonaux. Comme $E = V_\lambda \oplus V_\lambda^\perp$, on obtient la même conclusion pour u. Ceci prouve qu'il existe une b.o.n. $\mathfrak{B} = (e_1, \dots, e_n)$ de E formée de vecteurs propres de u.

Il en résulte que les espaces propres de u sont deux à deux orthogonaux : en effet, soient $\mu_1, \dots, \mu_p$ les valeurs propres, deux à deux distinctes, de u et $V_1, \dots, V_p$ les espaces propres associés. Alors $E = V_1 \oplus \cdots \oplus V_p$ et donc, notant $d_q = \dim V_q$ pour $q = 1, \dots, p$, on a :

$$n = d_1 + \cdots + d_p. \tag{1}$$

Pour chaque $q = 1, \dots, p$, soit d'_q le nombre d'indices $i \in \{1, \dots, n\}$ tels que le coefficient diagonal λ_i de $D = \mathrm{Mat}_{\mathfrak{B}}(u)$ égale μ_q (*i.e.* $u(e_i) = \mu_q e_i$) et soit V'_q le sous-espace de V_q engendré ces e_i ; comme les e_i sont linéairement indépendants et comme V'_q est un sous-espace de V_q, on a :

$$d'_q = \dim V'_q \leq d_q. \tag{2}$$

D'une part, comme chaque e_i appartient à un V'_q et à un seul, on a :

$$n = d'_1 + \cdots + d'_p. \tag{3}$$

Il en résulte que, pour chaque q, l'inégalité $d'_q \leq d_q$ est une égalité, d'où $V'_q = V_q$. Ceci montre que chaque V_q est engendré par les éléments $e_i \in \mathfrak{B}$ qu'il contient. Comme les e_i sont deux à deux orthogonaux, on en déduit que V_q et $V_{q'}$ sont orthogonaux si $q \neq q'$. Ceci achève la démonstration du théorème. □

On en déduit, en particulier, le théorème suivant.

Théorème C.37 (Diagonalisation des matrices hermitiennes, unitaires, ou anti-hermitiennes)**.** *On munit $\mathbb{C}^n$ du produit scalaire hilbertien standard. Soit $A \in M_n(\mathbb{C})$.*

1. *Si A est* **hermitienne** *(*i.e. *${}^t\bar{A} = A$, alors A est diagonalisable dans une base orthonormée $\mathfrak{B}$,* i.e. *il existe $P \in \mathrm{U}(n)$ telle que $P^{-1}AP = D$ soit une matrice diagonale. De plus, les valeurs propres de A sont* **réelles**.
2. *Si A est* **unitaire** *(*i.e. *si $A \in U(n)$), alors A est diagonalisable dans une base orthonormée $\mathfrak{B}$,* i.e. *il existe $P \in \mathrm{U}(n)$ telle que $P^{-1}AP = D$ soit une matrice diagonale. De plus, les valeurs propres de A sont des nombres complexes* **de module** 1.
3. *Si A est* **anti-hermitienne** *(*i.e. *${}^t\bar{A} = -A$), alors A est diagonalisable dans une base orthonormée $\mathfrak{B}$,* i.e. *il existe $P \in \mathrm{U}(n)$ telle que $P^{-1}AP = D$ soit une matrice diagonale. De plus, les valeurs propres de A sont* **imaginaires pures**.

Démonstration. Dans chaque cas, l'assertion « A est diagonalisable dans une base orthonormée $\mathfrak{B}$ » découle du théorème précédent. Comme la base canonique $\mathfrak{B}_0$ est elle-même orthonormée, la matrice de passage $P = \mathrm{Mat}_{\mathfrak{B}_0}(\mathfrak{B})$ appartient à U(n), d'où la 2ème assertion. Reste à voir l'assertion concernant les valeurs propres. On a

$$\bar{D} = {}^t\bar{D} = {}^t\bar{P}\,{}^t\bar{A}\,{}^t\bar{P^{-1}} = P^{-1}\,{}^t\bar{A}\,P = \begin{cases} P^{-1}AP = D & \text{si } A \text{ est hermitienne} \\ P^{-1}A^{-1}P = D^{-1} & \text{si } A \text{ est unitaire} \\ -P^{-1}AP = -D & \text{si } A \text{ est anti-hermitienne.} \end{cases}$$

Il en résulte que les termes diagonaux λ_i de D vérifient, respectivement, $\bar{\lambda_i} = \lambda_i$ (resp. $= \lambda_i^{-1}$, resp. $= -\lambda_i$), donc sont réels (resp. de module 1, resp. imaginaires purs). Le théorème est démontré. □

Remarque C.38. *Le point (1) du théorème précédent fournit une autre démonstration de la proposition 4.58 et donc du théorème 4.56.*

C.5 Forme normale des éléments de O(n)

On a décrit au Chap. 6 les éléments de O(2) et O(3). On va voir maintenant la « forme normale » (= une matrice aussi simple que possible) des éléments de O(n), pour $n \geq 3$ arbitraire. On note $\mathfrak{B}_0$ la base canonique de $\mathbb{R}^n$.

Théorème C.39 (Forme normale des éléments de O(n))**.** *Soient $A \in \mathrm{O}(n)$ et f l'endomorphisme de $V = \mathbb{R}^n$ associé à A. Notons $V_+ = \mathrm{Ker}(A - I_n)$ (resp. $V_- = \mathrm{Ker}(A + I_n)$) l'espace propre associé à la valeur propre 1 (resp. -1) et $p = \dim V_+$, $q = \dim V_-$. Alors il existe des bases orthonormées $\mathfrak{B}_+ = (x_1, \ldots, x_p)$ de V_+, $\mathfrak{B}_- = (y_1, \ldots, y_q)$ de V_-, et $\mathcal{C} = (v_1, u_1, \ldots, v_r, u_r)$ de $E = (V_+ \oplus V_-)^\perp$, et $\theta_1, \ldots, \theta_r \in]-\pi, \pi[- \{0\}$ telles que, notant $\mathfrak{B}$ la base orthonormée $\mathfrak{B}_+ \cup \mathfrak{B}_- \cup \mathcal{C}$ de V et P la matrice de passage $\mathrm{Mat}_{\mathfrak{B}_0}(\mathfrak{B}) \in \mathrm{O}(n)$, on ait*

$$P^{-1}AP = \mathrm{Mat}_{\mathfrak{B}}(f) = \left(\begin{array}{c|c|c|c|c} I_p & 0 & 0 & \cdots & 0 \\ \hline 0 & -I_q & 0 & \cdots & 0 \\ \hline 0 & 0 & R(\theta_1) & \ddots & \vdots \\ \hline \vdots & \ddots & \ddots & \ddots & 0 \\ \hline 0 & \cdots & 0 & 0 & R(\theta_r) \end{array}\right).$$

où $R(\theta)$ désigne la matrice $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \in \mathrm{O}(2)$. *(En particulier,* $\dim E = 2r$ *est paire). De plus, $\theta_1, \ldots, \theta_r \in]-\pi, \pi[- \{0\}$ sont uniques au signe près.*

Pour la démonstration, on a besoin du lemme suivant.

Lemme C.40. *Soit u une isométrie de l'espace euclidien V, et soit F un sous-espace vectoriel stable par u,* i.e. *$u(F) \subseteq F$. Alors :*

1. *On a $u(F) = F$ et donc $u^{-1}(F) = F$.*
2. *On a $u(F^\perp) = F^\perp = u^{-1}(F^\perp)$.*

Démonstration. D'abord l'isométrie u est bijective (*cf.* 4.46), donc en particulier injective, donc $u(F)$ a même dimension que F. Par conséquent, l'inclusion $u(F) \subseteq F$ entraîne $u(F) = F$, d'où

aussi $F = u^{-1}(F)$. Ceci prouve (1). Le même argument montre que, pour prouver (2), il suffit de prouver que $u(F^\perp) \subseteq F^\perp$. Soient $y \in F^\perp$ et $x \in F$, comme u est une isométrie, on a

$$(u(y) \mid x) = (y \mid u^{-1}(x)) = 0,$$

la 2ème égalité puisque $u^{-1}(x) \in F$ d'après (1). Ceci montre que $u(y) \in F^\perp$, d'où l'assertion (2). □

Démonstration. Commençons maintenant la démonstration du théorème C.39. Comme $V_+ \oplus V_-$ est stable par f alors, d'après le lemme, il en est de même de $E = (V_+ \oplus V_-)^\perp$. Notons f_E la restriction de f à E. Alors 1 et -1 ne sont pas valeurs propres de f_E, puisque $\mathrm{Ker}(f_E - \mathrm{id}_E) = \mathrm{Ker}(f - \mathrm{id}_V) \cap E = V_+ \cap E = \{0\}$ et de même $\mathrm{Ker}(f_E + \mathrm{id}_E) = V_- \cap E = \{0\}$.

Soit $\mathfrak{B}_+$ (resp. $\mathfrak{B}_-$) une b.o.n. de V_+ (resp. V_-). D'après **??**, on sait que V_+ et V_- sont orthogonaux, et que les valeurs propres réelles de f ne peuvent être que 1 et -1. Donc, d'une part, $\mathfrak{B}_+ \cup \mathfrak{B}_-$ est une b.o.n. de $V_+ \oplus V_-$ et, d'autre part, f_E n'a pas de valeurs propres réelles. Or, on a le lemme suivant :

Lemme C.41. *Soit W un espace euclidien de dimension $m > 0$, et soit f une isométrie de W n'ayant pas de valeurs propres réelles (*i.e. *telle que 1 et -1 ne soient pas valeurs propres de f). Alors il existe deux vecteurs* **unitaires et orthogonaux** *u et v et $\theta \in]-\pi, \pi[- \{0\}$ tels que :*

$$f(u) = \cos(\theta)\, u - \sin(\theta)\, v, \qquad f(v) = \sin(\theta)\, u + \cos(\theta)\, v$$

i.e. *le plan $P = \textsc{Vect}(u, v)$ est stable par f et l'on a*

$$\mathrm{Mat}_{(u,v)}(f_P) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \qquad \mathrm{Mat}_{(v,u)}(f_P) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

En particulier, on a $\dim W \geq 2$.

Admettons pour le moment ce lemme, et achevons la démonstration du théorème C.39. D'après le lemme précédent, il existe dans E un plan P_1 stable par f, une b.o.n. $\mathcal{C}_1 = (v_1, u_1)$ de P_1 et $\theta_1 \in]-\pi, \pi[- \{0\}$ tels que $\mathrm{Mat}_{\mathcal{C}_1}(f) = R(\theta_1)$. Notons E_1 l'orthogonal de P_1 dans E, *i.e.* :

$$E_1 = \{x \in E \mid (x \mid y) = 0, \quad \forall y \in P_1\}.$$

D'après le lemme C.40, E_1 est stable par f. Bien sûr, la restriction f_{E_1} de f à E_1 n'a pas de valeurs propres réelles (puisque f n'en avait pas) donc on peut à nouveau appliquer le lemme C.41 : il existe dans E_1 un plan P_2 stable par f, une b.o.n. $\mathcal{C}_2 = (v_2, u_2)$ de P_2 et $\theta_2 \in]-\pi, \pi[- \{0\}$ tels que $\mathrm{Mat}_{\mathcal{C}_2}(f) = R(\theta_2)$. Notons E_2 l'orthogonal de P_2 dans E_1. Si $E_2 \neq 0$, on peut recommencer...On obtient ainsi qu'il existe une b.o.n.

$$\mathcal{C} = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_r = (v_1, u_1, \ldots, v_r, u_r)$$

de E (en particulier, $\dim E = 2r$ est pair) et $\theta_1, \ldots, \theta_r \in]-\pi, \pi[- \{0\}$ tels que

$$(*) \qquad \mathrm{Mat}_{\mathcal{C}}(f_E) = \left(\begin{array}{c|c|c} R(\theta_1) & 0 & 0 \\ \hline 0 & \ddots & 0 \\ \hline 0 & 0 & R(\theta_r) \end{array}\right)$$

et alors $\mathfrak{B} = \mathfrak{B}_+ \cup \mathfrak{B}_- \cup \mathcal{C}$ est un b.o.n. de V telle que $\mathrm{Mat}_{\mathfrak{B}}(f)$ ait la forme indiquée. Ceci prouve l'existence.

Montrons l'unicité au signe près de $\theta_1, \dots, \theta_r$, *i.e.* montrons l'unicité des paires $\pm\theta_1, \dots, \pm\theta_r$. Comme le polynôme caractéristique de $R(\theta)$ est

$$X^2 - 2\cos(\theta)X + 1 = (X - e^{i\theta})(X - e^{-i\theta})$$

alors $(*)$ ci-dessus montre que le polynôme caractéristique de f_E est $\prod_{s=1}^{r}\left((X - e^{i\theta_s})(X - e^{-i\theta_s})\right)$ et que ses racines dans $\mathbb{C}$ sont :

$$e^{i\theta_1}, e^{-i\theta_1}, \cdots, e^{i\theta_r}, e^{-i\theta_r},$$

et donc $\pm\theta_1, \dots, \pm\theta_r$ sont uniquement déterminés. Enfin, en général on ne peut pas faire mieux que de déterminer les θ_s au signe près, puisque dans la base (u_s, v_s) la matrice de f_{P_s} est $R(-\theta_s)$. Ceci achève la démonstration du théorème C.39, modulo la démonstration du lemme C.41. □

Avant de démontrer le lemme C.41, faisons les remarques suivantes.

Remarque C.42. *(1) En dimension* 2*, on détermine le signe de θ en choisissant une orientation de E, donnée par le choix d'une b.o.n. $\mathfrak{B}_0$ de E. Alors pour toute b.o.n. $\mathfrak{B}$ directe (*i.e. *telle que* $\det_{\mathfrak{B}_0}(\mathfrak{B}) = 1$*), on a* $\mathrm{Mat}_{\mathfrak{B}}(f) = R(\theta)$ *(*cf. **??**).*

(2) De même, en dimension 3*, on choisit l'orientation de $\mathbb{R}^3$ donnée par la base canonique $\mathfrak{B}_0$. Si $f \in \mathrm{SO}(3)$ et $f \neq \mathrm{id}$, alors f possède un « axe de rotation » $D = \mathrm{Ker}(f - \mathrm{id})$ qui est une droite vectorielle ; on oriente D en choisissant un vecteur unitaire $u \in D$. Ayant fait ces choix, « l'angle de rotation » θ est uniquement déterminé par la condition que pour toute b.o.n. (v_1, v_2) du plan $P = D^\perp$ telle que la b.o.n. (v_1, v_2, u) de $\mathbb{R}^3$ soit directe, on a* $\mathrm{Mat}_{(v_1,v_2)}(f_P) = R(\theta)$ *(*cf. **??**).*

(3) Attention*! En dimension paire ≥ 4, une rotation ne possède pas nécessairement d'« axe de rotation »,* i.e. *on peut avoir* $\mathrm{Ker}(f - \mathrm{id}) = \{0\}$*, c'est le cas par exemple pour*

$$f = \left(\begin{array}{c|c} R(\theta_1) & 0 \\ \hline 0 & R(\theta_2) \end{array}\right) \in O(4)$$

avec $\theta_1, \theta_2 \in]-\pi, \pi[- \{0\}$.

Démonstration. Démontrons maintenant le lemme C.41. Fixons une base $\mathfrak{B} = (e_1, \dots, e_m)$ de W, ce qui permet d'identifier W à $\mathbb{R}^m$ et f à la matrice $A = \mathrm{Mat}_{\mathfrak{B}}(f) \in M_m(\mathbb{R})$. On plonge $\mathbb{R}^m$ dans $\mathbb{C}^m$, c'est-à-dire, on écrit :

$$\mathbb{R}^m = \{(x_1, \dots, x_m) \in \mathbb{C}^m \mid x_i \in \mathbb{R}, \quad \forall i = 1, \dots, m\}.$$

Alors, tout $w = (z_1, \dots, z_m) \in \mathbb{C}^m$ s'écrit de façon unique

$$w = u + iv \qquad \text{avec} \qquad u, v \in \mathbb{R}^m \quad : \quad \text{on a} \quad \begin{cases} u = (x_1, \dots, x_m) & \text{avec } x_j = \mathrm{Re}(z_j) \\ v = (y_1, \dots, y_m) & \text{avec } y_j = \mathrm{Im}(z_j). \end{cases}$$

On notera $\boxed{u = \mathrm{Re}(w)}$ et $\boxed{v = \mathrm{Im}(w).}$ Si $\lambda = a + ib \in \mathbb{C}$ (avec $a, b \in \mathbb{R}$), alors λw est le vecteur :

$$(a + ib)(u + iv) = \underbrace{(au - bv)}_{\in \mathbb{R}^m} + i\,\underbrace{(bu + av)}_{\in \mathbb{R}^m}. \tag{1}$$

Si l'on note $\bar{w}$ le vecteur $u - iv$, on a donc

$$\bar{\lambda}\bar{w} = (a - ib)(u - iv) = \underbrace{(au - bv)}_{\in \mathbb{R}^m} - i\,\underbrace{(bu + av)}_{\in \mathbb{R}^m} = \bar{\lambda w}. \tag{2}$$

Plus généralement, si $B \in M_m(\mathbb{R})$, alors les vecteurs Bu et Bv appartiennent encore à $\mathbb{R}^m$, et l'on a :

$$Bw = B(u+iv) = Bu + iBv \qquad \text{et} \qquad B\bar{w} = B(u-iv) = Bu - iBv = B\bar{w}. \tag{3}$$

Appliquons ce qui précède dans le cas suivant. Soit $\lambda = a + ib \in \mathbb{C} - \mathbb{R}$ une valeur propre de A, et soit $w \in \mathbb{C}^m$ un vecteur propre associé. Écrivons $w = u + iv$, avec $u, v \in \mathbb{R}^m$. Alors

$$Au + iAv = Aw = \lambda w = (au - bv) + i(bu + av) \qquad \text{d'où} \quad \begin{cases} Au = au - bv \\ Av = bu + av. \end{cases} \tag{4}$$

D'autre part, d'après (2) et (3) on a :

$$A\bar{w} = A\bar{w} = \lambda\bar{w} = \bar{\lambda}\bar{w} \tag{5}$$

donc $\bar{w}$ est vecteur propre de A pour la valeur propre $\bar{\lambda}$. Donc, puisque $\bar{\lambda} \neq \lambda$ (car $\lambda \notin \mathbb{R}$), les vecteurs propres w et $\bar{w}$ sont linéairement indépendants sur $\mathbb{C}$. Comme $w = u + iv$ et $\bar{w} = u - iv$, on en déduit que u, v sont linéairement indépendants sur $\mathbb{C}$ (sinon w et $\bar{w}$ seraient liés), donc a fortiori sur $\mathbb{R}$.

Il en résulte que le sous-espace vectoriel $P = \mathbb{R}u + \mathbb{R}v$ de $\mathbb{R}^m$ est de dimension 2, et d'après (4) il est stable par f et l'on a :

$$\mathrm{Mat}_{(u,v)}(f_P) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad \mathrm{Mat}_{(v,u)}(f_P) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}. \tag{6}$$

Tout ce qui précède est valable pour une matrice $A \in M_m(\mathbb{R})$ arbitraire, une valeur propre complexe non réelle $\lambda = a + ib$, et un vecteur propre $w = u + iv \in \mathbb{C}^m$ associé à λ.

Utilisons maintenant l'hypothèse additionnelle $A \in \mathrm{O}(m)$, *i.e.* ${}^tAA = I_m$. On étend le produit scalaire euclidien $(\ |\ )$ sur $\mathbb{R}^m$ en le produit scalaire hilbertien standard sur $\mathbb{C}^m$, qu'on notera $\langle\ |\ \rangle$, *i.e.*

$$\forall W = \begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix},\ \forall Z = \begin{pmatrix} z_1 \\ \vdots \\ z_m \end{pmatrix} \in \mathbb{C}^m, \qquad \langle W \mid Z\rangle = {}^tW\bar{Z} = w_1\,\bar{z_1} + \cdots + w_m\bar{z}_m.$$

Remarquons d'abord que si $W, Z \in \mathbb{R}^m$, alors $\langle W \mid Z\rangle = (W \mid Z)$, *i.e.* la restriction à $\mathbb{R}^m$ de $\langle\ |\ \rangle$ coïncide avec le produit scalaire euclidien. De plus, si l'on écrit $W = U + iV$ et $Z = X + iY$, avec $U, V, X, Y \in \mathbb{R}^m$, alors $\langle W \mid Z\rangle$ égale :

$$\langle U+iV \mid X+iY\rangle = \langle U \mid X\rangle + \langle V \mid Y\rangle + i\Big(\langle V \mid X\rangle - \langle U \mid Y\rangle\Big) = (U \mid X) + (V \mid Y) + i\Big[(V \mid X) - (Y \mid Y)\Big].$$

D'autre part, comme $A = \bar{A}$ et ${}^tAA = I_m$, on a $A \in \mathrm{U}(m)$ et donc, pour tout $W, Z \in \mathbb{C}^m$:

$$\langle AW \mid AZ\rangle = \langle W \mid Z\rangle. \tag{7}$$

Soient λ, w comme plus haut, avec $Aw = \lambda w$. On a vu qu'on a aussi $A\bar{w} = \bar{\lambda}\bar{w}$, donc w et $\bar{w}$ appartiennent aux espaces propres V_λ et $V_{\bar{\lambda}}$, qui sont orthogonaux, d'après C.37. Écrivant $w = u + iv$, avec $u, v \in \mathbb{R}^m$, on a donc :

$$0 = \langle u + iv \mid u - iv\rangle = (u \mid u) - (v \mid v) + 2i(u \mid v),$$

d'où $(u \mid v) = 0$ et $(u \mid u) = (v \mid v)$, donc $u, v \in \mathbb{R}^m$ sont orthogonaux et de même norme pour le produit scalaire euclidien. Remplaçant w par $\dfrac{1}{\|u\|}w$, on se ramène alors au cas où u, v sont

orthogonaux et unitaires. Alors $\mathcal{C} = (v, u)$ est une base orthonormée du plan P, et d'après (6) on a $\mathrm{Mat}_{\mathcal{C}}(f_P) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, avec $a, b \in \mathbb{R}$.

Enfin, comme f est une isométrie et n'a pas ± 1 comme valeurs propres, il en est de même de f_P, et donc $a^2 + b^2 = 1$ et il existe un unique $\theta \in]-\pi, \pi[- \{0\}$ tel que $a = \cos\theta$ et $b = \sin\theta$ (d'où $\lambda = e^{i\theta}$). Ceci achève la preuve du lemme C.41 et donc du théorème C.39. □

C.6 Appendice (†) : espaces préhilbertiens réels ou complexes

Si E, muni de $(\ |\ )$, est un $\mathbb{C}$-espace vectoriel (resp. $\mathbb{R}$-espace vectoriel) de dimension infinie muni d'un produit scalaire hilbertien (resp. euclidien), on dit que E est un espace **préhilbertien** complexe (resp. réel). Dans ce cas on sait, d'après l'inégalité de Cauchy-Schwarz, que $\|x\| = \sqrt{(x \mid x)}$ est une *norme* sur E. On dit alors que E est un espace hilbertien complexe (resp. réel) s'il est **complet** pour cette norme, *i.e.* si toute suite de Cauchy converge (ceci est automatiquement vérifié lorsque E est de dimension finie).

Ces espaces jouent un rôle important en Analyse. Par exemple, le $\mathbb{R}$-espace vectoriel $E = \mathcal{C}^0([0,1], \mathbb{R})$ des fonctions continues $f : [0,1] \to \mathbb{R}$, muni du produit scalaire euclidien

$$(f \mid g) = \int_0^1 f(t)g(t)dt\,,$$

est un espace préhilbertien réel. Il n'est pas complet pour la norme euclidienne $\|f\|_2 = \int_0^1 f^2(t)dt$, mais il se plonge dans l'espace $L^2([0,1], \mathbb{R})$ des (classes de) fonctions $f : [0,1] \to \mathbb{R}$ qui sont de carré intégrable au sens de Lebesgue (*i.e.* f est mesurable et $\int_0^1 f^2(t)dt < \infty$), et $L^2([0,1], \mathbb{R})$ muni du produit scalaire euclidien

$$(f \mid g) = \int_0^1 f(t)g(t)dt\,,$$

est un espace de Hilbert réel, *i.e.* il est complet pour la norme $\|f\|_2 = \int_0^1 f^2(t)dt$. (On parle ici de classes de fonctions, car on identifie deux fonctions f et g si elles coïncident en dehors d'un ensemble de mesure nulle, *i.e.* si $f - g$ est nulle presque partout.)

De même, le $\mathbb{C}$-espace vectoriel $E = \mathcal{C}^0([0,1], \mathbb{C})$ des fonctions continues $f : [0,1] \to \mathbb{C}$, muni du produit scalaire hilbertien

$$(f \mid g) = \int_0^1 f(t)\,\bar{g(t)}\,dt\,,$$

est un espace préhilbertien complexe. Il n'est pas complet pour la norme hilbertienne $\|f\|_2 = \int_0^1 |f(t)|^2 dt$, mais il se plonge dans l'espace $L^2([0,1], \mathbb{C})$ des (classes de) fonctions $f : [0,1] \to \mathbb{C}$ qui sont de carré intégrable au sens de Lebesgue, et $L^2([0,1], \mathbb{C})$ muni du produit scalaire hilbertien

$$(f \mid g) = \int_0^1 f(t)\,\bar{g(t)}\,dt\,,$$

est un espace de Hilbert complexe, *i.e.* il est complet pour la norme $\|f\|_2 = \int_0^1 |f(t)|^2 dt$.

Bibliographie

[1] Yves Coudène, *Algèbre linéaire et bilinéaire*, polycopié.

[2] Patrick Polo, Laurent Koelblen, Vincent Humilière, *Algèbre linéaire et géométrie*, polycopié.

[3] Lean prover community, *The natural number game*, jeu en ligne.

[4] William Lawvere et Robert Roseburgh, *Sets for mathematics*, Cambridge University Press.