Algèbre linéaire et bilinéaire

2023-2024

Table des matières

1 Algèbre linéaire **2**

1.1 Espaces vectoriels, applications linéaires . . . 2
1.1.1 Définitions et premières propriétés . . . 2
1.1.2 Familles libres, génératrices, bases . . . 4
1.1.3 Sommes de sous-espaces . . . 6
1.1.4 Dualité . . . 6
1.1.5 Espaces vectoriels quotients . . . 7
1.1.6 Produits tensoriels . . . 8
1.2 Applications multilinéaires . . . 11
1.2.1 Matrices . . . 14
1.2.2 À propos de propriétés universelles . . . 15
1.2.3 Exercices . . . 16
1.3 Réduction des endomorphismes . . . 18
1.3.1 Polynômes d'endomorphismes et lemme des noyaux . . . 18
1.3.2 Le théorème de Cayley-Hamilton . . . 19
1.3.3 Endomorphismes diagonalisables . . . 20
1.3.4 Exercices . . . 20
1.4 Décompositions usuelles . . . 21
1.4.1 Endomorphismes nilpotents . . . 21
1.4.2 Réduction de Jordan . . . 22
1.4.3 Décomposition LU . . . 23
1.4.4 Décomposition de Jordan-Chevalley . . . 23
1.4.5 Exercices . . . 23
1.5 Topologie . . . 25
1.5.1 Normes matricielles . . . 25
1.5.2 Propriétés topologiques . . . 26
1.5.3 Exponentielles de matrices . . . 26
1.5.4 Exercices . . . 27

2 Algèbre bilinéaire **28**

2.1 Formes bilinéaires et formes quadratiques . . . 28
2.1.1 Groupe orthogonal d'une forme quadratique . . . 30
2.1.2 Exercices . . . 30
2.2 Classification des formes quadratiques . . . 31
2.2.1 Méthode de Gauss . . . 32
2.2.2 Formes quadratiques complexes . . . 33

2.2.3 Formes quadratiques réelles, signature . . . 33
2.2.4 Formes quadratiques sur un corps fini . . . 33
2.2.5 Exercices . . . 34
2.3 Théorie de Witt . . . 36
2.3.1 Sous-espaces isotropes . . . 36
2.3.2 Théorème de Witt . . . 36
2.4 Espaces euclidiens, hermitiens . . . 37
2.4.1 Endomorphisme adjoint . . . 38
2.4.2 Exercices . . . 38
2.5 Réduction des endomorphismes normaux . . . 38
2.5.1 Réduction des endomorphismes normaux . . . 39
2.5.2 Théorème spectral . . . 39
2.5.3 Endomorphismes orthogonaux et unitaires . . . 39
2.5.4 Décomposition polaire . . . 40
2.5.5 Exercices . . . 40

1 Algèbre linéaire

Dans l'ensemble de ce document, la lettre K désignera un corps commutatif quelconque.

1.1 Espaces vectoriels, applications linéaires

1.1.1 Définitions et premières propriétés

Commençons par donner les définitions et propriétés élémentaires des espaces vectoriels et des applications linéaires.

Définition 1.1.1. Un *espace vectoriel* sur K (ou K-espace vectoriel) est la donnée d'un triplet $(E, +, \cdot)$ possédant les propriétés suivantes :
- le couple $(E, +)$ est un groupe abélien ;
- $\cdot : K \times E \to E$ est une application telle que pour tous $\lambda, \mu \in K$ et $x, y \in E$, on ait $\lambda\mu \cdot x = \lambda \cdot (\mu \cdot x)$ et $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$.

Dans ce cas, l'application $\cdot$ s'appelle *multiplication externe*, les éléments de E s'appellent les vecteurs et ceux de K s'appellent les scalaires. On omet souvent le symbole $\cdot$, et on note simplement λx pour $\lambda \cdot x$. Lorsqu'il n'y a pas de confusion possible, on parlera souvent du K-espace vectoriel E (plutôt que $(E, +, \cdot)$).

Exemple 1.1.2. Voici quelques exemples élémentaires :
- Le corps K muni de son addition et de sa multiplication constitue un K-espace vectoriel.
- L'ensemble $K^n = \{(x_1, \cdots, x_n) \mid \forall i, x_i \in K\}$, muni de l'addition composante par composante, et de la multiplication externe $\lambda \cdot (x_1, \cdots, x_n) = (\lambda x_1, \cdots, \lambda x_n)$ est un K-espace vectoriel.
- L'ensemble $K[X]$ des polynômes en l'indéterminée X et à coefficients dans K forme un K-espace vectoriel.

Définition 1.1.3. Soit E un K-espace vectoriel. Un sous-espace vectoriel de E est un sous-ensemble de E, stable par addition et multiplication externe, et sur lequel ces lois induisent une structure de K-espace vectoriel.

La caractérisation suivante est très utile en pratique :

Proposition 1.1.4. *Soit E un K-espace vectoriel et $F \subset E$, alors F est un sous-espace vectoriel de E si et seulement si*

— $0 \in F$

— $\forall x, y \in F$, $\forall \lambda \in K$, $\lambda x + y \in F$.

Démonstration. La première condition, et la deuxième condition pour $\lambda = 1$, montrent que F est un sous-groupe de E. La deuxième condition avec $y = 0$ montre que F est stable par multiplication externe. □

Exemple 1.1.5. Si $n \leq m$, alors $K^n \times \{(0, \ldots, 0)\}$ est un sous-espace vectoriel de K^m.

Lemme 1.1.6. *Une intersection quelconque de sous-espaces vectoriels de E est un sous-espace vectoriel de E. En particulier, si $X \subset E$, le plus petit sous-espace vectoriel de E contenant X existe, et est égal à l'intersection de tous les sous-espaces vectoriels de E contenant X : on le note Vect(X) ou $\langle X \rangle$.*

Démonstration. Soit $\mathcal{F}$ une famille de sous-espaces vectoriels de E. Comme intersection de sous-groupes de $(E, +)$, c'est un sous-groupe de $(E, +)$. Comme chacun des $F \in \mathcal{F}$ est stable par multiplication externe, leur intersection l'est aussi. Enfin, si $x, y \in \cap_{F \in \mathcal{F}} F$, alors pour tout $F \in \mathcal{F}$ et pour tout $\lambda \in K$, $\lambda x + y \in F$. Ainsi, $\cap_{F \in \mathcal{F}} F$ est bien un sous-espace vectoriel de E. □

Définition 1.1.7. Soit E, F deux K-espaces vectoriels, et soit $f : E \to F$ une application. On dit que f est une *application linéaire* lorsque l'on a pour tous $\lambda \in K$, $x, y \in E$:

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

On notera $\mathcal{L}(E, F)$ l'ensemble des applications linéaires de E vers F.

Proposition 1.1.8. *Soit E, F deux K-espaces vectoriels. L'ensemble $\mathcal{L}(E, F)$, muni de l'addition ponctuelle et de la multiplication externe déduite de celle de F, constitue un K-espace vectoriel.*

Démonstration. Montrons que $\mathcal{L}(E, F)$ muni de l'addition ponctuelle est un groupe abélien. Il est clair que l'application nulle est linéaire et est élément neutre pour cette loi. Si f, g sont linéaires, alors $f + g$ l'est aussi. En effet, pour $\lambda \in K$ et $x, y \in E$, on a :

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

De plus, cette loi est associative et commutative car la loi de F l'est. Vérifions maintenant que pour $f, g \in \mathcal{L}(E, F)$ et $\lambda \in K$, on a bien $\lambda f + g \in \mathcal{L}(E, F)$. Cela découle directement de la définition. Enfin, la multiplication externe a les propriétés demandées car F est un K-espace vectoriel. □

Remarque 1.1.9. D'une manière générale, si S est un ensemble, l'ensemble des applications de S vers un K-espace vectoriel F est un K-espace vectoriel.

Exemple 1.1.10. Pour tout $1 \leq i \leq n$, l'application

$$\pi_i \ : \ \left| \begin{array}{ccc} K^n & \to & K \\ (x_1, \cdots, x_n) & \mapsto & x_i \end{array} \right.$$

est linéaire. Cette application s'appelle *projection sur la i-ème composante.*

Proposition 1.1.11. *Soit E, F, H des K-espaces vectoriels. Soit $u : E \to F$ et $g : F \to H$ des applications linéaires, alors l'application $g \circ f : E \to H$ est linéaire.*

Démonstration. Exercice. □

Proposition 1.1.12. *Soit $u : E \to E'$ une application linéaire. Alors* $\ker u$ *et Im u sont des sous-espaces vectoriels respectifs de E et E'.*

Démonstration. Montrons que $\ker u$ est un sous-espace vectoriel. Déjà, $0 \in \ker u$, et si $x, y \in \ker u$ et $\lambda \in K$, alors $u(\lambda x + y) = \lambda u(x) + u(y) = 0$.
Montrons que Im u est un sous-espace vectoriel. Soient $x, y \in E$ et $\lambda \in K$, alors $\lambda u(x) + u(y) = u(\lambda x + y)$, d'où le résultat. □

Définition 1.1.13. Une application linéaire $f : E \to F$ est appelée *isomorphisme* si elle est bijective (et son inverse est linéaire, ce qui est automatique). On note $\mathcal{L}(E)$ pour $\mathcal{L}(E, E)$. Les éléments de $\mathcal{L}(E)$ s'appellent *endomorphismes* de E. On appelle *automorphisme* de E tout endomorphisme bijectif de E.

1.1.2 Familles libres, génératrices, bases

Définition 1.1.14. Soit E un K-espace vectoriel et $X \subset E$ une famille d'éléments de E. On dit que la famille X est :

- *libre* si pour toute combinaison linéaire à support fini $y = \sum_{x \in X} \lambda_x x$ d'éléments de X, on a
$$y = 0 \Rightarrow \forall x \in X, \lambda_x = 0 \ ;$$
- *génératrice* si tout élément $y \in E$ s'écrit comme combinaison linéaire à support fini d'éléments de X ;
- *une base de E* si X est libre et génératrice.

Exemple 1.1.15. La famille E est toujours génératrice, la famille vide est toujours libre. Si $x \in E$, la famille $\{x\}$ est libre si et seulement si $x \neq 0$.

Lemme 1.1.16. *Soit E un K-espace vectoriel admettant une famille génératrice finie G de cardinal n. Soit L une famille libre de E. Alors L est finie, et son cardinal m vérifie $m \leq n$.*

Démonstration. Soit L' une sous-famille finie de L : on note $L' = (a_1, \ldots, a_m)$ et $G = (g_1, \ldots, g_n)$. On peut écrire a_1 comme combinaison linéaire de $g_1, \ldots, g_n$. Puisque $a_1 \neq 0$, l'un des coefficients de cette combinaison linéaire est non nul ; quitte à réordonner, supposons que c'est le coefficient de g_1. On en déduit que g_1 s'écrit comme combinaison linéaire de $a_1, g_2, \ldots, g_n$, de sorte que la famille $(a_1, g_2, \ldots, g_n)$ est génératrice. Ainsi, a_2 s'écrit comme combinaison linéaire de $a_1, \ldots, g_n$, et l'un des g_i a un coefficient non nul dans cette combinaison linéaire, sinon (a_1, a_2) serait liée. Comme précédemment, on obtient une famille génératrice $(a_1, a_2, g_3, \ldots, g_n)$. Finalement, par récurrence, si $m \geq n$ la famille $(a_1, \ldots, a_n)$ (après réindexation éventuelle) est génératrice. Mais alors, si $m > n$, la famille $a_1, \ldots, a_m$ est liée. On a donc montré que si $m \geq n$, alors nécessairement $m = n$. Ainsi, toute sous-famille finie de L est de cardinal au plus n ; c'est donc que L est de cardinal au plus n. □

Théorème 1.1.17. *Soit E un K-espace vectoriel. Soient L une famille libre et G une famille génératrice de E telles que $L \subset G$. Alors il existe une base B de E telle que $L \subset B \subset G$.*

Démonstration. On prouve d'abord le résultat dans le cas où G est finie. Procédons par récurrence sur $c = \mathrm{Card}(G) - \mathrm{Card}(L)$. Si $L = G$, alors L est une base de E, et le théorème est démontré. Supposons le résultat vrai pour une valeur de $c \geq 0$, et supposons que $\mathrm{Card}(G) - \mathrm{Card}(L) = c + 1$. Si L est génératrice, alors L convient. Sinon, existe $x \in G$ tel que $x \notin \langle L \rangle$. On considère $L' = L \cup \{x\}$. Par construction, L' est une famille libre et $L' \subset G$. En outre, $\mathrm{Card}(G) - \mathrm{Card}(L') = c$. Par hypothèse de récurrence, il existe une base $\mathcal{B}$ de E telle que $L \subset L' \subset \mathcal{B} \subset G$.
Supposons maintenant que E admette une famille génératrice finie Γ. Comme tout élément de Γ est combinaison linéaire d'éléments de G, G admet une sous-famille génératrice finie G'. Comme la famille L est libre, le lemme montre que toute sous-famille finie de L est de cardinal majoré par $|G'|$. On a donc $|L| \leq |G'|$. En particulier, la famille finie $L \cup G'$ est génératrice, contient L et est contenue dans G. On peut donc lui appliquer le raisonnement du théorème 1.1.17, ce qui prouve ce résultat sous l'hypothèse où E admet une famille génératrice finie (mais où G ne l'est pas nécessairement).
Dans le cas général, on utilise le lemme de Zorn appliqué à l'ensemble des parties P de $G \setminus L$ telles que $L \cup P$ soit libre : c'est un ensemble inductif, qui admet donc un élément maximal, et cet élément est une base de E. □

Proposition 1.1.18. *Toutes les bases de E ont le même cardinal.*

Démonstration. On traite seulement le cas où E admet une famille génératrice finie. Dans ce cas, il existe une base $\mathcal{B} = (b_1, \ldots, b_n)$ finie. Soit $L = (a_1, \ldots, a_m)$ une famille libre finie de cardinal m, montrons que $m \leq n$.
On peut écrire a_1 comme combinaison linéaire de $b_1, \ldots, b_n$. Puisque $a_1 \neq 0$, l'un des coefficients de cette combinaison linéaire est non nul ; quitte à réordonner, supposons que c'est le coefficient de b_1. On en déduit que b_1 s'écrit comme combinaison linéaire de $a_1, b_2, \ldots, b_n$, de sorte que la famille $(a_1, \ldots, a_n)$ est génératrice. Ainsi, a_2 s'écrit comme combinaison linéaire de $a_1, \ldots, b_n$, et l'un des b_i a un coefficient non nul dans cette combinaison linéaire, sinon (a_1, a_2) serait liée. Comme précédemment, on obtient une famille génératrice $(a_1, a_2, b_3, \ldots, b_n)$. Finalement, par récurrence, si $m \geq n$ la famille $(a_1, \ldots, a_n)$ (après réindexation éventuelle) est génératrice. Mais alors, si $m > n$, la famille $a_1, \ldots, a_m$ est liée. On a donc montré que si $m \geq n$, alors nécessairement $m = n$.
Cela suffit à prouver le théorème, car alors si $\mathcal{B}'$ est une autre base, $\mathcal{B}'$ est nécessairement finie de cardinal $m \leq n$ (toute famille à $n + 1$ éléments de E est liée), et par l'argument précédent, $n \leq m$. □

Corollaire 1.1.19. *Tout K-espace vectoriel admet une base.*

Démonstration. Cela découle du théorème précédent appliqué à $L = \emptyset$ et $G = E$. □

Définition 1.1.20. Si E admet une base de cardinal fini n, alors toutes ses bases sont de cardinal n. On appelle cette entier la *dimension* du K-espace vectoriel E, et on le note $\dim_K E$ ou simplement $\dim E$.

Exemple 1.1.21. Soit X un ensemble et $E = K^{(X)}$ l'espace des fonctions $f : X \to K$ à support fini.

Proposition 1.1.22. *L'application*

$$\begin{array}{ccc} X & \to & K^{(X)} \\ x & \mapsto & \mathbf{1}_{\{x\}} \end{array}$$

induit une bijection de X sur une base de E.

Définition 1.1.23. On appelle *rang* d'une application linéaire la dimension de son image.

Théorème 1.1.24 (Théorème du rang)**.** *Soit $f : E \to F$ linéaire. On a la relation :*

$$\dim E = \operatorname{rg}\ f + \dim \ker f.$$

Démonstration. Voir exercices. □

Corollaire 1.1.25. *Soient E, F deux K-espaces vectoriels de même dimension finie. Alors $f \in \mathcal{L}(E, F)$ est injective si et seulement si elle est bijective si et seulement si elle est surjective.*

Démonstration. L'application f est injective si et seulement si $\dim \ker f = 0$, et surjective si et seulement si $\operatorname{rg}\ f = \dim F = \dim E$. D'après le théorème du rang, ces deux assertions sont équivalentes. □

1.1.3 Sommes de sous-espaces

Définition 1.1.26 (Somme de sous-espaces)**.** Soient $E_1, \dots, E_r \subset E$ des sous-espaces vectoriels de E. La somme de ces sous-espaces est définie comme :

$$E_1 + \cdots + E_r = \{x_1 + \cdots + x_r \mid \forall 1 \leq i \leq r, x_i \in E_i\}.$$

Proposition-Définition 1.1.27 (Somme directe)**.** L'application linéaire

$$\Sigma\ :\ \begin{array}{ccc} E_1 \times \cdots \times E_r & \to & E \\ (x_1, \dots, x_r) & \mapsto & x_1 + \cdots + x_r \end{array}$$

a pour image la somme $E_1 + \cdots + E_r$. En particulier, cette somme est un sous-espace vectoriel de E. En outre, si Σ est injective, on dit que la somme est une somme directe, et on note ce sous-espace $E_1 \oplus \cdots \oplus E_r$.

Exemple 1.1.28. Si E_1, E_2 sont deux sous-espaces vectoriels, ils sont en somme directe si et seulement si pour $(x_1, x_2) \in E_1 \times E_2$, $x_1 + x_2 = 0 \Rightarrow x_1 = x_2 = 0$. Si c'est le cas, soit $x \in E_1 \cap E_2$. Alors $x + (-x) \in E_1 \oplus E_2$ et est nul, donc $x = 0$. Réciproquement, si $E_1 \cap E_2 = \{0\}$, soit $(x_1, x_2) \in E_1 \times E_2$, tels que $x_1 + x_2 = 0$. On a alors $x_1 = -x_2 \in E_2$, donc $x_1 = 0$ et $x_2 = 0$. Ainsi, les deux sous-espaces E_1 et E_2 sont en somme directe si et seulement si $E_1 \cap E_2 = \{0\}$. Cette caractérisation par l'intersection n'est plus vraie pour les sommes de davantage de sous-espaces en général.

Proposition 1.1.29. *Soit E un K-espace vectoriel et $E_1, \dots, E_r$ des sous-espaces tels que $E = \bigoplus E_i$. Pour $1 \leq i \leq r$, fixons une base $\mathcal{B}_i$ de E_i. Alors la concaténation de ces bases est une base de E. Une telle base est dite adaptée à la décomposition précédente.*

1.1.4 Dualité

Définition 1.1.30. Soit E un K-espace vectoriel. On appelle *espace vectoriel dual* de E l'espace des formes linéaires sur E, c'est-à-dire l'espace E^* des applications linéaires de E dans K.

Proposition-Définition 1.1.31. Soit E de dimension finie, et soit $(e_1, \dots, e_n)$ une base de E. Alors il existe une unique famille $(e_1^*, \dots, e_n^*)$ d'éléments de E^* telle que pour tout $1 \leq i, j \leq n$, $e_i^*(e_j) = \delta_{ij}$. Cette famille forme une base de E^*, appelée *base duale* de $(e_1, \dots, e_n)$.

Démonstration. Puisqu'une application linéaire est entièrement déterminée par l'image d'une base, les e_i^* sont bien définis de manière unique par les formules précédentes. En outre, la famille (e_i^*) est libre car si $f = \sum_{i=1}^n \lambda_i e_i^* = 0$, alors pour tout $1 \leq j \leq n$ on a $f(e_j) = 0 = \lambda_j$. Enfin, cette famille est génératrice puisque la forme linéaire f envoyant e_i sur a_i est égale à $\sum_{i=1}^n a_i e_i^*$. □

Corollaire 1.1.32. *Les K-espaces vectoriels E et E^* sont de même dimension.*

Proposition 1.1.33 (Isomorphisme canonique avec le bidual)**.** *Soit E un K-espace vectoriel de dimension finie. L'application*

$$\begin{array}{ccccc} E & \longrightarrow & & & (E^*)^* \\ x & \mapsto & \psi_x & : & \left| \begin{array}{ccc} E^* & \to & K \\ f & \mapsto & f(x) \end{array} \right. \end{array}$$

est un isomorphisme.

Démonstration. Il est clair que ψ_x ainsi définie est bien une forme linéaire sur E^*, et que l'application $x \mapsto \psi_x$ est linéaire. De plus, si $\psi_x = 0$, alors pour tout $f \in E^*$, $f(x) = 0$. Si $x \neq 0$, quitte à compléter x en une base de E, on peut définir une application $f \in E^*$ telle que $f(x) \neq 0$. Donc $x = 0$, et $x \mapsto \psi_x$ est injective. On peut conclure par égalité des dimensions de E et son bidual. □

Définition 1.1.34. Soit $u \in \mathcal{L}(E, F)$, on définit la transposée de u, comme l'application :

$${}^t u \ : \ \left| \begin{array}{ccc} F^* & \to & E^* \\ f & \mapsto & f \circ u \end{array} \right. .$$

On a ${}^t u \in \mathcal{L}(F^*, E^*)$, et la transposition est une application linéaire $\mathcal{L}(E, F)$ dans $\mathcal{L}(F^*, E^*)$.

Proposition 1.1.35. *Soient $u, v \in \mathcal{L}(E, F)$ (resp. $\mathcal{L}(F, G)$). Alors ${}^t(v \circ u) = {}^t u \circ {}^t v$.*

1.1.5 Espaces vectoriels quotients

Définition 1.1.36. Soit $F \subset E$ un sous-espace vectoriel. On appelle quotient de E par F, noté E/F, le quotient de E par la relation d'équivalence $x \sim y \Leftrightarrow x - y \in F$.

Proposition 1.1.37. *Soit $F \subset E$ un sous-espace vectoriel. Alors E/F a une structure naturelle de K-espace vectoriel pour laquelle la projection canonique $E \to E/F$ est linéaire.*

Démonstration. Notons $\pi : E \to E/F$ la projection canonique. Soient $x, x' \in E$ tels que $\pi(x) = \pi(x')$, c'est-à-dire $x - x' \in F$. Alors pour $y \in E$ on a $\pi(x + y) = \pi(x' + y)$, et pour $\lambda \in K$ on a $\pi(\lambda x) = \pi(\lambda x')$. Cela montre que pour tous $x, y \in E$ et $\lambda \in K$, $\pi(x + \lambda y)$ ne dépend que des valeurs de $\pi(x), \pi(y)$ et λ.
Ainsi, pour $\bar{x}, \bar{y} \in E/F$, on dispose de $x, y \in E$ tels que $\pi(x) = \bar{x}$ et $\pi(y) = \bar{y}$, et on peut poser $\bar{x} + \bar{y} = \pi(x + y)$. Le résultat ne dépend pas des choix de x et y, et munit bien E/F d'une structure de groupe additif. Ensuite, en posant $\lambda \bar{x} = \pi(\lambda x)$, on munit E/F d'une structure de K-espace vectoriel qui par définition fait de π une application linéaire. □

Théorème 1.1.38 (Propriété universelle du quotient)**.** *Soit E un K-espace vectoriel et $F \subset E$ un sous-espace vectoriel. Notons π la projection canonique $E \to E/F$. Alors pour tout K-espace vectoriel E' et toute application linéaire $f : E \to E'$ telle que $f_{|F} = 0$ (*i.e. *$F \subset \ker f$), il existe une unique application linéaire $\tilde{f} : E/F \to E'$ telle que $\tilde{f} \circ \pi = f$.*

Démonstration. Soit E' un K-espace vectoriel et $f : E \to E'$ linéaire, telle que $f(x) = 0$ pour tout $x \in F$. Soient $x, y \in E$. Si $x - y \in \ker f$, alors $f(x) = f(y)$. Ainsi, $\pi(x) = \pi(y) \Rightarrow f(x) = f(y)$. En particulier, l'application $\tilde{f}$ définie sur E/F par la formule $\tilde{f}(\pi(x)) = f(x)$ est bien définie. La linéarité de $\tilde{f}$ se vérifie facilement (elle découle de celles de f et π). L'unicité est claire. □

Exemple 1.1.39. Soit $f : E \to E'$ une application linéaire. Alors $\ker f$ est un sous-espace vectoriel de E, et $E/\ker f$ est un K-espace vectoriel. Pour $x \in E$ et $y \in \ker f$, on a $f(x + y) = f(x)$. Ainsi, l'image d'un élément de E par f ne dépend pas de sa classe d'équivalence modulo $\ker f$. On peut donc définir une application $\tilde{f} : E/\ker f \to E'$, qui envoie un élément de $E/\ker f$ sur l'image de n'importe lequel de ses antécédents modulo $\ker f$ par f. On vérifie que $\tilde{f}$ est linéaire. En outre, si $x \in E/\ker f$ est tel que $\tilde{f}(x) = 0$, alors x a un antécédent dans $\ker f$, et donc x est dans la classe de 0. Donc $\tilde{f}$ est une injection.

Corollaire 1.1.40. *Soit $F \subset E$ un K-espace vectoriel. Soit V un K-espace vectoriel et $I \subset \mathcal{L}(E, V)$ le sous-espace constitué des applications linéaires f telles que $\ker f \subset F$. Alors l'application $\mathcal{L}(E/F, V) \to \mathcal{L}(E, V)$ définie par $f \mapsto f \circ \pi$ induit un isomorphisme $\mathcal{L}(E/F, V) \to I$.*

Démonstration. Le fait que l'application soit bien définie résulte de $\ker \pi = F$. Sa bijectivité est une reformulation de la propriété universelle du quotient. □

Remarque 1.1.41. Le quotient E/F est l'unique espace vectoriel (à isomorphisme près) ayant la propriété universelle précédente.

Proposition 1.1.42. *Soit $F \subset E$ un sous-espace vectoriel, alors* $\dim E/F + \dim F = \dim E$.

Démonstration. Soit $\bar{\mathcal{B}_0}$ une base de E/F, et $\mathcal{B}_0$ des relevés de ces éléments dans E. Notons aussi $\mathcal{B}_1$ une base de F, et $\mathcal{B} = \mathcal{B}_0 \cup \mathcal{B}_1$. Nous allons montrer que $\mathcal{B}$ est une base de E. Tout d'abord, remarquons que cette famille est libre. En effet, toute relation de dépendance linéaire entre ses éléments fournit une relation de dépendance linéaire analogue dans E/F entre des éléments de $\bar{\mathcal{B}_0}$. Par liberté, cette dernière relation est triviale, donc la relation de départ est en fait une relation entre éléments de $\mathcal{B}_1$, et est triviale par liberté de cette famille. Montrons enfin que $\mathcal{B}$ est génératrice de E. Soit $x \in E$, et soit $\bar{x}$ sa classe dans E/F. On décompose $\bar{x}$ sur la base $\bar{\mathcal{B}_0}$, et on considère la même combinaison linéaire entre éléments de $\mathcal{B}_0$. Cette combinaison linéaire est un certain $x' \in E$, et par hypothèse $x - x' \in F$. On peut donc décomposer $x - x'$ sur $\mathcal{B}_1$, ce qui fournit du même coup une décomposition de x sur $\mathcal{B}$.
Démonstration alternative. La projection $E \to E/F$ est surjective de noyau F. Par le théorème du rang, $\dim E/F + \dim F = \dim E$.

□

1.1.6 Produits tensoriels

Nous introduisons dans cette partie la notion de produit tensoriel, qui permet de manipuler les applications bilinéaires comme des applications linéaires (mais définies sur $E \otimes F$ plutôt que $E \times F$). Pour construire formellement le produit tensoriel, nous allons utiliser la notion d'espace vectoriel libre sur un ensemble.

Définition 1.1.43. Soit X un ensemble, on appelle K-espace vectoriel libre sur X, noté H_X, l'espace des fonctions à support fini de X dans K.

Remarque 1.1.44. Le K-espace vectoriel libre sur X est un sous-espace vectoriel de l'espace des fonctions de X dans K ; une base de ce sous-espace vectoriel est donné par les fonctions $\delta_x : X \to K$ définies par $\delta_x(y) = \delta_{x,y}$ pour chaque $x \in X$. Ainsi, H_X a une base qui est en bijection avec X ; on dira souvent (un peu abusivement) que les éléments de X forment une base de H_X.

Définition 1.1.45 (Produit tensoriel d'espaces vectoriels)**.** Soit E, F des K-espaces vectoriels. Le produit tensoriel $E \otimes F$ de E et F est le quotient de l'espace vectoriel $H = H_{E\times F}$ dont une base est donnée par les éléments de $E \times F$, par le sous-espace vectoriel T (dit sous-espace des relations) engendré par les éléments de la forme :

— $(x + x', y) - (x, y) - (x', y)$;
— $(x, y + y') - (x, y) - (x, y')$;
— $\lambda(x, y) - (\lambda x, y)$;
— $\lambda(x, y) - (x, \lambda y)$,

pour $x, x' \in E$, $y, y' \in F$, $\lambda \in K$.
Pour $(x, y) \in E \times F$, on note $x \otimes y$ l'image de (x, y) par la projection canonique de H dans $E \otimes F$: l'application $(x, y) \mapsto x \otimes y$ est bilinéaire.

Proposition 1.1.46 (Propriété universelle du produit tensoriel)**.** *Soient E, F des K-espaces vectoriels. Alors pour tout K espace vectoriel G et pour toute application bilinéaire $\varphi : E \times F \to G$, il existe une unique application linéaire $\bar{\varphi} : E \otimes F \to G$ telle que $\bar{\varphi}(x \otimes y) = \varphi(x, y)$.*

Démonstration. Soit $\varphi : E \times F \to G$ une application bilinéaire. En donnant l'image d'une base, une telle application définit une unique application linéaire $f : H \to G$. Il suffit donc de montrer que le noyau de f contient T. Vérifions par exemple qu'il contient les éléments de la forme $(x + x', y) - (x, y) - (x', y)$. On a $f((x + x', y) - (x, y) - (x', y)) = f((x + x', y)) - f((x, y)) - f(x', y)$ par linéarité de f. Par définition, cette quantité est égale à $\varphi(x + x', y) - \varphi(x, y) - \varphi(x', y) = 0$ par bilinéarité de φ. On montre de manière analogue que $T \subset \ker f$, et donc que f se factorise en une unique application linéaire $\bar{\varphi} : E \otimes F \to G$. □

Remarque 1.1.47. Si V est un K-espace vectoriel jouissant de la même propriété universelle (*i.e.* on dispose d'une application bilinéaire $E \times F \to V$ par laquelle toutes les applications bilinéaires se factorisent), alors il existe un unique isomorphisme $E \otimes F \to V$. En effet, l'application $(x, y) \mapsto x \otimes y$ étant bilinéaire, elle se factorise de manière unique en une application linéaire $V \to E \otimes F$; on obtient de même une application linéaire $E \otimes F \to V$ dont on vérifie sans peine qu'elle est inverse de la précédente.

Corollaire 1.1.48. *Soient E, F, V des K-espaces vectoriels, alors l'application $\mathcal{L}(E \otimes F, V) \to Bil(E \times F, V)$ définie par $f \mapsto ((x, y) \mapsto f(x \otimes y))$ est un isomorphisme.*

Démonstration. Cette application est bien définie et linéaire. La propriété universelle de $E \otimes F$ assure qu'elle est bijective. □

Corollaire 1.1.49. *Soient E, F, G des K-espaces vectoriels. Alors il existe un unique isomorphisme $f : (E \otimes F) \otimes G \to E \otimes (F \otimes G)$ tel que $f((x \otimes y) \otimes z) = (x \otimes y \otimes z)$.*

Démonstration. Fixons $z \in G$. On considère l'application $\varphi_z : E \times F \to E \otimes (F \otimes G)$ définie par $\varphi_z(x, y) = x \otimes (y \otimes z)$. On vérifie immédiatement que cette application est bilinéaire. Ainsi, il existe une unique application linéaire $f_z : E \otimes F \to E \otimes (F \otimes G)$ telle que $f_z(x \otimes y) = x \otimes (y \otimes z)$. On peut alors considérer l'application $\varphi : (E \otimes F) \times G \to E \otimes (F \otimes G)$ définie par $\varphi(u, z) = f_z(u)$. Là encore, on vérifie facilement la bilinéarité de φ, ce qui nous donne par propriété universelle une application linéaire f comme dans l'énoncé. Il reste à vérifier que f est bien un isomorphisme. Pour cela, on vérifie qu'on peut construire de manière analogue un inverse pour f en appliquant le même procédé dans l'autre sens (de manière à obtenir une application linéaire g vérifiant $g(x \otimes (y \otimes z)) = g((x \otimes y) \otimes z)$). □

Remarque 1.1.50. Ce corollaire permet de noter sans ambiguïté $E \otimes F \otimes G$ pour l'un ou l'autre des produits tensoriels de l'énoncé. Plus généralement, il donne un sens à l'écriture $E_1 \otimes \cdots \otimes E_n$.

Proposition-Définition 1.1.51 (Produit tensoriel d'applications linéaires)**.** Soient $f : E \to E'$ et $g : F \to F'$, alors la formule $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$ définit une application linéaire $f \otimes g : E \otimes F \to E' \otimes F'$ par propriété universelle.

Démonstration. L'application $\varphi : E \times F \to E' \otimes F'$ définie par $\varphi(x, y) = f(x) \otimes g(y)$ est bilinéaire. Par propriété universelle, il existe une unique application linéaire (notée $f \otimes g$) définie sur $E \otimes F$ telle que $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$. □

Lemme 1.1.52. *L'application linéaire définie par :*

$$\begin{array}{ccc} K \otimes K & \to & K \\ \lambda \otimes \mu & \mapsto & \lambda\mu \end{array}$$

est un isomorphisme.

Démonstration. L'application est bien définie par propriété universelle, clairement surjective. De plus, si $\sum_{i=1}^{r} \alpha_i \lambda_i \mu_i = 0$, alors en tensorisant par 1, on obtient $\sum_{i=1}^{r} \alpha_i \lambda_i \otimes \mu_i = 0$. Cela prouve l'injectivité. □

Proposition 1.1.53. *Si $(e_1, \ldots, e_n)$ est une base de E et $(f_1, \ldots, f_m)$ est une base de F, alors les éléments $e_i \otimes f_j$ ($1 \leq i \leq n$, $1 \leq j \leq m$) forment une base de $E \otimes F$.*

Démonstration. Montrons d'abord que cette famille est libre. On fixe $\lambda_{ij} \in K$ tels que $\sum_{i,j} \lambda_{ij} e_i \otimes f_j = 0$. Il s'agit de montrer que les λ_{ij} sont nuls. Pour cela, on note (φ_i) (resp. ψ_j) la base duale de E (resp. de F). Pour tous k, l, on a :

$$(\varphi_k \otimes \psi_l) \left(\sum_{i,j} \lambda_{ij} e_i \otimes f_j \right) = \sum_{i,j} \lambda_{ij} \varphi_k(e_i) \otimes \psi_l(f_j) = \lambda_{kl},$$

en identifiant K et $K \otimes K$ par l'isomorphisme canonique $\lambda \otimes \mu \mapsto \lambda\mu$. Ainsi, les λ_{ij} sont tous nuls, et notre famille est libre.
Montrons maintenant qu'elle est génératrice. Pour cela, il suffit de montrer que pour $(x, y) \in E \times F$, $x \otimes y$ est combinaison linéaire des $e_i \otimes f_j$. Si on écrit $x = \sum_i \lambda_i e_i$ et $y = \sum_j \mu_j f_j$, alors on voit clairement que $x \otimes y = \sum_{i,j} \lambda_i \mu_j (e_i \otimes f_j)$. □

Remarque 1.1.54. On a montré au passage que la base duale de $(e_i \otimes f_j)$ est $(\varphi_i \otimes \psi_j)$, car c'est une famille génératrice de $(E \otimes F)^*$ ayant le bon cardinal.

Proposition 1.1.55. *Soient E, F deux K-espaces vectoriels de dimension finie. Alors l'application*

$$\begin{array}{ccc} E^* \otimes F & \to & \mathcal{L}(E,F) \\ \varphi \otimes x & \mapsto & (y \mapsto \varphi(y)x) \end{array}$$

est bien définie et est un isomorphisme.

Démonstration. Cela découle de la bilinéarité de l'application définie par la même formule, vue comme application $E^* \times F \to \mathcal{L}(E,F)$, et de l'égalité des dimensions (en utilisant le fait que toute application linéaire s'écrit comme somme d'applications de rang 1, ce qui montre la surjectivité). □

1.2 Applications multilinéaires

Définition 1.2.1 (Applications multilinéaires)**.** Soit $E_1, \dots, E_p, F$ des K-espaces vectoriels, une *application p-linéaire* est la donnée d'une application

$$f \ : \ E_1 \times \cdots \times E_p \to F$$

telle que pour tout $1 \leq i \leq p$ et tout $x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_p$, l'application

$$f(x_1, \dots, x_{i-1}, \cdot, x_{i+1}, \dots, x_p)$$

soit linéaire.

Proposition 1.2.2. *Soient $E_1, \dots, E_p$ des K-espaces vectoriels. Il existe un K-espace vectoriel $E_1 \otimes \cdots \otimes E_p$ et une application p-linéaire $\otimes \cdots \otimes$ définie sur $E_1 \times \cdots \times E_p$ telle que pour K-espace vectoriel V et toute application p-linéaire $f : E_1 \times \cdots \times E_p \to V$, il existe une unique application linéaire $\bar{f} : E_1 \otimes \cdots \otimes E_p \to V$ telle que pour tout $(x_1, \dots, x_p)$ on ait $\bar{f}(x_1 \otimes \cdots \otimes x_p) = f(x_1, \dots, x_p)$.*

Démonstration. Le résultat se démontre par récurrence sur p en utilisant le produit tensoriel de deux espaces vectoriels. □

Remarque 1.2.3. Lorsque $E_1 = \cdots = E_p = E$, on note $T^pE = E^{\otimes p}$ le produit tensoriel de E avec lui-même p fois. On a $T^0E = K$ et $T^1E = E$. On peut considérer $T(E) = \bigoplus_{p \geq 0} T^pE$, l'algèbre tensorielle de E. Elle jouit de la propriété universelle suivante : *Toute application linéaire $f : E \to A$ à valeurs dans une K-algèbre A se prolonge de manière unique en un morphisme d'algèbres $T(E) \to A$.* On peut penser à $T(E)^*$ comme l'ensemble des fonctions polynomiales sur E (si $E = K^n$, un choix de base induit un isomorphisme $T(E) \to K[X_1, \dots, X_n]$).

Définition 1.2.4. Soit E, E' des K-espaces vectoriels et $p \in \mathbb{N}$. Une application p-linéaire $f : E^p \to E'$ est dite

— alternée si pour tout $(x_1, \dots, x_p) \in E^p$,

$$x_i = x_j \Rightarrow f(x_1, \dots, x_n) = 0.$$

— antisymétrique si pour tout $(x_1, \dots, x_p) \in E^p$, et pour toute transposition $\tau = (i\ j) \in \mathfrak{S}_p$,

$$f(x_{\tau(1)}, \dots, x_{\tau(p)}) = -f(x_1, \dots, x_p).$$

Proposition 1.2.5. *Si f est alternée, alors f est antisymétrique. La réciproque est vraie si K n'est pas de caractéristique 2.*

Démonstration. Supposons f alternée. Soit τ une transposition, on peut supposer que $\tau = (1\ 2)$. On a

$$0 = f(x_1 + x_2, x_1 + x_2, x_3, \dots, x_p) = f(x_1, x_2, \dots, x_p) + f(x_2, x_1, \dots, x_p).$$

Réciproquement, si f est antisymétrique, $f(x, x, x_3, \dots, x_p) = -f(x, x, \dots, x_p)$ donc $2f(x, x, \dots, x_p) = 0$. □

Corollaire 1.2.6. *Soit $f : E^p \to E'$ alternée, alors pour tout $(x_1, \dots, x_p) \in E^p$ et pour toute permutation $\sigma \in \mathfrak{S}_p$, on a*

$$f(x_{\sigma(1)}, \dots, x_{\sigma(p)}) = \varepsilon(\sigma) f(x_1, \dots, x_p).$$

Démonstration. Il suffit de décomposer σ en produit de transpositions et d'appliquer la formule précédente par récurrence sur le nombre de transpositions dans la décomposition. □

On suppose dans la suite que K est de caractéristique différente de 2.

Théorème 1.2.7. *Soit E un K-espace vectoriel et soit $p \geq 0$. Il existe un K-espace vectoriel $\bigwedge^p E$ et une application*

$$\begin{array}{ccc} \bigwedge^p E & \to & E \\ (x_1, \dots, x_p) & \mapsto & x_1 \wedge \cdots \wedge x_p \end{array}$$

tels que, pour tout K-espace vectoriel E' et pour toute application p-linéaire alternée $f : E^p \to E'$, il existe une unique application linéaire $\tilde{f} : \bigwedge^k E \to E'$ telle que pour tout $(x_1, \dots, x_p) \in E^p$, on ait

$$\tilde{f}(x_1 \wedge \cdots \wedge x_p) = f(x_1, \dots, x_p).$$

Démonstration. Soit $E^{\otimes p} = E \otimes E \otimes \cdots \otimes E$ (p fois). Soit $f : E^p \to E'$ p-linéaire alternée. Soit F le sous-espace vectoriel de $E^{\otimes p}$ engendré par les éléments de la forme $x_1 \otimes \cdots \otimes x \otimes \cdots \otimes x \otimes \cdots \otimes x_p$ (autrement dit, les tenseurs décomposés ayant au moins deux composantes égales). On pose $\bigwedge^p E = E^{\otimes p}/F$, et on définit $\cdot \wedge \cdots \wedge \cdot$ comme la composée de l'application p-linéaire canonique $E \to E^{\otimes p}$ et de la projection canonique $E^{\otimes p} \to E/F$.

Comme f est p-linéaire, par propriété universelle du produit tensoriel, il existe une unique application linéaire $\bar{f}$ définie sur $E^{\otimes p}$ telle que pour tout $(x_1, \dots, x_p) \in E^p$, $\bar{f}(x_1 \otimes \cdots \otimes x_p) = f(x_1, \dots, x_p)$.

Comme f est alternée, $\bar{f}$ s'annule sur la famille génératrice définissant F, donc sur F par linéarité de $\bar{f}$. Ainsi, il existe une unique application $\tilde{f} : \bigwedge^k E \to E'$ vérifiant la formule voulue. □

Définition 1.2.8. Soit E un K-espace vectoriel de dimension finie n. Soit $(e_1, \dots, e_n)$ une base de E. Soit $p \in \mathbb{N}$. Pour $I \subset \{1, \dots, n\}$ de cardinal p, on note $i_1 < i_2 < \cdots < i_p$ les élements de p rangés par ordre croissant, et

$$e_I = e_{i_1} \wedge \cdots \wedge e_{i_p} \in \bigwedge^p E.$$

Proposition 1.2.9. *Si $(e_1, \dots, e_n)$ est une base de E, alors la famille $(e_I)_{|I|=p}$ est une base de $\bigwedge^p E$.*

Démonstration. Comme les éléments de la forme $x_1 \wedge \cdots \wedge x_p$ forment une famille génératrice de $\bigwedge^p E$, par p-linéarité la famille considérée est génératrice.

Nous allons montrer que l'on peut définir une famille de formes linéaires φ_I sur $\bigwedge^p E$, indexée par l'ensemble des parties à p éléments de $\{1, \dots, n\}$, telle que pour toutes parties I, J à p éléments, $\varphi_I(e_J) = \delta_{IJ}$.

On fixe $I = \{1, \dots, p\} \subset \{1, \dots, n\}$ et on définit sur E^p l'application Φ par la formule :

$$\Phi(x_1, \dots x_p) = \sum_{\sigma \in \mathfrak{S}_p} \varepsilon(\sigma) \prod_{1 \leq i \leq p} e_i^*(x_{\sigma(i)}).$$

L'expression ci-dessus est bien p-linéaire en les x_i. De plus, si $1 \leq a < b \leq p$, en supposant que $x_a = x_b$ et en notant $\tau = (a\ b)$, on a $\Phi(x_1, \dots, x_p) = \sum_\sigma \varepsilon(\sigma\tau) \prod_i e_i^*(x_{\sigma\tau(i)}) = \varepsilon(\tau)\Phi(x_1, \dots, x_p)$. Ainsi, Φ est alternée.

En particulier, Φ permet bien de définir (par propriété universelle) une unique forme linéaire sur $\bigwedge^p E$. Cette forme linéaire, notée φ, vérifie clairement $\varphi(e_1 \wedge \cdots \wedge e_p) = 1$ et $\varphi(e_I) = 0$ si $I \neq \{1, \dots, p\}$ (car dans ce cas, l'un au moins des $e_i^*(e_j) = 0$). □

Corollaire 1.2.10. *Soit $(x_1, \dots, x_p) \in E^p$. La famille $(x_1, \dots, x_p)$ est liée si et seulement si $x_1 \wedge \cdots \wedge x_p = 0$.*

Démonstration. Supposons la famille liée. On peut sans perte de généralité supposer qu'on dispose d'une écriture

$$x_p = \lambda_1 x_1 + \cdots + \lambda_{p-1} x_{p-1}.$$

Par p-linéarité, il vient $x_1 \wedge \cdots \wedge x_p = \sum_{i=1}^{p-1} \lambda_i (x_1 \wedge \cdots \wedge x_{p-1} \wedge x_i) = 0$.
Réciproquement, si la famille est libre, on peut la compléter en une base de E, et le premier vecteur de la base de $\bigwedge^p E$ associé à cette base est $x_1 \wedge \cdots \wedge x_p \neq 0$. □

Corollaire 1.2.11. *Soit E un K-espace vectoriel de dimension n et $p \in \mathbb{N}$, alors*

$$\dim \bigwedge^p E = \binom{n}{p}.$$

Définition 1.2.12. Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E et $x_1, \dots, x_n$ une famille d'éléments de E. On appelle *déterminant* de la famille $(x_1, \dots, x_n)$ en base $\mathcal{B}$ l'unique scalaire $\det_{\mathcal{B}}(x_1, \dots, x_n)$ tel que

$$x_1 \wedge \cdots \wedge x_n = \det_{\mathcal{B}}(x_1, \dots, x_n)(e_1 \wedge \cdots \wedge e_n).$$

En d'autre termes, si on note $I = \{1, \dots, n\}$, on a $\det_{\mathcal{B}} = e_I^*$.

Définition 1.2.13. Soient E, E' des K-espaces vectoriels et $u \in \mathcal{L}(E, E')$. Soit $p \in \mathbb{N}$. On définit $\bigwedge^p u : \bigwedge^p E \to \bigwedge^p E'$ comme étant l'unique application linéaire vérifiant :

$$\forall x_1, \dots, x_p \in E,\ \bigwedge^p u(x_1 \wedge \cdots \wedge x_p) = u(x_1) \wedge \cdots \wedge u(x_p).$$

Définition 1.2.14. Soit E un K-espace vectoriel de dimension n et $u \in \mathcal{L}(E)$. On appelle *déterminant* de u, noté $\det u$, le rapport de l'homothétie $\bigwedge^n u$ de $\bigwedge^n E$ (qui est de dimension 1).

Proposition 1.2.15. *Soit $u \in \mathcal{L}(E, E')$, alors $\bigwedge^p u = 0$ si et seulement si u est de rang au plus $p-1$. En particulier, si E est de dimension finie, $u \in \mathcal{L}(E)$ est un isomorphisme si et seulement si* $\det(u) \neq 0$.

Notons que la validité de la formule dite « de Laplace » de calcul du déterminant par développement par rapport à une ligne ou une colonne découle du fait que l'expression donnée par la formule est p-linéaire alternée et coïncide avec $\det_{\mathcal{B}}$ sur $\mathcal{B}$.

Remarque 1.2.16. Soit $(e_1, \ldots, e_n)$ une base de E et soient $x_1, \ldots, x_p \in E$. On note (e_I) les vecteurs de la base de $\bigwedge^p E$ associée à $(e_1, \ldots, e_n)$. Alors $e_I^*(x_1 \wedge \cdots \wedge x_p)$ est le mineur de la sous-matrice extraite de $\mathrm{Mat}_{\mathcal{B}}(x_1, \ldots, x_p)$ obtenue en conservant les lignes indexées par les éléments de I.
De même, si on fixe des bases de E et E', les coefficients de la matrice de l'application linéaire $\bigwedge^p u$ dans les bases correspondantes de $\bigwedge^p E$ et $\bigwedge^p E'$ sont les mineurs de la matrice de u dans ces bases.

1.2.1 Matrices

Définition 1.2.17. Soient $m, n \geq 1$. Une matrice de taille $m \times n$ à coefficients dans K est un tableau à n lignes et m colonnes formé d'éléments de K. On note souvent m_{ij} le coefficient de la matrice M situé à l'intersection de la i-ème ligne et de la j-ème colonne. On note $\mathcal{M}_{m,n}(K)$ l'espace vectoriel des matrices de taille $m \times n$ à coefficients dans K (muni de l'addition coefficient par coefficient).

Définition 1.2.18. Soient E, F des K-espaces vectoriels de dimensions respectives n, m, et soit $u \in \mathcal{L}(E)$. Fixons des bases $\mathcal{B} = (e_1, \ldots, e_n)$ et $\mathcal{B}' = (e'_1, \ldots, e'_m)$ de E et F respectivement. Pour $1 \leq j \leq n$, on décompose $u(e_i)$ sur la base $\mathcal{B}'$: $u(e_i) = \sum_{j=1}^m m_{ij} e'_j$. On appelle matrice de u dans les bases $\mathcal{B}, \mathcal{B}'$ la matrice $M \in M_{m,n}(K)$ dont le coefficient i, j est m_{ij}.

Proposition 1.2.19. *L'application*

$$\begin{array}{ccc} \mathcal{L}(E,F) & \to & \mathcal{M}_{m,n}(K) \\ u & \mapsto & Mat_{\mathcal{B},\mathcal{B}'}(u) \end{array}$$

est un isomorphisme de K-espaces vectoriels. De plus, si G est un K-espace vectoriel muni d'une base $\mathcal{B}''$, et si $v \in \mathcal{L}(F, G)$, alors $Mat_{\mathcal{B}',\mathcal{B}''}(v) Mat_{\mathcal{B},\mathcal{B}'}(u) = Mat_{\mathcal{B},\mathcal{B}''}(vu)$.

Remarque 1.2.20. Si $\mathcal{B}$ est une base de E et $u \in \mathcal{L}(E)$, on note $\mathrm{Mat}_{\mathcal{B}}(u) = \mathrm{Mat}_{\mathcal{B},\mathcal{B}}(u)$. La proposition précédente montre que $u \mapsto \mathrm{Mat}_{\mathcal{B}}(u)$ est un isomorphisme de K-algèbres de $\mathcal{L}(E)$ sur $\mathcal{M}_n(K) = \mathcal{M}_{n,n}(K)$.

Proposition 1.2.21 (Formule de la comatrice)**.** *Soit $M \in \mathcal{M}_n(K)$. On note $com(M)$ la matrice des cofacteurs de M, c'est-à-dire la matrice dont le coefficient i, j est $(-1)^{i+j}$ fois le déterminant de la matrice obtenue en enlevant la i-ème ligne et la j-ème colonne de M. Alors, on a la formule suivante :*

$$^t com(M) M = \det(M) I_n$$

Remarque 1.2.22. Cette formule n'est rien d'autre qu'une réécriture compacte des formules de Cramer.

Rappelons enfin que la méthode la plus simple (dans le cas général) pour obtenir un base du noyau ou de l'image d'une matrice est d'échelonner cette matrice en colonnes. Les colonnes non nulles de la matrice ainsi obtenue forment une base de l'image, tandis que les dernières colonnes de la matrice ayant servi à l'échelonner forment une base du noyau.

1.2.2 À propos de propriétés universelles

Le but de ce paragraphe est de donner un bref aperçu de la notion de *propriété universelle* évoquée plusieurs fois dans ce chapitre. De manière informelle, une propriété universelle se formule souvent comme suit : pour tout objet X, il existe un objet $M(X)$ et un morphisme $X \to M(X)$ (ayant éventuellement des propriétés supplémentaires), tel que pour tout objet Y et tout morphisme $X \to Y$ (ayant les mêmes propriétés supplémentaires), il existe un unique morphisme $M(X) \to Y$ faisant commuter le diagramme :

$$\begin{array}{ccc} X & \longrightarrow & Y \\ \downarrow & \nearrow & \\ M(X) & & \end{array} .$$

Cette formulation est un peu vague, notamment en ce qui concerne les « propriétés supplémentaires ». Le bon langage pour exprimer ces notions est celui des catégories. Dans ce cadre, les objets sont souvent déjà des ensembles de morphismes entre objets partageant une certaine structure, et les morphismes entre objets sont des morphismes respectant les structures et faisant commuter certains diagrammes « naturels ». Un objet universel est un objet initial (resp. final), c'est-à-dire source (resp. but) d'un unique morphisme vers (resp. depuis) tout objet de la catégorie.

Par exemple, on peut considérer la catégorie des ensembles, dans laquelle les objets sont donc les ensembles, et les morphismes sont simplement les applications. Dans ce cas, l'ensemble vide est initial et les ensembles à un élément sont finaux.
Soit E un ensemble, on considère la catégorie des applications de source E, c'est-à-dire les couples (F, f), où F est un ensemble et f une application de E vers F. Dans ce cas, les morphismes de (F, f) vers (F', f') sont les applications $F \to F'$ qui font commuter le diagramme naturel

$$\begin{array}{ccc} E & \longrightarrow & F \\ \downarrow & \nearrow & \\ F' & & \end{array} .$$

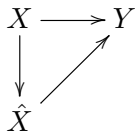
L'objet (E, id) est alors initial dans cette catégorie (mais c'est vraiment trivial). On peut citer quelques exemples plus intéressants, dans une version « avec les mains » et une version dans le langage des catégories.

— Espace vectoriel quotient : le théorème du cours donne la propriété universelle du quotient. On peut la reformuler dans le langage des catégories de la manière suivante : on fixe un couple (E, F) où E est un K-espace vectoriel et $F \subset E$ est un sous-espace vectoriel. On considère la catégorie dont les objets sont les couples (E', f) où E' est un K-espace vectoriel et f une application linéaire $f : E \to E'$ telle que $F \subset \ker f$. Les morphismes entre objets sont les applications linéaires faisant commuter le diagramme naturel. Le quotient E/F est alors un objet universel dans cette catégorie : pour tout (E', f), il existe un unique morphisme $(E/F, \pi) \to (E', f)$, *i.e.* une application linéaire faisant commuter le diagramme naturel :

$$\begin{array}{ccc} E & \longrightarrow & E' \\ \downarrow & \nearrow & \\ E/F & & \end{array}$$

— Le produit tensoriel. De même, la propriété universelle du produit tensoriel se reformule dans le langage des catégories. On fixe des K-espaces vectoriels E et F et on considère la catégorie des couples (E', b) où E' est un K-espace vectoriel et $b : E \times F \to E'$ est bilinéaire. Les objets sont les applications linéaires faisant commuter le diagrammes naturels. Alors le produit tensoriel est un objet universel dans cette catégorie.

— Le complété d'un espace métrique. Soit X un espace métrique. Le complété de X est un espace métrique complet $\hat{X}$, muni d'une application $\iota : X \to \hat{X}$, uniformément continue, ayant la propriété suivante : pour tout espace métrique complet Y et toute application uniformément continue $X \to Y$, il existe une unique application uniformément continue $\hat{X} \to Y$ qui fasse commuter le diagramme



Là encore, on peut reformuler cette propriété en considérant la catégorie dont les objets sont les couples (Y, f) où Y est un espace métrique complet et $f : X \to Y$ est uniformément continue. Le fait que $\iota(X)$ soit dense dans $\hat{X}$ découle de la propriété universelle (l'adhérence de $\iota(X)$ partage la propriété universelle de $\hat{X}$).

1.2.3 Exercices

Exercice 1

Soit E de dimension finie, et soit $u \in \mathcal{L}(E)$.

1. On fixe une base de E. Décrire la matrice de ${}^t u$ dans sa base duale.

2. Montrer que ${}^t({}^t u)$ s'identifie à u par l'isomorphisme canonique de E avec son bidual.

Exercice 2

Soit $u \in \mathcal{L}(E)$. Pour $A \subset E$ un sous-ensemble de E. On définit $A^0 \subset E^*$ comme l'ensemble des $f \in E^*$ telles que pour tout $x \in A$, $f(x) = 0$.

1. Décrire E^0 et $\{0\}^0$.

2. Montrer que A^0 est un sous-espace vectoriel de E^*.

3. Montrer que si $B \subset A$, alors $A^0 \subset B^0$.

4. Montrer que si $F \subset E$ est un sous-espace vectoriel, alors $(F^0)^0$ s'identifie à F par l'isomorphisme canonique de E avec son bidual.

5. Montrer que si $F, G \subset E$ sont des sous-espaces vectoriels, alors $(F + G)^0 = F^0 \cap G^0$.

6. En déduire que $\dim F^0 + \dim F = \dim E$.

Exercice 3

Soit E un espace vectoriel et F un sous-espace vectoriel de E. On note $\pi : E \to E/F$ la projection canonique.

1. Soit G un sous-espace vectoriel de E. Montrer que $F \oplus G = E$ si et seulement si la restriction de π à G est surjective.

2. En déduire le théorème du rang.

Exercice 4

Soit $u \in \mathcal{L}(E)$, et soit $F \subset E$ stable par u. On note π la projection canonique de E vers E/F.

1. Montrer que $F \subset \ker(\pi \circ u)$.

2. En déduire qu'il existe un endomorphisme $\tilde{u} \in \mathcal{L}(E/F)$ tel que $\pi \circ u = \tilde{u} \circ \pi$.

3. On suppose E de dimension finie. Que peut-on dire du polynôme caractéristique et du polynôme minimal de $\tilde{u}$?

Exercice 5

Soit E, E' des K-espaces vectoriels, et $F \subset E$ un sous-espace vectoriel. Montrer que $F \otimes E'$ est un sous-espace vectoriel de $E \otimes E'$ et que :

$$(E \otimes E')/(F \otimes E') \simeq (E/F) \otimes E'.$$

Exercice 6

Soit E un K-espace vectoriel de dimension finie.

1. Montrer que l'on a un isomorphisme naturel $E^* \otimes E \to \mathcal{L}(E)$.

2. Montrer que l'application linéaire $T : E^* \otimes E \to K$, donnée par la formule $T(\varphi \otimes x) = \varphi(x)$, est bien définie.

3. On note $\mathrm{Tr} : \mathcal{L}(E) \to K$ la composée des deux applications précédentes. On fixe une base $\mathcal{B}$ de E. Soit $u \in \mathcal{L}(E)$ et $M = (m_{ij}) = \mathrm{Mat}_{\mathcal{B}}(u)$. Montrer que $\mathrm{Tr}(u) = \sum_i m_{ii}$.

Exercice 7

Soit E un K-espace vectoriel de dimension finie.

1. Soit F le sous-espace de $E \otimes E$ engendré par les éléments de la forme $x \otimes y - y \otimes x$. Montrer qu'une application bilinéaire sur E est symétrique si et seulement si elle se factorise par $(E \otimes E)/F$. En déduire un problème universel dont $\mathrm{Sym}^2 E = (E \otimes E)/F$ est solution.

2. Construire un espace vectoriel $\bigwedge^2 E$ solution d'un problème analogue pour les applications bilinéaires alternées.

Exercice 8

Soit $u \in \mathcal{L}(E, F)$ et $v \in \mathcal{L}(E', F')$. On fixe des bases de E, F, E', F' (supposés de dimension finie) ainsi que les matrices de u et v dans ces bases.

1. Décrire la matrice de $u \otimes v$ dans les bases associées de $E \otimes F$ et $E' \otimes F'$.

2. On suppose désormais que $E = F$ et $E' = F'$. Déduire du calcul précédent que $\mathrm{Tr}(u \otimes v) = \mathrm{Tr}(u)\mathrm{Tr}(v)$.

3. Calculer $\det(u \otimes v)$.

Exercice 9

Donner une formule pour l'inverse de la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(K)$ lorsque son déterminant est non nul.

Exercice 10

Déterminer une base de l'image et du noyau des matrices réelles suivantes :

1. $\begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix}$

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

3. $\begin{pmatrix} 1 & 2 & -1 \\ 2 & 3 & -4 \\ -3 & -2 & 12 \end{pmatrix}$

Exercice 11

Calculer l'inverse de la matrice inversible de l'exercice précédent.

Exercice 12

On considère les sous espaces F et G de $\mathbb{R}^4$, F étant engendré par :

$$\begin{pmatrix} 1 \\ -1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ -5 \\ 4 \\ 5 \end{pmatrix}$$

et G engendré par :

$$\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 4 \\ -5 \\ 11 \\ 7 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ -3 \\ -2 \end{pmatrix}.$$

1. Déterminer les dimensions de F et G.

2. Montrer que $F \subset G$.

3. Donner une base d'un supplémentaire de F dans G.

1.3 Réduction des endomorphismes

Le but de cette partie est de présenter les résultats sur la réduction des endomorphismes. D'un point du vue algébrique, ce sont des résultats de classification : ils permettent par exemple de décrire plus ou moins précisément les orbites de l'action du groupe $GL(E)$ par conjugaison sur $\mathcal{L}(E)$.

1.3.1 Polynômes d'endomorphismes et lemme des noyaux

On commence cette partie en rappelant sans démonstration la propriété universelle des anneaux de polynômes.

Proposition 1.3.1 (Propriété universelle des anneaux de polynômes)**.** *Soit A une K-algèbre et $a \in A$, il existe un unique morphisme d'algèbres $K[X] \to A$ envoyant X sur a.*

Ce morphisme est appelé *évaluation en a* ; on note généralement $P(a)$ l'image de P par ce morphisme.

Lemme 1.3.2 (des noyaux)**.** *Soit $P_1, \cdots, P_s \in K[X]$ des polynômes deux à deux premiers entre eux, $P = \prod_{i=1}^{s} P_i$ et soit $u \in \mathcal{L}(E)$. Alors*

$$\ker P(u) = \bigoplus_{i=1}^{s} \ker P_i(u),$$

et les projections sur les $\ker P_i(u)$ sont des polynômes en u.

Démonstration. Il suffit de traiter le cas $i = 2$ et de raisonner par récurrence. On écrit une relation de Bézout entre P_1 et P_2 : $AP_1 + BP_2 = 1$. On a donc :

$$A(u)P_1(u) + B(u)P_2(u) = I.$$

Cela montre déjà que $\ker P_1(u)$ et $\ker P_2(u)$ sont en somme directe. De plus, tout élément $x \in E$ s'écrit $x = B(u)P_2(u)(x) + A(u)P_1(u)(x) = x_1 + x_2$. Si maintenant $x \in \ker P(u)$, alors $P_1(u)(x_1) = P_2(u)(x_2) = 0$, donc $x_1 \in \ker P_1(u)$ et $x_2 \in \ker P_2(u)$, ce qui démontre le résultat. Le fait que les projections soient polynomiales est clair d'après la formule exprimant x_1 et x_2. □

Corollaire 1.3.3. *Soit P un polynôme annulateur de $u \in \mathcal{L}(E)$ et $P = \prod_{i=1}^{s} P_i^{m_i}$ sa factorisation en produit d'irréductibles unitaires. Alors*

$$E \simeq \bigoplus \ker P_i^{m_i}(u).$$

De plus, les projections sur les $\ker P_i^{m_i}(u)$ sont des polynômes en u.

Proposition 1.3.4. *Soit $u \in \mathcal{L}(E)$, non nul. Alors il existe un unique polynôme unitaire de degré minimal $\pi_u \in K[X]$ tel que $\pi_u(u) = 0$: c'est le polynôme minimal de u.*

Démonstration. Le noyau du morphisme canonique d'anneaux $K[X] \to K[u]$ est un idéal non nul. Cet idéal est engendré par un élément π_u, unitaire, qui est de degré minimal parmi les éléments de l'idéal. Il est unique car la différence de deux éléments unitaires de même degré de cet idéal est également un élément de l'idéal, de degré strictement plus petit. □

1.3.2 Le théorème de Cayley-Hamilton

Théorème 1.3.5. *Soit $u \in \mathcal{L}(E)$, et soit χ_u son polynôme caractéristique. Alors $\chi_u(u) = 0$.*

Remarque 1.3.6. Si E est somme directe de sous-espaces stables par u, alors P annule u sur E si et seulement s'il annule chacun des endomorphismes induits.

Démonstration. Notons M la matrice de u dans la base canonique de E, et C la transposée de la comatrice de $M - XI$. D'après les formules de Cramer, on a $C(M - XI) = \det(M - XI)I = \chi_u(X)I$. On écrit $\chi_u(X) = \sum_{i=0}^{n} a_i X^i$ et $C = \sum_{i=0}^{n-1} B_i X^i$. On a alors $B_0 M = a_0 I$, $B_1 M - B_0 = a_1 I, \ldots, B_{n-1} M - B_{n-2} = a_{n-1} I$. En multipliant la i-ème égalité par M^i et en sommant, on obtient exactement $\chi_u(M) = 0$. □

Corollaire 1.3.7. *Le polynôme minimal de u divise le polynôme caractéristique de u.*

Remarque 1.3.8. Cela montre en particulier que u a un polynôme annulateur de degré $\dim E$, ce qui n'était pas clair *a priori* puisqu'on savait seulement que $\dim K[u] \leq \dim \mathcal{L}(E) = (\dim E)^2$.

1.3.3 Endomorphismes diagonalisables

Dans tout ce qui suit, E désigne un K-espace vectoriel de dimension finie. On fixe $u \in \mathcal{L}(E)$, et on note M la matrice de u dans la base canonique.

Définition 1.3.9. Soit $\lambda \in K$. On dit que λ est une valeur propre de u si $u - \lambda id$ n'est pas injectif. Dans ce cas, $\ker(u - \lambda id)$ s'appelle le *sous-espace propre* associé à la valeur propre λ, et ses éléments non nuls s'appellent vecteurs propres de u associés à la valeur propre λ.

Proposition 1.3.10. *Soit $\lambda \in K$. Alors λ est valeur propre de u si et seulement si λ est racine du polynôme caractéristique de u.*

Théorème 1.3.11. *Pour $\lambda \in Sp(u)$, on pose $E_\lambda = \ker(u - \lambda id)$. Les assertions suivantes sont équivalentes :*

(i) L'endomorphisme u est diagonalisable.

(ii) L'espace E est la somme directe des sous-espaces propres de u.

(iii) L'endomorphisme u est annulé par un polynôme scindé à racines simples.

(iv) Le polynôme minimal de u est scindé à racines simples.

(v) Le polynôme caractéristique de u est scindé, et pour toute valeur propre λ de u, la dimension du sous-espace propre E_λ est égale à multiplicité de λ comme racine du polynôme caractéristique de u.

Démonstration. Procédons par implications circulaires :
$(i) \Rightarrow (ii)$: Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E dans laquelle la matrice de u est diagonale : $u(e_i) = \lambda_i e_i$. Pour λ valeur propre de u, on pose N_λ l'ensemble des $1 \leq i \leq n$ tels que $\lambda_i = \lambda$. Alors, $E_\lambda = \langle e_j \mid j \in N_\lambda \rangle$. Ainsi, $E = \bigoplus_{i=1}^n \langle e_i \rangle = \bigoplus_{\lambda \in \mathrm{Sp}(u)} E_\lambda$.
$(ii) \Rightarrow (iii)$: On suppose u diagonalisable, alors $E = \bigoplus_{k \in \mathrm{Sp}(u)} \ker(u - \lambda id)$. Notons $P = \prod_{\lambda \in \mathrm{Sp}(u)} (X - \lambda)$. Pour tout $\lambda \in \mathrm{Sp}(u)$ et pour tout $x \in E_\lambda$, on a alors $P(u)(x) = 0$. Vu la décomposition précédente, $P(u) = 0$.
$(iii) \Rightarrow (iv)$: Par définition du polynôme minimal de u, tout polynôme annulateur de u est divisible par son polynôme minimal. Ainsi, si u a un polynôme annulateur scindé à racines simples, alors son polynôme minimal est également scindé à racines simples. $(iv) \Rightarrow (v)$: Supposons par l'absurde que l'un des E_λ ne soit pas de dimension égale à la multiplicité de λ. Alors il existe $x \in E$ et $m \geq 2$ tel que $(u - \lambda id)^m(x) = 0$ et $u(x) \neq \lambda x$. Ainsi, parmi les facteurs irréductibles du polynôme minimal de u, le facteur $X - \lambda$ apparaît avec multiplicité ≥ 2, ce qui est impossible.
$(v) \Rightarrow (i)$: Comme les E_λ sont en somme directe, on a $\dim \bigoplus E_\lambda = \deg \chi_u = \dim E$, donc $\bigoplus E_\lambda = E$. Dans une base adaptée à cette décomposition, la matrice de u est diagonale. □

Remarque 1.3.12. Les polynômes χ_u et π_u ont les mêmes facteurs irréductibles.

Remarque 1.3.13. Si P est scindé, et si le corps est de caractéristique nulle, le produit des $X - \lambda$ avec λ racine de P est $P/\mathrm{pgcd}(P, P')$. Ainsi, sur un corps algébriquement clos de caractéristique 0 (par exemple $\mathbb{C}$), u est diagonalisable si et seulement s'il est annulé par $\chi_u/\mathrm{pgcd}(\chi_u, \chi_u')$ (qui est alors son polynômes minimal).

1.3.4 Exercices

Exercice 1

Soit $u \in GL(E)$. Montrer que $u^{-1} \in K[u]$.

Exercice 2

Montrer que toute matrice $M \in \mathcal{M}_n(K)$ est semblable à une matrice diagonale par blocs dont les blocs diagonaux ont pour polynôme caractéristique une puissance d'un polynôme irréductible.

Exercice 3

Soit $u, v \in \mathcal{L}(E)$. On suppose que u et v commutent et sont diagonalisables. Montrer qu'il existe une base commune de diagonalisation pour u et v.

Exercice 4

On rappelle qu'un endomorphisme $u \in \mathcal{L}(E)$ est dit *trigonalisable* s'il existe une base de E dans laquelle la matrice de u est triangulaire supérieure.

1. Montrer que si u est trigonalisable, alors son polynôme caractéristique est scindé.

2. Montrer que si le polynôme caractéristique de u est scindé, alors u est trigonalisable (on pourra raisonner par récurrence, et éventuellement considérer l'endomorphisme induit par u sur un quotient judicieusement choisi de E).

1.4 Décompositions usuelles

1.4.1 Endomorphismes nilpotents

Définition 1.4.1. Un endomorphisme $u \in \mathcal{L}(E)$ est dit *nilpotent* s'il existe un entier $m \geq 1$ tel que $u^m = 0$. Le plus petit tel entier m s'appelle indice de nilpotence de u.

Lemme 1.4.2. *Soit $u \in \mathcal{L}(E)$, alors u est nilpotent si et seulement si son polynôme caractéristique (et donc son polynôme minimal) est une puissance de X.*

Démonstration. On sait que le polynôme minimal de u divise le polynôme annulateur X^m, c'est donc une puissance de X. De plus, les facteurs irréductibles du polynôme caractéristique de u sont également des facteurs irréductibles du polynôme minimal de u, et le seul facteur irréductible du polynôme minimal est X. □

Proposition 1.4.3. *Soit $u \in \mathcal{L}(E)$ un endomorphisme nilpotent. Alors il existe une base $(e_1, \ldots, e_n)$ de E, et des entiers $1 \leq r_1 \leq \cdots \leq r_s \leq n$, tels que :*

- *Pour tout $1 \leq i \leq s$ et pour tout $r_i \leq j < r_{i+1} - 1$, $u(e_j) = e_{j+1}$;*
- *Pour tout $1 \leq i \leq s$, $u(e_{r_i - 1}) = 0$.*

Démonstration. On raisonne par récurrence sur $n = \dim E$. Soit $m \geq 1$ l'indice de nilpotence de u, c'est-à-dire le plus petit entier tel que $u^m = 0$. Soit $x \in E$ tel que $u^{m-1}(x) \neq 0$. Montrons que la famille $(x, u(x), \ldots, u^{m-1}(x))$ est libre. En effet, si $\lambda_0 x + \cdots + \lambda_{m-1} u^{m-1}(x) = 0$, en appliquant successivement $u^{m-1}, u^{m-2}, \ldots, u$ on voit successivement que tous les λ_i sont nuls. Dans la base $(u^{m-1}(x), \ldots, x)$ du sous-espace (stable par u) F engendré par ces vecteurs, la matrice de l'endomorphisme induit par u est un bloc de Jordan. Il suffit donc de montrer que ce sous-espace admet un supplémentaire stable par

u. Pour cela, fixons $f \in E^*$ telle que $f(u^{m-1}(x)) \neq 0$, et notons G le sous-espace de E^* engendré par les ${}^t u^i(f)$ (où ${}^t u$ est l'endomorphisme de E^* défini par ${}^t u(\varphi) = \varphi \circ u$). Par définition, ${}^t u^{m-1}(f) \neq 0$, et ${}^t u^m(f) = 0$. Ainsi, G est un sous-espace de E^* stable par ${}^t u$, de dimension m. Notons enfin $F' = \{y \in E \mid \forall \varphi \in G, \varphi(y) = 0\} = G^\perp$. Il est clair que F' est stable par u et de dimension $n - m$, il suffit donc de montrer que $F \cap F' = \{0\}$. Soit donc $y \in F \cap F'$. On écrit $y = \sum_i \lambda_i u^i(x)$. On a alors $f(u^{m-1}(y)) = 0 = \lambda_0 u^{m-1}(x)$, d'où $\lambda_0 = 0$, et en réappliquant le même raisonnement on voit que $y = 0$. □

Remarque 1.4.4. Pour $i \geq 0$, on pose $d_i = \dim \ker u^i$. La suite d_i est strictement croissante puis stationnaire à partir de $i = m$. Ainsi, $d_i - d_{i-1}$ est le nombre de blocs de Jordan de u de taille au moins i. Cela montre qu'une telle décomposition par blocs est uniquement déterminée par u.

1.4.2 Réduction de Jordan

Définition 1.4.5 (Blocs de Jordan)**.** Soit $\lambda \in K$ et soit $r \geq 1$ un entier. Un *bloc de Jordan* de taille r associé à λ est une matrice de la forme

$$J_{\lambda,r} = \begin{pmatrix} \lambda & 1 & \cdots & 0 \\ 0 & \lambda & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 0 & 0 & 0 & \lambda \end{pmatrix},$$

où la taille de la matrice est r.

Théorème 1.4.6 (Jordan)**.** *Soit $M \in \mathcal{M}_n(K)$ dont le polynôme caractéristique est scindé sur K. Alors il existe une matrice $P \in GL_n(K)$ telle que $P^{-1}MP$ soit diagonale par blocs, avec pour blocs diagonaux des blocs de Jordan associés aux valeurs propres de M. De plus, une telle décomposition est unique à l'ordre des blocs près, et s'appelle décomposition de Jordan de M.*

Démonstration. On appelle $\lambda_1, \ldots, \lambda_s$ les valeurs propres distinctes de M et $m_1, \ldots, m_s$ leurs multiplicités respectives en tant que racines de χ_M. On note $E_i = \ker(M - \lambda_i I)^{m_i}$. D'après le lemme des noyaux (Lemme 1.3.2), on a :

$$K^n \simeq \bigoplus_{i=1}^{s} E_i.$$

Chacun des sous-espaces E_i est stable par M. On fixe $1 \leq i \leq s$. L'endomorphisme u_i induit par (l'endomorphisme canoniquement associé à) M sur E_i est annulé par $(X - \lambda_i)^{m_i}$. Ainsi, $u_i - \lambda_i I$ est nilpotent. On choisit une base adaptée à la décomposition $K^n = \bigoplus E_i$ telle que pour chaque E_i, l'endomorphisme $u_i - \lambda_i Id$ ait une matrice dans cette base qui soit surdiagonale avec des 0 et des 1 dans la surdiagonale. La matrice de u dans cette base est alors de la forme annoncée. Enfin, remarquons que si $k \geq 1$, le nombre de blocs de Jordan de taille au moins k associés à la valeur propre λ dans une décomposition de Jordan de M est $\dim \ker(M - \lambda I)^k - \dim(M - \lambda I)^{k-1}$, d'où l'unicité de la décomposition. □

1.4.3 Décomposition LU

Proposition 1.4.7. *Soit $M \in GL_n(K)$. On suppose que tous les mineurs principaux de M sont non nuls. Alors M admet une unique écriture sous la forme $M = LU$, avec L triangulaire inférieure et U triangulaire supérieure avec des 1 sur la diagonale.*

Démonstration. On procède par récurrence sur n. Si $n = 1$, le résultat est clair. On suppose donc $n \geq 2$. Comme le coefficient en haut à gauche de M est non nul, on peut effectuer un pivot de Gauss sur M en utilisant ce coefficient comme pivot : la matrice M s'écrit donc L_1U_1 avec L_1 triangulaire inférieure et U_1 ayant le premier vecteur de la base canonique comme première colonne. De plus, puisque chaque sous-matrice carrée en haut à gauche de U_1 se déduit de la sous-matrice correspondante de M en retranchant un multiple de la première ligne de M, tous les mineurs principaux de U_1 sont non nuls. Par développement selon la première colonne, on en déduit que les mineurs principaux de la sous-matrice $(n-1) \times (n-1)$ en bas à droite de U_1 sont non nuls. Finalement, on applique l'hypothèse de récurrence à cette sous-matrice, ce dont découle le résultat. □

1.4.4 Décomposition de Jordan-Chevalley

Proposition 1.4.8 (Décomposition de Jordan-Chevalley)**.** *On suppose que K est algébriquement clos. Soit $u \in GL(E)$, alors il existe un unique couple d, n tel que :*

- *d est diagonalisble ;*
- *n est nilpotent ;*
- *$dn = nd$;*
- *$u = d + n$. De plus, d et n s'expriment comme des polynômes en u.*

Démonstration. L'existence découle directement de celle de la décomposition de Jordan, le fait que d et n puissent être choisis comme des polynômes en u provient du lemme des noyaux. Pour l'unicité, remarquons que si $u = d + n = d' + n'$, alors $d - d' = n' - n$. Comme d est un polynôme en u et que d' commute avec u (il commute avec d' et n'), les endomorphismes d et d' commutent. Comme ils sont diagonalisables, $d - d'$ est diagonalisable. De même, $n - n'$ est nilpotent. Ainsi, $d - d'$ est diagonalisable et nilpotent, donc nul, de même que $n - n'$. □

1.4.5 Exercices

Exercice 1

Soit $u \in \mathcal{L}(E)$ nilpotent. Montrer que $\mathrm{id} - u$ est inversible.

Exercice 2

Calculer la décomposition de Jordan-Chevalley des matrices suivantes :

1. $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$

2. $\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$

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

Exercice 3

Soit $u \in \mathcal{L}(E)$ nilpotent.

1. Montrer que pour tout $k \geq 1$, $\mathrm{Tr}(u^k) = 0$.

2. On suppose que K est de caractéristique nulle. Montrer que la réciproque est vraie.

Indication : On pourra considérer les valeurs propres λ_i de u ainsi que leurs multiplicités m_i, et voir que l'hypothèse montre que les m_i sont solutions d'un système linéaire judicieusement choisi.

3. Donner un contre-exemple en caractéristique positive. Quelle information sur les valeurs propres de u la démonstration précédente fournit-elle dans ce cas ?

Exercice 4

Soit $u \in \mathcal{L}(E)$. Pour $x \in E$, on note π_x le polynôme unitaire de degré minimal tel que $\pi_x(u)(x) = 0$.

1. Soit $x \in E$. Montrer que π_x est bien défini et divise le polynôme minimal de u.

2. Soit $x \in E$. Montrer que $\{P(u)(x) \mid P \in K[X]\}$ est un sous-K-espace vectoriel de E de dimension $\deg \pi_x$.

3. Montrer qu'il existe $x \in E$ tel que $\pi_x = \pi_u$ (on pourra commencer par traiter le cas où π_u est une puissance d'un polynôme irréductible).

4. En déduire une nouvelle démonstration du théorème de Cayley-Hamilton.

Exercice 5

On dit qu'un endomorphisme $u \in \mathcal{L}(E)$ est *cyclique* lorsqu'il existe une base de E de la forme $(x, u(x), \ldots, u^{n-1}(x))$.

1. Montrer que si u est cyclique, alors son polynôme minimal est égal à son polynôme caractéristique.

2. Montrer que u est cyclique, alors il existe une base de E dans laquelle la matrice de u est la matrice compagnon d'un polynôme $P \in K[X]$.

3. Montrer que si les polynômes minimal et caractéristique de u sont égaux, alors u est cyclique (on pourra utiliser l'exercice précédent).

4. Que dire de la décomposition de Jordan d'un endomorphisme cyclique ? (On pourra d'abord s'intéresser au cas d'un endomorphisme cyclique nilpotent.)

Exercice 6

Soit $u \in \mathcal{L}(E)$, et soit $x \in E$ tel que $\pi_x = \pi_u$. On note $d = \deg \pi_u$.

1. Pour $1 \leq i \leq d$, on note $e_i = u^{i-1}(x)$, et on complète cette famille en une base $(e_1, \ldots, e_n)$ de E dont on note $(e_1^*, \ldots, e_n^*)$ la base duale. Montrer que

$$\{y \in E \mid \forall i \geq 0, {}^t u^i(e_d^*)(y) = 0\}$$

est un supplémentaire de $K[u](x)$ stable par u.

2. En déduire qu'il existe une famille de sous-espaces $E_1, \ldots, E_r$ de E et une famille de polynômes $P_1, \ldots, P_r$ tels que

— $E = \bigoplus_{i=1}^r E_i$,

— pour tout i, E_i soit stable par u,

— l'endomorphisme induit par u sur E_i soit cyclique de polynôme caractéristique P_i,

— pour tout $1 \leq i \leq r-1$, P_{i+1} divise P_i.

3. Montrer que les polynômes P_i ne dépendent que de u et non de la décomposition. Ces polynômes s'appellent les *facteurs invariants* de u.
4. Montrer que $v \in \mathcal{L}(E)$ est semblable à u si et seulement si u et v ont les mêmes facteurs invariants.
5. En déduire une autre démonstration de l'existence et l'unicité de la forme de Jordan des endomorphismes nilpotents.

Exercice 7

On considère une suite récurrente linéaire d'ordre n : $x_0, \dots, x_{n-1} \in K$, et pour tout $k \geq 0$,

$$x_{k+n} = \sum_{i=0}^{n-1} a_i x_{k+i}.$$

1. Montrer que les suites obéissant à cette relation de récurrence forment un K-espace vectoriel.
2. Pour $k \geq 0$, on considère le vecteur colonne X_k de coordonnées $(x_k, \dots, x_{k+n-1})$. Exprimer X_{k+1} en fonction de X_k.
3. On considère la matrice compagnon C_P du polynôme $P(T) = T^n - \sum_{i=0}^{n-1} a_i T^i$. Exprimer X_k en fonction de M et X_0.
4. Dans le cas où C est diagonalisable, donner une base de l'espace des suites vérifiant cette relation de récurrence.
5. On suppose seulement que P est scindé, et on note $\lambda_1, \dots \lambda_r$ les racines de P, et $m_1, \dots, m_r$ leurs multiplicités respectives. Montrer qu'une base de l'espace des suites vérifiant cette relation de récurrence est $\{(k^p \lambda_i^k)_{k\in\mathbb{N}},\ 1 \leq i \leq r, 0 \leq p \leq m_r - 1\}$ (on pourra considérer la décomposition de Jordan de C, et montrer qu'il y a un seul bloc de Jordan pour chaque valeur propre).

1.5 Topologie

Dans cette partie, on suppose que $K = \mathbb{R}$ ou $\mathbb{C}$. La plupart des raisonnements présentés fonctionneraient de la même manière sur un corps topologique complet (par exemple, $\mathbb{Q}_p$, le corps des nombres p-adiques).

1.5.1 Normes matricielles

Définition 1.5.1 (Norme matricielle)**.** Une norme matricielle est une norme $\|\cdot\|$ sur $\mathcal{M}_n(K)$ telle que pour tous $A, B \in \mathcal{M}_n(K)$, $\|AB\| \leq \|A\|\|B\|$.

Remarque 1.5.2. Si $\|\cdot\|$ est une norme matricielle sur $\mathcal{M}_n(K)$, alors $\|I_n\| = 1$.

Proposition 1.5.3. *Toute norme subordonnée est une norme matricielle.*

Démonstration. Soit $x \in K^n$ et $A, B \in \mathcal{M}_n(K)$, et soit N la norme subordonnée à une norme $\|\cdot\|$ sur K^n. Alors :

$$\|ABx\| \leq N(A)\|Bx\| \leq N(A)N(B)\|x\|,$$

d'où $N(AB) \leq N(A)N(B)$. □

Lemme 1.5.4. *Si $\|\cdot\|$ est une norme matricielle et $P \in GL_n(K)$, alors $M \mapsto \|P^{-1}MP\|$ est une norme matricielle.*

Démonstration. C'est évident. □

1.5.2 Propriétés topologiques

Proposition 1.5.5. *On a les propriétés topologiques suivantes :*
- *L'ensemble des matrices diagonalisables est dense dans $\mathcal{M}_n(\mathbb{C})$.*
- *$GL_n(K)$ est un ouvert dense de $\mathcal{M}_n(K)$.*
- *L'intérieur de l'ensemble des matrices diagonalisables est l'ensemble des matrices dont le polynôme caractéristique est scindé à racines simples.*

Démonstration. On note $\lambda_1, \ldots, \lambda_n$ les valeurs propres (pas nécessairement distinctes) de $M \in \mathcal{M}_n(\mathbb{C})$. Quitte à fixer une matrice de changement de base qui trigonalise M, on peut supposer M triangulaire supérieure, et on choisit la norme du sup des coefficients. Soit $\varepsilon > 0$, alors il existe $t_1, \ldots, t_n$ tous $< \varepsilon$ tels que les $\lambda_i + t_i$ soient tous distincts. Alors $M + \mathrm{Diag}(t_1, \ldots, t_n)$ est diagonalisable et est à distance $< \varepsilon$ de M.
Pour le deuxième point, on applique le même raisonnement en modifiant les valeurs propres nulles.
Pour le dernier point, il suffit de montrer que l'ensemble des matrices dont le polynôme caractéristique est scindé à racines simples est un ouvert de l'ensemble des matrices diagonalisables qui est dense dans $\mathcal{M}_n(\mathbb{C})$. La densité découle du même raisonnement qu'au premier point. Montrons donc que cet ensemble est ouvert. Soit M dont le polynôme caractéristique est scindé à racines simples, on peut effectuer un changement de base qui diagonalise M et choisir la norme du sup des coefficients. Comme toutes les valeurs propres de M sont distinctes, il existe $\varepsilon > 0$ tel que $M + \varepsilon A$ ait son polynôme caractéristique à racines simples pour tout A de norme ≤ 1. □

Remarque 1.5.6. Les matrices diagonalisables ne sont pas denses dans $\mathcal{M}_n(\mathbb{R})$. On peut pour le voir (en dimension 2) considérer une matrice dont le polynôme caractéristique a un discriminant strictement négatif. Comme le discriminant du polynôme caractéristique est une fonction continue des coefficients de la matrice, une telle matrice ne peut être approchée par une suite de matrices diagonalisables.

Proposition 1.5.7. *L'ensemble $GL_n(\mathbb{C})$ est connexe par arcs. En revanche, $GL_n(\mathbb{R})$ n'est pas connexe par arcs.*

Démonstration. Soit $A, B \in GL_n(\mathbb{C})$, l'application $z \mapsto \det(zA+(1-z)B)$ est un polynôme en z, non nul. Il admet donc un nombre fini de zéros. Comme $\mathbb{C}$ privé d'un nombre fini de points est connexe par arcs, il existe un chemin de 0 à 1 tel que $\det(zA + (1-z)B) \neq 0$ pour tout z dans l'image de ce chemin.
Pour le cas de $GL_n(\mathbb{R})$, la continuité du déterminant associée à la non connexité de $\mathbb{R} \setminus \{0\}$ prouve que $GL_n(\mathbb{R})$ n'est pas connexe. □

1.5.3 Exponentielles de matrices

Théorème 1.5.8. *L'application*

$$\exp \ : \ \mathcal{M}_n(\mathbb{C}) \to GL_n(\mathbb{C})$$

est surjective.

Démonstration. On se fixe $M \in GL_n(\mathbb{C})$, et on note $X = K[M]$ l'algèbre des polynômes en M. C'est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$. On va montrer que l'exponentielle induit un isomorphisme de groupes entre $(X, +)$ et $X^\times = X \cap GL_n(\mathbb{C})$ muni de la multiplication des matrices (ce dernier ensemble est un groupe l'inverse d'une matrice est un polynôme en cette matrice). Comme les éléments de X commutent, exp est bien un morphisme de groupes dont l'image est contenue dans $X^\times$. La différentielle de exp en zéro est $D\exp_0(H) = \exp(0)H$ qui est inversible. Par le théorème d'inversion locale, il existe un voisinage U de 0 dans X et un voisinage V de I dans $\mathcal{M}_n(\mathbb{C})$ tels que exp réalise une bijection de U sur V. Comme $\exp(U) \subset X^\times$, $\exp(X)$ est un sous-groupe de $X^\times$ qui contient un voisinage de l'identité. Ce sous-groupe est alors ouvert : en effet, $\exp(X) = \cup_{A \in \exp(X)} AV$. Mais il est aussi fermé, car $(\exp(X))^c = \cup_{A \notin \exp(X)} AV$ est ouvert. Par connexité de $X^\times$, on a $X^\times = \exp(X)$. En particulier, $M \in X^\times$ est dans l'image de exp. □

Corollaire 1.5.9. *Une matrice $M \in GL_n(\mathbb{R})$ est dans l'image de l'exponentielle si et seulement si c'est le carré d'une matrice réelle.*

Démonstration. Si $M \in GL_n(\mathbb{R})$ et $A \in GL_n(\mathbb{R})$ telle que $M = A^2$. On écrit $A = \exp(B)$ avec $B \in \mathcal{M}_n(\mathbb{C})$. D'après le théorème précédent, on peut même choisir B sous la forme $P(A)$ avec $P \in \mathbb{C}[X]$. On a alors $\bar{B} = \bar{P}(\bar{A}) = \bar{P}(A)$. Ainsi, $B\bar{B} = P\bar{P}(A) = \bar{P}P(A) = \bar{B}B$, et $\exp(B + \bar{B}) = \exp(B)\overline{\exp(B)} = A^2 = M$. La réciproque est évidente. □

Proposition 1.5.10. *Soit $M \in GL_n(\mathbb{C})$, alors M est diagonalisable si et seulement si $\exp M$ est diagonalisable.*

Démonstration. Soit $D + N$ la décomposition de Jordan-Chevalley de M. Alors comme D et N commutent, $\exp(M) = \exp(D)\exp(N)$. Comme N est nilpotente, $\exp(N) = I + \sum_{i=1}^{n-1} \frac{1}{i!} N^i$ donc $\exp(N) - I$ est nilpotente. Ainsi, la décomposition de Jordan-Chevalley de $\exp M$ est $\exp D + \exp D(\exp N - I)$. On remarque alors que M est diagonalisable si et seulement si $N = 0$, ce qui est le cas si et seulement si $\exp N = I$ car N est nilpotente. □

1.5.4 Exercices

Exercice 1

Soit E un $\mathbb{R}$-espace vectoriel de dimension finie.

1. Montrer que l'ensemble des endomorphismes nilpotents est fermé dans $\mathcal{L}(E)$.

2. Montrer que $u \in \mathcal{L}(E)$ est nilpotent si et seulement si 0 est dans l'adhérence de sa classe de conjugaison.

3. Soit u nilpotent et C la classe de conjugaison de u dans $\mathcal{L}(E)$. Quelle est l'adhérence de C dans $\mathcal{L}(E)$?

Exercice 2

Soit E un $\mathbb{R}$-espace vectoriel de dimension finie.

1. Soit $u \in \mathcal{L}(E)$, montrer que l'ensemble des $x \in E$ tels que $(x, u(x), \ldots, u^{n-1}(x))$ forme une base de E est un ouvert de E. Dans quel cas cet ouvert est-il non vide ?

2. Montrer que l'ensemble des endomorphismes cycliques est un ouvert dense de $\mathcal{L}(E)$.

Exercice 3

1. Montrer que l'image de $M_n(\mathbb{R})$ par la fonction exponentielle est l'ensemble des matrices $M \in GL_n(\mathbb{R})$ s'écrivant comme le carré d'une matrice réelle.

2 Algèbre bilinéaire

On fixe un corps K de caractéristique différente de 2 et un K-espace vectoriel E de dimension finie.

2.1 Formes bilinéaires et formes quadratiques

Définition 2.1.1. Une forme bilinéaire sur E est une application $f : E \times E \to K$ telle que pour tout $x \in E$, $f(\cdot, x)$ et $f(x, \cdot)$ soient des formes linéaires sur E. Une telle forme est dite symétrique si pour tout $x, y \in E$, on a $f(x, y) = f(y, x)$.

Définition 2.1.2. Une forme quadratique est une application $q : E \to K$ telle que pour tout $\lambda \in K$, $q(\lambda x) = \lambda^2 q(x)$ telle que la forme polaire

$$f(x, y) = q(x + y, x + y) - q(x) - q(y)$$

soit une forme bilinéaire symétrique.
On appelle *espace quadratique* la donnée d'un couple (E, q) où E est un K-espace vectoriel de dimension finie et q est une forme quadratique sur E.

Exemple 2.1.3. Sur K^n, l'application $(x_1, \ldots, x_n) \mapsto \sum_{i=1}^n x_i^2$ est une forme quadratique.

Définition 2.1.4. Soient (E, q) et (F, q') deux K-espaces vectoriels. On appelle *morphisme métrique* de E vers F toute application $u \in \mathcal{L}(E, F)$ telle que pour tout $x \in E$, $q(x) = q'(u(x))$. On dit que E et F sont isométriques s'il existe un isomorphisme de E vers F qui soit métrique. Un tel isomorphisme est appelé isométrie.

Remarque 2.1.5. Si u est un isomorphisme isométrique, alors u^{-1} est une isométrie, donc la relation « être isométriques »entre deux espaces quadratiques est une relation d'équivalence.

Définition 2.1.6. Soit $(e_1, \ldots, e_n)$ une base de l'espace quadratique (E, q). La matrice de q dans la base E est la matrice dont le coefficient (i, j) est $f(e_i, e_j)$, où f est la forme polaire associée à q.

Proposition 2.1.7. *Soit (E, q) un espace quadratique et soit M la matrice de q dans la base $(e_1, \ldots, e_n)$ de E. Soit $x \in E$ et soit X le vecteur représentant x dans cette même base. Alors $q(x) = {}^tXMX$.*
Si $u \in GL(E)$ et si P est la matrice de u dans la base précédente, alors la matrice de q dans la base $(u(e_1), \ldots, u(e_n))$ est $PM{}^tP$.

Démonstration. Cela découle directement du calcul, en décomposant les vecteurs sur la base. □

Remarque 2.1.8. Cela montre que si M et M' sont les matrices d'une même forme quadratique dans des bases différentes, ces matrices sont congruentes. En particulier, $\det M$ et $\det M'$ sont égales à multiplication par un carré près. Si ce déterminant est non nul, l'image de $\det M$ dans $K^\times/(K^\times)^2$ s'appelle *discriminant* de q.

Définition 2.1.9. Une forme quadratique q de forme polaire f est dite non dégénérée si $\{x \in E \mid \forall y \in E,\ f(x, y) = 0\} = \{0\}$.

Proposition 2.1.10. *Soit (E, q) un espace quadratique et f la forme polaire associée à q. Alors les conditions suivantes sont équivalentes :*

(i) *q est non dégénérée ;*

(ii) *l'application :*

$$\begin{array}{ccc} E & \to & E^* \\ y & \mapsto & f_y \\ & & x \quad \mapsto f(x,y) \end{array}$$

est un isomorphisme ;

(iii) *le déterminant de la matrice de q dans une base de E est non nul.*

Démonstration. $(i) \Leftrightarrow (ii)$: il est clair que l'application définie en (ii) est linéaire par bilinéarité de f. Comme E et E^* ont même dimension, il s'agit de montrer qu'elle est injective si et seulement si q est non dégénérée. Or, par définition, le noyau de cette application est $\{x \in E \mid \forall y \in E,\ f(x,y) = 0\}$, qui est nul si et seulement si q est non dégénérée.
$(ii) \Rightarrow (iii)$: Fixons une base $(e_1, \ldots, e_n)$ de E et notons $u_j = f_{e_i} = f(\cdot, e_j)$. Alors la matrice de q dans la base (e_i) est la matrice des $u_j(e_i)$. En particulier, elles ont le même déterminant, et $\det q \neq 0$ si et seulement si la famille des u_j est libre, autrement dit si et seulement si l'application du (ii) est un isomorphisme. □

Définition 2.1.11. On appelle radical (ou noyau) de q le noyau de l'application $y \mapsto f_y$, et rang de q le rang de cette application. Une forme quadratique est donc non dégénérée si et seulement si son radical est nul, et si et seulement si son rang est maximal.

Remarque 2.1.12. On dit que $x \in E$ est *isotrope* si $q(x) = 0$. En général, le fait que q soit non dégénérée ne signifie pas que q n'admet pas de vecteurs isotropes non nuls ! Par exemple, $q(x,y) = x^2 - y^2$ est non dégénérée mais admet des vecteurs isotropes.

Définition 2.1.13. Soit (E,q) un espace quadratique et f la forme polaire associée à q. On dit que $x, y \in E$ sont orthogonaux si $f(x,y) = 0$. Si $F \subset E$, on appelle orthogonal de F, noté $F^\perp$, l'ensemble des $y \in E$ tel que $f(x,y) = 0$ pour tout $x \in F$.

Remarque 2.1.14. En particulier, $\mathrm{rad}(E) = E^\perp$, donc q est non dégénérée si et seulement si $E^\perp = \{0\}$.

Proposition 2.1.15. *Soit (E,q) un espace quadratique. Il existe un sous-espace $F \subset E$ tel que $E = F \oplus^\perp rad(E)$ et tel que $q_{|F}$ soit non dégénérée.*

Démonstration. Il suffit de choisir pour F n'importe quel supplémentaire de $\mathrm{rad}(E)$, c'est par définition du radical un supplémentaire orthogonal et on a $\mathrm{rad}(E) = \mathrm{rad}(F) \oplus \mathrm{rad}(\mathrm{rad}(E))$, donc $q_{|F}$ est non dégénéré. □

Proposition 2.1.16. *Si q est non dégénérée, tous les résultats précédents sur l'orthogonalité sont préservés.*

Démonstration. Cela découle directement de l'isomorphisme $y \mapsto f_y$ entre E et E^*. □

Théorème 2.1.17. *Tout espace quadratique (E,q) admet une base constituée de vecteurs deux à deux orthogonaux. De plus, si $\mathcal{F}$ est une famille de représentants de $K^\times/(K^\times)^2$, on peut choisir une telle base $(e_1, \ldots, e_n)$ de sorte que pour tout i, $q(e_i) \in \mathcal{F} \cup \{0\}$.*

Démonstration. Démontrons d'abord la première assertion. On procède par récurrence sur la dimension n de E. On peut directement supposer que q est non dégénérée en vertu de la décomposition en somme directe orthogonale $E = F \oplus \mathrm{rad}(E)$. Soit alors $x \in E$ tel que

$q(x) \neq 0$: un tel x existe, sinon q serait nulle, ce qui contredirait la non-dégénérescence de q. Soit $F = \langle x \rangle^{\perp}$. Comme q est non dégénérée, $\dim F = n-1$. De plus, $\langle x \rangle \cap F = \{0\}$ (sinon x serait isotrope) donc $E = \langle x \rangle \oplus^{\perp} F$. On obtient le résultat en appliquant l'hypothèse de récurrence à F.
Si $\lambda \in K^{\times}$, $q(\lambda e_i) = \lambda^2 q(e_i)$, on peut donc en outre se ramener au cas où les $q(e_i)$ sont dans une famille de représentants fixés de $K^{\times}/(K^{\times})^2$. □

Exemple 2.1.18. La forme $q(xe_1+ye_2) = xy$ admet comme base orthogonale (e_1+e_2, e_1-e_2).

Remarque 2.1.19. La preuve précédente montre en fait que tout vecteur non isotrope peut être complété en une base orthogonale.

Remarque 2.1.20. On verra au paragraphe suivant la *méthode de Gauss* permettant de calculer une base orthogonale.

2.1.1 Groupe orthogonal d'une forme quadratique

Proposition-Définition 2.1.21. Soit (E, q) un espace quadratique, l'ensemble des automorphismes isométriques de E forme un sous-groupe de $GL(E)$, appelé *groupe orthogonal* de q, et noté $O(q)$.

Remarque 2.1.22. Si on fixe une base de E dans laquelle la matrice de q est M, le fait que l'automorphisme u de matrice P soit isométrique s'écrit $PM^tP = M$. Remarquons au passage que si q est non dégénérée, toutes les isométries de E dans E sont nécessairement des automorphismes.

2.1.2 Exercices

Exercice 1

Soit E un K-espace vectoriel de dimension finie n. On fixe une base $(e_1, \ldots, e_n)$ de E.
1. Soit q une forme quadratique sur E et $M = (m_{ij})_{1 \leq i,j \leq n}$ la matrice de q dans la base précédente. Montrer que

$$q(\sum_{i=1}^{n} x_i e_i) = \sum_{i=1}^{n} m_{ii} x_i^2 + 2 \sum_{1 \leq i < j \leq n} m_{ij} x_i x_j.$$

2. Réciproquement, on se donne une application $Q : K^n \to K$ définie par

$$Q(x_1, \ldots, x_n) = \sum_{i=1}^{n} a_{ii} x_i^2 + 2 \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j.$$

Montrer que l'application $\sum_{i=1}^{n} x_i e_i \mapsto Q(x_1, \ldots x_n)$ définit une forme quadratique sur E dont la matrice dans la base canonique est $A = (a_{ij})_{1 \leq i,j \leq n}$.

Exercice 2

On dit qu'une forme quadratique q sur E *représente* l'élément $\alpha \in K^{\times}$ s'il existe $x \in E$ tel que $q(x) = \alpha$.
1. Montrer que deux formes quadratiques isométriques représentent exactement le même ensemble de scalaires.

2. Montrer que si q représente $\alpha \in K^\times$, alors il existe $\alpha_2, \ldots, \alpha_n \in K$ tels que q soit isométrique à :

$$\alpha x_1^2 + \alpha_2 x_2^2 + \cdots + \alpha_n x_n^2.$$

Exercice 3

Soit $\varepsilon_{ii\in I}$ une famille de représentants de $K^\times/(K^\times)^2$. Montrer que toute forme quadratique non dégénérée est équivalente à une forme quadratique de la forme :

$$\varepsilon_{i_1} x_1^2 + \varepsilon_{i_2} x_2^2 + \cdots + \varepsilon_{i_n} x_n^2.$$

Exercice 4

Soit (E, q) un espace quadratique.

1. Montrer que $E \cap E^\perp = \mathrm{rad}(E)$.

2. En déduire que si q est non dégénérée et si $F \subset E$ est un sous-espace totalement isotrope de E, alors $2 \dim F \leq \dim E$.

Exercice 5

On dit qu'un espace quadratique (E, q) de forme polaire f est un *plan hyperbolique* s'il admet une base $\{e_1, e_2\}$ formée de vecteurs isotropes, tels que $f(e_1, e_2) \neq 0$.

1. Soit (E, q) un plan hyperbolique. Montrer qu'il existe une base de E dans laquelle la matrice de q est $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. La forme q est-elle dégénérée ?

2. Soit (E, q) un espace quadratique non dégénéré possédant un vecteur isotrope non nul x. Montrer que E contient un sous-espace$F$ contenant x qui est un plan hyperbolique.

3. En déduire qu'une forme quadratique non dégénérée admettant un vecteur isotrope non nul représente tous les éléments de K.

Exercice 6

Soit (E, q) un espace quadratique non dégénéré sur $\mathbb{Q}$.

1. On suppose que q représente α. Montrer que la famille $q^{-1}(\{\alpha\}$ engendre E.

2. Montrer que $q^{-1}(\{\alpha\})$ est vide ou infini.

3. Montrer que

$$\{(x, y, z) \in \mathbb{Q}^3 \mid x^2 + y^2 + z^2 = 1\}$$

est infini.

2.2 Classification des formes quadratiques

Il s'agit dans ce paragraphe de donner une *classification* des formes quadratiques à isométrie près, c'est-à-dire de donner pour chaque classe de congruence d'espace quadratique, un représentant (« canonique ») de cette classe.

2.2.1 Méthode de Gauss

On va décrire un algorithme permettant de déterminer une base orthogonale pour une forme quadratique.

Théorème 2.2.1. *Soit (E, q) un espace quadratique de dimension n. Alors il existe un algorithme permettant de déterminer une base $(f_1, \dots, f_n)$de E^* et $a_1, \dots, a_n \in K$ tels que pour tout $x \in E$,*

$$q(x) = \sum_{i=1}^{n} a_i f_i(x)^2.$$

Démonstration. On raisonne par récurrence sur n. Si $q = 0$, n'importe quelle base de E convient. Sinon, fixons une base de E et écrivons

$$q(x_1, \dots, x_n) = \sum_{i=1}^{n} m_{ii} x_i^2 + 2 \sum_{1 \leq i < j \leq n} m_{ij} x_i x_j.$$

Supposons dans un premier temps que l'un des m_{ii} est non nul. On écrit alors

$$q(x_1, \dots, x_n) = m_{11} \left(x_1 + \sum_{j=2}^{n} \frac{m_{1j}}{m_{11}} x_j \right)^2 - \frac{1}{m_{11}} \left(\sum_{j=2}^{n} m_{1j} x_j \right)^2 + \sum_{i=2}^{n} m_{ii} x_i^2 + 2 \sum_{2 \leq i < j \leq n} m_{ij} x_i x_j.$$

Les trois derniers termes de cette somme définissent une forme quadratique en $n-1$ variables. Par hypothèse de récurrence, en appliquant l'algorithme à cette forme quadratique, on peut l'écrire comme combinaison linéaire de carrés de formes linéaires linéairement indépendantes $(f_2, \dots, f_n)$. Puisque la coordonnée x_1 n'apparaît dans aucune de ces formes linéaires, en posant $f_1(x_1, \dots, x_n) = x_1 + \sum_{j=2}^{n} \frac{m_{1j}}{m_{11}} x_j$, la famille $(f_1, \dots, f_n)$ est libre, c'est donc une base de E^*.
Enfin, si tous les m_{ii} sont nuls, on peut choisir i, j tels que $m_{ij} \neq 0$. On peut supposer que $i = 1$. On remplace alors e_1 par $e_1 + e_j$. Si on note f la forme polaire de q, on a $f(e_1+e_j, e_1+e_j) = q(e_1)+q(e_j)+2f(e_1, e_j) = 2m_{1j}$, et ainsi dans la base $(e_1+e_j, e_2, \dots, e_n)$, la forme q a son premier coefficient diagonal non nul, et est ramené au cas précédent. □

L'algorithme de Gauss appliqué à $q(x_1, \dots, x_n)$ de matrice M est donc le suivant :

1. Si $M = 0$, renvoyer la base canonique de E^*.
2. Sinon, si M a tous se coefficients diagonaux nuls, trouver i, j tels que $m_{ij} \neq 0$ et remplacer e_1 par $e_i + e_j$, récrire la matrice dans cette nouvelle base.
3. Ecrire q comme somme d'un multiple du carré d'une forme linéaire et d'une forme quadratique à $n-1$ variables par « identité remarquable »comme dans la démonstration.
4. Appliquer l'algorithme à la forme en $n-1$ variables.

Exemple 2.2.2. On considère $q(x_1, x_2, x_3) = 2x_1x_2 - x_3^2 + 4x_1x_3$. On a donc :

$$\begin{aligned} q(x_1, x_2, x_3) &= -(x_3 - 2x_1)^2 + 4x_1^2 + 2x_1x_2 \\ &= -(x_3 - 2x_1)^2 + 4(x_1 + \tfrac{1}{2}x_2)^2 - x_2^2. \end{aligned}$$

Remarque 2.2.3. Ce théorème est simplement une reformulation de l'existence de base orthogonales pour une forme quadratique, les formes linéaires intervenant dans ce dernier théorème étant les coordonnées du changement de base dans le théorème précédent. L'intérêt principal ici est l'aspect algorithmique.

Nous allons maintenant *classifier* les formes quadratiques sur différents corps.

2.2.2 Formes quadratiques complexes

Proposition 2.2.4. *Deux formes quadratiques sur un $\mathbb{C}$-espace vectoriel de dimension finie E sont équivalentes si et seulement si elles ont même rang.*

Démonstration. La condition est évidemment nécessaire. Réciproquement, comme tout élément de $\mathbb{C}$ est un carré, la matrice d'une forme quadratique de rang r est congruente à la matrice :

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Ainsi, deux formes quadratiques de même rang sont équivalentes. □

Remarque 2.2.5. Le résultat persiste sur tout corps algébriquement clos, et plus généralement sur tout corps *quadratiquement clos*, c'est-à-dire tout corps K tel que $K^\times/(K^\times)^2 = \{1\}$.

2.2.3 Formes quadratiques réelles, signature

Théorème 2.2.6 (Théorème d'inertie de Sylvester)**.** *Soit (E, q) un espace quadratique réel non dégénéré. Alors il existe un unique couple d'entiers (s, t) tel que la matrice de q soit congruente à :*

$$\begin{pmatrix} I_s & 0 & 0 \\ 0 & -I_t & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Le couple (s, t) s'appelle signature de q, et on a $s + t = rg(q)$.

Démonstration. L'existence d'un tel couple (s, t) et le fait que $s+t = r$ découle directement du fait que $\mathbb{R}^\times/(\mathbb{R}^\times)^2 = \{\pm 1\}$ et du théorème 2.1.17. Il reste donc à démontrer l'unicité pour les formes quadratiques non dégénérées.
On suppose q non dégénérée, et notons (e_i) et (e'_i) deux bases de E telles que $q(e_i)$ et $q(e'_i)$ soient égaux à ± 1. On note s (resp. s') le nombre de i tels que $q(e_i) = 1$ (resp. $q(e'_i) = 1$). Remarquons que la famille $(e_1, dots, e_s, e'_{s+1}, \ldots, e'_n)$ est libre. En effet, si $\sum_{i=1}^{s} a_i e_i = \sum_{i=s+1}^{n} a'_i e'_i$, alors en appliquant q on obtient $\sum a_i^2 = -\sum (a'_i)^2$, d'où la nullité de tous les coefficients. En particulier, $s + (n - s') \leq n$, donc $s \leq s'$. Par symétrie, $s = s'$, d'où le résultat. □

Remarque 2.2.7. L'existence persiste sur tous les corps dans lesquels le groupe des carrés est $\{\pm 1\}$, mais pas l'unicité. Nous allons en voir plus tard un exemple avec les corps finis.

Corollaire 2.2.8. *Deux formes quadratiques sur un espace vectoriel réel de dimension finie sont équivalentes si et seulement si elles ont même rang et même signature.*

2.2.4 Formes quadratiques sur un corps fini

Lemme 2.2.9. *Soit K un corps fini de caractéristique différente de 2, alors $K^\times/(K^\times)^2 = \{\pm 1\}$.*

Démonstration. Notons q le cardinal de K. Le morphisme de groupes

$$\begin{array}{ccc} K & \to & K \\ x & \mapsto & x^{\frac{q-1}{2}} \end{array}$$

a pour noyau $(K^\times)^2$ et pour image $\{\pm 1\}$. □

Proposition 2.2.10. *Une forme quadratique sur K de rang ≥ 2 (resp. de rang ≥ 3) représente tous les éléments de $K^\times$ (resp. de K).*

Démonstration. Soient $a, b, c \in \mathbb{F}_q$ non nuls, montrons que l'équation $ax^2 + by^2 = c$ a une solution $(x, y) \in K^2$. Soit A l'ensemble des éléments de K de la forme ax^2 et B l'ensemble des éléments de K de la forme $c - by^2$. Comme les carrés de K forment un ensemble à $\frac{q+1}{2}$ éléments, on a $\#A = \#B = \frac{q+1}{2}$, d'où $A \cap B \neq \emptyset$.
Soit maintenant q une forme quadratique de rang au moins 2, fixons-en une base orthonormée. Dans cette base, $q(x_1, \ldots, x_n) = ax_1^2 + bx_2^2 + \cdots$, avec $a, b \neq 0$. Si $c \neq 0$ et (x, y) est une solution de l'équation $ax^2 + by^2 = c$, alors $q(x, y, 0, \ldots, 0) = c$, d'où le résultat en rang ≥ 2. Si maintenant q est de rang au moins trois, on peut écrire $q(x_1, \ldots, x_n) = ax_1^2 + bx_2^2 - cx_3^2 + \cdots$, avec $a, b, c \neq 0$. On a alors $q(x, y, 1, 0, \ldots, 0) = 0$ d'où le fait que q représente de plus 0. □

Fixons maintenant un élément a de K qui n'est pas un carré.

Proposition 2.2.11. *Toute forme quadratique non dégénérée de rang n sur K est équivalente à :*

$$x_1^2 + \cdots + x_{n-1}^2 + x_n^2$$

ou

$$x_1^2 + \cdots + x_{n-1}^2 + ax_n^2$$

suivant que son discriminant est ou non un carré dans K.

Démonstration. Procédons par récurrence sur n. Si $n = 1$, c'est clair. Sinon $n \geq 2$, la proposition précédente montre que q représente 1. Elle est donc équivalente à $x_1^2 + g$ où g est une forme quadratique à $n-1$ variables à laquelle on applique l'hypothèse de récurrence. □

Corollaire 2.2.12. *Deux formes quadratiques sur K sont équivalentes si et seulement si elles ont même rang et même discriminant.*

2.2.5 Exercices

Exercice 1

1. Montrer que le groupe $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ est infini.
2. En déduire qu'il y a une infinité de classes de formes quadratiques sur un $\mathbb{Q}$-espace vectoriel non nul.

Exercice 2

Montrer qu'une forme quadratique est de rang r si et seulement si elle s'écrit comme combinaison linéaire de r carrés de formes linéaires indépendantes.

Exercice 3

Soit q une forme quadratique réelle non dégénérée de signature $(p, n-p)$.
1. Montrer que l'ensemble des solutions de l'équation $q(x) = 1$ est homéomorphe à $\mathbb{S}^{p-1} \times \mathbb{R}^{n-p}$.
2. Montrer que $SL_2(\mathbb{R})$ est homéomorphe à $\mathbb{S}^1 \times \mathbb{R}^2$.

Exercice 4

Soit $A \subset \mathcal{P}$ un sous-ensemble du plan affine réel. On appelle droite de A toute droite passant par deux points de A, et cercle de A tout cercle centré en un point de A et dont le rayon est la distance entre deux points de A. On dit qu'un point $P \in \mathcal{P}$ est *constructible* en une étape à partir de A s'il est point d'intersection de deux droites, deux cercles ou une droite et un cercle de A. On dit qu'un point P est constructible à partir de A s'il existe une suite finie d'ensembles

$$A = A_0 \subset A_1 \subset \cdots \subset A_n$$

telle que tous les points de A_{i+1} soient constructibles en une étape à partir de A_i, et $P \in A_n$. Enfin, on dit qu'un point $P \in \mathcal{P}$ est constructible si P est constructible à partir de $\{(0,0),(1,0)\}$, et qu'un nombre $z \in \mathbb{C}$ est constructible si c'est l'affixe d'un point constructible.

1. Montrer que si P est constructible en une étape à partir de A, alors les coordonnées de P sont solutions d'une équation de degré 1 ou 2 dont les coefficients sont des coordonnées d'éléments de A.

2. Montrer qu'un nombre complexe $z \in \mathbb{C}$ est constructible si et seulement si ses parties réelle et imaginaire le sont.

3. Montrer que si les nombres réels x et y sont constructibles, alors $-x$, $x+y$ et xy sont constructibles. Montrer que si x est non nul, alors $1/x$ est constructible. Que peut-on en déduire sur l'ensemble des nombres complexes constructibles ?

4. Montrer que si $x \in \mathbb{R}$ est constructible, alors $\sqrt{x}$ est constructible. En déduire que la réciproque du résultat de la question 1. est vraie.

5. On note K le corps des nombres constructibles. Montrer que deux formes quadratiques sur K sont équivalentes si et seulement si elles ont même rang.

Exercice 5

Le but de cet exercice est de démontrer le *lemme de Morse* :

Proposition 2.2.13 (Lemme de Morse)**.** *Soit U un ouvert de $\mathbb{R}^n$ contenant l'origine et $f : U \to \mathbb{R}$ une application de classe $\mathcal{C}^3$. On suppose que $f(0) = 0$, $Df(0) = 0$ et que la hessienne de f en 0 est une forme quadratique non dégénérée de signature $(s, n-s)$. Alors il existe des voisinages $0 \in V \subset U$ et $0 \in W \subset \mathbb{R}^n$ et un difféomorphisme φ de V dans W tels que $\varphi(0) = 0$ et pour tout $x \in V$, si on note $(u_1, \ldots, u_n)$ les coordonnées de $\varphi(x)$, on ait :*

$$f(x) = u_1^2 + \cdots + u_s^2 - u_{s+1}^2 - \cdots - u_n^2.$$

1. *On note S l'ensemble des matrices symétriques réelles. Soit $A \in S$, montrer qu'il existe un difféomorphisme ψ d'un voisinage V de A dans S vers $GL_n(\mathbb{R})$ tel que pour tout $M \in V$, $M = {}^t\psi(M)A\psi(M)$. (On pourra chercher à appliquer le théorème d'inversion locale).*

2. *Démontrer le lemme de Morse en appliquant la formule de Taylor avec reste intégrale à la fonction f.*

Exercice 6

Soient $(E,q), (F,q')$ des espaces quadratiques réels de dimension finie, de formes polaires respectives f, f'.

1. Montrer que l'on peut définir une structure d'espace quadratique sur $E \otimes F$ en posant $g(x \otimes x', y \otimes y') = f(x, x')g(y, y')$.
2. Déterminer le rang et la signature de $E \otimes F$ en fonction de ceux de E et F.

2.3 Théorie de Witt

Le but de la théorie de Witt est de comprendre les propriétés de prolongement des formes quadratiques.

2.3.1 Sous-espaces isotropes

Définition 2.3.1. On rappelle qu'un sous-espace est dit *isotrope* s'il admet une base de vecteurs isotropes.

2.3.2 Théorème de Witt

On se donne deux espaces quadratiques non dégénérés (E, q) et (E', q'). Soit $F \subset E$ un sous-espace vectoriel et $u : F \to E'$ un morphisme métrique *injectif*. On veut prolonger u à un sous-espace plus grand que F.

Lemme 2.3.2. *Si F est dégénéré, il existe un sous-espace $F \subset F_1 \subset E$ dont F est un hyperplan, tel que u se prolonger en un morphisme métrique injectif $F_1 \to E$.*

Démonstration. On note f la forme polaire associée à q. Soit $x \in \mathrm{rad}(F)$, non nul, et soit $g \in E^*$ tel que $g(x) = 1$. Comme E est non dégénéré, il existe $y \in E$ tel que $g(z) = f(z, y)$ pour tout $z \in E$. On peut supposer que y est isotrope quitte à le remplacer par $y - \lambda x$ avec $\lambda = \frac{1}{2}q(y)$. Alors $F_1 = F \oplus Ky$ admet F comme hyperplan. On peut réaliser la même construction avec $F' = u(F) \subset E'$, pour obtenir $F'_1 = F' \oplus Ky'$ (*via* la forme quadratique q' et $g' = g \circ u^{-1}$). On prolonge alors u en envoyant y sur y'. L'application u ainsi obtenue est toujours injective, et si $z_1 \in F_1$, avec $z_1 = z + \alpha y$, on a $q(z_1) = q(z) + \alpha f(z, y)$ et $q'(u(z_1)) = q'(u(z)) + \alpha f'(u(z), y') = q(u(z)) + \alpha g(z) = q(z) + \alpha f(z, y)$. Cela démontre le résultat. □

Théorème 2.3.3 (Witt)**.** *Si (E, q) et (E', q') sont isométriques et non dégénérés, alors tout morphisme métrique injectif $u : F \to E'$ se prolonge à E en une isométrie.*

Démonstration. On peut supposer que $E = E'$ (car ils sont isométriques) et que F est non dégénéré (d'après le lemme). Notons f la forme polaire associée à q. Raisonnons alors par récurrence sur la dimension de F. Si $\dim F = 1$, soit $\{x\}$ une base de F. Comme F est non dégénéré, x n'est pas isotrope. On a $q(x) = q(u(x))$. Posons $y = u(x)$, on peut choisir $\varepsilon \in \pm 1$ tel que $x + \varepsilon y$ soit non isotrope. Sinon, $q(x+y) = 0 = q(x-y)$, d'où $q(x) = q(y) = 0$. On fixe un tel ε, soit H l'hyperplan orthogonal à $z = x + \varepsilon y$. On a donc $E = H \oplus^{\perp} Kz$. Soit maintenant σ la symétrie par rapport à H, c'est-à-dire l'automorphisme fixant les éléments de H et envoyant z sur $-z$. On a $f(x - \varepsilon y, x + \varepsilon y) = q(x) - \varepsilon^2 q(y) = 0$, donc $x - \varepsilon y \in H$. Il en découle que $\sigma(x) = -\varepsilon y$. Ainsi, $-\varepsilon\sigma$ est une isométrie qui prolonge u.
Si $\dim F > 1$, on écrit $F = F_1 \oplus^{\perp} F_2$ avec $F_1, F_2 \neq \{0\}$. Par hypothèse de récurrence, $u_{|F_1}$ se prolonge en une isométrie de E. Quitte à composer par l'inverse de cette isométrie, on peut donc supposer que $u_{|F_1} = \mathrm{id}$. On a alors $u(F_2) \subset F_1^{\perp} (\subset E)$. En effet, si $x_1 \in F_1$ et $x_2 \in F_2$, on a $f(u(x_2), x_1) = f(u(x_2), u(x_1)) = f(x_2, x_1) = 0$. Par hypothèse de récurrence,

$u_{|F_2}$ se prolonge donc en une isométrie v de $F_1^\perp$. L'isométrie qui est l'identité sur F_1 et v sur $F_1^\perp$ prolonge u. □

Corollaire 2.3.4. *Deux sous-espaces isométriques d'un espace quadratique ont des orthogonaux isométriques.*

Démonstration. On prolonge une isométrie entre les sous-espaces en une isométrie de l'espace ambiant, elle induit alors une isométrie entre les orthogonaux. □

Corollaire 2.3.5. *Soit (E, q) un espace quadratique non dégénéré, il existe une décomposition en somme directe orthogonale :*

$$E = \left(\bigoplus_{i=1}^{m} H_i \right) \oplus F$$

où les H_i sont des plans hyperboliques et où $q_{|F}$ ne représente pas zéro. Cette décomposition est unique à isométrie près, en particulier l'entier m ne dépend pas de la décomposition choisie.

Démonstration. Existence. Si q ne représente pas zéro, c'est clair. Sinon, E contient un sous-espace H_1 isométrique à un plan hyperbolique : $E = H_1 \oplus F_1$, et on conclut par récurrence sur $\dim E$.
Unicité. Supposons que $E = (\bigoplus_{i=1}^{m} H_i) \oplus F = \left(\bigoplus_{i=1}^{m'} H_i'\right) \oplus F'$ et $m \leq m'$. Les espaces $\bigoplus_{i=1}^{m} H_i$ et $\bigoplus_{i=1}^{m} H_i'$ sont isométriques, donc (d'après le théorème de Witt) $\left(\bigoplus_{i=m+1}^{m'} H_i\right) \oplus F'$ et F sont isométriques. Si $m' > m$, alors $q_{|F}$ représente 0, ce qui est absurde. Donc $m = m'$ et F' est isométrique à F. □

2.4 Espaces euclidiens, hermitiens

Définition 2.4.1. Soit E un espace vectoriel sur $\mathbb{R}$ (resp. sur $\mathbb{C}$). On appelle produit scalaire (resp. produit hermitien) une application sesquilinéaire, définie positive sur E. Un espace euclidien (resp. hermitien) est un espace vectoriel sur $\mathbb{R}$ (resp. sur $\mathbb{C}$) muni d'un produit scalaire (resp. hermitien). La racine carrée de la forme quadratique associée est appelée *norme*.

Lemme 2.4.2 (Inégalité de Cauchy-Schwarz)**.** *Soit $(\cdot, \cdot)$ un produit scalaire ou hermitien sur E. Alors pour tous $x, y \in E$, on a*

$$|(x, y)| \leq \|x\| \|y\|.$$

Théorème 2.4.3 (Riesz)**.** *Soit E un espace euclidien. L'application*

$$\begin{array}{ccc} E & \to & E^* \\ x & \mapsto & (\cdot, x) \end{array}$$

est un isomorphisme.

Démonstration. Comme le produit scalaire fournit une forme quadratique non dégénérée, la proposition 2.1.10 montre que directement que cette application est un isomorphisme. □

Comme précédemment, tous les résultats concernant l'orthogonalité persistent :

Corollaire 2.4.4. *Soit E un espace euclidien. Pour $A \subset E$, on note*

$$A^\perp = \{x \in E \mid \forall y \in A, (x, y) = 0\}.$$

Alors :

- *$A^\perp$ est un sous-espace vectoriel de E,*
- *si $B \subset A$, alors $A^\perp \subset B^\perp$,*
- *si $F \subset E$ est un sous-espace vectoriel, alors*

$$E = F \oplus F^\perp,$$

- *si $F, G \subset E$ sont deux sous-espaces vectoriels, alors*

$$(F + G)^\perp = F^\perp \cap G^\perp.$$

Remarque 2.4.5. On a des résultats analogues pour les espaces hermitiens. Dans ce cas, on ne peut pas directement utiliser la proposition 2.1.10 car l'application $E \to E^*$ ainsi définie n'est pas linéaire mais anti-linéaire. Pour conserver la linéarité, on peut remplacer cette application par $x \mapsto (\cdot, \bar{x})$.

2.4.1 Endomorphisme adjoint

Proposition-Définition 2.4.6. Soit E un espace euclidien ou hermitien, et soit $u \in \mathcal{L}(E)$. Alors il existe un unique $u^* \in \mathcal{L}(E)$ tel que pour tous $x, y \in E$, on ait :

$$(u(x), y) = (x, u^*(y)).$$

L'endomorphisme u^* s'appelle *adjoint* de u.

Démonstration. L'application $x \mapsto (u(x), y)$ est une forme linéaire sur E. D'après le théorème de Riesz, il existe $u^*(y) \in E$ tel que $(u(x), y) = (x, u^*(y))$. Il reste donc à montrer que u^* est linéaire. Soient $\lambda \in K$, $y, y' \in E$, on a par définition, pour tout $x \in E$, $(u(x), \lambda y + y') = (x, u^*(\lambda y + y'))$. Par semi-linéarité à droite, on a donc pour tout $x \in E$,

$$(x, \lambda u^*(y) + u^*(y')) = \bar{\lambda}(x, u^*(y)) + (x, u^*(y')) = \bar{\lambda}(u(x), y) + (u(x), y') = (x, u^*(\lambda y + y')).$$

Comme $x \mapsto (y \mapsto (x, y))$ est injective, on a bien $u^*(\lambda y + y') = \lambda u^*(y) + u^*(y')$. □

Définition 2.4.7. On dit que u est *autoadjoint* (ou *symétrique*, si $K = \mathbb{R}$) lorsque $u = u^*$.

2.4.2 Exercices

2.5 Réduction des endomorphismes normaux

Définition 2.5.1. Soit E un espace euclidien ou hermitien, et $u \in \mathcal{L}(E)$. On dit que u est *normal* si u et $u*$ commutent.

Le but de cette partie est d'étudier la réduction des endomorphismes normaux, et de l'appliquer aux cas particuliers des endomorphismes hermitiens et des endomorphismes orthogonaux.

2.5.1 Réduction des endomorphismes normaux

Théorème 2.5.2. *Soit E un espace hermitien, alors $u \in \mathcal{L}(E)$ est normal si et seulement si E admet une base orthonormée de vecteurs propres de u.*
Soit E un espace euclidien, alors $u \in \mathcal{L}(E)$ est normal si et seulement s'il existe une base orthonormée de E dans laquelle la matrice de u est diagonale par blocs, et dont les blocs diagonaux sont des homothéties ou des similitudes en dimension 2.

Pour la démonstration de ce théorème, nous aurons besoin du lemme suivant :

Lemme 2.5.3. *Soit $u \in \mathcal{L}(E)$ normal, et soit $\lambda \in \mathbb{C}$. Alors*

$$\ker(u - \lambda id) = \ker(u^* - \bar{\lambda} id).$$

Démonstration. Puisque u est normal, $u - \lambda\mathrm{id}$ est encore normal, et son adjoint est $u^* - \bar{\lambda}\mathrm{id}$. Par conséquent, il suffit de traiter le cas $\lambda = 0$. Or $x \in \ker u$ si et seulement si $(u(x), u(x)) = 0$, ce qui équivaut à $(u * (x), u^*(x)) = 0$ car u est normal. □

Démonstration du théorème. Traitons d'abord par récurrence le cas hermitien. Soit λ une valeur propre de u, alors $E_\lambda = \ker(u - \lambda) = \ker(u^* - \bar{\lambda})$. Comme E_λ est stable par u^*, son orthogonal est stable par u. Notons F cet orthogonal, l'endomorphisme induit par u sur F est également normal (et son adjoint est l'endomorphisme induit par u^*). Par hypothèse de récurrence, cet endomorphisme est diagonalisable dans une base orthonormée. Comme on peut fixer une base orthonormée de E_λ, le résultat est démontré.
Le cas euclidien sera traité en exercice. □

2.5.2 Théorème spectral

Théorème 2.5.4 (Théorème spectral)**.** *Soit E un espace euclidien (resp. hermitien), et soit $u \in \mathcal{L}(E)$ symétrique (resp. autoadjoint). Alors u est diagonalisable dans une base orthornormée, et ses valeurs propres sont réelles.*

Démonstration. Traitons d'abord le cas complexe. Puisque u est autoadjoint, il est normal. De plus, ses valeurs propres dans $\mathbb{C}$ sont réelles. En effet, si $\lambda \in \mathbb{C}$, on a $\ker(u - \lambda\mathrm{id}) = \ker(u - \bar{\lambda}\mathrm{id})$, donc lorsque λ est valeur propre de u, $\lambda = \bar{\lambda}$ et $\lambda \in \mathbb{R}$. Pour conclure sur le cas réel, il faut vérifier que deux matrices réelles unitairement semblables sont orthogonalement semblables, ce qui sera fait en exercice. □

Corollaire 2.5.5. *Soient A symétrique (resp. hermitienne) définie positive, et B symétrique. Alors il existe P inversible telle que*

$$^tPAP = I \text{ et } ^tPBP \text{ diagonale.}$$

Démonstration. La matrice A définit un produit scalaire pour lequel on vérifie que $A^{-1}B$ est autoadjointe. Il existe donc une base orthogonale pour A formée de vecteurs propres pour $A^{-1}B$: il suffit de prendre pour P la matrice de passage vers cette base. □

2.5.3 Endomorphismes orthogonaux et unitaires

Soit E un espace euclidien (resp. hermitien). On rappelle qu'un endomorphisme u de$E$ est orthogonal (resp. unitaire) si $uu^* = \mathrm{id}$.

Théorème 2.5.6. *Soit E un espace hermitien. Alors $u \in \mathcal{L}(E)$ est unitaire si et seulement si u est diagonalisable dans une base orthonormée et a pour valeurs propres des nombres complexes de module* 1.
Soit E un espace euclidien. Alors $u \in \mathcal{L}(E)$ est orthogonal si et seulement s'il existe une base orthonormée de E dans laquelle la matrice de u est diagonale par blocs, avec des blocs diagonaux qui sont homothéties de rapport ± 1 ou des matrices de rotations en dimension 2.

2.5.4 Décomposition polaire

Théorème 2.5.7. *Soit $u \in GL_n(\mathbb{R})$, alors il existe une unique décomposition $u = so$ avec s symétrique défini positif et o orthogonal.*

Remarque 2.5.8. L'appellation « décomposition polaire » est à rapprocher de l'utilisation des coordonnées polaires. En effet, la similitude d'angle θ et de rapport ρ admet pour décomposition polaire s = l'homothétie de rapport ρ et o = la rotation d'angle θ. C'est également la multiplication par $\rho e^{i\theta}$ dans $\mathbb{C}$, vue comme application $\mathbb{R}$-linéaire.

Démonstration. Soit $u \in GL_n(\mathbb{R})$, alors uu^* est symétrique, défini et positif pour la structure euclidienne canonique de $\mathbb{R}$. Si $u = so$, alors $uu^* = soo^*s^* = s^2$. Soit alors s une racine carrée de l'endomorphisme uu^*. Une telle racine carrée existe car u est diagonalisable (dans une base orthonormée) et a toutes ses valeurs propres strictement positives. On peut alors considérer l'endomorphisme dont la matrice dans cette base a pour i-ème coefficient la racine carrée de la i-ème valeur propre de uu^* qui nous fournit une racine carrée. En posant $o = s^{-1}u$, on vérifie immédiatement que o est orthogonal. L'unicité découle du fait qu'un endomorphisme symétrique défini positif a une unique racine carrée symétrique définie positive. □

2.5.5 Exercices

Exercice 1

Soit (E, q) un espace quadratique non dégénéré. On rappelle qu'un sous-espace totalement isotrope de E est un sous-espace vectoriel de E constitué de vecteurs isotropes.
1. Expliquer pourquoi tout sous-espace totalement isotrope est contenu dans un sous-espace totalement isotrope maximal pour l'inclusion.
2. Soient F, F' deux sous-espaces totalement isotropes de E. On suppose que $\dim F \leq \dim F'$. Montrer qu'il existe une isométrie u de E telle que $u(F) \subset F'$.
3. En déduire que le groupe des isométries de E opère transitivement sur l'ensemble des sous-espaces totalement isotropes maximaux de E, et qu'ils ont donc tous la même dimension.

Exercice 2

Soit (E, q) un espace quadratique non dégénéré, que l'on suppose isométrique à la somme directe orthogonale :

$$\left(\bigoplus_{1 \leq i \leq r} \mathbf{H}_i \right) \oplus F,$$

avec F anisotrope et les $\mathbf{H}_i$ sont des plans hyperboliques.
1. Montrer que E a un sous-espace totalement isotrope maximal de dimension r.

2. En déduire que la dimension des sous-espaces totalement isotropes maximaux de E est égale à son indice d'isotropie.
3. On suppose que E est un espace quadratique réel (non dégénéré) de signature (s,t). Montrer que son indice d'isotropie est $\min\{s,t\}$.
4. On suppose que E est un espace quadratique complexe (non dégénéré) de dimension n. Déterminer son indice d'isotropie.

Exercice 3

Soit E un espace euclidien.
1. On suppose que $\dim E = 2$. Soit $u \in \mathcal{L}(E)$ est normal et n'a pas de valeurs propres réelles. Montrer que dans toute base orthonormée, la matrice de u est une similitude.
2. On suppose $\dim E \geq 2$. On suppose que $u \in \mathcal{L}(E)$ est normal et n'a pas de valeurs propres réelles, montrer que u admet un sous-espace stable de dimension 2 dont l'orthogonal est stable.
3. Démontrer le théorème de réduction des endomorphismes normaux dans un espace euclidien.

Exercice 4

1. Soit $A, B \in \mathcal{M}_n(\mathbb{R})$. On suppose que A et B sont unitairement semblables. Montrer que A et B sont orthogonalement semblables.
2. En déduire le théorème spectral pour les endomorphismes symétriques réels.

Exercice 5

Soit $(E, \langle .,. \rangle)$ un espace euclidien et soit G un sous-groupe fini de $GL(E)$.
1. Montrer que l'application

$$(x,y) \mapsto \frac{1}{|G|} \sum_{g \in G} \langle gx, gy \rangle$$

est un produit scalaire sur E.
2. Montrer que le produit scalaire précédent, noté $\langle .,. \rangle_G$ est invariant par tous les éléments de G (c'est-à-dire que pour tous $x, y \in E$ et pour tout $g \in G$, on a $\langle x,y \rangle_G = \langle gx, gy \rangle_G$).
3. En déduire que G est conjugué à un sous-groupe de $O(E)$.
Remarque. On peut montrer (mais c'est plus difficile) que ce résultat reste vrai dans le cas où G est seulement supposé compact.

Exercice 6

Soit $E = \mathbb{R}[X]$, et pour $n \geq 0$, $E_n = \mathbb{R}_n[X]$. On définit sur $E \times E$ l'application :

$$(P,Q) = \int_0^1 P(t)Q(t)dt.$$

On fixe un entier $n \geq 0$.
1. Montrer que la restriction à $E_n \times E_n$ de l'application précédente fait de E_n un espace euclidien.

2. Pour tout $0 \leq i \leq n$, on note P_i le polynôme obtenu en appliquant le procédé d'orthonormalisation de Gram-Schmidt à la base $(1, X, \ldots, X^n)$ de E_n. Montrer que P_n a n racines réelles distinctes dans l'intervalle $]0, 1[$.

3. On note $x_1, \ldots, x_n$ les racines de P_n. Montrer qu'il existe une unique famille de nombres réels $(\omega_1, \ldots, \omega_n)$ tels que pour tout $P \in E_{n-1}$, $\int_0^1 P(t)dt = \sum_{i=1}^n \omega_i P(x_i)$.

4. En utilisant la division euclidienne par P_n, montrer que la formule précédente reste valable pour $P \in E_{2n-1}$. Montrer que la formule n'est pas valable pour $P \in E_{2n}$.

5. Montrer que s'il existe $x'_1, \ldots, x'_n \in \mathbb{R}$ et $\omega'_1, \ldots \omega'_n$ tels que pour tout $P \in E_{2n-1}$ on ait $\int_0^1 P(t)dt = \sum_{i=1}^n \omega_i P(x_i)$, alors nécessairement les x'_i sont les x_i et les ω'_i sont les ω_i.