Sommaire

$(G,\cdot)$ est un groupe, $\mathcal{S}(E)$ le groupe des permutations d'un ensemble $E \neq \emptyset$.

1 Définitions et exemples

Définition 1 *On dit que G opère à gauche sur E si on a une application :*

$$\begin{array}{ccc} G \times E & \to & E \\ (g,x) & \mapsto & g \cdot x \end{array}$$

telle que :

$$\begin{cases} \forall x \in E,\ 1 \cdot x = x \\ \forall (g,g',x) \in G^2 \times E,\ g \cdot (g' \cdot x) = (gg') \cdot x \end{cases}$$

Exemple 1 *G agit sur lui même par translations à gauche : $(g,h) \in G \times G \mapsto g \cdot h = gh$*
G agit sur lui même par conjugaison : $(g,h) \in G \times G \mapsto g \cdot h = ghg^{-1}$
G agit sur tout sous-groupe distingué H par conjugaison : $(g,h) \in G \times H \mapsto g \cdot h = ghg^{-1} \in H$
$\mathcal{S}(E)$ agit naturellement sur E par :

$$(\sigma, x) \in \mathcal{S}(E) \times E \mapsto \sigma \cdot x = \sigma(x) \in E$$

2 Orbites et stabilisateurs

Soit G un groupe opérant sur un ensemble non vide E.

Définition 2 *Pour tout $x \in E$, le sous-ensemble de E : $G \cdot x = \{g \cdot x \mid g \in G\}$ est appelé orbite de x sous l'action de G.*

Ces orbites forment une partition de E.

Exemple 2 *Pour l'action de $\mathcal{S}(E)$ sur E il y a une seule orbite.*
Pour l'action de G sur lui même par conjugaison, les orbites sont appellées classes de conjugaison.
Si H est un sous-groupe de G, il agit par translation à droite sur G :

$$(h,g) \in H \times G \mapsto h \cdot g = gh$$

et pour tout $g \in G$ l'orbite de g est la classe à gauche modulo H, gH. L'ensemble de ces orbites et l'ensemble quotient G/H des classes à gauche modulo H.

Définition 3 *On dit que l'action de G sur E est transitive si :*

$$\forall (x,y) \in E^2,\ \exists g \in G \mid y = g \cdot x$$

Dans le cas d'une action transitive, il y a une seule orbite.

Théorème 1 (Cayley) *L'action de G sur lui même par translation à gauche est fidèle (i. e. $g \in G \mapsto (x \mapsto g \cdot x) \in \mathcal{S}(E)$ est injective) et G est isomorphe à un sous-groupe de $\mathcal{S}(G)$.*

Exercice 1 *Déterminer les orbites pour l'action de $\mathcal{O}_n(\mathbb{R})$ sur $\mathbb{R}^n$ définie par :*

$$\forall (A,x) \in \mathcal{O}_n(\mathbb{R}) \times \mathbb{R}^n,\ A \cdot x = A(x)$$

Exercice 2 *Déterminer les orbites pour l'action de $G = GL_n(\mathbb{K}) \times GL_m(\mathbb{K})$ sur $E = \mathcal{M}_{n,m}(\mathbb{K})$ définie par :*

$$\forall (P,Q) \in G,\ \forall A \in E,\ (P,Q) \cdot A = PAQ^{-1}$$

Définition 4 *Pour tout $x \in X$, le sous-ensemble de G : $G_x = \{g \in G \mid g \cdot x = x\}$est le stabilisateur de x sous l'action de G.*

Théorème 2 *Pour tout $x \in E$ l'application :*

$$\begin{array}{rccc} \varphi_x : & G/G_x & \to & G \cdot x \\ & \overline{g} = gG_x & \mapsto & g \cdot x \end{array}$$

est bien définie et bijective. Dans le cas où G fini, on a :

$$\operatorname{card}(G \cdot x) = [G : G_x] = \frac{\operatorname{card}(G)}{\operatorname{card}(G_x)}$$

3 Équation des classes

Soit $(G,\cdot)$ est un groupe fini opérant sur un ensemble fini E.

Théorème 3 (équation des classes) *En notant $G\cdot x_1,\cdots,G\cdot x_r$ toutes les orbites deux à deux distinctes, on a :*

$$\operatorname{card}(E)=\sum_{i=1}^{r}\operatorname{card}(G\cdot x_i)=\sum_{i=1}^{r}\frac{\operatorname{card}(G)}{\operatorname{card}(G_{x_i})}$$

Théorème 4 *Pour tout nombre premier p, le centre d'un p-groupe n'est pas réduit à $\{1\}$.*

Théorème 5 *Tout groupe d'ordre p^2 avec p premier est commutatif.*

Théorème 6 (Cauchy) *Si G est un groupe fini d'ordre $n\geq 2$, alors pour tout diviseur premier p de n, il existe dans G un élément d'ordre p (et donc un sous-groupe d'ordre p).*

Exercice 3 *Pour tout $g\in G$, on note :* $\operatorname{Fix}(g)=\{x\in E\mid g\cdot x=x\}$.
Montrer que le nombre d'orbites est : $r=\dfrac{1}{\operatorname{card}(G)}\sum_{g\in G}\operatorname{card}(\operatorname{Fix}(g))$.

4 Le groupe des isométries du cube

On se place dans l'espace vectoriel euclidien $\mathbb{R}^3$ muni d'un repère orthonormé, $A_1,\cdots,A_8$ sont les huits points de coordonnées $(\pm1,\pm1,\pm1)$ et $\mathcal{C}$ est le cube de sommets $A_1,\cdots,A_8$.

Le cube $\mathcal{C}$ est l'enveloppe convexe de l'ensemble $\mathcal{S}=\{A_1,\cdots,A_8\}$ de ses sommets.

On désigne par $Is(\mathcal{C})=\left\{\varphi\in\mathcal{O}(\mathbb{R}^3)\mid\varphi(\mathcal{C})=\mathcal{C}\right\}$ le groupe des isométries de $\mathbb{R}^3$ qui conservent $\mathcal{C}$ et par $Is^+(\mathcal{C})=Is(\mathcal{C})\cap\mathcal{O}^+(\mathbb{R}^3)$ le sous-groupe de $\mathcal{O}(\mathbb{R}^3)$ formé des rotations qui conservent $\mathcal{C}$.

Théorème 7 *$Is(\mathcal{C})=Is(\mathcal{S})$ est un groupe fini isomorphe à un sous groupe du groupe symétrique $\mathcal{S}_8$. On a :* $\operatorname{card}(Is(\mathcal{C}))=2\operatorname{card}(Is^+(\mathcal{C}))$.

Théorème 8 *Le groupe $Is(\mathcal{C})$ agit de façon transitive sur $\mathcal{S}$ et a 48 éléments.*

On peut donner la liste de tous les éléments de $Is^+(\mathcal{C})$ en fonction de leurs ordres.

Comme élément d'ordre 1, il n'y a que $Id_{\mathbb{R}^3}$.

Comme éléments d'ordre 2, on a les 3 rotations d'axes Ox, Oy et Oz, d'angle π et les 6 rotations d'axes dirigés par les milieux des arêtes $[A_1,A_4]$, $[A_1,A_2]$, $[A_2,A_3]$, $[A_3,A_4]$, $[A_1,A_4]$, $[A_1,A_5]$, $[A_4,A_8]$, d'angle π.

Commes éléments d'ordre 3, on à les 8 rotations d'axes les 4 grandes diagonales et d'angles $\pm\dfrac{2\pi}{3}$.

Commes éléments d'ordre 4, on a les 6 rotations d'axes respectifs Ox, Oy et Oz, d'angles de $\pm\dfrac{\pi}{2}$.

Ce qui donne un total de $1+9+8+6=24$ et on les a toutes.

Permutations d'un ensemble fini, groupe symétrique. Applications

E est un ensemble fini de cardinal $n \geq 2$.

1 Permutations d'un ensemble fini

On note $\mathcal{S}(E)$ le groupe des permutations de E et $\mathcal{S}_n$ le groupe symétrique.
Tout groupe de permutations d'un ensemble E à n éléments est isomorphe à$\mathcal{S}_n$.

Théorème 1 $\text{card}(\mathcal{S}(E)) = n!$

Exercice 1 *Calculer le nombre de dérangement de* $\{1, 2, \cdots, n\}$.

Définition 1 *Le support d'une permutation* $\sigma \in \mathcal{S}(E)$ *est le complémentaire dans* E *de l'ensemble de ses points fixes.*

Exercice 2 $\mathcal{S}_3$ *est, à isomorphisme près, le seul groupe d'ordre* 6 *non commutatif.*

2 Décomposition en produits de cycles

On note, pour $\sigma \in \mathcal{S}(E)$ et $x \in E$, $Orb_\sigma(x) : Orb_\sigma(x) = \{\sigma^r(x) \mid r \in \mathbb{Z}\}$ l'orbite de x suivant σ. Ces orbites forment une partition de E.

Définition 2 *Un cycle est une permutation pour laquelle il n'existe qu'une seule orbite non réduite à un point. Le cardinal* $r \geq 2$ *de cette orbite est la longueur de ce cycle. On dit que* σ *est un* r*-cycle.*

Un r-cycle est d'ordre r dans le groupe $\mathcal{S}(E)$.

Définition 3 *On appelle transposition un* 2*-cycle.*

Exercice 3 *Montrer que deux cycles sont de même longueur si, et seulement si, ils sont conjugués dans* $\mathcal{S}(E)$*).*

Exercice 4 *Déterminer, pour* $n \geq 3$, *le centre* $Z(\mathcal{S}(E))$ *de* $\mathcal{S}(E)$.

Théorème 2 *Toute permutation* $\sigma \in \mathcal{S}(E) \setminus \{Id_E\}$ *se décompose en produit de cycles de supports deux à deux disjoints. Cette décomposition est unique à l'ordre près.*[1]

Corollaire 1 *Si* $\sigma = \sigma_1 \cdots \sigma_p$ *est « la » décomposition de* $\sigma \in \mathcal{S}(E) \setminus \{Id_E\}$ *en produit de cycles de supports deux à deux disjoints, on a alors :*

$$\text{ordre}(\sigma) = \text{ppcm}(\text{ordre}(\sigma_1), \cdots, \text{ordre}(\sigma_r))$$

Corollaire 2 *Toute permutation* $\sigma \in \mathcal{S}(E)$ *se décompose en produit de transpositions (le groupe* $\mathcal{S}(E)$ *est engendré par les transpositions).*

Exercice 5 *Montrer que* $\mathcal{S}_n$ *est engendré par*

1. *les* $n-1$ *transpositions* $(1, k)$ *où* $2 \leq k \leq n$ *;*
2. *les* $n-1$ *transpositions* $(k, k+1)$ *où* $1 \leq k \leq n-1$ *;*
3. *par* $(1, 2)$ *et* $(1, 2, \cdots, n)$ *(on dit que* $\mathcal{S}_n$ *est dicyclique) ;*
4. *pour* $n \geq 3$, *par* $(1, 2)$ *et* $(2, 3, \cdots, n)$.

3 Signature d'une permutation

Définition 4 *La signature de* $\sigma \in \mathcal{S}(E)$ *est :* $\varepsilon(\sigma) = (-1)^{n-\mu(\sigma)}$, *où* $\mu(\sigma)$ *est le nombre de* σ*-orbites distinctes.*

Théorème 3 *Si* $\sigma \in \mathcal{S}(E)$ *est produit de* p *transpositions, on a alors* $\varepsilon(\sigma) = (-1)^p$.

Théorème 4 *Pour toute permutation* $\sigma \in \mathcal{S}_n$, *on a :* $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$.

Théorème 5 *Les seuls morphismes de groupes de* $\mathcal{S}(E)$ *dans* $\{-1, 1\}$ *sont l'application constante égale à* 1 *et la signature* ε.

[1] Développement possible

4 Le groupe alterné

Définition 5 *Le groupe alterné est le sous-ensemble de $\mathcal{S}(E)$ formé des permutations de signature égale à 1.*

Pour $E = \{1, 2, \cdots, n\}$, on note $\mathcal{A}_n$ le groupe alterné.

Remarque 1 *$\mathcal{A}(E)$ est un sous-groupe distingué d'indice 2 de $\mathcal{S}(E)$ et $\text{card}(\mathcal{A}(E)) = \dfrac{n!}{2}$.*

Pour $n = 2$, on a $\mathcal{A}(E) = \{Id_E\}$. Dans ce qui suit, on suppose que $n \geq 3$.

Remarque 2 *$\mathcal{A}_3$ est cyclique engendré par $(1, 2, 3)$.*

Exercice 6 *Montrer que $\mathcal{A}_4$ (qui est d'ordre 12) n'a pas de sous-groupe d'ordre 6.*

Exercice 7 *Montrer que, pour $n \geq 5$, le produit de deux transpositions de supports disjoints sont conjugués dans $\mathcal{A}(E)$.*

Théorème 6 *Pour $n \geq 3$, $\mathcal{A}(E)$ est engendré par les 3-cycles.*

Théorème 7 *Pour $n \geq 5$, les sous-groupes distingués de $\mathcal{S}(E)$ sont $\{Id\}$, $\mathcal{A}(E)$ et $\mathcal{S}(E)$.*[2]

Exercice 8 *Montrer que $\mathcal{A}(E)$ est stable par tout automorphisme de $\mathcal{S}(E)$.*

Exercice 9 *Montrer que, pour $n \geq 3$, $\mathcal{A}_n$ est engendré par*

1. *les 3-cycles $\gamma_k = (1, 2, k)$ où $3 \leq k \leq n$;*
2. *les 3-cycles $(k, k+1, k+2)$ où $1 \leq k \leq n-2$.*

Exercice 10 *Déterminer, pour $n \geq 4$, le centre de $\mathcal{A}(E)$.*

Exercice 11 *Ici E est un ensemble à 5 éléments.*

1. *Donner une description de $\mathcal{A}(E)$ en classant ses élément en fonction de leur ordre.*
2. *Montrer que $\mathcal{A}(E)$ est simple.*

Théorème 8 *Pour $n = 3$ ou $n \geq 5$ le groupe $\mathcal{A}(E)$ est simple (i. e. n'a pas de sous groupes distingués autres que lui même et $\{Id\}$).*

Théorème 9 *Les sous groupes d'indice n de $\mathcal{S}_n$ sont isomorphes à $\mathcal{S}_{n-1}$.*

5 Utilisations du groupe symétrique

$\mathbb{K}$ est un corps commutatif de caractéristique différente de 2.

Définition 6 *On dit qu'un polynôme $P \in \mathbb{K}[X_1, \cdots, X_n]$ est symétrique si $P\left(X_{\sigma(1)}, \cdots, X_{\sigma(n)}\right) = P(X_1, \cdots, X_n)$ pour toute permutation $\sigma \in \mathcal{S}_n$.*

Les polynômes $\Sigma_k = \displaystyle\sum_{i_1 < \cdots < i_k} X_{i_1} \cdots X_{ik}$ sont les polynômes symétriques élémentaires.

Théorème 10 *Si $P \in \mathbb{K}[X_1, \cdots, X_n]$ est symétrique, il existe alors un unique polynôme $Q \in \mathbb{K}[X_1, \cdots, X_n]$ tel que $P(X_1, \cdots, X_n) = Q(\Sigma_1, \cdots, \Sigma_n)$.*

Théorème 11 (Cayley) *Tout groupe fini d'ordre n est isomorphe à un sous-groupe de $\mathcal{S}_n$.*

Théorème 12 *Soient H, F deux $\mathbb{K}$-espaces vectoriels. Une application n-linéaire $\varphi : E^n \to F$ est alternée si, et seulement si, $\varphi\left(x_{\sigma(1)}, \cdots, x_{\sigma(n)}\right) = \varepsilon(\sigma)\varphi(x_1, \cdots, x_n)$ pour tout $(x_1, \cdots, x_n) \in E^n$ et toute permutation $\sigma \in \mathcal{S}_n$.*

Théorème 13 *Soit $\mathbb{K}$ un corps commutatif de caractéristique différente de 2. L'application $\det : \mathcal{M}_n(\mathbb{K}) \to \mathbb{K}$ définie par :*

$$\det(A) = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$$

est une forme linéaire alternée.

Théorème 14 *Le groupe des isométries positives du tétraèdre [resp. du cube, du dodécaèdre] est isomorphe à $\mathcal{A}_4$ [resp. à $\mathcal{S}_4$, $\mathcal{A}_5$].*[3]

Théorème 15 *Le groupe des isométries du tétraèdre [resp. du cube, du dodécaèdre] est isomorphe à $\mathcal{S}_4$ [resp. à $\mathcal{S}_4 \times \{-Id, Id\}$, $\mathcal{A}_5 \times \{-Id, Id\}$].*

[2] Développement possible
[3] Développement possible

1 Congruences dans $\mathbb{Z}$. Anneaux $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$

Définition 1 *Soient $n \in \mathbb{N}$ et a, b dans $\mathbb{Z}$. On dit que a est congru à b modulo n si n divise $a-b$. On note $a \equiv b\ (n)$*

Cette relation est une relation d'équivalence sur $\mathbb{Z}$ et pour tout $a \in \mathbb{Z}$, on note $\overline{a} = a + n\mathbb{Z}$ sa classe d'équivalence modulo n.

L'ensemble des classes d'équivalence est noté $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ ou plus simplement $\mathbb{Z}_n$.

On suppose dans ce qui suit que $n \geq 2$ ($\mathbb{Z}_0 = \left\{\overline{0}\right\}$ et $\mathbb{Z}_1 = \mathbb{Z}$).

Les congruences peuvent ête utilisées pour obtenir des critères de divisibilité

Si $a = \overline{a_p \cdots a_1 a_0}^b$ est l'écriture en base b d'un entier a ($0 \leq a_k \leq b-1$, $a_p \neq 0$), alors :

- si d est un diviseur de b alors a est divisible par d si, et seulement si a_0 est divisible par d :
- si d est un diviseur de $b-1$ alors a est divisible par d si, et seulement si $\sum_{k=0}^{p} a_k$ est divisible par d ;
- a est divisible par $b+1$ si, et seulement si $\sum_{k=0}^{p} (-1)^k a_k$ est divisible par $b+1$.

Théorème 1 *Il existe une unique structure d'anneau commutatif unitaire sur $\mathbb{Z}_n$ telle que la surjection canonique $\pi_n : \mathbb{Z} \to \mathbb{Z}_n$ soit un morphisme d'anneaux.*

Théorème 2 *Tous les sous groupes de $\mathbb{Z}_n$ sont cycliques d'ordre qui divise n. Réciproquement pour tout diviseur d de n, il existe un unique sous groupe de $\mathbb{Z}_n$ d'ordre d, c'est le groupe cyclique engendré par $q = \dfrac{n}{d}$:*

$$H = \langle \overline{q} \rangle = \left\{\overline{0}, \overline{q}, \cdots, (d-1)\,\overline{q}\right\}.$$

Théorème 3 *Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}_n$.*

2 Inversibles de inversibles de $\mathbb{Z}_n$. Fonction indicatrice d'Euler

On note $\mathbb{Z}_n^\times$ le groupe multiplicatif des éléments inversibles de $\mathbb{Z}_n$ et $\varphi(n) = \operatorname{card}(\mathbb{Z}_n^\times)$.

Théorème 4 *Soit $a \in \mathbb{Z}$. On a :*

$$\left(\overline{a} \in \mathbb{Z}_n^\times\right) \Leftrightarrow (a \wedge n = 1) \Leftrightarrow (\overline{a} \text{ est générateur de } (\mathbb{Z}_n, +))$$

On note δ le pgcd de a et n et on a $a = \delta a'$, $n = \delta n'$ avec a' et n' premiers entre eux.

Théorème 5 *Soient $n \geq 2$, $a \geq 1$ et $b \in \mathbb{Z}$. L'équation diophantienne :*

$$ax \equiv b\ (n)$$

a des solutions entières si, et seulement si, $\delta = a \wedge n$ divise b. Dans ce cas, l'ensemble des solutions est :

$$S = \{b'x'_0 + kn' \mid k \in \mathbb{Z}\}$$

où x'_0 est une solution particulière de $a'x \equiv 1$ modulo n'.

Théorème 6 (Euler) *Pour tout entier relatif a premier avec n, on a $a^{\varphi(n)} \equiv 1\ (n)$.*

Théorème 7 *Pour $n \geq 2$ on a :*

$$(n \text{ premier}) \Leftrightarrow (\mathbb{Z}_n \text{ est un corps}) \Leftrightarrow (\mathbb{Z}_n \text{ est intègre})$$

Théorème 8 (Wilson) *Un entier n est premier si et seulement si $(n-1)! \equiv -1\ (n)$.*

Théorème 9 (chinois) *Les entiers n et m sont premiers entre eux si, et seulement si, les anneaux $\mathbb{Z}_{nm}$ et $\mathbb{Z}_n \times \mathbb{Z}_m$ sont isomorphes.*

Théorème 10 *L'équation diophantienne :*

$$\begin{cases} x \equiv a\ (n) \\ x \equiv b\ (m) \end{cases}$$

a des solutions entières si, et seulement si, $a-b$ est multiple de $n \wedge m$. Dans ce cas, l'ensemble des solutions est :

$$S = \{x_0 + k\,(n \vee m) \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de cette équation.

Théorème 11 *Soit* $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ *décomposé en facteurs premiers. On a :*

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Théorème 12 *Pour tout entier* $n \geq 2$*, on a :*

$$\forall n \geq 2,\ \sqrt{n} - 1 < \varphi(n) < n.$$

Exercice 1 *Soit* $n = pq$ *avec* p, q *premiers distincts. Montrer que si* a *et* b *dans* $\mathbb{N}^*$ *sont tels que* $ab \equiv 1 \pmod{\varphi(n)}$*, alors pour tout* $c \in \mathbb{Z}$*, on a* $c^{ab} \equiv c \pmod{n}$*. Ce résultat est à la base du système cryptographique R.S.A.*

Théorème 13 *Le groupe* $(\mathrm{Aut}(\mathbb{Z}_n), \circ)$ *est isomorphe à* $(\mathbb{Z}_n^*, \cdot)$*.*

Théorème 14 *Soient* p *un nombre premier impair et* α *un entier supérieur ou égal à* 1*. Le groupe multiplicatif* $\mathbb{Z}_{p^\alpha}^\times$ *est cyclique.*

Exercice 2 *Le groupe* $\mathbb{Z}_{2^\alpha}^*$ *est-il cyclique ?*

3 Formule de Möbius

Théorème 15 *Si* Φ_n *est le polynôme cyclotomique défini par :*

$$\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ k \wedge n = 1}} \left(X - \omega_n^k\right),$$

où $\mathcal{D}_n$ *est l'ensemble des diviseurs positifs de* n *et* $\omega_n = e^{\frac{2i\pi}{n}}$ *(*$\Phi_1(X) = X - 1$*), on a alors* $X^n - 1 = \prod_{d \in \mathcal{D}_n} \Phi_d$*.*

Corollaire 1 *Pour tout* $n \geq 2$*, on a la formule de Möbius :*

$$n = \sum_{d \in \mathcal{D}_n} \varphi(d).$$

4 Nombres de Carmichael

On appelle nombre de Carmichael tout entier $n \geq 2$ non premier tel que :

$$\forall x \in \mathbb{Z}_n^*, \quad x^{n-1} = \overline{1}.$$

Théorème 16 *Pour* $n \geq 2$ *: la condition* $k^{n-1} \equiv 1 \pmod{n}$ *pour tout* k *premier avec* n *est équivalente à* n *premier ou* $n = \prod_{i=1}^{r} p_i$ *avec* $r \geq 3$*,* $3 \leq p_1 < \cdots < p_r$ *premiers tels que pour tout* i *compris entre* 1 *et* r*,* $p_i - 1$ *divise* $n - 1$*.*

Par exemple 561, 1105, 1729, sont des nombres de Carmichael (il y en a une infinité).

1 L'ensemble $\mathcal{P}$ des nombres premiers

Définition 1 *On dit qu'un entier naturel p est premier s'il est supérieur ou égal à 2 et si les seuls diviseurs positifs de p sont 1 et p.*

On note $\mathcal{P}$ l'ensemble de tous les nombres premiers.

Exemple 1 *$n = 111111$ est non premier.*

Théorème 1 (Euclide) *Tour entier n supérieur ou égal à 2 a au moins un diviseur premier.*

Un entier naturel non premier s'écrit donc $n = pq$ avec $p \geq 2$ premier et $q \geq 2$. On dit alors qu'il est composé.

Exercice 1 *Montrer que si $p = a^m - 1$ est premier alors $a = 2$ et m est premier. La réciproque est-elle vraie ?*

Théorème 2 *Tout entier n supérieur ou égal à 2 qui est composé a au moins un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$.*

Le théorème précédent nous donne un premier algorithme, relativement simple, permettant de savoir si un entier $n \geq 2$ est premier ou non : on effectue successivement la division euclidienne de n par tous les entiers $p \leq \sqrt{n}$: si l'une de ces divisions donne un reste nul, alors n n'est pas premier, sinon, n est premier.

Pour tester la divisibilité de n par les nombres premiers $p \leq \sqrt{n}$, on doit disposer de la liste de tous ces nombres premiers. Le crible d'ERATOSTHENE nous permet d'obtenir une telle liste.

Théorème 3 (Euclide) *L'ensemble $\mathcal{P}$ des nombres premiers est infini*

Exercice 2 *On note :*

$$\mathcal{P}_1 = \{p \in \mathcal{P} \mid \exists n \in \mathbb{N} \ ; \ p = 4n + 3\}$$
$$\mathcal{P}_2 = \{p \in \mathcal{P} \mid \exists n \in \mathbb{N} \ ; \ p = 6n + 5\}$$

Montrer, en s'inspirant de la démonstration du théorème précédent, que $\mathcal{P}_1$ [resp. $\mathcal{P}_2$] est infini et conclure.

Exercice 3 *On note :*

$$2 = p_1 < p_2 < \cdots < p_n < p_{n+1} < \cdots$$

la suite infinie des nombres premiers rangée dans l'ordre croissant.

1. *Montrer que :*
$$\forall n \geq 1, \ 2n - 1 \leq p_n \leq 2^{2^{n-1}}.$$
2. *En déduire que $\pi(x) = \operatorname{card}(\mathcal{P} \cap [0, x]) > \ln(\ln(x))$.*

Exercice 4 *Montrer que pour tout entier naturel $n \geq 2$, on peut trouver n entiers naturels consécutifs non premiers (la distribution des nombres premiers n'est pas régulière).*

2 Décomposition en facteurs premiers

Théorème 4 *Tout entier naturel $n \geq 2$ se décompose de manière unique sous la forme :*

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha r}, \tag{1}$$

où les p_k sont des nombres premiers vérifiant :

$$2 \leq p_1 < p_2 < \cdots < p_r$$

et les α_k sont des entiers naturels non nuls.

Exercice 5 *Soient $p_1 < p_2 < \cdots < p_r$ des nombres premiers. Montrer que les réels $\ln(p_1), \ln(p_2), \cdots, \ln(p_r)$ sont $\mathbb{Q}$-libres dans $\mathbb{R}$.*

Exercice 6 *Soit $n \geq 2$ un entier sans facteur carré, c'est-à-dire que n a une décomposition en facteurs premiers de la forme $n = \prod_{k=1}^{r} p_k$ où les p_k sont premiers deux à deux distincts. Montrer que $\sqrt{n}$ est irrationnel.*

Exercice 7 *Soit n un entier de la forme $n = 2^m + 1$ avec $m \geq 0$. Montrer que si n est premier alors $m = 0$ ou m est une puissance de 2.*

Si $n=\prod_{k=1}^{r} p_k^{\alpha_k}$ est un entier décomposé en produit de facteurs premiers, alors les diviseurs de n sont de la forme $d=\prod_{k=1}^{r} p_k^{\gamma_k}$ où les γ_k sont des entiers naturels tels que $\gamma_k \leq \alpha_k$ pour tout k compris entre 1 et r. Il y a donc $\prod_{k=1}^{r} (\alpha_k+1)$ diviseurs positifs possibles de n.

Théorème 5 *Soient n, m deux entiers naturels supérieur ou égal à 2 et :*

$$n=\prod_{k=1}^{r} p_k^{\alpha_k},\ m=\prod_{k=1}^{r} p_k^{\beta_k}$$

leurs décompositions en facteurs premiers avec les p_k premiers deux à deux distincts et les α_k, β_k entiers naturels (certains de ces entiers pouvant être nuls). On a alors :

$$n\wedge m=\prod_{k=1}^{r} p_k^{\min(\alpha_k,\beta_k)},\ n\vee m=\prod_{k=1}^{r} p_k^{\max(\alpha_k,\beta_k)}.$$

3 Valuation p-adique

Pour tout nombre premier p et tout entier naturel non nul n, on note $\nu_p(n)$ l'exposant de p dans la décomposition de n en facteurs premiers avec $\nu_p(n)=0$ si p ne figure pas dans cette décomposition et $\nu_p(1)=0$. Cet entier $\nu_p(n)$ est appelé la valuation p-adique de n.

La décomposition en facteurs premiers de n peut donc s'écrire sous la forme :

$$n=\prod_{p\in\mathcal{D}_n\cap\mathcal{P}} p^{\nu_p(n)}$$

où $\mathcal{D}_n$ désigne l'ensemble des diviseurs positifs de n, ce qui peut aussi s'écrire $n=\prod_{p\in\mathcal{P}} p^{\nu_p(n)}$, le produit étant fini puisque $\nu_p(n)=0$ si p ne divise pas n.

Théorème 6

1. *Si p est un nombre premier et n,m sont deux entiers naturels non nuls, alors :*

$$\begin{cases} \nu_p(nm)=\nu_p(n)+\nu_p(m) \\ \nu_p(n+m)\geq \min(\nu_p(n),\nu_p(m)) \end{cases}$$

   l'égalité étant réalisée dans la deuxième formule si $\nu_p(n)\neq\nu_p(m)$.

2. *Soient n,m deux entiers naturels non nuls.*

   (a) *n divise m si, et seulement si, $\nu_p(n)\leq\nu_p(m)$ pour tout $p\in\mathcal{P}$.*

   (b) *Pour tout $p\in\mathcal{P}$, on a :*

$$\begin{cases} \nu_p(n\wedge m)=\min(\nu_p(n),\nu_p(m)) \\ \nu_p(n\vee m)=\max(\nu_p(n),\nu_p(m)) \end{cases}$$

Exercice 8 *On se donne un entier $n\geq 2$ et un nombre premier p.*

1. *Déterminer, pour tout entier naturel non nul k, le nombre n_k de multiples de p^k compris entre 1 et n.*
2. *Montrer que :*

$$\nu_p(n!)=\sum_{k=1}^{+\infty}\left[\frac{n}{p^k}\right]$$

   (formule de Legendre).

3. *Donner un équivalent de $\nu_p(n!)$ quand n tend vers l'infini.*
4. *Déterminer le nombre de zéros qui terminent l'écriture décimale de* 100!

Exercice 9 *On note $2=p_1<p_2<\cdots<p_n<\cdots$ la suite infinie des nombres premiers et on se propose de montrer la divergence de la série $\sum_{n=1}^{+\infty}\frac{1}{p_n}$. Pour ce faire, on introduit la suite $(u_n)_{n\geq 1}$ définie par :*

$$\forall n\geq 1,\ u_n=\frac{1}{\prod_{k=1}^{n}\left(1-\frac{1}{p_k}\right)}.$$

1. *Montrer que, pour tout $n \geq 1$, on a :*
$$u_n = \sum_{k \in E_n} \frac{1}{k}$$
où E_n est l'ensemble des entiers naturels non nuls qui ont tous leurs diviseurs premiers dans $\mathcal{P}_n = \{p_1, \cdots, p_n\}$.
2. *En déduire que, pour tout $n \geq 1$, on a :*
$$u_n \geq \sum_{k=1}^{p_n} \frac{1}{k}.$$
3. *En déduire que la série $\sum \ln\left(1 - \frac{1}{p_n}\right)$ est divergente et conclure.*
4. *Quelle est la nature de la série $\sum \frac{1}{p_n^\alpha}$ où α est un réel ?*
5. *Quelle est le rayon de convergence de la série entière $\sum \frac{z^{p_n}}{p_n}$.*

4 Les théorème de Fermat et de Wilson

Théorème 7 (Fermat) *Soit p un entier naturel premier. Pour tout entier relatif n non multiple de p, on a :*
$$n^{p-1} \equiv 1 \ (p).$$

La réciproque du théorème de Fermat est fausse. On peut en fait montrer que pour $p \geq 2$, la condition $n^{p-1} \equiv 1 \pmod{p}$ pour tout n premier avec p est équivalente à p premier ou $p = \prod_{k=1}^{r} p_k$ avec $r \geq 3$, $3 \leq p_1 < \cdots < p_r$ premiers tels que pour tout k compris entre 1 et r, $p_k - 1$ divise $p - 1$ (un tel entier est appelé nombre de Carmichaël ou nombre pseudo-premier). Par exemple 561, 1105, 1729, sont des nombres de Carmichaël.

Exercice 10 *Calculer le reste dans la division euclidienne de 5^{2008} par 11.*

Exercice 11 *Soit $p \geq 7$ un nombre premier. Montrer que $p^4 - 1$ est divisible par 240.*

Le résultat qui suit donne une généralisation du petit théorème de Fermat.

Définition 2 *On dit que deux polynômes P et Q à coefficients entiers sont congrus modulo un nombre premier p s'ils sont de mêmes degré et tous leurs coefficients sont égaux modulo p (ce qui se traduit aussi par $P = Q$ dans l'anneau $\mathbb{Z}_p[X]$ des polynômes à coefficients dans le corps $\mathbb{Z}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$).*

Théorème 8 *p est premier si, et seulement si, il existe un entier relatif n premier avec p tel que $(X + n)^p$ soit congru à $X^p + n$ modulo p.*

Théorème 9 (Wilson) *Un entier p supérieur ou égal à 2 est premier si, et seulement si, $(p-1)!$ est congru à -1 modulo p.*

Exercice 12 *Montrer qu'un entier p supérieur ou égal à 2 est premier si, et seulement si, $(p-2)!$ est congru à 1 modulo p.*

5 Les anneaux $\mathbb{Z}/n\mathbb{Z}$

Théorème 10 *Pour $n \geq 2$ il y équivalence entre :*
1. *n est premier ;*
2. *$\mathbb{Z}_n$ est un corps ;*
3. *$\mathbb{Z}_n$ est un intègre.*

Le calcul de $\varphi(n)$ pour $n \geq 2$, où φ est la fonction indicatrice d'Euler, peut se faire en utilisant la décomposition de n en facteurs premiers grâce au théorème chinois.

Si $n \geq 1$ a pour décomposition en facteurs premiers $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec $2 \leq p_1 < \cdots < p_r$ premiers et les α_i entiers naturels non nuls, alors :
$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Valeurs propres

On s'intéresse ici aux propriétés des valeurs propres et on suppose connus les principaux résultats sur les polynômes d'endomorphisme dans le cas de la dimension finie, ainsi que les résultats classiques de réduction des endomorphismes.

$\mathbb{K}$ est un corps commutatif et $\mathbb{K}[X]$ est l'algèbre des polynômes à coefficients dans $\mathbb{K}$.

E est un $\mathbb{K}$-espace vectoriel de dimension infinie ou de dimension finie $n \geq 1$.

Dans ce qui suit, u est un endomorphisme de E.

1 Valeurs et vecteurs propres

Définition 1 *On dit que $\lambda \in \mathbb{K}$ est valeur propre de u si $\ker(u - \lambda Id) \neq \{0\}$.*

Dire que $\lambda \in \mathbb{K}$ est valeur propre de u équivaut à dire qu'il existe un vecteur non nul x dans E tel que $u(x) = \lambda x$.

On dit alors que x est un vecteur propre de u associé à la valeur propre λ et que le sous espace vectoriel de E, $E_\lambda = \ker(u - \lambda Id)$, est le sous espace propre associé à λ.

L'ensemble des valeurs propres de $u \in \mathcal{L}(E)$ est appelé le spectre de u et noté $\mathrm{Sp}(u)$.

En identifiant une matrice $A \in \mathcal{M}_n(\mathbb{K})$ à l'endomorphisme de $\mathbb{K}^n$ qu'elle définit dans la base canonique, on peut donner la définition suivante.

Définition 2 *On dit que λ dans $\mathbb{K}$ est valeur propre de $A \in \mathcal{M}_n(\mathbb{K})$ s'il existe un vecteur non nul x dans $\mathbb{K}^n$ tel que $Ax = \lambda x$.*
On dit alors que x est un vecteur propre de A associé à la valeur propre λ et que le sous espace vectoriel de $\mathbb{K}^n$, $E_\lambda = \{x \in \mathbb{K}^n \mid Ax = \lambda x\}$ (que l'on peut noter $\ker(A - \lambda I_n)$) est le sous espace propre associé à λ.

L'ensemble des valeurs propres de A est appelé le spectre de A et noté $\mathrm{Sp}(A)$.

Dans le cas où E est de dimension finie $n \geq 1$, un scalaire $\lambda \in \mathbb{K}$ est valeur propre de $u \in \mathcal{L}(E)$ si, et seulement si, $u - \lambda Id$ est non inversible, ce qui équivaut à dire que le polynôme caractéristique de u défini par $P_u(X) = \det(u - XId)$ est nul pour $X = \lambda$.

On a donc, dans le cas où $\dim(E) = n$:

$$\mathrm{Sp}(u) = P_u^{-1}\{0\} = \{\lambda \in \mathbb{K} \mid \det(u - \lambda Id) = 0\}$$

et c'est une partie finie de $\mathbb{K}$ ayant au plus n éléments.

Le polynôme caractéristique d'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est défini par $P_A(X) = \det(A - XId)$.

Si u a pour matrice A dans une base de E, alors A et u ont même polynôme caractéristique et mêmes valeurs propres.

Exemple 1 *$E = \mathcal{C}^\infty(\mathbb{R})$ et u est l'opérateur de dérivation, $u : f \mapsto f'$. $\mathrm{Sp}(u) = \mathbb{R}$ et les espaces propres sont des droites.*

Exemple 2 *$E = \mathcal{C}^0([a,b])$ et u est l'opérateur de primitivation $u : f \mapsto g$, où g est définie par :*

$$\forall x \in [a,b],\ g(x) = \int_a^x f(t)\,dt$$

$\mathrm{Sp}(u) = \emptyset$.

Exercice 1 *On se place sur $\mathcal{C}^\infty(\mathbb{R}^{+,*})$ et u est l'opérateur différentiel, $u : f \mapsto xf'$. Déterminer les valeurs propres et espaces propres de u.*

Théorème 1 *Les valeurs propres d'une matrice symétrique réelle A sont toutes réelles.*

En utilisant le théorème de diagonalisation des matrices symétriques réelles, on vérifie que si $A \in \mathcal{S}_n(\mathbb{R})$, alors A est positive [resp. A définie positive] si et seulement si toutes ses valeurs propres sont positives [resp. strictement positives].

Exercice 2 *On suppose que $\mathbb{K} = \mathbb{R}$ et que u^2 a une valeur propre $\mu > 0$. Montrer que $\sqrt{\mu}$ ou $-\sqrt{\mu}$ est valeur propre de u.*

Exercice 3 *On suppose que le corps $\mathbb{K}$ est infini et que l'espace E est de dimension finie $n \geq 1$. Montrer pour tous u et v dans $\mathcal{L}(E)$, $u \circ v$ et $v \circ u$ ont même polynôme caractéristique et même polynôme minimal.*

Remarque 1 *Il est facile de vérifier que si $\lambda \in \mathbb{K}$ est une valeur propre de u et $x \in E \setminus \{0\}$ un vecteur propre associé, alors pour tout polynôme $P \in \mathbb{K}[X]$, on a $P(u)x = P(\lambda)x$.*

Théorème 2 *Si $\dim(E) = n$, alors les valeurs propres de u sont les racines de son polynôme minimal.*

Exercice 4 *On suppose que $\mathbb{K}$ est algébriquement clos. Déterminer les valeurs propres de $P(u)$ pour $P \in \mathbb{K}[X]$.*

Théorème 3 *Si $\mathrm{Sp}(u) = \{\lambda_1, \cdots, \lambda_p\}$, alors les sous-espaces propres $E_k = \ker(u - \lambda_k Id)$, pour k compris entre 1 et p, sont en somme directe.*

Une conséquence intéressante de ce théorème dans le cas de la dimension finie est la suivante : si $\dim(E) = n$ et u a n valeurs propres distinctes dans $\mathbb{K}$, il est alors diagonalisable.

Exercice 5 *$E = \mathcal{C}^0(\mathbb{R}, \mathbb{C})$ et u est l'endomorphisme de E défini par :*

$$\forall f \in E,\ \forall x \in \mathbb{R},\ u(f)(x) = \begin{cases} f(0) & \text{si } x = 0 \\ \frac{1}{x}\int_0^x f(t)\,dt & \text{si } x \neq 0 \end{cases}$$

Déterminer l'ensemble des valeurs propres de u et les espaces propres associés.

2 Valeurs propres des endomorphismes nilpotents en dimension finie

On suppose ici que E est de dimension finie.

Théorème 4 *Pour $\mathbb{K}$ algébriquement clos, u est nilpotent si, et seulement si, 0 est la seule valeur propre de u.*

Remarque 2 *Pour $\mathbb{K}$ non algébriquement clos, un endomorphisme u peut avoir 0 pour seule valeur propre dans $\mathbb{K}$ sans être nilpotent comme le montre l'exemple de l'endomorphisme u de $\mathbb{R}^3$ de matrice :*

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ & \sin(\theta) & \cos(\theta) \end{pmatrix}$$

dans la base canonique avec $\theta \notin \pi\mathbb{Z}$.

Théorème 5 *On suppose le corps $\mathbb{K}$ de caractéristique nulle.*
Un endomorphisme u est nilpotent si, et seulement si, $\mathrm{Tr}\left(u^k\right) = 0$ pour tout k compris entre 1 et n.

3 Localisation des valeurs propres d'une matrice réelle ou complexe

Ici, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.
Si $x \mapsto \|x\|$ est une norme sur $E = \mathbb{K}^n$, on lui associe alors la norme matricielle induite qui est définie par :

$$\forall A \in \mathcal{M}_n(\mathbb{K}),\ \|A\| = \sup_{x \in E\setminus\{0\}} \frac{\|Ax\|}{\|x\|} = \sup_{\substack{x \in E \\ \|x\|=1}} \|Ax\|$$

On notera $\|A\|_\infty$, $\|A\|_2$ les normes matricielles respectivement associées aux normes $\|x\|_\infty = \max\limits_{1\le i\le n} |x_i|$ et $\|x\|_2 = \sqrt{\sum\limits_{i=1}^{n} |x_i|^2}$.

Théorème 6 (Gerschgörin-Hadamard) *Soient A dans $\mathcal{M}_n(\mathbb{K})$ et λ dans $\mathbb{C}$ une valeur propre de A. Il existe un indice $i \in \{1, 2, \cdots, n\}$ tel que :*

$$|\lambda - a_{ii}| \le \sum_{\substack{j=1 \\ j\neq i}}^{n} |a_{ij}| \ \ (1 \le i \le n).$$

L'exercice qui suit donne une application du théorème de Gerschgörin-Hadamard au calcul des valeurs propres d'une matrice.

Exercice 6 *Soient $(a, b) \in \mathbb{R}^2$ et :*

$$A(a,b) = \begin{pmatrix} a & b & 0 & \cdots & 0 \\ b & a & b & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & b & a & b \\ 0 & \cdots & 0 & b & a \end{pmatrix}.$$

Calculer les valeurs propres et les vecteurs propres associés de $A(a, b)$.

Définition 3 *Une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est dite à diagonale strictement dominante si :*

$$\forall i \in \{1, 2, \cdots, n\}, \quad |a_{ii}| > \sum_{\substack{j=1 \\ j\neq i}}^{n} |a_{ij}|.$$

Corollaire 1 *Une matrice $A \in \mathcal{M}_n(\mathbb{K})$ à diagonale strictement dominante a toutes ses valeurs propres non nulles dans $\mathbb{C}$. En conséquence elle est inversible.*

Théorème 7 (Ostrowski) *Soit A dans $\mathcal{M}_n(\mathbb{K})$. Pour tout réel $\alpha \in [0, 1]$ et toute valeur propre$\lambda \in \mathbb{C}$ de A, il existe $i \in \{1, \cdots, n\}$ tel que :*

$$|\lambda - a_{ii}| \le \left(\sum_{\substack{j=1 \\ j\neq i}}^{n} |a_{ij}|\right)^{\alpha} \left(\sum_{\substack{j=1 \\ j\neq i}}^{n} |a_{ji}|\right)^{1-\alpha}$$

4 Rayon spectral des matrices complexes

Définition 4 *Le rayon spectral de $u \in \mathcal{L}(E)$ [resp. $A \in \mathcal{M}_n(\mathbb{C})$] est le réel $\rho(u) = \max_{\lambda \in \mathrm{sp}(u)} |\lambda|$ [resp. $\rho(A) = \max_{\lambda \in \mathrm{sp}(A)} |\lambda|$].*

Théorème 8 *Pour toute matrice $A \in \mathcal{M}_n(\mathbb{C})$, on a :*

$$\|A\|_2 = \sqrt{\|A^* A\|_2} = \sqrt{\rho(A^* A)}.$$

Théorème 9 *Soit $A \in \mathcal{M}_n(\mathbb{C})$.*

1. *Pour toute norme matricielle induite par une norme vectorielle, on a :*

$$\rho(A) \leq \|A\|,$$

l'inégalité pouvant être stricte.

2. *Pour tout $\varepsilon > 0$, il existe une norme matricielle induite par une norme vectorielle telle que :*

$$\|A\| \leq \rho(A) + \varepsilon.$$

3. *$\rho(A) = \inf_{\|\cdot\| \in \mathcal{N}} \|A\|$, où $\mathcal{N}$ désigne l'ensemble de toutes les normes matricielles induites par une norme vectorielle.*

Théorème 10 *L'application ρ qui associe à toute matrice de $\mathcal{M}_n(\mathbb{C})$ son rayon spectral est continue.*

Théorème 11 *Soit A dans $\mathcal{M}_n(\mathbb{C})$, les conditions suivantes sont équivalentes.*

(i) $\lim_{k \to +\infty} A^k = 0$.

(ii) *Pour toute valeur initiale x_0, la suite $(x_k)_{k \in \mathbb{N}}$ définie par $x_{k+1} = A x_k$, pour $k \geq 0$, converge vers le vecteur nul.*

(iii) $\rho(A) < 1$.

(iv) *Il existe au moins une norme matricielle induite telle que $\|A\| < 1$.*

(v) *La matrice $I_n - A$ est inversible et la série de terme général A^k est convergente de somme $(I_n - A)^{-1}$.*

(vi) *La matrice $I_n - A$ est inversible et la série de terme général* $\mathrm{trace}\left(A^k\right)$ *est convergente de somme* $\mathrm{trace}\left((I_n - A)^{-1}\right)$.

(vii) $\lim_{k \to +\infty} \mathrm{trace}\left(A^k\right) = 0$.

Corollaire 2 *Quelle que soit la norme choisie sur $\mathcal{M}_n(\mathbb{C})$ on a :*

$$\rho(A) = \lim_{k \to +\infty} \left(\left\| A^k \right\|^{\frac{1}{k}} \right).$$

Ce résultat peut aussi se montrer en utilisant la décomposition $D + N$ de Dunford-Schwarz.

Pour ce chapitre, $\mathbb{K}$ est un corps commutatif et E un $\mathbb{K}$-espace vectoriel de dimension finie ou non.

1 L'espace dual E^*

Définition 1 *Une forme linéaire sur E est une application linéaire de E dans $\mathbb{K}$.*

On note $E^* = \mathcal{L}(E, \mathbb{K})$ l'ensemble de toutes les formes linéaires sur E. C'est un $\mathbb{K}$-espace vectoriel.

Théorème 1 *Pour E de dimension finie égale à n, l'espace E^* de toutes les formes linéaires sur E est de dimension n, de base $\mathcal{B}^* = (p_i)_{1\leq i\leq n}$, où les p_i sont les projections relativement à une base $\mathcal{B}$ donnée.*

On note $p_i = e_i^*$, pour i compris entre 1 et n et on dit que $\mathcal{B}^* = (e_i^*)_{1\leq i\leq n}$ est la base duale de $\mathcal{B}$.

Théorème 2 *Étant donnée une base $\mathcal{B}' = (\ell_i)_{1\leq i\leq n}$ de E^*, il existe une base $\mathcal{B} = (f_i)_{1\leq i\leq n}$ de E telle que $\mathcal{B}'$ soit la base duale de $\mathcal{B}$.*

Avec les notations du théorème, on dit que $\mathcal{B}$ est la base anté-duale de $\mathcal{B}'$.

Exercice 1 *On suppose que E est de dimension finie. Montrer que si $\varphi_1, \cdots, \varphi_p, , \varphi$ sont des formes linéaires sur E qui vérifient $\bigcap_{i=1}^{p} \ker(\varphi_i) \subset \ker(\varphi)$, alors φ est combinaison linéaire des φ_i.*

2 Exemples dans $\mathbb{K}_n[x]$

Exercice 2 *Déterminer la base duale de la base canonique $E = \mathbb{K}_n[x]$.*

Exercice 3 *Soient $E = \mathbb{K}_n[x]$ et $n+1$ scalaires deux à deux distincts $x_0, x_1, \cdots, x_n$ dans $\mathbb{K}$.*

1. *Montrer que la famille $\mathcal{L} = (L_i)_{0\leq i\leq n}$ de polynômes définis par :*

$$L_i(x) = \prod_{\substack{j=0\\ j\neq i}}^{n} \frac{x - x_j}{x_i - x_j} \ (1 \leq i \leq n)$$

   est une base de E.
2. *Déterminer la base duale de $\mathcal{L}$.*
3. *On suppose que $\mathbb{K} = \mathbb{R}$ et que les points x_i sont dans un intervalle $[a, b]$. Montrer qu'il existe des constantes réelles uniquement déterminées $\alpha_0, \alpha_1, \cdots, \alpha_n$ telles que :*

$$\forall P \in \mathbb{R}_n[x], \ \int_a^b P(t)\, dt = \sum_{j=0}^{n} \alpha_j P(x_j)$$

   Détailler le cas où $n = 2$, $x_0 = a$, $x_1 = \dfrac{a+b}{2}$ et $x_2 = b$.

Exercice 4 *Soit $E = \mathbb{K}[x]$ muni de sa base canonique $\mathcal{B} = (e_j)_{j\in\mathbb{N}}$, où $e_j(X) = X^j$.*

1. *Montrer que le système dual $\mathcal{B}^* = \left(e_j^*\right)_{j\in\mathbb{N}}$ défini par $e_i^*(e_j) = \delta_{ij}$ pour tous i, j dans $\mathbb{N}$, n'est pas une base de E^*.*
2. *Montrer que E^* est isomorphe à l'espace $\mathbb{K}^{\mathbb{N}}$ des suites à coefficients dans $\mathbb{K}$.*

3 Exemples dans $\mathcal{M}_n(\mathbb{K})$

$(e_i)_{1\leq i\leq n}$ est la base canonique de $E = \mathbb{K}^n$ et $(E_{ij})_{1\leq i,j\leq n}$ celle de $\mathcal{M}_n(\mathbb{K})$.

Exercice 5 *On se place dans $\mathcal{M}_n(\mathbb{K})$.*

1. *Soit φ une forme linéaire sur $\mathcal{M}_n(\mathbb{K})$ telle que $\varphi(AB) = \varphi(BA)$ pour toutes matrices A, B dans $\mathcal{M}_n(\mathbb{K})$.*
   (a) *Montrer que $\varphi(E_{ii}) = \varphi(E_{jj})$ pour tous i, j compris entre 1 et n. On note λ cette valeur commune.*
   (b) *Montrer que $\varphi(E_{ij}) = 0$ pour tous $i \neq j$ dans $\{1, \cdots, n\}$.*
   (c) *Montrer que $\varphi(A) = \lambda \operatorname{Tr}(A)$ pour toute matrice A dans $\mathcal{M}_n(\mathbb{K})$.*

2. *Soit u un endomorphisme de $\mathcal{M}_n(\mathbb{K})$ tel que $u(I_n) = I_n$ et $u(AB) = u(BA)$ pour toutes matrices A, B dans $\mathcal{M}_n(\mathbb{K})$. Montrer que u conserve la trace.*
On peut remplacer $\mathcal{M}_n(\mathbb{K})$ par $\mathcal{L}(E)$, où E est de dimension n.

Exercice 6

1. *Montrer que le centre de $\mathcal{M}_n(\mathbb{K})$ est formé des homothéties.*
2. *On désigne par θ l'application linéaire qui associe à toute matrice $B \in \mathcal{M}_n(\mathbb{K})$ la forme linéaire $\theta(B)$ définie sur $\mathcal{M}_n(\mathbb{K})$ par :*
$$\forall A \in \mathcal{M}_n(\mathbb{K}),\ \theta(B)(A) = \operatorname{Tr}(BA).$$
   (a) *Montrer que θ est injective.*
   (b) *En déduire que si φ est une forme linéaire sur $\mathcal{M}_n(\mathbb{K})$, il existe alors une unique matrice $B \in \mathcal{M}_n(\mathbb{K})$ telle que :*
$$\forall A \in \mathcal{M}_n(\mathbb{K}),\ \varphi(A) = \operatorname{Tr}(BA).$$
   (on peut remplacer $\mathcal{M}_n(\mathbb{K})$ par $\mathcal{L}(E)$, où E est de dimension n).
3. *En utilisant le résultat précédent, montrer que si φ est une forme linéaire sur $\mathcal{M}_n(\mathbb{K})$ telle que $\varphi(AB) = \varphi(BA)$ pour toutes matrices A, B dans $\mathcal{M}_n(\mathbb{K})$, il existe alors un scalaire λ tel que $\varphi(A) = \lambda \operatorname{Tr}(A)$ pour toute matrice $A \in \mathcal{M}_n(\mathbb{K})$ (résultat de l'exercice précédent).*

Exercice 7 *Soit $E = \mathbb{K}^n$. Pour $x \in E$ et $\varphi \in E^*$, on désigne par $\varphi \otimes x$ la matrice définie par :*
$$\varphi \otimes x = (\varphi(e_1)x, \cdots, \varphi(e_n)x) = ((\varphi(e_j)x_i))_{1 \leq i,j \leq n}$$

1. *Calculer $(\varphi \otimes e_i)z$ pour tout vecteur $z \in E$, toute forme linéaire $\varphi \in E^*$ et tout i compris entre 1 et n.*
2. *Calculer $e_j^* \otimes x$ pour tout vecteur $x \in E$ et tout j compris entre 1 et n.*
3. *Calculer $(\varphi \otimes e_i) A \left(e_j^* \otimes y\right)$ pour tout vecteur $y \in E$, toute forme linéaire $\varphi \in E^*$, toute matrice $A \in \mathcal{M}_n(\mathbb{K})$ et tous i, j compris entre 1 et n.*
4. *Montrer que les idéaux bilatères de $\mathcal{M}_n(\mathbb{K})$ sont $\{0\}$ et $\mathcal{M}_n(\mathbb{K})$ (on peut remplacer $\mathcal{M}_n(\mathbb{K})$ par $\mathcal{L}(E)$, où E est de dimension n).*

4 Hyperplans

Définition 2 *On appelle hyperplan de E, le noyau d'une forme φ linéaire non nulle sur E.*

Si $H = \ker(\varphi)$ est un hyperplan de E, on dit alors que φ (ou $\varphi(x) = 0$) est une équation de E.

Théorème 3 *Un hyperplan de E est un sous-espace de E supplémentaire d'une droite.*

Remarque 1 *Le résultat précédent est valable que E soit de dimension finie ou non.*

Exercice 8 *Soient $\varphi, \psi \in E^*$ telles que* $\ker(\varphi) \subset \ker(\psi)$.

1. *Montrer que φ et ψ et sont proportionnelles.*
2. *Si $\psi \neq 0$, montrer alors que* $\ker(\varphi) = \ker(\psi)$.

Remarque 2 *On déduit de l'exercice précédent que deux formes linéaires non nulles définissent le même hyperplan si, et seulement si, elles sont proportionnelles (que E soit de dimension finie ou non).*

Théorème 4 *Dans un espace vectoriel E de dimension n un hyperplan est un sous-espace de E de dimension $n-1$.*

Exercice 9 *Montrer que pour tout hyperplan H de $\mathcal{M}_n(\mathbb{K})$, où $n \geq 2$, on a $H \cap GL_n(\mathbb{K}) \neq \emptyset$.*

5 Orthogonalité

Définition 3 *On dit que $\varphi \in E^*$ et $x \in E$ sont orthogonaux si $\varphi(x) = 0$.*

Définition 4 *L'orthogonal dans E^* d'une partie non vide X de E est l'ensemble :*
$$X^{\perp} = \{\varphi \in E^* \mid \forall x \in X,\ \varphi(x) = 0\}.$$
L'orthogonal dans E d'une partie non vide Y de E^* est l'ensemble :
$$Y^{\circ} = \{x \in E \mid \forall \varphi \in Y,\ \varphi(x) = 0\}.$$

Théorème 5 *Soient A, B des parties non vides de E et U, V des parties non vides de E^*.*

1. *Si $A \subset B$, alors $B^\perp \subset A^\perp$.*
2. *Si $U \subset V$, alors $V^\circ \subset U^\circ$.*
3. *$A \subset \left(A^\perp\right)^\circ$, l'égalité n'étant pas réalisée en général.*
4. *$U \subset (U^\circ)^\perp$, l'égalité n'étant pas réalisée en général.*
5. *$A^\perp = (\mathrm{Vect}\,(A))^\perp$.*
6. *$U^\circ = (\mathrm{Vect}\,(U))^\circ$.*
7. *$\{0\}^\perp = E^*$, $E^\perp = \{0\}$, $\{0\}^\circ = E$ et $(E^*)^\circ = \{0\}$.*

Théorème 6 *On suppose que E est de dimension finie $n \geq 1$.*

1. *Pour tout sous-espace vectoriel F de E, on a :*
$$\dim(F) + \dim\left(F^\perp\right) = \dim(E)$$
2. *Pour tout sous-espace vectoriel G de E^*, on a :*
$$\dim(G) + \dim(G^\circ) = \dim(E)$$
3. *Pour tout sous-espace vectoriel F de E et tout sous-espace vectoriel G de E^*, on a :*
$$F = \left(F^\perp\right)^\circ \text{ et } G = (G^\circ)^\perp$$
4. *Pour toute partie X de E, on a :*
$$\left(X^\perp\right)^\circ = \mathrm{Vect}\,(X).$$
5. *Pour tous sous-espaces vectoriels F_1 et F_2 de E, on a $(F_1 + F_2)^\perp = F_1^\perp \cap F_2^\perp$.*
6. *Pour tous sous-espaces vectoriels F_1 et F_2 de E, on a $(F_1 \cap F_2)^\perp = F_1^\perp + F_2^\perp$.*
7. *Pour tous sous-espaces vectoriels G_1 et G_2 de E^*, on a $(G_1 + G_2)^\circ = G_1^\circ \cap G_2^\circ$.*
8. *Pour tous sous-espaces vectoriels G_1 et G_2 de E^*, on a $(G_1 \cap G_2)^\circ = G_1^\circ + G_2^\circ$.*

Remarque 3

1. *L'égalité $F = \left(F^\perp\right)^\circ$ est toujours vraie, que la dimension soit finie ou non.*
   On en déduit l'égalité $\left(X^\perp\right)^\circ = \mathrm{Vect}\,(X)$, pour toute partie X de E.
2. *L'égalité $(F_1 + F_2)^\perp = F_1^\perp \cap F_2^\perp$ est toujours vraie, que la dimension soit finie ou non.*
3. *L'égalité $(F_1 \cap F_2)^\perp = F_1^\perp + F_2^\perp$ est encore vraie, que la dimension soit finie ou non, mais la démonstration est plus délicate dans le cas général (on utilise l'axiome du choix).*

Exercice 10 *Montrer que si F_1, F_2 sont deux sous-espaces supplémentaires dans E, alors $F_1^\perp$ et $F_2^\perp$ sont supplémentaires dans E^*.*

Exercice 11 *On suppose que E est de dimension n.*
Montrer que $(\varphi_i)_{1 \leq i \leq n}$ est une base de E^* si, et seulement si, $\bigcap_{i=1}^{n} \ker(\varphi_i) = \{0\}$.

6 Équations des sous-espaces d'un espace de dimension finie

On suppose ici que E est de dimension $n \geq 2$.

Théorème 7 *Si $(\varphi_1, \varphi_2, \cdots, \varphi_p)$ est une famille de formes linéaires sur E de rang r, alors le sous-espace vectoriel $F = \bigcap_{i=1}^{p} \ker(\varphi_i)$ de E est de dimension $n - r$.*
Réciproquement si F est un sous-espace vectoriel de E de dimension m, il existe une famille $(\varphi_1, \varphi_2, \cdots, \varphi_r)$ de formes linéaires sur E de rang $r = n - m$, telle que $F = \bigcap_{i=1}^{r} \ker(\varphi_i)$.

7 Transposition

E, F sont deux $\mathbb{K}$-espaces vectoriels.

Définition 5 *La transposée de l'application linéaire $u \in \mathcal{L}(E,F)$ est l'application ${}^t u$ de F^* dans E^* définie par :*

$$\forall \varphi \in F^*, \quad {}^t u(\varphi) = \varphi \circ u$$

On vérifie facilement que ${}^t u$ est linéaire.

Théorème 8 *L'application de transposition $u \mapsto {}^t u$ est linéaire et injective de $\mathcal{L}(E,F)$ dans $\mathcal{L}(F^*, E^*)$.*

Théorème 9 *Soient u dans $\mathcal{L}(E,F)$ et v dans $\mathcal{L}(F,G)$ On a :*

1. ${}^t(v \circ u) = {}^t u \circ {}^t v$;
2. *pour $F = E$, ${}^t Id_E = Id_{E^*}$;*
3. *si u est un isomorphisme de E sur F, alors ${}^t u$ est un isomorphisme de F^* sur E^* et $({}^t u)^{-1} = {}^t u^{-1}$;*
4. $\ker({}^t u) = (\mathrm{Im}(u))^{\perp}$;
5. *u est surjective si, et seulement si, ${}^t u$ est injective ;*
6. $\mathrm{Im}({}^t u) = (\ker(u))^{\perp}$;
7. *u est injective si, et seulement si, ${}^t u$ est surjective ;*
8. *si E et F sont de dimension finie, alors u et ${}^t u$ ont même rang.*

On suppose maintenant que E est de dimension n, F de dimension m et on se donne une base $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ de E et $\mathcal{B}' = (f_j)_{1 \leq j \leq m}$ une base de F. Les bases duales correspondantes sont notées respectivement $\mathcal{B}^*$ et $\mathcal{B}'^*$.

Théorème 10 *Si $A \in \mathcal{M}_{m,n}(\mathbb{K})$ est la matrice de $u \in \mathcal{L}(E,F)$ dans les bases $\mathcal{B}$ et $\mathcal{B}'$, alors la matrice de ${}^t u$ dans les bases $\mathcal{B}'^*$ et $\mathcal{B}^*$ est la transposée ${}^t A$.*

Une application importante de la transposition est la réduction de Jordan des matrices carrées à coefficients dans $\mathbb{C}$ ou, plus généralement dans un corps algébriquement clos. Voir la leçon sur la réduction des endomorphismes.

8 Bidual

Définition 6 *Le bidual de E est le dual de E^*, soit E^{**}.*

Théorème 11 *L'application $\theta : E \to E^{**}$ qui associe à tout vecteur $x \in E$, la forme linéaire $\theta(x)$ définie sur E^* par :*

$$\forall \varphi \in E^*, \ \theta(x)(\varphi) = \varphi(x)$$

est linéaire et injective.

Réduction d'un endomorphisme d'un espace vectoriel de dimension finie. Applications

E est un $\mathbb{K}$-espace vectoriel de dimension finie $n \geq 1$, u est un endomorphisme de E et P_u est son polynôme caractéristique.

1 Diagonalisation

Définition 1 *On dit que u est diagonalisable s'il existe une base de E dans laquelle la matrice de u est diagonale.*

Définition 2 *On dit qu'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est diagonalisable si elle est semblable à une matrice diagonale.*

Théorème 1 *Si u a n valeurs propres distinctes dans $\mathbb{K}$, il est alors diagonalisable.*

Théorème 2 *Les conditions suivantes sont équivalentes.*

(i) *l'endomorphisme u est diagonalisable ;*

(ii) *si $\mathrm{Sp}(u) = \{\lambda_1, \cdots, \lambda_p\}$, alors $E = \bigoplus_{k=1}^{p} \ker(u - \lambda_k Id)$;*

(iii) *si $\mathrm{Sp}(u) = \{\lambda_1, \cdots, \lambda_p\}$, alors $\sum_{k=1}^{p} \dim(\ker(u - \lambda_k Id)) = n$;*

(iv) *le polynôme caractéristique de u est scindé sur $\mathbb{K}$ de racines deux à deux distinctes $\lambda_1, \cdots, \lambda_p$ dans $\mathbb{K}$, chaque λ_k $(1 \leq k \leq p)$ étant de multiplicité $\alpha_k = \dim(\ker(u - \lambda_k Id))$;*

(v) *il existe un polynôme annulateur de u scindé à racines simples dans $\mathbb{K}$;*

(vi) *le polynôme minimal π_u est scindé à racines simples dans $\mathbb{K}$.*

Exercice 1 *Soit u un endomorphisme de E diagonalisable avec $\mathrm{Sp}(u) = \{\lambda_1, \cdots, \lambda_p\}$. Montrer que pour $1 \leq k \leq p$ la projection de E sur le sous espace propre $\ker(u - \lambda_k Id)$ est donnée par :*

$$p_k = \alpha_k \prod_{\substack{j=1 \\ j \neq k}}^{p} (u - \lambda_j Id),$$

où $\alpha_k = \dfrac{1}{\prod_{\substack{j=1 \\ j \neq k}}^{p} (\lambda_k - \lambda_j)}$ (utiliser la décomposition en éléments simples de $\dfrac{1}{\pi_u}$).

Exercice 2 *On considère une famille $(u_i)_{i \in I}$ d'endomorphismes de E diagonalisables (l'ensemble I ayant au moins deux éléments). On suppose que ces endomorphismes commutent deux à deux :*

$$\left(\forall (i,j) \in I^2\right),\ u_i \circ u_j = u_j \circ u_i$$

Montrer l'existence d'une base commune de diagonalisation dans E pour la famille $(u_i)_{i \in I}$, c'est-à-dire qu'il existe une base $\mathcal{B}$ de E qui est une base de vecteurs propres pour chaque endomorphisme u_i, $i \in I$.

2 Trigonalisation

Définition 3 *On dit que u est trigonalisable s'il existe une base de E dans laquelle la matrice de u est triangulaire.*

Définition 4 *On dit qu'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est trigonalisable si elle est semblable à une matrice triangulaire.*

Théorème 3 *L'endomorphisme u est trigonalisable sur $\mathbb{K}$ si et seulement si son polynôme caractéristique est scindé sur $\mathbb{K}$.*

Corollaire 1 *Si le corps $\mathbb{K}$ est algébriquement clos, alors toute endomorphisme $u \in \mathcal{L}(E)$ est trigonalisable.*

Corollaire 2 *Si u est trigonalisable alors la trace de u est égale à la somme des valeurs propres de u et le déterminant de u est égal au produit des valeurs propres de u.*

Exercice 3 *On considère une famille $(u_i)_{i \in I}$ d'endomorphismes trigonalisables de E qui commutent deux à deux (l'ensemble I ayant au moins deux éléments).*

1. *Montrer qu'il existe un vecteur propre non nul commun à tous les u_i.*
2. *Montrer l'existence d'une base commune de trigonalisation dans E pour la famille $(u_i)_{i \in I}$, c'est-à-dire qu'il existe une base $\mathcal{B}$ de E dans laquelle la matrice T_i de chaque endomorphisme u_i est triangulaire.*

3 Réduction de Jordan

Théorème 4 *Soit $u \in \mathcal{L}(E) - \{0\}$ tel que P_u soit scindé sur $\mathbb{K}$:*

$$P_u(X) = (-1)^n \prod_{k=1}^{p} (X - \lambda_k)^{\alpha_k},$$

avec $\alpha_k \geq 1$ et les λ_k distincts deux à deux.
Il existe une base $\mathcal{B}$ de E dans laquelle la matrice de u est de la forme :

$$A = \begin{pmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & J_p \end{pmatrix} \tag{2}$$

avec :

$$\forall k \in \{1, 2, \cdots, p\},\ J_k = \begin{pmatrix} \lambda_k & 0 & 0 & \cdots & 0 \\ \varepsilon_{k,2} & \lambda_k & 0 & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \varepsilon_{k,\alpha_k - 1} & \lambda_k & 0 \\ 0 & \cdots & 0 & \varepsilon_{k,\alpha_k} & \lambda_k \end{pmatrix} \in M_{\alpha_k}(\mathbb{K})$$

où $\varepsilon_{k,i} \in \{0, 1\}$ (forme réduite de Jordan).

Si le corps $\mathbb{K}$ est algébriquement clos, la réduction de Jordan est toujours possible.

Corollaire 3 *Toute matrice non nulle A d'ordre n à coefficients dans un corps commutatif algébriquement clos est semblable à une matrice triangulaire de la forme (2).*

4 Réduction des matrices symétriques réelle

$(E, \langle \cdot \mid \cdot \rangle)$ est un espace réel euclidien de dimension $n \geq 1$.
On note $\mathcal{S}(E)$ l'ensemble des endomorphismes symétriques de E et $\mathcal{S}_n(\mathbb{R})$ l'ensemble des matrices symétriques réelles.

Théorème 5 *Un endomorphisme symétrique réel $u \in \mathcal{S}(E)$ a n valeurs propres réelles distinctes ou confondues et se diagonalise dans une base orthonormée.*

Corollaire 4 *Toute matrice symétrique réelle $A \in \mathcal{S}_n(\mathbb{R})$ se diagonalise dans une base orthonormée, c'est-à-dire qu'il existe une matrice orthogonale $P \in \mathcal{O}_n(\mathbb{R})$ et une matrice diagonale D telles que ${}^tPAP$ soit diagonale.*

5 Réduction des matrices orthogonales réelle

On se place ici dans un espace réel euclidien $(E, \langle \cdot \mid \cdot \rangle)$ de dimension $n \geq 1$.
On note $\mathcal{O}(E)$ l'ensemble des endomorphismes orthogonaux de E.

Théorème 6 *Soit $u \in \mathcal{O}(E)$ avec $n \geq 2$. Il existe une base orthonormée $\mathcal{B}$ de E dans laquelle la matrice de u s'écrit :*

$$D = \begin{pmatrix} I_p & 0 & 0 & 0 & \cdots & 0 \\ 0 & -I_q & 0 & \ddots & \ddots & \vdots \\ 0 & 0 & R_1 & 0 & \ddots & 0 \\ 0 & \ddots & 0 & R_2 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 0 & 0 & R_r \end{pmatrix}$$

où, pour tout $k \in \{1, \cdots, r\}$, on a noté :

$$R_k = \begin{pmatrix} \cos(\theta_k) & -\sin(\theta_k) \\ \sin(\theta_k) & \cos(\theta_k) \end{pmatrix}$$

avec $\theta_k \in]0, 2\pi[- \{\pi\}$ et p, q, r sont des entiers naturels tels $p + q + 2r = n$ (si l'un de ces entiers est nul, les blocs de matrices correspondants n'existent pas).

Remarque 1 *On a* $p = \dim(\ker(u - Id))$ *et* $q = \dim(\ker(u + Id))$ *avec* $p + q + 2r = n$. *De plus* $u \in \mathcal{O}^+(E)$ *[resp.* $u \in \mathcal{O}^-(E)$*] si et seulement si* q *est pair [resp. impair].*

Corollaire 5 *Soit* $A \in \mathcal{O}_n(\mathbb{R})$ *avec* $n \geq 2$. *Il existe une matrice* $P \in \mathcal{O}_n(\mathbb{R})$ *telle que :*

$$ {}^tPAP = \begin{pmatrix} I_p & 0 & 0 & 0 & \cdots & 0 \\ 0 & -I_q & 0 & \ddots & \ddots & \vdots \\ 0 & 0 & R_1 & 0 & \ddots & 0 \\ 0 & \ddots & 0 & R_2 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 0 & 0 & R_r \end{pmatrix}, $$

6 Réduction des matrices normales

Définition 5 *Une matrice complexe* A *est dite normale si* $A^*A = AA^*$.

Théorème 7 *Si* A *une matrice complexe normale, alors elle se diagonalise dans une base orthonormée, c'est-à-dire qu'il existe une matrice unitaire* U *et une matrice diagonale* D *telles que* $A = UDU^*$, *les coefficients diagonaux de* D *étant les valeurs propres dans* $\mathbb{C}$ *de la matrice* A.

Du fait qu'une matrice hermitienne ou unitaire est normale on déduit les résultats suivants.

Corollaire 6 *Une matrice hermitienne [resp. unitaire] a ses valeurs propres réelles [resp de module* 1*] et se diagonalise dans une base orthonormée.*

Corollaire 7 *Si* A *est une matrice complexe hermitienne positive, alors il existe une unique matrice hermitienne positive* B *telle que* $A = B^2$.

Corollaire 8 *Toute matrice complexe [resp. réelle] inversible* A *peut s'écrire de manière unique* $A = UH$ *[resp.* $A = \Omega S$*] où* U *[resp.* Ω*] est une matrice unitaire [resp. orthogonale] et* H *[resp.* S*] une matrice hermitienne [resp. symétrique] définie positive.*

7 Propriétés topologiques de l'ensemble des matrices diagonalisables de $\mathcal{M}_n(\mathbb{C})$

On désigne par $\mathcal{D}'_n(\mathbb{C})$ l'ensemble des matrices $M \in \mathcal{M}_n(\mathbb{C})$ ayant n valeurs propres distinctes dans $\mathbb{C}$ et par $\mathcal{D}_n(\mathbb{C})$ l'ensemble des matrices diagonalisables de $\mathcal{M}_n(\mathbb{C})$.

Théorème 8 *L'ensemble* $\mathcal{D}'_n(\mathbb{C})$ *est l'intérieur de* $\mathcal{D}_n(\mathbb{C})$.

Théorème 9 *Les ensembles* $\mathcal{D}'_n(\mathbb{C})$ *et* $\mathcal{D}_n(\mathbb{C})$ *sont denses dans* $\mathcal{M}_n(\mathbb{C})$.

Remarque 2 *L'ensemble* $\mathcal{D}_n(\mathbb{R})$ *des matrices diagonalisables de* $\mathcal{M}_n(\mathbb{R})$ *n'est pas dense dans* $\mathcal{M}_n(\mathbb{R})$. *De manière plus précise on peut montrer que l'adhérence de* $\mathcal{D}_n(\mathbb{R})$ *est l'ensemble* $\mathcal{T}_n(\mathbb{R})$ *des matrices trigonalisables de* $\mathcal{M}_n(\mathbb{R})$.

Corollaire 9 *Pour* $n \geq 2$, *l'application qui associe à une matrice* $A \in \mathcal{M}_n(\mathbb{C})$ *son polynôme minimal n'est pas continue.*

8 Quelques applications

Exercice 4 *En utilisant le théorème de trigonalisation, montrer le théorème de Cayley-Hamilton dans* $\mathcal{M}_n(\mathbb{K})$ *pour* $\mathbb{K}$ *algébriquement clos.*

Exercice 5 *On suppose* $\mathbb{K}$ *algébriquement clos.*
Montrer que toute matrice $A \in \mathcal{M}_n(\mathbb{K})$ *est semblable à sa transposée.*

Exercice 6 *Déduire le théorème de Cayley-Hamilton de la densité de* $\mathcal{D}_n(\mathbb{C})$ *dans* $\mathcal{M}_n(\mathbb{C})$.

Exercice 7 *Montrer que* $GL_n(\mathbb{C})$ *est connexe par arcs en utilisant le fait que toute matrice complexe est semblable à une matrice triangulaire.*

Polynômes d'endomorphismes en dimension finie. Applications

Les notions de valeurs, vecteurs, espaces propres et de polynôme caractéristique sont supposées connues.
u est un endomorphisme de E.

1 Polynôme minimal

Définition 1 *On appelle idéal annulateur de u l'idéal I_u et polynôme minimal de u le générateur unitaire de cet idéal. On note π_u ce polynôme.*

On définit de manière analogue l'idéal annulateur et le polynôme minimal d'une matrice $A \in \mathcal{M}_n(\mathbb{K})$.

Exemple 1 *Le polynôme minimal d'un endomorphisme nilpotent est X^q et réciproquement.*

2 Le théorème de Cayley-Hamilton

Théorème 1 (Cayley-Hamilton) *Si P_u est le polynôme caractéristique de u, on a alors $P_u(u) = 0$.*

Corollaire 1 *Le polynôme minimal π_u divise le polynôme caractéristique P_u. Il est donc de degré inférieur ou égal à n.*

Remarque 1 *On retrouve le fait que les racines de π_u sont valeurs propres de u.*

Remarque 2 *Dans le cas où l'endomorphisme u est inversible, le théorème de Cayley-Hamilton nous donne un moyen de calculer l'inverse de u, si on connaît son polynôme caractéristique P_u.*
Il permet également de calculer A^p pour tout entier p supérieur ou égal à n en fonction de $I_n, A, \cdots, A^{n-1}$.

3 Le théorème de décomposition des noyaux

Théorème 2 (de décomposition des noyaux) *Soient p un entier supérieur ou égal à 2, $P_1, \cdots, P_p$ des polynômes non nuls dans $\mathbb{K}[X]$ deux à deux premiers entre eux et $P = \prod_{k=1}^{p} P_k$.*
On a :

$$\ker(P(u)) = \bigoplus_{k=1}^{p} \ker(P_k(u))$$

et les projecteurs $\pi_k : \ker(P(u)) \to \ker(P_k(u))$, pour k compris entre 1 et p, sont des éléments de $\mathbb{K}[u]$.

Remarque 3 *Dans le cas où $P(u) = 0$, on a $E = \bigoplus_{k=1}^{p} \ker(P_k(u))$.*

Exercice 1 *Soient p un entier supérieur ou égal à 2 et :*

$$P(X) = \prod_{k=1}^{p} (X - \lambda_k)^{\alpha_k},$$

un polynôme scindé sur $\mathbb{K}$, où les α_k sont des entiers naturels non nuls et les λ_k des scalaires deux à deux distincts. En utilisant la décomposition en éléments simples de la fraction rationnelle $\frac{1}{P}$, donner une expression des projecteurs π_k de $\ker(P(u))$ sur $\ker(P_k(u))$ pour tout k compris entre 1 et p.

4 La décomposition de Dunford-Schwarz

On suppose que le polynôme caractéristique P_u de u est scindé sur $\mathbb{K}$. Une telle situation est assurée pour $\mathbb{K}$ algébriquement clos.

Définition 2 *On appelle sous-espaces caractéristiques de u les sous espaces $N_k = \ker(u - \lambda_k Id)^{\alpha_k}$ où les λ_k sont les valeurs propres de u de multiplicité α_k.*

Théorème 3 *Avec ces notations, on a :*

1. $E = \bigoplus_{k=1}^{p} N_k$;
2. $N_k = \ker(u - \lambda_k Id)^{\beta_k}$;
3. *λ_k est la seule valeur propre de la restriction de u à N_k ;*

4. $\dim(N_k) = \alpha_k$;
5. *la restriction de* $u - \lambda_k Id$ *à* N_k *est nilpotente d'indice* β_k.

Théorème 4 (Dunford-Schwarz) *Soit* u *un endomorphisme de* E *dont le polynôme caractéristique est scindé sur* $\mathbb{K}$. *Il existe un unique couple* (d, v) *d'endomorphismes de* E *tel que* d *soit diagonalisable,* v *soit nilpotent,* d *et* v *commutent et* $u = d + v$.

Pratiquement la décomposition de Dunford-Schwarz d'un endomorphisme de E dont le polynôme caractéristique est scindé sur $\mathbb{K}$ passe par le calcul des projecteurs spectraux π_k.

La décomposition de Dunford-Schwarz d'un endomorphisme u de E dont le polynôme caractéristique est scindé sur $\mathbb{K}$ permet le calcul de ses puissances successives.

Exercice 2 *Ecrire la décomposition de Dunford-Schwarz de la matrice :*

$$A = \begin{pmatrix} 1 & 0 & -1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \in M_4(\mathbb{C}).$$

En déduire un calcul de A^r *pour tout entier* r *strictement positif.*

5 Endomorphismes semi-simples

Si le corps $\mathbb{K}$ n'est pas algébriquement, on a encore une décomposition de Dunford-Schwarz, l'endomorphisme diagonalisable d étant remplacé par un endomorphisme semi-simple.

On se donne $u \in \mathcal{L}(E)$.

Définition 3 *On dit que* u *est semi-simple si tout sous-espace vectoriel de* E *stable par* u *admet un supplémentaire stable par* u.

Théorème 5 *Si le corps* $\mathbb{K}$ *est algébriquement clos, alors* u *est semi-simple si, et seulement si, il est diagonalisable.*

Théorème 6 u *est semi-simple si, et seulement si, son polynôme minimal est sans facteurs carrés dans sa décomposition en facteurs irréductibles dans* $\mathbb{K}[x]$.

Théorème 7 (Dunford-Schwarz) *Pour* $\mathbb{K} = \mathbb{R}$ *ou* $\mathbb{C}$, *il existe un unique couple* (d, v) *d'endomorphismes de* E *tel que* d *soit semi-simple,* v *soit nilpotent,* d *et* v *commutent et* $u = d + v$.

6 Applications

6.1 Équations différentielles linéaires

On s'intéresse aux équations différentielles sur$\mathbb{R}$:

$$y^{(n)} = a_{n-1} y^{(n-1)} + \cdots + a_0 y \tag{3}$$

où les a_k sont des scalaires donnés.

Définition 4 *Avec ces notations, le polynôme :*

$$P(X) = X^n - \sum_{k=0}^{n-1} a_k X^k$$

est le polynôme caractéristique de (3).

L'ensemble S des solutions de (3) est $\ker(P(D))$, où P est le polynôme caractéristique de cette équation différentielle. C'est donc un espace vectoriel.

En notant $\lambda_1, \cdots, \lambda_p$ les racines complexes deux à deux distinctes de multiplicités respectives $m_1, \cdots, m_p$ de P, on a $P(X) = \prod_{k=1}^{p} (X - \lambda_k)^{m_k}$ et $P(D) = \prod_{k=1}^{p} (D - \lambda_k I_d)^{m_k}$.

Théorème 8 *Les solutions définies sur* $\mathbb{R}$ *et à valeurs complexes de l'équation différentielle* (3) *sont de la forme :*

$$x \mapsto y(x) = \sum_{k=1}^{p} e^{\lambda_k x} P_k(x),$$

où, pour tout k *compris entre* 1 *et* p, P_k *est une fonction polynomiale à coefficients complexes de degré inférieur ou égal à* $m_k - 1$, *ce qui revient à dire que l'ensemble* S *des solutions de cette équation est un* $\mathbb{C}$*-espace vectoriel de dimension* n *engendré par les fonctions :*

$$x \mapsto x^j e^{\lambda_k x} \ (1 \leq k \leq p,\ 0 \leq j \leq m_k - 1)$$

On suppose que les coefficients a_k sont réels et on note $\alpha_1, \cdots, \alpha_r$ les racines réelles distinctes de P (s'il en existe) et $\alpha_{r+1} \pm i\beta_{r+1}, \cdots, \alpha_s \pm i\beta_s$ les racines complexes non réelles (s'il en existe) de P, les β_j étant tous non nuls.

Corollaire 2 *On suppose que les coefficients a_k sont réels. Les solutions définies sur $\mathbb{R}$ et à valeurs réelles de l'équation différentielle* (3) *sont de la forme*

$$y(x) = \sum_{k=1}^{r} e^{\alpha_k x} P_k(x) + \sum_{k=r+1}^{s} e^{\beta_k x} \cos(\gamma_k x) P_k(x) + \sum_{k=r+1}^{s} e^{\beta_k x} \sin(\gamma_k x) Q_k(x),$$

où, pour tout k compris entre 1 et r, P_k est une fonction polynomiale à coefficients réels de degré inférieur ou égal à $m_k - 1$ et pour tout k compris entre $r+1$ et s, P_k et Q_k sont des fonctions polynomiales à coefficients réels de degré inférieur ou égal à $m_k - 1$, ce qui revient à dire que l'ensemble S des solutions réelles de cette équation est un $\mathbb{R}$-espace vectoriel de dimension n engendré par les fonctions :

$$\begin{cases} x^j e^{\alpha_k x},\ (1 \leq k \leq r,\ 0 \leq j \leq m_k - 1) \\ x^j e^{\beta_k x} \cos(\gamma_k x),\ x^j e^{\beta_k x} \sin(\gamma_k x),\ (r+1 \leq k \leq s,\ 0 \leq j \leq m_k - 1) \end{cases}$$

6.2 Suites définies par une récurrence linéaire

Dans ce paragraphe on s'intéresse aux suites $(u_n)_{n\in\mathbb{N}}$ de nombres complexes définies par une relation de récurrence linéaire et à coefficients constants de la forme :

$$\forall n \in \mathbb{N},\ u_{n+p} = a_0 u_n + a_1 u_{n+1} + \cdots + a_{p-1} u_{n+p-1} \tag{4}$$

où $p \geq 2$ et $a_0, \cdots, a_{p-1}$ sont des nombres complexes.

En notant φ l'endomorphisme de l'espace vectoriel $E = \mathbb{C}^{\mathbb{N}}$ des suites complexes défini par :

$$\forall u \in E,\ \varphi(u) : n \mapsto u_{n+1} - \sum_{k=0}^{p-1} a_k u_{n+k},$$

L'espace vectoriel S des solutions de (4) est un espace vectoriel de dimension p.

On désigne par T l'opérateur linéaire de translation défini sur E par :

$$\forall u \in E,\ T(u) : n \mapsto u_{n+1}$$

et on définit la suite de ses itérés $\left(T^k\right)_{k\in\mathbb{N}}$ par $T^0 = I_d$ et $T^{k+1} = T^k \circ T$ pour tout $k \in \mathbb{N}$ (pour tout $u \in E$, on a $T^k(u) : n \mapsto u_{n+k}$). À tout polynôme $P(X) = \sum_{k=0}^{p} \alpha_k X^k$ dans $\mathbb{C}[X]$ on peut associer l'opérateur $P(T) = \sum_{k=0}^{p} \alpha_k T^k$ et il est facile de vérifier que si P, Q sont deux polynômes alors $P(T) \circ Q(T) = Q(T) \circ P(T) = (PQ)(T)$.

Définition 5 *Avec ces notations, $P(X) = X^p - \sum_{k=0}^{p-1} a_k X^k$ est le polynôme caractéristique de* (4),

Si $\lambda_1, \cdots, \lambda_r$ sont les racines deux à deux distinctes de multiplicités respectives $m_1, \cdots, m_r$ du polynôme caractéristique P, on a alors :

$$\begin{cases} P(X) = \prod_{k=1}^{r} (X - \lambda_k)^{m_k}, \\ \varphi = P(T) = \prod_{k=1}^{r} (T - \lambda_k I_d)^{m_k}. \end{cases}$$

Théorème 9 *Avec les notations qui précèdent, les solutions de* (4), *où le coefficient a_0 est non nul ($\lambda = 0$ n'est pas racine du polynôme caractéristique) sont les suites de la forme :*

$$u_n = \sum_{k=1}^{r} Q_k(n) \lambda_k^n,$$

où, pour tout k compris entre 1 et r, Q_k est une fonction polynomiale à coefficients complexes de degré inférieur ou égal à $m_k - 1$, ce qui revient à dire que l'ensemble S des solutions de cette équation de récurrence est un $\mathbb{C}$-espace vectoriel de dimension p engendré par les suites :

$$n \mapsto n^j \lambda_k^n\ (1 \leq k \leq r,\ 0 \leq j \leq m_k - 1).$$

Dans le cas où les coefficients a_k sont réels, les racines du polynôme caractéristique sont stables par conjugaison complexe, c'est-à-dire que :

$$P(X) = \prod_{k=1}^{s} (X - \alpha_k)^{m_k} \prod_{k=s+1}^{t} (X - \lambda_k)^{m_k} \left(X - \overline{\lambda_k}\right)^{m_k}$$

les α_k étant réels et les $\lambda_k = \rho_k e^{i\theta_k}$ complexes non réels (dans le cas où il n'y a pas de racines réelles [resp. complexes non réelles] le produit correspondant vaut 1) et on a le résultat suivant.

Théorème 10 *Les suites réelles solutions de* (4) *sont de la forme*

$$u_n = \sum_{k=1}^{s} Q_k(n)\,\alpha_k^n + \sum_{k=s+1}^{t} Q_k(n)\,\rho_k^n \cos(n\theta_k) + \sum_{k=s+1}^{t} R_k(n)\,\rho_k^n \sin(n\theta_k),$$

où, pour tout k compris entre 1 *et* s, Q_k *est une fonction polynomiale à coefficients réels de degré inférieur ou égal à* $m_k - 1$ *et pour tout k compris entre* $s+1$ *et* t, Q_k *et* R_k *sont des fonctions polynomiales à coefficients réels de degré inférieur ou égal à* $m_k - 1$, *ce qui revient à dire que l'ensemble S des suites réelles solutions de cette équation de récurrence est un* $\mathbb{R}$*-espace vectoriel de dimension p engendré par les suites :*

$$\begin{cases} n^j \alpha_k^n, \ (1 \leq k \leq s, \ 0 \leq j \leq m_k - 1) \\ n^j \rho_k^n \cos(n\theta_k), \ n^j \rho_k^n \sin(n\theta_k), \quad (s+1 \leq k \leq t, \ 0 \leq j \leq m_k - 1) \end{cases}$$

Cette méthode d'étude des équations récurrentes linéaires à coefficients constants est analogue à celle utilisée pour la résolution d'équations différentielles linéaires à coefficients constants d'ordre p.

6.3 Calcul du rayon spectral d'une matrice complexe

En utilisant la décomposition de Dunford-Schwarz, on peut montrer le résultat suivant.

Théorème 11 *On a* $\rho(u) = \lim_{k \to +\infty} \left(\left\| u^k \right\|^{\frac{1}{k}} \right)$ *où* $\|\cdot\|$ *est une norme quelconque sur* $\mathcal{L}(E)$.

Corollaire 3 *La série* $\sum u^k$ *est convergente dans* $\mathcal{L}(E)$ *si, et seulement si,* $\rho(u) < 1$. *En cas de convergence de* $\sum u^k$, *l'endomorphisme* $Id - u$ *est inversible d'inverse* $\sum_{k=0}^{+\infty} u^k$.

6.4 Exponentielle d'un endomorphisme

Lemme 1 *En notant* $u = d + v$ *la décomposition de Dunford-Schwarz de* u, *on a :*

$$e^u = e^d e^v = e^d \sum_{k=0}^{q-1} \frac{1}{k!} v^k$$

où $q \geq 1$ *est l'indice de nilpotence de* v.

Théorème 12 *Si* $u = d + v$ *est la décomposition de Dunford-Schwarz de* u, *alors celle de* e^u *est donnée par :*

$$e^u = e^d + e^d (e^v - Id),$$

avec e^d *diagonalisable et* $e^d (e^v - I_n)$ *nilpotente.*

Corollaire 4 *u est diagonalisable si, et seulement si,* e^u *est diagonalisable.*

Exercice 3 *Déterminer toutes les solutions dans* $\mathcal{L}(E)$ *de l'équation* $e^u = Id$.

Opérations élémentaires sur les lignes ou les colonnes d'une matrice. Applications

$\mathbb{K}$ est un corps commutatif, $\mathcal{M}_{n,m}(\mathbb{K})$ est l'espace des matrices à n lignes, m colonnes et à coefficients dans $\mathbb{K}$. Pour $m=n$, on note $\mathcal{M}_n(\mathbb{K})$.

On note $(E_{ij})_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}$ la base canonique de $\mathcal{M}_{n,m}(\mathbb{K})$.

Pour $A\in\mathcal{M}_{n,m}(\mathbb{K})$, on note L_i sa ligne numéro i et C_j sa colonne numéro j.

1 Dilatations, transvections et opérations élémentaires

On appelle matrice déduite de A par opération élémentaire sur les lignes de A toute matrice de la forme :

$$A_i(\lambda)=\begin{pmatrix} L_1\\ \vdots\\ L_{i-1}\\ \lambda L_i\\ L_{i+1}\\ \vdots\\ L_n\end{pmatrix},\ \text{ou } A_{ij}(\lambda)=\begin{pmatrix} L_1\\ \vdots\\ L_{i-1}\\ L_i+\lambda L_j\\ L_{i+1}\\ \vdots\\ L_n\end{pmatrix}$$

On appelle matrice déduite de A par opération élémentaire sur les colonnes de A toute matrice de la forme :

$$A'_j(\lambda)=\begin{pmatrix} C_1 & \cdots & C_{j-1} & \lambda C_j & C_{j+1} & \cdots & C_m\end{pmatrix},$$

ou :

$$A'_{ij}(\lambda)=\begin{pmatrix} C_1 & \cdots & C_{j-1} & C_j+\lambda C_i & C_{j+1} & \cdots & C_m\end{pmatrix}$$

Définition 1 *On appelle matrice de transvection toute matrice dans $\mathcal{M}_n(\mathbb{K})$ de la forme :*

$$T_{ij}(\lambda)=I_n+\lambda E_{ij},$$

avec $1\leq i\neq j\leq n$ et $\lambda\in\mathbb{K}$.
On appelle matrice de dilatation toute matrice dans $\mathcal{M}_n(\mathbb{K})$ de la forme :

$$D_i(\lambda)=I_n+(\lambda-1)E_{ii},$$

avec $1\leq i\leq n$ et $\lambda\in\mathbb{R}^*$.

Théorème 1 *Avec les notations qui précèdent on a :*

$$\begin{cases} A_i(\lambda)=D_i(\lambda)A \text{ pour } 1\leq i\leq n\\ A_{ij}(\lambda)=T_{ij}(\lambda)A \text{ pour } 1\leq i\neq j\leq n\\ A'_j(\lambda)=AD_j(\lambda) \text{ pour } 1\leq j\leq m\\ A'_{ij}(\lambda)=AT_{ij}(\lambda) \text{ pour } 1\leq i\neq j\leq m\end{cases}$$

Remarque 1 *On sera amené à utiliser deux autres types d'opérations élémentaires que sont les permutations de lignes ou de colonnes. En fait ces opérations se déduisent des précédentes. Par exemple pour permuter les lignes i et j où $1\leq i<j\leq n$ on effectue les opérations suivantes :*

$$\begin{pmatrix} L_1\\ \vdots\\ L_n\end{pmatrix}\mapsto\begin{pmatrix} L_1\\ \vdots\\ L_{i-1}\\ L_i+L_j\\ L_{i+1}\\ \vdots\\ L_n\end{pmatrix}\mapsto\begin{pmatrix} L_1\\ \vdots\\ L_i+L_j\\ \vdots\\ -L_i\\ \vdots\\ L_n\end{pmatrix}\mapsto\begin{pmatrix} L_1\\ \vdots\\ L_j\\ \vdots\\ -L_i\\ \vdots\\ L_n\end{pmatrix}\mapsto\begin{pmatrix} L_1\\ \vdots\\ L_j\\ \vdots\\ L_i\\ \vdots\\ L_n\end{pmatrix},$$

ce qui revient à effectuer les produits :

$$D_j(-1)T_{ij}(1)T_{ji}(-1)T_{ij}(1)A.$$

La matrice $D_j(-1)T_{ij}(1)T_{ji}(-1)T_{ij}(1)$ est la matrice de permutation qui se déduit de la matrice I_n en permutant ses colonnes i et j. Elle s'écrit plus simplement :

$$P_{ij}=I_n-(E_{ii}+E_{jj})+(E_{ij}+E_{ji}).$$

De même la permutation des colonnes i et j est obtenue avec :

$$AT_{ij}(1)T_{ji}(-1)T_{ij}(1)D_i(-1).$$

Le produit de matrices $T_{ij}(1)T_{ji}(-1)T_{ij}(1)D_i(-1)$ est la matrice de permutation ${}^tP_{ij}=P_{ji}$.

Lemme 1 *Une matrice de permutation P_{ij} est inversible d'inverse $P_{ij}^{-1} = P_{ji}$.*

Définition 2 *On appelle matrice élémentaire une matrice de dilatation, de transvection ou de permutation.*

Définition 3 *On appelle opération élémentaire sur une matrice $A \in \mathcal{M}_{n,m}(\mathbb{K})$ le résultat de la multiplication à gauche ou à droite de A par une matrice élémentaire.*

Lemme 2 *Les opérations élémentaires conservent le rang.*

Théorème 2 *Une matrice $A \in \mathcal{M}_n(\mathbb{K})$ (où $n \geq 2$) est inversible si, et seulement si, elle est produit de matrices élémentaires. Précisément si $A \in \mathcal{M}_n(\mathbb{K})$ est inversible, il existe alors des matrices de transvection $P_1, \cdots, P_r$ et $Q_1, \cdots, Q_s$ et une matrice de dilatation $D_n(\lambda)$ telles que :*

$$A = P_1 \cdots P_r D_n(\lambda) Q_1 \cdots Q_s.$$

Les propriétés du déterminant d'une matrice carrée peuvent être montrées à partir des opérations élémentaires.

2 Méthode des pivots de Gauss

En effectuant des opérations élémentaires sur les lignes du système linéaire $Ax = b$, on le transforme en un système triangulaire supérieur $Rx = c$. Du fait qu'une permutation de lignes change le déterminant de signe et que d'ajouter un multiple d'une ligne à une autre ne change pas ce dernier, on a :

$$\det(A) = \det(R) = \pm \prod_{i=1}^{n} r_{ii}.$$

On note ici L_i la ligne numéro i du système linéaire $Ax = b$.

Etape 0 — On se ramène à un système tel que a_{11} non nul.

Si pour tout $i = 1, 2, \cdots, n$, on a $a_{i1} = 0$, alors $\det(A) = 0$ et c'est fini. Sinon, il existe $i > 1$ tel que a_{i1} soit non nul, et en permutant les lignes 1 et i (si $i = 1$, on ne fait rien), on se ramène à un système $A^{(1)}x = b^{(1)}$, avec $a_{11}^{(1)}$ non nul.

Le coefficient $a_{11}^{(1)}$ est le premier pivot.

On a alors $\det(A) = \pm \det\left(A^{(1)}\right)$, avec le signe moins si et seulement si il y a une permutation des lignes 1 et i avec $i > 1$.

Etape k — Elimination de x_k dans les équations $k+1, \cdots, n$.

À la fin de l'étape $k-1$, on a obtenu le système $A^{(k)}x = b^{(k)}$, avec :

$$A^{(k)} = \begin{pmatrix} a_{11}^{(1)} & a_{12}^{(1)} & \cdots & a_{1k}^{(1)} & \cdots & a_{1n}^{(1)} \\ 0 & a_{22}^{(2)} & \cdots & a_{2k}^{(2)} & \cdots & a_{2n}^{(2)} \\ \vdots & \ddots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{kk}^{(k)} & \cdots & a_{kn}^{(k)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{nk}^{(k)} & \cdots & a_{nn}^{(k)} \end{pmatrix}$$

et $a_{kk}^{(k)}$ non nul.

Le coefficient $a_{kk}^{(k)}$ est le pivot numéro k.

On effectue alors les transformations élémentaires suivantes :

$$L_i^{(k)} \mapsto L_i^{(k)} - \frac{a_{ik}^{(k)}}{a_{kk}^{(k)}} L_k^{(k)} \ (i = k+1, \cdots, n),$$

puis une éventuelle permutation des lignes $k+1$ et $j > k+1$ pour se ramener à $a_{k+1,k+1}^{(k+1)}$ non nul.

Au bout de $n-1$ étapes, on est donc ramené à un système triangulaire supérieur $A^{(n)}x = b^{(n)}$.

De plus, on a $\det(A) = (-1)^p \det\left(A^{(n)}\right)$, où p est le nombre de permutations qui ont été nécessaires pour avoir des pivots non nuls et $\det\left(A^{(n)}\right)$ est le produit des pivots.

Remarque 2 *Pour éviter de faire une division par un nombre trop petit, dans le choix du pivot, on aura intérêt, à l'étape $k-1$, à permuter la ligne k avec la ligne $j \geq k$ telle que :*

$$|a_{jk}| = \max\{|a_{ik}| \mid i = k, \cdots, n\},$$

de manière à avoir le pivot le plus grand possible en valeur absolue.
Si ce maximum est trop petit, alors le système est numériquement dégénéré.

3 Décomposition LR (méthode de Crout)

Définition 4 *On appelle sous-matrices principales d'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ les matrices :*

$$A_k = ((a_{ij}))_{1 \leq i,j \leq k}, \ (k = 1, \cdots, n).$$

Les déterminants principaux sont les $\Delta_k = \det(A_k)$.

La méthode des pivots de Gauss est basée sur les résultats suivants.

Lemme 3 *Soit $A \in \mathcal{M}_n(\mathbb{K})$ de coefficient a_{11} non nul. Il existe des matrices de transvection $P_1, \cdots, P_r$ telles que :*

$$P_r \cdots P_1 A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22}^{(1)} & \cdots & a_{2n}^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2}^{(1)} & \cdots & a_{nn}^{(1)} \end{pmatrix}.$$

Définition 5 *On appelle matrice de Frobenius une matrice carrée d'ordre n qui ne diffère de l'identité que par une colonne (ou une ligne).*

Théorème 3 *Toute matrice $A \in GL_n(\mathbb{K})$ peut être réduite à la forme triangulaire supérieur en la multipliant à gauche par des matrices de transvection ou de dilatation de la forme $D_i(-1)$.*

Dans l'hypothèse où tous les déterminants principaux de la matrice A sont non nuls (on n'effectue pas de permutations de lignes dans la méthode de Gauss) le résultat précédent s'exprime en disant qu'il existe des matrices de Frobenius de la forme :

$$F_k = \prod_{i=k+1}^{n} T_{ik}(\lambda_{ik})$$

telles que :

$$F_{n-1} \cdots F_1 A = R$$

où R est une matrice triangulaire supérieure.

La matrice produit $F_{n-1} \cdots F_1$ est triangulaire inférieure à diagonale unité. En notant $L = (F_{n-1} \cdots F_1)^{-1}$ on a alors la décomposition $A = LR$ avec L triangulaire inférieure à diagonale unité et R triangulaire supérieure.

Théorème 4 *Une matrice inversible A possède une décomposition $A = LR$, avec L triangulaire inférieure à diagonale unité et R triangulaire supérieure si et seulement si tous les déterminants principaux de A sont non nuls. Une telle décomposition est unique et les coefficients diagonaux de R sont donnés par :*

$$\begin{cases} r_{11} = a_{11}, \\ r_{kk} = \dfrac{\det(A_k)}{\det(A_{k-1})} \ (k = 2, \cdots, n), \end{cases}$$

où les A_k désignent les sous matrices principales de A.

Pour obtenir pratiquement de la décomposition LR on peut procéder par coefficients indéterminés.

En utilisant la décomposition $A = LR$, le système $Ax = b$ équivaut aux deux systèmes triangulaires :

$$\begin{cases} Ly = b \quad \text{(triangulaire inférieur)}, \\ Rx = y \quad \text{(triangulaire supérieur)}. \end{cases}$$

La méthode obtenue est appelée méthode de Crout.

En utilisant la décomposition $A = LR$, on a $A^{-1} = R^{-1}L^{-1}$ et il suffit alors d'utiliser des procédures d'inversion des matrices triangulaires.

4 Décomposition $LD\,{}^tL$ des matrices symétriques réelles

On suppose que A est inversible symétrique et qu'il n'y a pas de permutations dans la méthode de Gauss.

Dans la décomposition LR de A, on a $\det(R) = \det(A) \neq 0$, donc tous les termes diagonaux de R sont non nuls et on peut écrire R sous la forme $R = DR'$, où D est diagonale et R' est triangulaire supérieure à diagonale unité (il suffit de diviser chaque ligne de R par son terme diagonal). On a donc $A = LDR'$, puis en écrivant que ${}^tA = A$ et en utilisant le fait que la décomposition LR est unique, on déduit que $R' = {}^tL$.

On a donc pour toute matrice symétrique A, dont tous les déterminants principaux sont non nuls, la décomposition unique $A = LD\,{}^tL$, la matrice L étant triangulaire inférieure et à diagonale unité et la matrice D diagonale.

Remarque 3 *Cette décomposition nous donne un moyen de calculer la signature de la matrice symétrique réelle A.*

Remarque 4 *La matrice A est définie positive si et seulement si tous les coefficients de D sont strictement positifs.*

Comme pour la décomposition LR, on trouve les coefficients de L et D par identification, ce qui donne, $d_1 = a_{11}$ et pour $i = 2, \cdots, n$:

$$\begin{cases} L_{ij} = \dfrac{\left(a_{ij} - \sum\limits_{k=1}^{j-1} L_{ik} d_k L_{jk}\right)}{d_j} & (j = 1, \cdots, i-1), \\ d_i = \left(a_{ii} - \sum\limits_{k=1}^{i-1} L_{ik}^2 d_k\right). \end{cases}$$

5 Décomposition de Cholesky des matrices symétriques réelles définies positives

Théorème 5 *Une matrice réelle A est symétrique définie positive si et seulement si il existe une matrice B triangulaire inférieure et inversible telle que $A = B\,{}^tB$. De plus une telle décomposition est unique si on impose la positivité des coefficients diagonaux de la matrice B.*

Le calcul effectif des coefficients de B se fait par identification ce qui donne :

$$\begin{cases} b_{ij} = \dfrac{\left(a_{ij} - \sum\limits_{k=1}^{j-1} b_{ik} b_{jk}\right)}{b_{jj}} & (j = 1, \cdots, i-1), \quad (i = 1, \cdots, n). \\ b_{ii}^2 = a_{ii} - \sum\limits_{k=1}^{i-1} b_{ik}^2, \end{cases}$$

Le déterminant de A se calcule avec :

$$\det(A) = \prod_{i=1}^{b} b_{ii}^2.$$

La résolution du système $Ax = e$ se ramène à la résolution de deux systèmes triangulaires.
Pour calculer l'inverse de A il suffit d'inverser la matrice triangulaire B.

6 Méthode d'élimination de Gauss-Jordan

À l'étape k, on ne se contente pas seulement d'éliminer le coefficient de x_k dans les lignes $k+1$ à n, mais on l'élimine aussi dans les lignes du dessus soit 1 à $k-1$. Ce qui donnera au bout de n étapes un système diagonal.

Description de la k$^{\text{ème}}$ étape du calcul ($1 \leq k \leq n$) — À la $k^{ème}$ étape, on est au départ dans la situation suivante :

$$\begin{cases} x_1 + & & & & + a_{1k}^{(k)} x_k & + \cdots & + a_{1n}^{(k)} x_n & = & b_1^{(k)} \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & x_{k-1} & + a_{k-1,k}^{(k)} x_k & + \cdots & + a_{k-1,n}^{(k)} x_n & = & b_{k-1}^{(k)} \\ & & & & + a_{kk}^{(k)} x_k & + \cdots & + a_{kn}^{(k)} x_n & = & b_k^{(k)} \\ & & & & + a_{k+1,k}^{(k)} x_k & + \cdots & + a_{k+1,n}^{(k)} x_n & = & b_{k+1}^{(k)} \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & & + a_{nk}^{(k)} x_k & + \cdots & + a_{nn}^{(k)} x_n & = & b_n^{(k)} \end{cases}$$

On peut supposer que $a_{kk}^{(k)}$ est le pivot maximum, sinon, il suffit de permuter avec une des lignes suivantes.

On commence par extraire x_k de la $k^{ème}$ équation :

$$x_k = \frac{\left(b_k^{(k)} - a_{k,k+1}^{(k)} x_{k+1} - \cdots - a_{kn}^{(k)} x_n\right)}{a_{k,k}^{(k)}},$$

que l'on reporte ensuite dans les autres équations, ce qui donne :

$$\begin{cases} x_1 + & & & & + a_{1k+1}^{(k+1)} x_{k+1} & + \cdots & + a_{1n}^{(k+1)} x_n & = & b_1^{(k+1)} \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & x_{k-1} & + a_{k-1,k+1}^{(k+1)} x_{k+1} & + \cdots & + a_{k-1,n}^{(k+1)} x_n & = & b_{k-1}^{(k+1)} \\ & & & x_k & + a_{k,k+1}^{(k+1)} x_{k+1} & + \cdots & + a_{kn}^{(k+1)} x_n & = & b_k^{(k+1)} \\ & & & & + a_{k+1,k+1}^{(k+1)} x_{k+1} & + \cdots & + a_{k+1,n}^{(k+1)} x_n & = & b_{k+1}^{(k+1)} \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & & + a_{nk+1}^{(k+1)} x_{k+1} & + \cdots & + a_{nn}^{(k+1)} x_n & = & b_n^{(k+1)} \end{cases}$$

avec, pour $j = k+1, \cdots, n$:

$$a_{kj}^{(k+1)} = \frac{a_{kj}^{(k)}}{a_{kk}^{(k)}},\ b_k^{(k+1)} = \frac{b_k^{(k)}}{a_{kk}^{(k)}}$$

et, pour $i \in \{1, \cdots, n\} - \{k\}$, $j \in \{k+1, \cdots, n\}$:

$$a_{ij}^{(k+1)} = a_{ij}^{(k)} - a_{ik}^{(k)} a_{kj}^{(k+1)},\ b_i^{(k+1)} = b_i^{(k)} - a_{ik}^{(k)} b_k^{(k+1)}.$$

On obtient alors directement la solution, après la $n^{ème}$ étape :

$$\begin{cases} x_1 = b_1^{(n)} \\ . \\ . \\ x_n = b_n^{(n)} \end{cases}$$

Endomorphismes symétriques d'un espace vectoriel euclidien. Applications

Les résultats de base concernant l'algèbre linéaire, l'algèbre bilinéaire et les espaces euclidiens sont supposés connus.
$\mathcal{S}_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) \mid {}^tA = A\}$ est l'espace des matrices symétriques.

1 Endomorphismes symétriques

Théorème 1 *Pour tout endomorphisme $u \in \mathcal{L}(E)$, il existe un unique endomorphisme $u^* \in \mathcal{L}(E)$ tel que :*

$$\forall (x,y) \in E^2,\ \langle u(x) \mid y\rangle = \langle x \mid u^*(y)\rangle$$

Définition 1 *Avec les notations du théorème précédent, on dit que u^* est l'adjoint de u.*

Théorème 2 *Si $\mathcal{B} = (e_i)_{1\leq i\leq n}$ est une base orthonormée de E et u un endomorphisme de E de matrice A dans cette base, alors la matrice de u^* dans $\mathcal{B}$ est la transposée ${}^tA$.*

Remarque 1 *Si $A = (a_{ij})_{1\leq i,j\leq n}$ est la matrice de u dans une base orthonormée, on a alors pour tous i, j compris entre 1 et n :*

$$a_{ij} = \langle u(e_j) \mid e_i\rangle$$

Définition 2 *Un endomorphisme $u \in \mathcal{L}(E)$ est dit symétrique (ou auto-adjoint) si $u^* = u$.*

On note $\mathcal{S}(E)$ l'ensemble de tous les endomorphismes symétriques de E.

Théorème 3 *Un endomorphisme $u \in \mathcal{L}(E)$ est symétrique si, et seulement si, sa matrice dans une base orthonormée de E est symétrique.*

Corollaire 1 *$\mathcal{S}(E)$ est un sous-espace vectoriel de $\mathcal{L}(E)$ de dimension $\dfrac{n(n+1)}{2}$.*

2 Réduction des endomorphismes symétriques

Théorème 4 (spectral) *Tout endomorphisme symétrique $u \in \mathcal{S}(E)$ se diagonalise dans une base orthonormée.*

Corollaire 2 *Toute matrice symétrique réelle $A \in \mathcal{S}_n(\mathbb{R})$ se diagonalise dans une base orthonormée, c'est-à-dire qu'il existe une matrice orthogonale $P \in \mathcal{O}_n(\mathbb{R})$ telle que ${}^tPAP$ soit diagonale.*

Exercice 1 *Diagonaliser :*

$$A(a,b) = \begin{pmatrix} b & a & a & \cdots & a \\ a & b & a & \cdots & a \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ a & \cdots & a & b & a \\ a & \cdots & a & a & b \end{pmatrix}$$

dans une base orthonormée.

3 Endomorphismes symétriques positifs ou définis positifs

Définition 3 *Un endomorphisme $u \in \mathcal{L}(E)$ est dit symétrique positif [resp. défini positif] s'il est symétrique avec $\langle x \mid u(x)\rangle \geq 0$ pour tout $x \in E$ [resp. $\langle x \mid u(x)\rangle > 0$ pour tout $x \in E \setminus \{0\}$].*

On note $\mathcal{S}^+(E)$ [resp. $\mathcal{S}^{++}(E)$] l'ensemble des endomorphismes symétriques positifs [resp. définis positifs] de E.

Définition 4 *Une matrice $A \in \mathcal{M}_n(\mathbb{R})$ est dite symétrique positive [resp. définie positive] si elle est symétrique avec $\langle x \mid Ax\rangle \geq 0$ pour tout $x \in \mathbb{R}^n$ [resp. $\langle x \mid Ax\rangle > 0$ pour tout $x \in \mathbb{R}^n \setminus \{0\}$].*

On note $\mathcal{S}_n^+(\mathbb{R})$ [resp. $\mathcal{S}_n^+(\mathbb{R})$] l'ensemble des matrices symétriques positives [resp. définies positives].

Théorème 5 *Soit $u \in \mathcal{S}(E)$. On a $u \in \mathcal{S}^+(E)$ [resp. $u \in \mathcal{S}^{++}(E)$] si, et seulement si, toutes ses valeurs propres sont positives [resp. strictement positives].*

Corollaire 3 *Soit $A \in \mathcal{M}_n(\mathbb{R})$. La matrice A est dans $\mathcal{S}_n^+(\mathbb{R})$ si, et seulement si, il existe $B \in \mathcal{M}_n(\mathbb{R})$ telle que $A = {}^tBB$.*

Théorème 6 *Soit $u \in \mathcal{S}(E)$ de matrice $A = ((a_{ij}))_{1\leq i,j\leq n} \in \mathcal{S}_n(\mathbb{R})$ dans une base orthonormée $\mathcal{B} = (e_i)_{1\leq i\leq n}$. L'endomorphisme symétrique u est défini positif si, et seulement si, tous les mineurs principaux de A sont strictement positifs.*

Corollaire 4 *L'ensemble $\mathcal{S}_n^{++}(\mathbb{R})$ est un ouvert de $\mathcal{M}_n(\mathbb{R})$.*

Exercice 2 *Montrer que $\mathcal{S}_n^+(\mathbb{R})$ est un fermé convexe de $\mathcal{M}_n(\mathbb{R})$ et que son intérieur est $\mathcal{S}_n^{++}(\mathbb{R})$.*

Exercice 3 *Soit $u \in \mathcal{S}(E)$. Montrer que $\mathrm{Tr}(u) = 0$ si, et seulement si, il existe une base orthonormée de E telle que la matrice de u dans cette base a tous ses termes diagonaux nuls.*

4 Réduction des endomorphismes symétriques et des formes quadratiques sur $\mathbb{R}^n$

On peut associer une forme quadratique à une matrice symétrique réelle $A = ((a_{ij}))_{1\leq i,j\leq n}$ en posant, pour tout $x \in \mathbb{R}^n$:

$$q(x) = \langle Ax \mid x\rangle = \sum_{i=1}^{n}\left(\sum_{j=1}^{n} a_{ij}x_j\right)x_i = \sum_{i=1}^{n} a_{ii}x_i^2 + 2\sum_{1\leq i<j\leq n} a_{ij}x_ix_j.$$

Réciproquement si q est une forme quadratique sur $\mathbb{R}^n$ de forme polaire φ, sa matrice dans la base canonique $(e_i)_{1\leq i\leq n}$ (ou dans une base quelconque) de $\mathbb{R}^n$, $A = ((\varphi(e_i,e_j)))_{1\leq i,j\leq n}$, est symétrique.

On se donne $A \in \mathcal{S}_n(\mathbb{R})$ et on désigne par $u \in \mathcal{S}(\mathbb{R}^n)$ l'endomorphisme symétrique de $\mathbb{R}^n$ et par q la forme quadratique qui lui sont canoniquement associés. On note φ la forme polaire de q.

Théorème 7 *La matrice A se diagonalise dans une base orthonormée de $\mathbb{R}^n$.*

Du théorème spectral, on peut déduire le théorème de réduction de Gauss qui suit.

On se donne une forme quadratique non nulle q sur $\mathbb{R}^n$.

Théorème 8 *Il existe un entier r compris entre 1 et n, des réels non nuls $\lambda_1,\cdots,\lambda_r$ et des formes linéaires indépendantes $\ell_1,\cdots,\ell_r$ tels que :*

$$\forall x \in \mathbb{R}^n,\ q(x) = \sum_{j=1}^{r}\lambda_j\ell_j^2(x)$$

5 Quelques applications du théorème spectral

5.1 La norme euclidienne sur $\mathcal{M}_n(\mathbb{R})$

Théorème 9 *Pour toute matrice $A = ((a_{ij}))_{1\leq i,j\leq n} \in \mathcal{S}_n(\mathbb{R})$ de valeurs propres $\lambda_1,\cdots,\lambda_n$, on a :*

$$\sum_{1\leq i,j\leq n} a_{ij}^2 = \sum_{i=1}^{n}\lambda_i^2.$$

5.2 Diagonalisation simultanée d'endomorphismes symétriques

Théorème 10 *Soit $(u_i)_{i\in I}$ une famille d'endomorphismes symétriques de E (l'ensemble I ayant au moins deux éléments). Il existe une base orthonormée commune de diagonalisation dans E pour la famille $(u_i)_{i\in I}$ si, et seulement si, ces endomorphismes commutent deux à deux.*

5.3 Racine carrée d'une matrice réelle symétrique positive

Théorème 11 *Si $A \in \mathcal{S}_n^+(\mathbb{R})$, il existe alors une unique $B \in \mathcal{S}_n^+(\mathbb{R})$ telle que $A = B^2$.*

Avec les notations du théorème, on dit que B est la racine carrée positive de $A \in \mathcal{S}_n^+(\mathbb{R})$.

Exercice 4 *Soient $A \in \mathcal{S}_n^{++}(\mathbb{R})$ et $B \in \mathcal{S}_n^+(\mathbb{R})$. Montrer que AB a toutes ses valeurs propres réelles positives et est diagonalisable.*

5.4 Décomposition polaire

Corollaire 5 *Toute matrice $A \in GL_n(\mathbb{R})$ peut s'écrire de manière unique $A = \Omega S$ où Ω est une matrice orthogonale et S une matrice symétrique définie positive.*

Démonstration. Si $A = \Omega S$, alors ${}^tAA = S\,{}^t\Omega\Omega S = S^2$ et S est la racine carrée positive de la matrice symétrique définie positive ${}^tAA$ ($\langle {}^tAAx \mid x\rangle = \|Ax\|^2 > 0$ pour x non nul). La matrice Ω est alors donnée par $\Omega = AS^{-1}$ (A inversible entraîne S inversible). On a donc, en cas d'existence, l'unicité des matrices Ω et S.

Si $A \in GL_n(\mathbb{R})$, alors ${}^tAA$ est symétrique définie positive et elle admet une unique racine carrée symétrique définie positive S. En posant $\Omega = AS^{-1}$, on a $A = \Omega S$ et :

$${}^t\Omega\Omega = {}^t\left(S^{-1}\right)\left({}^tAA\right)S^{-1} = \left({}^tS\right)^{-1}S^2S^{-1} = S^{-1}S = I_n,$$

c'est-à-dire que Ω est orthogonale. ■

De la densité de $GL_n(\mathbb{R})$ dans $\mathcal{M}_n(\mathbb{R})$, on peut déduire une généralisation à $\mathcal{M}_n(\mathbb{R})$ du théorème de décomposition polaire des matrices inversibles.

Théorème 12 *Toute matrice $A \in \mathcal{M}_n(\mathbb{R})$ peut s'écrire $A = \Omega S$ où Ω est une matrice orthogonale et S une matrice symétrique positive.*

Théorème 13 *L'application $(\Omega, S) \longmapsto \Omega S$ réalise un homéomorphisme de $\mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R})$ sur $GL_n(\mathbb{R})$.*

5.5 Rayon spectral des matrices symétriques réelles

Lemme 1 *Si* $A \in \mathcal{S}_n(\mathbb{R})$, *alors :*

$$\|A\| = \rho(A).$$

Théorème 14 *Pour toute matrice* $A \in \mathcal{M}_n(\mathbb{R})$, *on a :*

$$\|A\| = \sqrt{\| {}^tAA\|} = \sqrt{\rho({}^tAA)}.$$

Exercice 5 *Calculer* $\|A\|$, *où :*

$$A = \begin{pmatrix} 1 & 0 & \cdots & 0 & -1 \\ -1 & 1 & 0 & \ddots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & -1 & 1 & 0 \\ 0 & \cdots & 0 & -1 & 1 \end{pmatrix}.$$