Algèbre bilinéaire
préparation à l'agrégation

Alexis Tchoudjem

Université Lyon I

11 janvier 2016

Dans ce cours $\mathbb{K}$ est un corps qui peut être, par exemple, $\mathbb{F}_q, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{C}(X), \ldots$

1 Références

Par odre croissant de difficulté :

1. Xavier Gourdon, *Les maths en tête, Algèbre*
2. Vinberg, *Algebra*
3. Cohn, *Algebra I*
4. Victor Prasolov, *Problèmes et théorèmes d'algèbre linéaire*

Table des matières

2 Dual

Définition 1 $E^* := \mathrm{Hom}_{\mathbb{K}}(E, \mathbb{K})$.

2.1 Formes linéaires, hyperplans

On a une bijection $\mathbb{P}(E^*) \stackrel{1:1}{\to} \{\text{hyperplans}\}$, $\lambda \mapsto \ker \lambda$.

2.2 Bases duales

Exemple : la base duale des formes linéaires $P \mapsto P^{(i)}(0)$
En dimension finie, $E \simeq E^*$ mais en dimension infinie, $\dim E < \dim E^*$.

Exercice 1 $(\mathbb{R}^{(\mathbb{N})})^* \simeq \mathbb{R}^{\mathbb{N}}$ *et* $\dim \mathbb{R}^{\mathbb{N}}$ *est le cardinal de* $\mathbb{R}$ *(indication : les suites* $(\lambda^n)_{n\in\mathbb{N}}$, $\lambda \in \mathbb{R}$ *sont* $\mathbb{R}-$*linéairement indépendantes ...).*

2.3 Bidual

L'application $E \to E^{**}$, $x \mapsto \mathrm{ev}_x$ est un isomorphisme en dimension finie.

2.4 Orthogonalité

Si V est un sous-espace de E, on note

$$V^\perp := \Big\{\lambda \in E^* \ : \ {}^\forall x \in V,\ \langle \lambda, x\rangle = 0\Big\}$$

c'est un sous-espace vectoriel de E^* (*exo*) , appelé *l'orthogonal* de V. Si W est un sous-espace de E^*, on note :

$$W^\circ := \Big\{x \in E \ : \ {}^\forall \lambda \in W,\ \langle \lambda, x\rangle = 0\Big\}$$

c'est un sous-espace vectoriel de E (*exo*) , appelé *l'orthogonal* de W.

Exercice 2 *Vérifier que l'on a toujours :*

$$V \subseteq V^{\perp\circ}\,,\ W \subseteq W^{\circ\perp}\,,\ V^\perp = V^{\perp\circ\perp}\,,\ W^\circ = W^{\circ\perp\circ}$$

pour tous sous-espaces V de E et W de E^*.

Exercice 3 *Vérifier que l'on a toujours :*

$$V \subseteq V^{\perp\circ}\,,\ W \subseteq W^{\circ\perp}\,,\ V^\perp = V^{\perp\circ\perp}\,,\ W^\circ = W^{\circ\perp\circ}$$

pour tous sous-espaces V de E et W de E^*.

Proposition 2.1 *Si F est un sous-espace de E, alors $F = E \Leftrightarrow F^\perp = 0$.*

Démonstration : Soit $\pi : E \to E/F$ la surjection canonique. Si $F^\perp = 0$ alors, pour tout $\mu \in (E/F)^*$, $\mu \circ \pi \in F^\perp$ donc $\mu \circ \pi = 0$. Donc, pour tout $x \in E$, $\langle \mu, \pi(x) \rangle = 0$, pour tout $\mu \in (E/F)^*$. Donc $\pi(x) = 0$ *i.e.* $x \in F$ pour tout $x \in E$. *q.e.d.*

Corollaire 2.1.1 (Équations des sous-espaces en dimension finie) *Si E est de dimension n alors :*

i) Si $\lambda_1, ..., \lambda_p \in E^*$ sont des formes linéaires telles que $\dim\langle \lambda_1, ..., \lambda_p \rangle = r$ alors : le sous-espace

$$F := \{x \in E \, : \, {}^\forall i, \, \langle \lambda_i, x \rangle = 0\}$$

est de dimension $n - r$.

ii) Réciproquement, si F est un sous-espace de E de dimension q, il existe $n - q$ formes linéaires linéairement indépendantes $\lambda_1, ..., \lambda_{n-q}$ telles que :

$$F = \{x \in E \, : \, {}^\forall 1 \le i \le n - q, \, \langle \lambda_i, x \rangle = 0\} \ .$$

Proposition 2.2 *On suppose E de dimension finie. Soient V_1, V_2 deux sous-espaces de E. Alors : i) $(V_1 + V_2)^\perp = V_1^\perp \cap V_2^\perp$, ii) $(V_1 \cap V_2)^\perp = V_1^\perp + V_2^\perp$.*

Soient W_1, W_2 deux sous-espaces de E^*. Alors : i) $(W_1 + W_2)^\circ = W_1^\circ \cap W_2^\circ$, ii) $(W_1 \cap W_2)^\circ = W_1^\circ + W_2^\circ$.

Démonstration :

i) : $V_1 \subseteq V_1 + V_2 \Rightarrow (V_1 + V_2)^\perp \subseteq V_1^\perp$. De même : $(V_1 + V_2)^\perp \subseteq V_2^\perp$. Donc $(V_1 + V_2)^\perp \subseteq V_1^\perp \cap V_2^\perp$. Pour la réciproque, soit $\lambda \in V_1^\perp \cap V_2^\perp$. Alors, ${}^\forall v_1 \in V_1, {}^\forall v_2 \in V_2$, $\langle \lambda, v_1 + v_2 \rangle = \langle \lambda, v_1 \rangle + \langle \lambda, v_2 \rangle = 0$. Donc, $\lambda \in (V_1 + V_2)^\perp$.

Démontrons ii) :

$V_1 \cap V_2 \subseteq V_1 \Rightarrow V_1^\perp \subseteq (V_1 \cap V_2)^\perp$. De même, $V_2^\perp \subseteq (V_1 \cap V_2)^\perp$ donc : $(V_1 \cap V_2)^\perp \supseteq V_1^\perp + V_2^\perp$. Pour montrer l'égalité, nous allons comparer les dimensions :

$$\begin{aligned}
\dim(V_1 \cap V_2)^\perp &= \dim E - \dim(V_1 \cap V_2) \\
&= \dim E - (\dim V_1 + \dim V_2 - \dim(V_1 + V_2) \\
&= \dim E - \dim V_1 + \dim E - \dim V_2 - (\dim E - \dim(V_1 + V_2)) \\
&= \dim V_1^\perp + \dim V_2^\perp - \dim(V_1 + V_2)^\perp \\
&= \dim V_1^\perp + \dim V_2^\perp - \dim(V_1^\perp \cap V_2^\perp) \\
&= \dim(V_1^\perp + V_2^\perp) \ .
\end{aligned}$$

De même pour iii) et iv). *q.e.d.*

3 Transposée

Soient E, F deux $\mathbb{K}-$espaces-vectoriels. Soit $u : E \to F$ une application linéaire. Pour tout $\lambda \in F^*$, $\lambda \circ u \in E^*$. L'application : ${}^t u : F^* \to E^*$, $\lambda \mapsto \lambda \circ u$ est linéaire ; c'est la *transposée* de u.

Proposition 3.1 *Soient E, F deux $\mathbb{K}-$espaces-vectoriels de dimension finie. Alors :*
i) $\operatorname{rg} u = \operatorname{rg} {}^t u$, *ii)* $\operatorname{Im} ({}^t u) = (\ker u)^\perp$, *iii)* $\ker({}^t u) = (\operatorname{Im} u)^\perp$.

Démonstration : iii) : Soit $\lambda \in F^*$. Alors :

$$\lambda \in \ker {}^t u \Leftrightarrow {}^t u(\lambda) = 0$$

$$\Leftrightarrow \lambda \circ u = 0$$

$$\Leftrightarrow {}^\forall x \in E,\ \lambda(u(x)) = 0$$

$$\Leftrightarrow {}^\forall y \in \operatorname{Im} u, \lambda(y) = 0 \Leftrightarrow \lambda \in (\operatorname{Im} u)^\perp \ .$$

ii) : Soit $\lambda \in F^*$. Alors :

$${}^\forall x \in \ker u,\ {}^t u(\lambda)(x) = \lambda(u(x)) = \lambda(0) = 0 \ .$$

Donc $\operatorname{Im} ({}^t u) \subseteq (\ker u)^\perp$.

Réciproquement, si $\mu \in (\ker u)^\perp$, alors : ${}^\forall x \in \ker u$, $\mu(x) = 0$. Soit S un supplémentaire de $\operatorname{Im} u$ dans F : $\operatorname{Im} u \oplus S = F$. On pose :

$$\lambda(u(x) + s) := \mu(x)$$

pour tout $x \in E$ et tout $s \in S$. L'application $\lambda : F \to \mathbb{K}$ est bien définie car si $x, x' \in E$, $s, s' \in S$, alors :

$$u(x) + s = u(x') + s' \Rightarrow u(x) = u(x')$$

$$\Rightarrow x - x' \in \ker u$$

$$\Rightarrow \mu(x - x') = 0 \Rightarrow \mu(x) = \mu(x') \ .$$

De plus λ est linéaire *i.e.* $\lambda \in F^*$. On a donc $\mu = {}^t u(\lambda) \in \operatorname{Im} ({}^t u)$.

i) : $\operatorname{rg} ({}^t u) = \dim \operatorname{Im} {}^t u = \dim(\ker u)^\perp = \dim E - \dim \ker u = \operatorname{rg} u$, d'après le théorème du rang. *q.e.d.*

Proposition 3.2 *Soient E, F, G trois $\mathbb{K}-$espaces vectoriels. Soient : $u : E \to F$, $v : F \to G$ deux applications linéaires. Alors ${}^t(v \circ u) = {}^t u \circ {}^t v$.*

Proposition 3.3 *Soit E un $\mathbb{K}-$espace vectoriel. Soit $u : E \to E$ un endomorphisme. Un sous-espace vectoriel F de E est stable par u si et seulement si $F^\perp$ est stable par ${}^t u$.*

Démonstration : Supposons que F est stable par u, *i.e.* : $^\forall x \in F$, $u(x) \in F$. Si $\lambda \in F^\perp$, alors :

$$^\forall x \in F,\ \langle {}^t u(\lambda), x\rangle = \langle \lambda \circ u, x\rangle = \lambda(u(x)) = 0\ .$$

Donc ${}^t u(\lambda) \in F^\perp$ et $F^\perp$ est stable par ${}^t u$.

Réciproquement, supposons que $F^\perp$ est stable par ${}^t u$. Soit $\pi : E \to E/F$ la surjection canonique. Soit $\lambda \in (E/F)^*$.

Pour tout $x \in F$, $\langle \lambda, u(x) \bmod F\rangle = (\lambda \circ \pi)(u(x)) = ({}^t u(\lambda \circ \pi))(x)$.

Or, $\lambda \circ \pi \in F^\perp$ donc ${}^t u(\lambda \circ \pi) \in F^\perp$. Donc : $\langle \lambda, u(x) \bmod F\rangle = 0$. Cela est vrai pour tout $\lambda \in (E/F)^*$ donc $u(x) \bmod F = 0 \bmod F$ *i.e.* : $u(x) \in F$ pour tout $x \in F$. *q.e.d.*

Matrices

Proposition 3.4 *Soit E un $\mathbb{K}-$espace vectoriel de base $(e_1, ..., e_m)$ et F un $\mathbb{K}-$espace vectoriel de base $B' = (f_1, ..., f_n)$. Soit $u : E \to F$ linéaire. Notons A la matrice :*

$$A := [u]_{B,B'}$$

alors : $[{}^t u]_{B'^*,B^*} = {}^t A$.

4 Formes bilinéaires

$\mathrm{Bil}(U \times V, \mathbb{K}) \simeq \mathscr{L}(U, V^*) \simeq \mathscr{L}(V, U^*)$.

Exemple : si $A \in M_{m,n(\mathbb{K})}$, alors $M_{m,1}(\mathbb{K}) \times M_{n,1}(\mathbb{K}) \to \mathbb{K}$, $(X, Y) \mapsto {}^t XAY$ est une forme bilinéaire.

Changement de bases : soit $B \in \mathrm{Bil}(U, V)$, si e, e' bases de U, f, f' bases de V, si M est la matrice de B dans les bases e, f et M' dans les bases e', f', alors $M' = {}^t PMQ$ où $P := P_e^{e'}$ et $Q := P_f^{f'}$.

Définition 2 *Si $U = V$, on dit que B est symétrique si $^\forall x, y$, $B(x, y) = B(y, x)$, alternée si $^\forall x$, $B(x, x) = 0$.*

Remarque : en caractéristique $\neq 2$, alternée $\Leftrightarrow$ antisymétrique.

Exemple : le déterminant des matrices 2×2 est alterné en les colonnes.

Exercice 4 *Soit $B : E \times E \to \mathbb{K}$ une forme bilinéaire telle que pour tous $x, y \in E$, $B(x, y) = 0 \Leftrightarrow B(y, x) = 0$. Alors B est symétrique ou alternée.*

4.1 Noyau, rang, orthogonal

Supposons $U = V$, et $B \in \mathrm{Bil}(U, U)$ symétrique ou alternée.
Noyau : $\ker B = \{x \in U \ : \ ^\forall y \in U, B(x, y) = 0\}$.
Rang : $\mathrm{rang} B = \mathrm{rang}$ de $U \to U^*$, $x \mapsto B(x, .)$.
(C'est le rang de la matrice associée dans une base quelconque).
$\dim U = \mathrm{rang} B + \dim \ker B$.

Définition 3 *Si $U \to U^*$, $x \mapsto B(x, .)$ est un isomorphisme, on dit que B est non dégénérée. En dimension finie, cela veut dire* $\mathrm{rang} B = \dim U$ i.e. $\ker B = 0$.

4.2 Orthogonal

Soit $V \leq U$ un sous-espace, on note $V^\perp := \{x \in U : {}^\forall v \in V, \ B(x, v) = 0\}$.

Proposition 4.1 *Si U de dimension finie, alors pour tout sev $V \leq U$, on a :*

$$\dim V + \dim V^\perp = \dim U + \dim(V \cap \ker B)$$

$$V^{\perp\perp} = V + \ker B \ .$$

4.3 Classification des formes quadratiques

On suppose $\mathbb{K}$ de caractéristique $\neq 2$.

Une forme bilinéaire symétrique est entièrement déterminée par ses valeurs sur la diagonale car :

$$Q(x, y) = \frac{Q(x + y, x + y) - Q(x, x) - Q(y, y)}{2}$$

$$= \frac{Q(x + y, x + y) - Q(x - y, x - y)}{4} \ .$$

Définition 4 $q : \mathbb{K}^n \to \mathbb{K}$ *est une forme quadratique s'il existe une forme bilinéaire symétrique telle que $q(x) = B(x, x)$.*

Exemples : une forme quadratique sur $\mathbb{K}^n$ est un polynôme homogène de degré 2 en les coordonnées $=$; par ex. le déterminant sur $M_2(\mathbb{R})$ est une forme quadratique.

Attention, ne pas confondre le cône isotrope et le noyau d'une forme quadratique.

Soit B une forme bilinéaire symétrique.

Théorème 4.2 *Il existe une base $B-$orthogonale.*

Démonstration : Méthode de Gauss $Q(x_1,...,x_n) = \sum_i a_i x_i^2 + \sum_{1\le i<j\le n} a_{i,j}x_ix_j$.

1er cas : il existe un i tel que $a_i \neq 0$. Par ex. $i = 1$. Alors $Q = a_1x_1^2 + x_1\underbrace{B(x_2,...,x_n)}_{\text{linéaire}} + \underbrace{C(x_2,...,x_n)}_{quadratique} = a_1\left(x_1 + \frac{B(x_2,...,x_n)}{2a})^2\right) + \left(C - \frac{B^2}{(2a)^2}\right)$.

2ème cas : tous les a_i sont nuls et il existe $i < j$ tels que $a_{i,j} \neq 0$. Par ex. $a_{1,2} \neq 0$.

$$Q = a_{1,2}x_1x_2 + x_1\underbrace{B(x_3,...,x_n)}_{\text{linéaire}} + x_2\underbrace{C(x_3,...,x_n)}_{\text{linéaire}} + \underbrace{D(x_3,...,x_n)}_{quadratique}$$

$$= \frac{a_{1,2}}{4}\left(\left(x_1 + x_2 + \frac{B+C}{a}\right)^2 - \left(x_1 - x_2 + \frac{C-B}{a}\right)^2\right) + \left(D - \frac{BC}{a^2}\right) \ .$$

<u>*q.e.d.*</u>

Théorème 4.3 (Procédé de Gram-Schmidt) *Soit $(e_1,...,e_n)$ une base de U. Soit A la matrice de B dans cette base. On suppose que les mineurs principaux $d_1,...,d_n$ sont non nuls. Il existe une unique base orthogonale $f_1,...,f_n$ de U telle que :*

$$^\forall 1 \le k \le n,\ f_k = e_k \bmod \mathrm{Vect}\{e_1,...,e_{k-1}\}\,;$$

$$B(f_k,f_k) = d_k/d_{k-1} \ .$$

4.3.1 sur $\mathbb{C}$

Soit q une forme quadratique sur U. Soit $e_1,...,e_n$ une base orthogonale. Alors le nombre de $q(e_i) \neq 0$ est le rang de q et quitte à changer les $e_i \neq 0$ en $\frac{e_i}{\sqrt{q(e_i)}}$ et à permuter, on peut supposer que $q(a_1e_1 + ... + a_ne_n) = a_1^2 + ... + a_r^2$ où $r = \mathrm{rang}q$.

Exemple : $\mathrm{PGL}_2(\mathbb{C}) \simeq \mathrm{SO}_3(\mathbb{C})$.

Soit E le $\mathbb{C}-$espace vectoriel des matrices 2×2 de trace nulle muni de la forme quadratique :

$$q : E \to \mathbb{C},\ A \mapsto \mathrm{tr}(A^2) \ .$$

Si $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$, alors $q(A) = 2(a^2 + bc)$. Donc q est de rang 3. Dans la base $M_1 := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $M_2 := \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $M_3 := \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, on a :

$$q(x_1M_1 + x_2M_2 + x_3M_3) = x_1^2 + x_2^2 + x_3^2 \ .$$

L'action de $G := \mathrm{GL}_2(\mathbb{C})$ sur E par conjugaison préserve q d'où un morphisme de groupes $G \to O(q)$.

En prenant les matrices dans la base M_1, M_2, M_3, on obtient un morphisme de groupes : $\phi : G \to O_3(\mathbb{C})$. L'image est contenue dans $\mathrm{SO}_3(\mathbb{C})$ car, par exemple, tout $g \in G$ est de la forme $g = h^2$ pour un certain $h \in G$ (exo). Donc $\text{dét}\, \phi(g) = \text{dét}\, \phi(h)^2 = (\pm 1)^2 = 1$.

De plus, si $\phi(g) = I_3$, alors $^\forall i, ,\ gM_i = M_ig \Rightarrow g \in \mathbb{C}^\times I_3$. Donc $\ker \phi = \mathbb{C}^\times I_3$ et ϕ induit un morphisme injectif $\overline{\phi} : G \to So_3(\mathbb{C})$. Ce morphisme est un isomorphisme. Pour la surjectivité, on remarque que $\phi\left(\begin{pmatrix} e^{it} & 0 \\ 0 & e^{-it} \end{pmatrix}\right) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos t & -\sin t \\ 0 & \sin t & \cos t \end{pmatrix}$. Soit $M \in E$ telle que $q(M) = 1$. Alors il existe $g \in G$ tel que $gMg^{-1} = M_1$ (exo).

Soient $x_1, x_2, x_3 \in \mathbb{C}$ tels que $x_1^2 + x_2^2 + x_3^2 = 1$. Alors $r := -I_3 + 2^t(x_1, x_2, x_3).(x_1, x_2, x_3) \in \mathrm{SO}_3(\mathbb{C})$. De telles matrices engendrent $\mathrm{SO}_3(\mathbb{C})$ (exo). Il suffit donc de montrer que $r \in \mathrm{Im}\phi$. Or, si $g \in \mathrm{GL}_2(\mathbb{C})$, vérifie $g(x_1M_1 + x_2M_2 + x_3M_3)g^{-1} = M_1$, on a bien :

$$\phi(g)r\phi(g^{-1}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos t & -\sin t \\ 0 & \sin t & \cos t \end{pmatrix}$$

pour un certain t. Donc $\phi(g)r\phi(g^{-1}) \in \mathrm{Im}\phi \Rightarrow r \in \mathrm{Im}\phi$.

4.3.2 sur $\mathbb{R}$

On dit que q est positive si $^\forall x,\ q(x) \geq 0$; *définie positive* si $^\forall x \neq 0,\ q(x) > 0$.

Exemple : $q(f) = \int_I w(x)f(x)^2 dx$ où w est une fonction positive sur l'intervalle I.

Théorème 4.4 *Soit q une forme quadratique sur U un $\mathbb{R}-$ev de dimension n. Il existe une base $e_1, .., e_n$ de U telle que :*

$$q(a_1e_1 + ... + a_ne_n) = a_1^2 + ... + a_p^2 - a_{p+1}^2 - ... - a_{p+q}^2$$

(p, q) est la signature de q, est indépendant de la base choisie et $p+q = \mathrm{rang} q$.

Démonstration : $p = \max \dim V \ : \ V \leq U,\ q|_V \text{est définie positive}\}$ *q.e.d.*

Proposition 4.5 *Si q est positive, alors $^\forall x, y$, $|B(x,y)| \leq \sqrt{q(x)}\sqrt{q(y)}$. Avec égalité si q est définie positive si et seulement si x, y liés.*

Exercice 5 *Si q positive, alors le cône isotrope de q est son noyau.*

Théorème 4.6 (Méthode de Jacobi) *Si tous les mineurs principaux $d_1, ..., d_n$ d'une matrice symétriques sont non nuls, alors p est le nombre de changement de signes dans la liste.*

Corollaire 4.6.1 *q est définie positive si et seulement si tous les mineurs principaux sont > 0.*

On peut donc appliquer Gram-Schmidt à une forme bilinéaire symétrique définie positive comme par exemple : $B(f,g) = \int_I wfg$ où w est une fonction positive sur un intervalle I de $\mathbb{R}$. *Exemples :* les polynômes orthogonaux. Ce sont des familles de polynômes p_n, $n \geq 0$ qui vérifient :

$^\forall$, m, n, $\int_I wp_m p_n = c_n \delta_{m,n}$ pour certaines constantes c_n. On les obtient par le procédé d'orthogonalisation de Gram-Schmidt, en partant de la base $1, X, ..., X^k, ...$ de $\mathbb{R}[X]$.

$$w = (1 - X^2)^{-1/2}, I = [-1, 1], p_n = \text{Tchébychev I}, c_0 = \pi, c_n = \pi/2,\ n > 0$$

$$Hermite (-1)^n \frac{d^n}{dx^n}(e - x^2), I = \mathbb{R}\, w = e^{-x^2}, c_n = \sqrt{\pi} 2^n n!$$

$$Laguerre \frac{e^x}{n!}\frac{d^n}{dx^n}(x^n e^{-x}), I = \mathbb{R}_+, w = e^{-x}, c_n = 1$$

$$Legendre \frac{1}{2^n n!}\frac{d^n}{dx^n}(x^2 - 1)^n, I = [-1, 1], c_n = 2/(n + 1)$$

4.3.3 sur $\mathbb{F}_q$

Théorème 4.7 *Soit Q une forme quadratique non dégénérée sur U un $\mathbb{F}_q-$espace vectoriel de dimension n. Soit $\epsilon \in \mathbb{F}_q^\times \setminus (\mathbb{F}_q^\times)^2$. Il existe une base orthogonale $e_1, ..., e_n$ de U telle que :*

$$Q(x_1 e_1 + ... + x_n e_n) = x_1^2 + ... + x_{n-1}^2 + x_n$$

ou

$$Q(x_1 e_1 + ... + x_n e_n) = x_1^2 + ... + x_{n-1}^2 + \epsilon x_n$$

et $\epsilon = \text{dét}\, q \bmod (\mathbb{F}_q^\times)^2$.

Lemme 4.8 *Si $n \geq 2$, alors l'équation $Q(x) = 1$ a au moins une solution dans U.*

Démonstration : Il suffit de traiter le cas où $n = 2$ et où $Q(x) = a_1x_1^2 + a_2x_2^2$ avec $a_1, a_2 \neq 0$. On a $Q(x) = 1 \Leftrightarrow a_1x_1^2 = 1 - a_2x_2^2$. Quand x_1 décrit $\mathbb{F}_q$, le terme de gauche prend $\frac{q+1}{2}$ valeurs distinctes. Quand x_2 décrit $\mathbb{F}_q$, le terme de droite prend $\frac{q+1}{2}$ valeurs distinctes. Comme $\frac{q+1}{2} + \frac{q+1}{2} > q$, il existe x_1, x_2 tels que $a_1x_1^2 = 1 - a_2x_2^2$. *q.e.d.*

La classification des formes quadratiques dépend donc du corps $\mathbb{K}$. Curieusement, celle des formes alternées n'en dépend pas :

4.4 Classification des formes alternées

Soit B une forme bilinéaire alternée sur un $\mathbb{K}-$ev U de dimension n.

Définition 5 *Une base $e_1, ..., e_n$ de U est symplectique si pour un certain $m \leq n/2$, $B(e_{2k-1}, e_{2k}) = 1$ et $B(e_i, e_j) = 0$ si $i < j$ dans les autres cas. En d'autres termes la matrice de B dans la base e est de la forme :*

$$\begin{pmatrix} 0 & 1 & & & \\ -1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & 1 & \\ & & & -1 & 0 & \\ & & & & & \boxed{0} \end{pmatrix}$$

Théorème 4.9 *Toute forme bilinéaire alternée a une base symplectique.*

Démonstration : On raisonne par récurrence sur $\dim U$. Soit B une forme bilinéaire alternée. Si B non nulle, il existe $e_1, e_2 \in U$ tels que $B(e_1, e_2) \neq 0$. On peut multiplier e_1 par un scalaire non nul pour obtenir :

$$B(e_1, e_2) = -B(e_2, e_1) = 1 \ .$$

Alors comme $\ker B \cap \langle e_1, e_2 \rangle = 0$, on a $U = \langle e_1, e_2 \rangle \oplus \langle e_1, e_2 \rangle^{\perp}$. On applique l'hypothèse de récurrence à $\langle e_1, e_2 \rangle^{\perp}$. *q.e.d.*

Corollaire 4.9.1 *Toute forme bilnéaire alternée est de rang pair.*

4.4.1 Pfaffien

Définition 6 *Il existe une application Pf polynomiale en les coefficients telle que pour toute matrice antisymétrique A de taille $2n$, on ait :*

$$\text{dét}\, A = Pf(A)^2$$

et telle que $Pf(J) = 1$. C'est le Pfaffien.

Démonstration : Soit

$$A := \begin{pmatrix} 0 & t_{1,2} & t_{1,3} & \cdots \\ -t_{1,2} & 0 & t_{2,3} & \ddots \\ \vdots & \ddots & \ddots & \ddots \\ & & & 0 \end{pmatrix} \in \mathscr{M}_{2n}(\mathbb{K})$$

où $\mathbb{K} := \mathbb{Q}(t_{1,2}, t_{1,3}, ..., t_{2n-1,2n})$, le corps des fractions rationnelles en les variables $t_{i,j}$, $1 \leq i < j \leq 2n$.

Le déterminant de A est un polynôme en les $t_{i,j}$. Si on spécialise les variables $t_{i,j}$ en les entrées de la matrice J, on trouve la valeur $\text{dét}\, J = 1$. Donc $\text{dét}\, A$ est un polynôme non nul et la matrice A est de rang $2n$ (inversible dans $\mathscr{M}_{2n}(\mathbb{K})$). En particulier, il existe $P \in \text{GL}_{2n}(\mathbb{K})$ tel que :

$$^tPAP = J \ .$$

On pose $f := \text{dét}\, P^{-1}$. A priori $f \in \mathbb{K}$ mais :

Exercice 6 *Déduire du fait que $f^2 = \text{dét}\, A \in \mathbb{Q}[t_{i,j} : 1 \leq i < j \leq 2n]$, que f est une fraction rationnelle, mais nous allons montrer que f est un polynôme en les $t_{i,j}$ et un polynôme à coefficients entiers.*

On peut donc dans f spécialiser chaque variable $t_{i,j}$ en une valeur appartenant à $\mathbb{K}$. En particulier $f(J) \in \mathbb{K}$ et $f(J)^2 = \text{dét}\, J = 1$. Donc $f(J) = \pm 1$. On pose alors $Pf(A) := f(A)$ si $f(J) = 1$ et $Pf(A) := -f(A)$ si $f(J) = -1$.

On a bien : $Pf(A)^2 = \text{dét}\, A$ pour toute matrice $A \in \mathscr{M}_{2n}(\mathbb{K})$ antisymétrique et $Pf(J) = 1$.

q.e.d.

Propriétés :

— si $2n = 2$:

$$Pf \begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix} = a \ ;$$

— si $2n = 4$:

$$Pf\begin{pmatrix} 0 & t_{1,2} & t_{1,3} & t_{1,4} \\ -t_{1,2} & 0 & t_{2,3} & t_{2,4} \\ -t_{1,3} & -t_{2,3} & 0 & t_{3,4} \\ -t_{1,4} & -t_{2,4} & -t_{3,4} & 0 \end{pmatrix} = t_{1,2}t_{3,4} + t_{1,4}t_{2,3} - t_{1,3}t_{2,4} \ ;$$

— Pour toute matrice antisymétrique B, pour toute matrice C,

$$Pf({}^tCBC) = \text{dét}\, C Pf(B) \ ;$$

—

$$Pf({}^tA) = (-1)^n Pf(A) \ ;$$

— le polynôme Pf est homogène de degré n est de degré 1 en chaque variable $t_{i,j}$.

—

$$Pf\begin{pmatrix} 0 & \lambda_1 & & & \\ -\lambda_1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & \lambda_n \\ & & & -\lambda_n & 0 \end{pmatrix} = \lambda_1 ... \lambda_n \ .$$

Exercice 7 $Pf(A) = \sum_{(i_1 i_2|...|i_{2n-1}i_{2n})} \text{sign}(i_1, ..., i_{2n}) a_{i_1 i_2} ... a_{i_{2n-1}i_{2n}}$ *(somme sur les partitions de* $\{1, .., 2n\}$ *en union disjointe de* n *paires (sans tenir compte de l'ordre des paires ni de l'ordre à l'intérieur des paires))*

5 Formes hermitiennes

Soit E un $\mathbb{C}-$ev.

Une *forme hermitienne* est une application $\varphi : E \to \mathbb{R}$ telle qu'il existe $\Phi : E \times E \to \mathbb{C}$ *sesquilinéaire à symétrie hermitienne* (*i.e.* : $^\forall x \in E$, $\Phi(x, \cdot)$ est linéaire et $^\forall x, y \in E$, $\overline{\Phi(x,y)} = \Phi(y,x)$).

Exercice 8 *Sur* $\mathbb{C}^n$ *une forme hermitienne est une combinaison* $\mathbb{R}-$*linéaire des* $x_i\overline{x_i}$ *et des* $i(x_i\overline{x_j} - \overline{x_i}x_j)$, $x_i\overline{x_j} + \overline{x_i}x_j$.

Exercice 9 *On a* $\text{Re}(\Phi)$ *qui est bilinéaire et* $\text{Im}(\Phi)$ *qui est alternée. De plus* Φ *est unique :*

$$\Phi(x,y) = \frac{1}{4}(\varphi(x+y) - \varphi(x-y) + i\varphi(x-iy) - i\varphi(x+iy)) \ .$$

5.1 Matrices, changement de bases

Si $v_1, ..., v_n$ est une base de E, on appelle matrice de φ dans la base $v_1, ..., v_n$ la matrice $A := (\Phi(v_i, v_j))_{1 \le i,j \le n}$.

La matrice A est *hermitienne i.e.* ${}^t\overline{A} = A$.

Réciproquement si A est hermitienne, alors $x \mapsto {}^t\overline{x}Ax$ est une forme hermitienne sur $\mathcal{M}_{n,1}(\mathbb{C})$.

Si $v_1', ..., v_n'$ est une autre base de E et $P := P_v^{v'}$, alors la matrice de φ dans la base v' est ${}^t\overline{P}AP$.

5.2 Réduction

Soit h une forme hermitienne sur un $\mathbb{C}-$espace vectoriel E. On dit que h est *positive* si $\forall x \in E$, $h(x) \ge 0$, *définie positive* si $\forall x \in E \setminus \{0\}$, $h(x) > 0$.

Théorème 5.1 *Il existe une base $e_1, ...e_n$ de E telle que $h(\sum_i x_i e_i) = |x_1|^2 + ... + |x_p|^2 - |x_{p+1}|^2 - ... - |x_{p+q}|^2$ où (p, q) est la signature de h, $p + q$ son rang.*

Exercice 10 *Réduire : $h(x, y, z) = x\overline{x} + y\overline{y} - 2i(\overline{x}y) + 2ix\overline{y} + 2y\overline{z} + 2\overline{y}z$.*

Exercice 11 *Vérifier que p, q ne dépendent que de h, que $p+q$ est le rang de de la matrice de h dans une base quelconque indication : p est la dimension maximale d'un sous-espace où la restriction de h est définie positive.*

Voici un critère pour reconnaître une matrice hermitienne définie positive :

Théorème 5.2 *Soit A une matrice hermitienne. Alors A est définie positive si et seulement si tous ses mineurs principaux sont > 0.*

Exercice 12 *Démontrer le sens difficile. Indication : on fait le changement de variables $x_1' := \frac{a_{11}x_1 + ... + a_{n1}x_n}{a_{11}}$, $x_i' := x_i$ si $i > 1$. On a alors $h(x) = a_{11}x_1'\overline{x_1'} + \sum_{i,j>1} b_{ij}x_i\overline{x_j}$ où $b_{ij} = \overline{b_{ji}} = a_{ij} - \frac{a_{i1}a_{1j}}{a_{11}}$ et*

$$\text{dét } A_k = \begin{vmatrix} a_{11} & a_{12} & ... & a_{1k} \\ a_{21} & a_{22} & ... & a_{2k} \\ \vdots & & & \vdots \\ a_{k1} & a_{k2} & ... & a_{kk} \end{vmatrix} = \begin{vmatrix} a_{11} & 0 & ... & 0 \\ a_{21} & b_{22} & ... & b_{2k} \\ \vdots & & & \vdots \\ a_{k1} & b_{k2} & ... & b_{kk} \end{vmatrix} \dots$$

Exercice 13 *Le théorème ci-dessus est une généralisation du théorème de Cauchy-Schwarz. Justifier cette affirmation.*

Exercice 14 *Montrer que si h est une forme hermitienne positive, alors h est une semi-norme.*

5.3 Espaces hermitiens

Définition 7 *Un espace de dimension finie avec une forme hermitienne définie positive est un espace hermitien.*

Exemple : $\mathbb{C}^n$ *et* $h(x) := |x_1|^2 + ... + |x_n|^2$.

Remarque : on peut utiliser le procédé de Gram-Schmidt pour construire des bases orthonormées.

Exercice 15 *Montrer que la famille* $e^{2i\pi nx}$, $n \in \mathbb{Z}$, *forme une famille orthonormale pour le produit scalaire* $\langle f, g\rangle = \int_0^1 \overline{f}g$.

Exercice 16 (Inégalité de Bessel) *Soit* E *un espace hermitien. Soit* $u_1, ..., u_n$ *une famille orthonormale de* E. *Montrer que* $\sum_i |\langle x, u_i\rangle|^2 \leq ||x||^2$. *Indication : trouver des scalaires* $t_1, ..., t_n$ *tels que* $x - \sum_i t_i u_i$ *est orthogonal à tous les* u_i ...

Exercice 17 (Égalité de Parseval) *Si* u_i, $1 \leq i \leq n$, *est une base orthonormale de* E, *alors pour tous* $x, y \in E$, $\langle x, y\rangle = \sum_i \langle x, u_i\rangle\langle u_i, y\rangle$.

Exercice 18 (Matrices de Gram) *Si* $x_1, ..., x_n \in E$, *on pose* $G(x_1, ..., x_n) =$ dét $(\langle x_i, x_j\rangle)$. *Montrer que* $G(x_1, ...x_n) \geq 0$ *avec égalité si et seulement si, le système* $x_1, ..., x_n$ *est lié. Soit* $\{x_, ..., x_n\}$ *une base d'un sous-espace* F *de* E. *Montrer que* $d(x, F)^2 = \frac{G(x, x_1, ..., x_n)}{G(x_1, ..., x_n)}$. *En déduire par exemple* $\min_{a_1, ..., a_n \in \mathbb{R}} \int_0^1 (1 + a_1 x + ... + a_n x^n)^2 dx$. *Montrer que si* $a_1, ..., a_n \in \mathbb{R}^n$, *alors* $G(a_1, ..., a_n) = \mathrm{vol}(P(a_1, ..., a_n))^2$ *où* $P(a_1, ..., a_n)$ *est le parallélépipède* $\{\sum_{i=1}^n t_i a_i : {}^\forall 1 \leq i \leq n,\ 0 \leq t_i \leq 1\}$.

5.4 Angles

Soit E un espace euclidien avec un produit scalaire $\langle \cdot, \cdot \rangle$. Si $x, y \in E$ sont des vecteurs non nuls, il existe un unique $0 \leq a \leq \pi$ tel que $\cos a = \frac{\langle x, y\rangle}{||x||||y||}$. C'est l'angle entre x et y.

Exercice 19 *Déterminer l'angle entre les faces d'un tétraèdre régulier (* i.e. *l'angle entre les vecteurs orthogonaux aux faces.*

5.5 Matrices unitaires

Soit E un espace hermitien avec une norme hermitienne $|| \cdot ||$. L'ensemble des endomorphismes de E qui préservent la norme est un sous-groupe de $\mathrm{GL}(E)$: le groupe unitaire de E. Ce groupe est isomorphe à $U_n(\mathbb{C}) := \{A \in M_n(\mathbb{C}) : {}^t\overline{A}A = I_n\}$ le groupe des matrices unitaires $n \times n$.

Exercice 20 *Justifier cet isomorphisme. Montrer qu'une matrice unitaire à pour déterminant un complexe de module* 1.

5.6 Diagonalisation des matrices hermitiennes

Lemme 5.3 *Les valeurs propres d'une matrice hermitienne sont réelles.*

Exercice 21 *Démontrer ce lemme et démontrer aussi que les valeurs propres d'une matrice unitaire sont des nombres complexes de module* 1.

Exercice 22 *Montrer que les espaces propres d'une matrice hermitienne associés à deux valeurs propres distinctes sont orthogonaux.*

Exercice 23 *Soit* $c \in \mathbb{R}$. *Soit* A *une matrice hermitienne. Soit* $E_c := \ker A - cI_n$. *Montrer que* $E_c^\perp$ *est un sous-espace* $A-$*stable et en déduire que* $\dim E_c =$ *la multiplicité de* c *comme racine du polynôme caractéristique de* A.

Théorème 5.4 *Soit* A *une matrice hermitienne. Il existe* $P \in U_n(\mathbb{C})$ *telle que* $A = PD{}^t\overline{P}$ *pour une matrice diagonale* D.

Corollaire 5.4.1 *Soient* A, B *deux matrices hermitiennes dont l'une,* A*, est définie positive. Il existe une matrice* Q *inversible telle que :*

$$^t\overline{Q}AQ = I_n \text{ et } {}^t\overline{Q}BQ = D$$

une matrice diagonale dont les coefficients diagonaux sont les racines du polynôme $\text{dét}\,(XA - B)$.

Exercice 24 *Trouver* Q *et* D *pour les matrices*

$$A := \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & -1 \\ 3 & -1 & 9 \end{pmatrix} \text{ et } B := \begin{pmatrix} 0 & 1 & -1 \\ 1 & 2 & -1 \\ -1 & -1 & 1 \end{pmatrix} .$$

Exercice 25 *Pour une matrice hermitienne* $A = (a_{i,j})_{1 \leq i,j \leq n}$, *on note ses valeurs propres* $\lambda_1(A) \geq ... \geq \lambda_n(A)$. *Montrer que pour tous* $1 \leq k \leq n$, $\sum_{i=1}^k a_{i,i} \leq \lambda_1(A) + ... + \lambda_k(A)$.

Soient A, B *deux matrices hermitiennes, montrer que* $\lambda_1(A+B) \leq \lambda_1(A) + \lambda_1(B)$ *(indication :* $\lambda_1(A) = \sup_{X \in \mathbb{C}^n \,:\, ||X||=1} {}^t\overline{X}AX$*).*

b) *Montrer que*

$$\lambda_{i+j-1}(A+B) \leq \lambda_i(A) + \lambda_j(B)$$

pour tous $i, j \geq 1$ *tels que* $i+j-1 \leq n$ *et que*

$$\lambda_1(A+B) + ... + \lambda_k(A+B) \leq \lambda_1(A) + ... + \lambda_k(A) + \lambda_1(B) + ... + \lambda_k(B)$$

pour tous $1 \leq k \leq n$.

Théorème 5.5 *Soit A une matrice hermitienne positive. Il existe une unique matrice hermitienne positive B telle que $B^2 = A$. De plus, B est un polynôme (réel) en A.*

Démonstration : existence : soient $\lambda_1, ..., \lambda_r$ les valeurs propres distinctes de A . Il existe un polynôme réel f tel que $f(\lambda_i) = \sqrt{\lambda_i}$. On a $f(A)^2 = A$.

q.e.d.

Exercice 26 *Démontrer l'unicité.*

Exercice 27 (décomposition polaire) *Soit $A \in \mathrm{GL}_n(\mathbb{C})$. montrer qu'il existe un unique couple (U, P) où U est unitaire et P hermitienne définie positive tel que $A = UP$. (si A n'est pas inversible on a seulement l'existence !).*

Exercice 28 *Soit A hermitienne définie positive. Montrer que $A = {}^t\overline{P}P$ pour une certaine matrice triangulaire supérieure P.*

Exercice 29 *Soit $A \in \mathrm{GL}_n(\mathbb{C})$. Montrer qu'il existe U unitaire et P triangulaire supérieure telle que $A = UP$. En déduire l'inégalité d'Hadamard :*

$$|\text{dét}\, A|^2 \leq \prod_i {}^t\overline{C_i}C_i$$

où les C_i sont les colonnes de A.

Exercice 30 *Montrer qu'une matrice antisymétrique réelle ne peut avoir pour valeur propre -1. Montrer que si S est antisymétrique réelle, alors $(I-S)(I+S)^{-1}$ est spécial orthogonal. En déduire que $\mathrm{SO}_n(\mathbb{R})$ est connexe.*

5.7 Endomorphismes normaux

Soit E un espace hermitien avec un produit scalaire hermitien $\langle \cdot, \cdot \rangle$. Soit u un endomorphisme de E.

Définition 8 *L'adjoint de u est l'endomorphisme u^* tel que :*

$$^\forall x, y, \ \langle u(x), y \rangle = \langle x, u^*(y) \rangle \ .$$

Exercice 31 *Justifier cette définition et montrer que u^* n'existe pas toujours en dimension infinie.*

Remarques : $u^{**} = u$ et si A est la matrice de u dans une base orthonormée, u^* a pour matrice ${}^t\overline{A}$ dans la même base.

Théorème 5.6 *Soit $u \in \mathcal{L}(E)$. Montrer que sont équivalentes :*

(i) *u est normal (*i.e. $uu^* = u^*u$*) ;*

(ii) *u se diagonalise dans une base orthonormée ;*

(iii) *u et u^* se diagonalisent dans une base orthonormée commune.*

Exercice 32 *Montrer que si u est hermitien (respectivement antihermitien (respectivement unitaire)), alors les valeurs propres de u sont réelles (respectivement imaginaires pures (respectivement de module 1)).*

Exercice 33 *Soit u un endomorphisme normal.*

Montrer que $||u(x)|| = ||u^*(x)||$ pour tout $x \in E$.

b) Montrer que si E_c est un sous-espace propre de u, alors $E_c^\perp$ est stable par u.

c) Démontrer le théorème.