Leçon 170 : Formes quadratiques sur un e.v. de dim $<\infty$. Orthogonalité, isotropie, applications. Trinome B : DALMOLIN, MASSON, MORIANI

Soit $\mathbb{K}$ un corps de caractéristique $\neq 2$. Soit E un $\mathbb{K}$-ev de dimension $n<\infty$. On suppose connues les définitions de formes bilinéaires symétriques et alternées sur E, et on note leurs ensembles respectifs $\mathcal{B}$, $\mathcal{B}_S$ et $\mathcal{B}_A$.

I. Définitions

1) Formes quadratiques

Définition 1 : $q : E \to \mathbb{K}$ est une forme quadratique sur E si il existe $b \in \mathcal{B}$ telle que $q(x) = b(x,x)$ $\forall x \in E$. On note $\mathcal{Q}(E)$ l'ensemble des ~~formes~~ formes quadratiques sur E. (E,q) est appelé espace quadratique.

Remarque 2 : Il est équivalent de dire que q est une fonction polynôme homogène de degré 2 en les coefficients de x dans une base et que cette propriété ne dépend pas du choix de la base.

Exemple 3 : $E=\mathbb{R}^n$, $q=\|\cdot\|^2$ la norme euclidienne au carré est une forme quadratique. $q(x)=\sum x_i^2$ où $(x_i)_i$ coordonnées de x dans la base canonique

Proposition 4 : $\mathcal{B} = \mathcal{B}_A \oplus \mathcal{B}_S$

Proposition 5 : (Formule de polarisation) $\begin{array}{l}\mathcal{B} \longrightarrow \mathcal{Q}\\ b \longmapsto q_b\end{array}$ où $q_b(x)=b(x,x)$ $\forall x\in E$. est un morphisme surjectif d'espaces vectoriels, de noyau $\mathcal{B}_A$. De plus, $\begin{array}{l}\mathcal{Q} \longrightarrow \mathcal{B}_S\\ q \longmapsto b_q\end{array}$ (où $b_q(x,y) = \frac{q(x+y)-q(x)-q(y)}{2}$) est un isomorph

Corollaire 6 : $\dim_{\mathbb{K}} \mathcal{Q}(E) = \dim_{\mathbb{K}} \mathcal{B}_S = \frac{n(n+1)}{2}$.

Définition 7 : Soit $q\in\mathcal{Q}(E)$. Le noyau de q est défini par : $\operatorname{Ker} q := \{x\in E \mid b_q(x,y)=0 \ \forall y \in E\}$. q est dite non-dégénérée si $\operatorname{Ker} q = \{0\}$. Un sous-espace A de E est dit régulier si $q|_A$ est non dégénérée. Le rang de q est défini par $\operatorname{rg} q := \dim(E) - \dim(\operatorname{Ker} q)$. Le cône isotrope de q est défini par $\mathcal{C}_q := \{x\in E \mid q(x)=0\}$.

Remarque 8 : Attention, en général $\mathcal{C}_q \neq \operatorname{Ker} q$. Mais on a toujours $\operatorname{Ker} q \subset \mathcal{C}_q$

Définition 9 : Soient (F,q) et (G,q') deux espaces quadratiques. On dit que $u \in \mathcal{L}(F,G)$ est un morphisme d'espaces quadratiques si le diagramme suivant est commutatif :

$$\begin{array}{ccc} F & \xrightarrow{u} & G \\ & q\searrow \ \ \swarrow q' & \\ & \mathbb{K} & \end{array}$$

On appelle isométries les morphismes injectifs. On appelle isomorphismes les morphismes bijectifs, et q et q' sont équivalentes (noté $q \simeq q'$) si il existe un isomorphisme $u\in\mathcal{L}(F,G)$.

2) Matrices

Proposition 10 : $\begin{array}{l}\mathcal{B} \xrightarrow{\varphi} \mathcal{L}(E,E^*)\\ b \longmapsto \varphi_b\end{array}$ (où $\varphi_b(x) = b(\cdot,x)$ $\forall x\in E$) est un isomorphisme d'espaces vectoriels. En choisissant une base de E on va pouvoir écrire tout élément de $\mathcal{B}$ avec une matrice.

Définition 11 : Soit $b\in\mathcal{B}$, $\underline{e}$ une base de E. On définit : $\operatorname{Mat}_{\underline{e}}(b) := \operatorname{Mat}_{\underline{e},\underline{e}^*}(\ )$. On a alors : si $x,y\in E$, $X,Y\in\mathbb{K}^n$ leurs vecteurs coordonnées respectifs dans $\underline{e}$, si $A=\operatorname{Mat}_{\underline{e}}(b)$, alors $b(x,y) = \varphi_b(y)(x) = \langle AY, X\rangle_{\mathbb{K}^n} = {}^tXAY$ et donc $A_{ij} = b(e_i,e_j)$ pour tout $1\leq i\leq n$, $1\leq j \leq n$. D'où $A\in\mathcal{S}_n(\mathbb{K})$ si $b\in\mathcal{B}_S$.

Proposition 12 : Soit $b\in\mathcal{B}$, $\underline{e}$ et $\underline{e}'$ deux bases de E ; A, A' les matrices de b dans $\underline{e}$ et $\underline{e}'$. Soit P la matrice de passage de $\underline{e}$ à $\underline{e}'$. ~~Soit~~ Alors $A' = {}^tPAP$

Définition/Proposition 13 : (Action de congruence) Soient $P\in GL_n(\mathbb{K})$, $A\in\mathcal{S}_n(\mathbb{K})$, alors $P\cdot A = PA{}^tP \in \mathcal{S}_n(\mathbb{K})$ et définit une action à gauche

Remarque 14 : Si $q\simeq q'$ alors elles ont même classe de congruence de matrices symétriques associées. (où E,E' ont forcément même dimension)

Exemple 15 : $E=\mathbb{R}^n$, $q=\|\cdot\|^2$, $\operatorname{Mat}_{\underline{e}}(q) = I_n$ où $\underline{e}$ base canonique.

Exemple 16 : Si $E = \mathcal{M}_2(\mathbb{K})$, $q(A) = \operatorname{tr}(A^2)$ alors la matrice de q dans la base $\left(\begin{pmatrix}1&0\\0&0\end{pmatrix};\begin{pmatrix}0&1\\0&0\end{pmatrix};\begin{pmatrix}0&0\\1&0\end{pmatrix};\begin{pmatrix}0&0\\0&1\end{pmatrix}\right)$ est $\begin{pmatrix}1&0&0&0\\0&0&\frac12&0\\0&\frac12&0&0\\0&0&0&1\end{pmatrix}$

3) Premiers résultats

Proposition 17 : (Théorème de Riesz généralisé) Soit $q\in\mathcal{Q}(E)$. q est non dégénérée ssi φ_b est un isomorphisme de $E\to E^*$ (voir 10). Dans ce cas, $\forall f\in E^*$, $\exists!\, a\in E$ $f(x) = b(x,a)$ $\forall x\in E$.

Exemple 18 : $q : \mathcal{M}_n(\mathbb{K}) \to \mathbb{K}$, $A \mapsto tr(A^2)$ est non-dégénérée donc $\forall f \in \mathcal{M}_n(\mathbb{K})^*$, $\exists ! A \in \mathcal{M}_n(\mathbb{K})$ tq $f(X) = tr(AX)$ $\forall X \in \mathcal{M}_n(\mathbb{K})$

Proposition 19 : (Théorème de Pythagore généralisé) Soit $q \in \mathcal{Q}(E)$ alors $b_q(x,y) = 0$ ssi $q(x+y) = q(x) + q(y)$

II - Orthogonalité, isotropie

1) Généralités

Définition 20 : Soit $A \subseteq E$, $b \in \mathcal{B}_s$. On définit $A^{\perp b}$ l'orthogonal de A pour b par $A^{\perp b} = \{x \in E \mid b(x,y) = 0 \ \forall y \in A\}$ que l'on notera $A^\perp$ si il n'y a pas d'ambiguïté.

Remarque 21 : Si b est non dégénérée, on peut traduire en b-orthogonalité les propriétés de l'orthogonalité duale car φ_b iso. et $A^{\perp b} = \varphi^{-1}(A^0)$.

Proposition 22 : Soient $A, B \subseteq E$.
- (i) $A^\perp$ est un sev de E contenant $\operatorname{Ker} q$.
- (ii) $A^\perp = \operatorname{Vect}(A)^\perp$
- (iii) Si $A \subset B$ alors $B^\perp \subset A^\perp$
- (iv) Si A sev de E alors $A \cap A^\perp = \operatorname{Ker} q_A$
- (v) Si A et B sev de E alors $(A+B)^\perp = A^\perp \cap B^\perp$
- (vi) $A \subset (A^\perp)^\perp$
- (vii) Si q non-dégénérée, alors $A \subset B$ ssi $B^\perp \subset A^\perp$

Proposition 23 : Si q non-dégé, A sev de E alors $\dim E = \dim A + \dim A^\perp$

Remarque 24 : C'est faux si q dégénérée, penser au cas $A = E$.

Exemple 25 : Si $q : \mathcal{M}_n(\mathbb{K}) \to \mathbb{K}$, $A \mapsto tr(A^2)$ alors $\mathcal{S}_n(\mathbb{K})^\perp = \mathcal{A}_n(\mathbb{K})$

Remarque 26 : Attention ; même si q non-dégé. on n'a pas en général $E = A \oplus A^\perp$. Par exemple toute droite $D \subset \mathcal{C}_q$ est aussi incluse dans $D^\perp$.

Proposition 27 : Soient A, B sev de E. q non-dégénérée, alors $A = B^\perp$ ssi $B = A^\perp$ ssi $A \perp B$ et $\dim A + \dim B = E$

2) Orthogonalisation

Notation : On note $\langle a_1, \dots, a_n \rangle$ la forme quad. sur $\mathbb{K}^n$ dont la matrice dans la base canonique est $\begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$

Théorème 28 : Il existe une base de E orthogonale pour q c'est-à-dire dans laquelle $\operatorname{Mat}(q)$ est diagonale.

Proposition 29 : Soient $a_1, \dots, a_n \in \mathbb{K}$, $\lambda_1, \dots, \lambda_n \in \mathbb{K}^*$. Alors
$$\langle (\lambda_1^2) a_1, \dots, (\lambda_n)^2 a_n \rangle \simeq \langle a_1, \dots, a_n \rangle$$

Algorithme 30 : (de Gauss) : On fixe une base $\underline{e}$ de E. Soit $x \in E$, X ses coordonnées dans $\underline{e}$. On a $q(x) = {}^tX A X$ donc
$$q(x) = \sum_{i=1}^n a_{ii} x_i^2 + 2 \sum_{1 \le i < j \le n} a_{ij} x_i x_j$$

On souhaite se ramener à une somme de carrés :
- Si $a_{11} \neq 0$, $q(x) = a_{11}\left(x_1 + \frac{1}{a_{11}} \sum_{i=2}^n a_{1i} x_i\right)^2 - \frac{1}{a_{11}}\left(\sum_{i=2}^n a_{1i} x_i\right)^2 + \sum_{2 \le i \le j \le n} a_{ij} x_i x_j$
- Si $a_{ii} = 0 \ \forall i$, $a_{12} \neq 0$:
$$\frac{1}{2} q(x) = a_{12}\left(x_1 + \sum_{i=3}^n \frac{a_{2i}}{a_{12}} x_i\right)\left(x_2 + \sum_{i=3}^n \frac{a_{1i}}{a_{12}} x_i\right) - \left(\sum_{i=3}^n \frac{a_{2i}}{a_{12}} x_i\right)\left(\sum_{i=3}^n \frac{a_{1i}}{a_{12}} x_i\right) + \sum_{3 \le i \le j \le n} a_{ij} x_i x_j$$

et on utilise l'astuce $xy = \frac{1}{4}((x+y)^2 - (x-y)^2)$

On obtient alors $q(x) = \sum_{i=1}^n \lambda_i \, l_i(x_1, \dots, x_n)^2$ où (l_i) formes linéaires indépendantes sur $\mathbb{K}^n$.

donc $q \simeq \langle \lambda_1, \dots, \lambda_n \rangle$

3) Groupe orthogonal

Définition/proposition 31 : $O(q) = \{u \in \mathcal{L}(E) \mid$ isomorphisme isométrie pour $q\}$ est un groupe, appelé groupe orthogonal.

Proposition 32 : Deux formes quadratiques équivalentes ont même groupe orthogonal

Définition 33 : $O_n(\mathbb{K}) = \{A \in \mathcal{M}_n(\mathbb{K}) \mid {}^tA A = I_n\}$

Proposition 34 : Pour tout $u \in O(q)$, $\det u = \pm 1$

Proposition 35 : Pour $n \geq 3$, $Z(O(q)) = \{-Id, Id\}$ et $O(q)$ est engendré par les réflexions.

Proposition/déf 36 : $SO(q) = \{u \in O(q) \mid \det u = 1\}$; $O(q) \simeq SO(q) \rtimes \mathbb{Z}/2\mathbb{Z}$

4) Isotropie

Définition 37 : $x \in E$ est dit isotrope si $q(x) = 0$ (si $x \in \mathcal{C}_q$)

Définition 38 : Si E est de dimension 2, on appelle (E,q) plan quadratique. C'est un plan hyperbolique si $q \simeq \langle 1,-1 \rangle$.

Proposition 39 : Les plans quadratiques réguliers (ie non-dégé.) et isotropes sont les plans hyperboliques (donc sont tous equivalents).

Définition 40 : Un sous-espace F de E est dit totalement isotrope si $F \subset \mathcal{C}_q$. On notera F SETI.

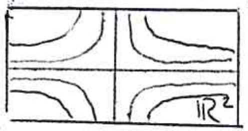
Proposition 41 : Soit F SETI. Alors $\dim F \in [\frac{\dim E}{2}]$

Définition 42 : Soit F SETI, si F est maximal pour l'inclusion alors on l'appelle SETI maximal ou SETIM. On note l'indice de q : $\nu(q) = \max\{\dim F \mid F \text{ SETI}\}$.

Proposition 43 : Tous les SETIM ont même dimension : $\nu(q)$.

Définition 44 : Soit $k \in \mathbb{K}$. On définit la nappe : $\mathcal{N}_k^q = \{x \mid q(x) = k\}$

Exemple 45 : $E = \mathbb{R}^2$ $q\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = x^2 - y^2$



En vert : $\mathcal{C}_q = \langle e_1 \rangle \cup \langle e_2 \rangle$

en rouge et bleu : les nappes $\mathcal{N}_1$ et $\mathcal{N}_2$.

Théorème 46 : (Springer) Soit $q \in \mathcal{Q}(\mathbb{K}^n)$, $\mathbb{L}$ une extension de degré impair de $\mathbb{K}$. Alors on a : si il existe $x \in \mathbb{L}^n \setminus \{0\}$ isotrope alors il existe $x' \in \mathbb{K}^n \setminus \{0\}$ isotrope. **DEV1**

III. Classification :

Remarque 47 : On a vu que dans tout corps $\mathbb{K}$, q est équivalente à $\langle a_1, \dots, a_n \rangle$ où $a_i \in \mathbb{K}^*/(\mathbb{K}^*)^2 \cup \{0\}$ $\forall i$.

Théorème 48 : Sur $\mathbb{C}$, q et q' sont équivalentes si et seulement si elles ont même rang ($\mathbb{C}^*/(\mathbb{C}^*)^2 = \{1\}$).

Exemple 49 : $\langle 1,-1 \rangle \simeq \langle 1,1 \rangle$ sur $\mathbb{C}$

Corollaire 50 : Toute forme quad. sur $\mathbb{C}$ non-dégé. admet une base orthonormée.

Définition 51 : Soit q quelconque, $\in \mathcal{Q}(E)$, $\underline{e}$ une base de E. On définit $\Delta(q)$ comme la classe de $\det(\mathrm{Mat}_{\underline{e}}(q))$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$ ou 0 si q est dégénérée.

Proposition 52 : Soit (E,q) un plan quadratique non-dégé. sur $\mathbb{F}_{p^n}$. Alors $q \simeq \langle 1, \varepsilon \rangle$ où $\varepsilon = \Delta(q)$ dans $\mathbb{K}^*/\mathbb{K}^{*2}$

Théorème 53 : Soit (E,q) espace quadratique non-dégé. sur $\mathbb{F}_{p^n}$, alors $q \simeq \langle 1, \dots, 1, \varepsilon \rangle$ où $\varepsilon \equiv \Delta(q)$. Donc deux formes quad. régulières sur $\mathbb{F}_{p^n}$ sont équivalentes ssi elles ont même Δ.

Exemple 54 : Sur $\mathbb{F}_p$, $\langle 1,-1 \rangle \simeq \langle 1,1 \rangle$ ssi -1 est un carré de $\mathbb{F}_p$.

Définition 55 : Soit $a \in \mathbb{Z}$, $p \in \mathbb{N}$ premier $\neq 2$. $\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{si } \bar{a} \text{ carré de } \mathbb{F}_p \\ 0 & \text{si } a \in p\mathbb{Z} \\ -1 & \text{si } \bar{a} \text{ non carré de } \mathbb{F}_p \end{cases}$

Proposition 56 : $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.

Théorème 57 : (Loi de réciprocité quadratique) Soient p, q premiers $\neq 2$ distincts. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$

DEV2

IV. Cas réel

Ici soit E un $\mathbb{R}$-ev, $q \in \mathcal{Q}(E)$.

Définition 60 : $i_+ := \max\{\dim F \mid F \text{ sev de } E \text{ et } q_F > 0\}$

$i_- := \max\{\dim F \mid F \text{ sev de } E \text{ et } q_F < 0\}$

La signature de q est $(i_+, i_-) \in \mathbb{N}^2$

Définition 58 : q est dite définie si $(q(x) = 0 \Rightarrow x = 0)$ $\forall x \in E$. q est dite positive (resp négative) si $q \geq 0$ (resp $q \leq 0$)

On note $q > 0$ pour définie positive, $q < 0$ pour définie négative.

Théorème 61 : (Sylvester) Soit (r,s) la signature de q. Alors $q \simeq \langle 1, \dots, 1, -1, \dots, -1, 0, \dots, 0 \rangle$ où il y a r "1", s "-1", et $n-(r+s)$ "0".

Ainsi deux formes quad. réelles sont équivalentes ssi même signature.

Exemple 62 : $\langle 1,-1 \rangle \not\simeq \langle 1,1 \rangle$ sur $\mathbb{R}$ car de signatures $(1,1)$ et $(2,0)$

Exemple 63 : $q : A \mapsto \mathrm{tr}(A^2)$ sur $\mathcal{M}_n(\mathbb{R})$ de signature $\left(\frac{n(n+1)}{2}; \frac{n(n-1)}{2}\right)$

$q : A \mapsto \mathrm{tr}({}^tAA)$ définie positive donc $(n^2, 0)$

Proposition 59 : q définie $\Rightarrow$ q définie positive ou définie négative

Proposition 64 (Critère de Sylvester). $q \simeq \langle \Delta_1, \frac{\Delta_2}{\Delta_1}, \dots, \frac{\Delta_n}{\Delta_{n-1}} \rangle$

Remarque 64: Les formes quadratiques définies positives sont les carrés des normes euclidiennes et leurs formes polaires sont les produits scalaires ~~eucli~~ réels.

Définition 65: Si $r, s \in \mathbb{N}^*$, $O(r,s) = \{P \in GL_n(\mathbb{R}) \mid P I_{r,s} {}^tP = I_{r,s}\}$

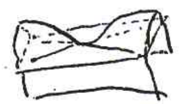
Proposition 66: $O(r,s) \underset{homéo}{\simeq} O(r) \times O(s) \times \mathbb{R}^{rs}$ $\boxed{\text{DEV 3}}$

Théorème 67: (Lemme de Morse): Soit U ouvert de $\mathbb{R}^n$, $a \in U$; soit $f : U \to \mathbb{R}$ de classe $\mathcal{C}^k$ pour $k \geq 3$.
On suppose $f(a) = 0$, $df(a) = 0$ et $d^2f(a)$ non-dégénérée.
Alors il existe un voisinage ouvert U_1 de a dans $\mathbb{R}^n$, un vois. ouvert V_1 de 0 dans $\mathbb{R}^n$ et un $\mathcal{C}^{k-2}$-difféo $v : U_1 \to V_1$ tel que $v(a) = 0$, $dv(a) = Id_{\mathbb{R}^n}$ et $\forall x \in U_1$, $f(x) = \frac{1}{2} d^2f(a)[v(x), v(x)]$

Exemple 68: $f : \begin{array}{l} \mathbb{R}^2 \to \mathbb{R} \\ \binom{x}{y} \mapsto f(x,y) \end{array}$ comme dans $\boxed{67}$,

alors on peut connaître la position de S, la surface de $\mathbb{R}^3$ définie par $z = f(x,y)$ par rapport à son plan tangent en fonction de la signature (p,q) de $d^2f(a)$:

(2,0)  Intersection: 
Cone isotrope $\{0\}$

(1,1)  Intersection: 
Cône Iso : deux droites

(0,2)  Intersection: 
Cône iso : $\{0\}$

Références :
- Invitation aux formes quad. Seguin-Pazzis
- NH^2G^2 Caldero, Germoni CVA Caldero, Peronnet
- Cours d'algèbre Daniel Perrin

Soit $\mathbb{K}$ un corps, $\mathbb{L}$ une extension de $\mathbb{K}$ de degré m impair.
Soit q une forme quadratique sur $\mathbb{K}^n$, $n \in \mathbb{N}^*$, et $q_{\mathbb{L}}$ son prolongement à $\mathbb{L}^n$, $Q \in \mathbb{K}[X]$ le polynôme homogène de degré 2 associé. Si $q_{\mathbb{L}}$ possède un vecteur isotrope non nul dans $\mathbb{L}^n$ alors q possède un vecteur isotrope non-nul dans $\mathbb{K}^n$.

Démonstration :

- Par récurrence sur m, $\mathbb{L} = \mathbb{K}[\alpha_1][\alpha_2] \cdots [\alpha_k]$. Par multiplicativité du degré toutes les extensions intermédiaires sont de degré impair. On peut donc supposer $\mathbb{L} = \mathbb{K}[\alpha]$, $[\mathbb{L} : \mathbb{K}] = m$ impair
- On note $x \in \mathbb{L}^n$ tel que $q_{\mathbb{L}}(x) = 0$, $x \neq 0_{\mathbb{L}^n}$.
- On note μ le polynôme minimal de α sur $\mathbb{K}$.

μ est irréductible de degré m et $\mathbb{K}[\alpha] \simeq \mathbb{K}[X]/(\mu)$

On peut donc écrire $x = (P_i(\alpha))_{i=1}^n$ où $P_i \in \mathbb{K}[X]$, et quitte à faire la division euclidienne des P_i par μ on peut supposer $\deg P_i \leq m-1$ $\forall i \in [\![1,n]\!]$

les P_i sont non tous nuls car $(P_i(\alpha))_i = x \neq 0$

$Q(P_1, \ldots, P_n) \in \mathbb{K}[X]$. $Q(P_1, \ldots, P_n)(\alpha) = Q(x) = 0$ donc $\mu \mid Q(P_1, \ldots, P_n)$

On note $A \in \mathbb{K}[X]$ le polynôme tel que $Q(P_1, \ldots, P_n) = \mu A$

Soit $D := \operatorname{pgcd}(P_i)$. Montrons que $D^2 \mid A$:

- Comme $D \mid P_i$ $\forall i \in [\![1,n]\!]$, et Q homogène de degré 2, $D^2 \mid Q(P_1, \ldots, P_n)$ et $\frac{Q(P_1, \ldots, P_n)}{D^2} = Q\left(\frac{P_1}{D}, \ldots, \frac{P_n}{D}\right)$ donc $D^2 \mid \mu A$.

- Montrons que μ et D^2 sont premiers entre eux : μ irréd. donc reste à mq $\mu \nmid D$. Si $\mu \mid D$, $x = (P_1(\alpha), \ldots, P_n(\alpha)) = 0$ absurde donc $\mu \nmid D$

Par le lemme de Gauss on conclut que $D^2 \mid A$ et donc $Q\left(\frac{P_1}{D}, \ldots, \frac{P_n}{D}\right) = \mu \frac{A}{D^2}$. On pose $P_i^\circ = \frac{P_i}{D}$, $A^\circ = \frac{A}{D^2}$.

Se présentent alors deux cas : (i) A° est nul
(ii) A° est non-nul

(i) $Q(P_1^\circ, \ldots, P_n^\circ) = 0$.
Soit $\beta \in \mathbb{K}$. Il existe $j \in [\![1,n]\!]$ tel que $P_j^\circ(\beta) \neq 0$ car les P_i° sont globalement premiers entre eux.
(et sinon $(X-\beta) \mid P_i^\circ$ $\forall i$, absurde).
En posant $x_0 := (P_1^\circ(\beta), \ldots, P_n^\circ(\beta))$ on obtient $Q(x_0) = 0$
et on a bien $x_0 \neq 0_{\mathbb{K}^n}$.

(ii) $Q(P_1^\circ, \ldots, P_n^\circ) = \mu A^\circ$. Le membre de gauche est de degré pair et μ de degré impair. Donc A° est nécessairement de degré impair, et ce n'est pas une constante, il possède donc des diviseurs irréductibles. Un de ces diviseurs irréductibles est nécessairement de degré impair, on le note B°.

– On démontre maintenant le théorème par récurrence sur $m = \dim_{\mathbb{K}} \mathbb{L}$

Initialisation : $m = 1$, $\mathbb{K} = \mathbb{L}$ il n'y a rien à dire (à part m impair ...)

Hérédité : Supposons le théorème vrai pour tout entier impair $< m$. Comme $\deg P_i < m$ $\forall i$, on a :

$\deg B^\circ \leq \deg A^\circ \leq \deg A = \deg Q(P_1, \dots, P_n) - \deg \mu < 2m - m = m$

Comme B° irréductible sur $\mathbb{K}$, $\mathbb{L}^\circ := \mathbb{K}[X]/(B^\circ)$ est un corps

$\mathbb{L}^\circ = \mathbb{K}[\beta_0]$ où $\beta_0 = \overline{X}$ dans $\mathbb{K}[X]/(B^\circ)$

$[\mathbb{L}^\circ : \mathbb{K}] = \deg B^\circ < m$ et impair.

Trouvons un zéro non trivial de Q dans $\mathbb{L}^{\circ n}$:

Comme $B^\circ(X)$ s'annule sur $\mathbb{L}^\circ$ on a $B^\circ(\beta_0) = B^\circ(\overline{X}) = \overline{B^\circ(X)} = 0$

et comme B° irréductible, c'est le polynôme minimal de β_0 sur $\mathbb{K}$.

En particulier, $A^\circ(\beta_0) = 0$ car $B^\circ \mid A^\circ$.

D'où $Q(P_1^\circ(\beta_0), \dots, P_n^\circ(\beta_0)) = \mu(\beta_0) A^\circ(\beta_0) = 0$

et $x_0 := (P_1^\circ(\beta_0), \dots, P_n^\circ(\beta_0)) \in \mathbb{L}^{\circ n}$.

Si par l'absurde $x_0 = 0$, alors β_0 est une racine commune à tous les $P_i^\circ \in \mathbb{K}[X]$. Ainsi $B^\circ \mid P_i^\circ$ $\forall i$ ce qui est absurde car les P_i° sont globalement premiers entre eux.

On applique l'hypothèse de récurrence à $\mathbb{L}^\circ$ qui nous fournit un $x_1 \in \mathbb{K}^n$ non nul tel que $Q(x_1) = 0$.

$\square$

On veut montrer :

$\mathcal{O}(p,q) \simeq \mathcal{O}(p) \times \mathcal{O}(q) \times \mathbb{R}^{pq}$

avec $p+q=n$

Préliminaire : $\mathcal{O}(p,q) = \{ M \in GL_n(\mathbb{R}) \mid M I_{pq} {}^tM = I_{pq} \}$

C'est un groupe car c'est le stabilisateur de I_{pq} par l'action de congruence.

Soit $M \in \mathcal{O}(p,q) \subset GL_n(\mathbb{R})$, on admet donc sa décomposition polaire $M = OS$ avec $O \in \mathcal{O}(n)$ et $S \in \mathcal{S}_n^{++}(\mathbb{R})$

on pose $T = {}^tMM = {}^tS\,{}^tO\,O\,S = S^2$

* $\mathcal{O}(p,q)$ stable par transposition :

$M I_{pq} {}^tM = I_{pq} \Leftrightarrow {}^tM^{-1} I_{pq} M^{-1} = I_{pq}$

donc ${}^tM^{-1} \in \mathcal{O}(p,q)$ et ${}^tM \in \mathcal{O}(p,q)$ car c'est un groupe. Ainsi $T = {}^tMM \in \mathcal{O}(p,q)$

l'exponentiel réalise un homéo entre $\mathcal{S}_n$ et $\mathcal{S}_n^{++}$ et $T \in \mathcal{S}_n^{++}$ car $T = S^2$ donc $\exists U \in \mathcal{S}_n$ tel que $T = \exp(U)$

$T \in \mathcal{O}(p,q)$ donc $T I_{pq} {}^tT = I_{pq}$

$\Leftrightarrow {}^tT = I_{pq}^{-1} T^{-1} I_{pq}$

$\Leftrightarrow \exp({}^tU) = I_{pq}^{-1} \exp(-U) I_{pq}$

$\Leftrightarrow \exp({}^tU) = \exp(-I_{pq}^{-1} U I_{pq})$

$\Leftrightarrow {}^tU = -I_{pq} U I_{pq}$ par injectivité

$\Leftrightarrow I_{pq} U + U I_{pq} = 0 \quad (*)$

en divisant par 2 et en remontant les équivalence on obtient :

${}^t\exp\left(\frac{U}{2}\right) I_{pq} \exp\left(\frac{U}{2}\right) = I_{pq}$

donc $\exp\left(\frac{U}{2}\right) \in \mathcal{O}(p,q)$ or $\exp\left(\frac{U}{2}\right) \in \mathcal{S}_n^{++}$ et $\exp\left(\frac{U}{2}\right)^2 = T = S^2$

donc $\exp\left(\frac{U}{2}\right) = S$ par unicité de la racine carré sur $\mathcal{S}_n^{++}$

donc $S \in \mathcal{O}(p,q)$

et $O = MS^{-1} \in \mathcal{O}(p,q)$ aussi.

Comme la décomposition polaire est un homéomorphisme on a :

$\mathcal{O}(p,q) \overset{\text{homéo}}{\simeq} (\mathcal{O}(p,q) \cap \mathcal{O}(n)) \times (\mathcal{O}(p,q) \cap \mathcal{S}_n^{++})$

* Soit $P \in \mathcal{O}(p,q) \cap \mathcal{O}(n)$, $P = \begin{array}{cc} \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right) & \begin{array}{c} p \\ q \end{array} \\ \begin{array}{cc} p & q \end{array} & \end{array}$

$P I_{pq} {}^tP = I_{pq}$ donc $\begin{cases} A{}^tA - B{}^tB = I_p \\ C{}^tC - D{}^tD = -I_q \end{cases}$

et

${}^tPP = I_n$ donc $\begin{cases} A{}^tA + B{}^tB = I_p \\ C{}^tC + D{}^tD = I_q \end{cases}$

ainsi $\begin{cases} B{}^tB = 0 \\ C{}^tC = 0 \end{cases} \Rightarrow \begin{cases} \mathrm{tr}(B{}^tB) = 0 \\ \mathrm{tr}(C{}^tC) = 0 \end{cases} \Rightarrow \begin{cases} B = 0 \\ C = 0 \end{cases}$

et $A \in \mathcal{O}(p)$, $D \in \mathcal{O}(q)$

finalement $(\mathcal{O}(p,q) \cap \mathcal{O}(n)) = \mathcal{O}(p) \times \mathcal{O}(q)$

* Soit $L = \{ U \in \mathcal{M}_n(\mathbb{R})$ qui respecte $(*) \}$

exp réalise un homéo entre $\mathcal{S}_n$ et $\mathcal{S}_n^{++}$

donc d'après $(*)$: $\mathcal{S}_n \cap L \overset{h}{\simeq} \mathcal{S}_n^{++} \cap \mathcal{O}(p,q)$

Soit $U \in \mathcal{S}_n \cap L$, $U = \begin{pmatrix} A & B \\ {}^tB & D \end{pmatrix}$ car $U \in \mathcal{S}_n$

et $U \in L$ donc $A = D = 0$

ainsi $L \cap \mathcal{S}_n = \left\{ \begin{pmatrix} 0 & B \\ {}^tB & 0 \end{pmatrix}, B \in \mathcal{M}_{pq}(\mathbb{R}) \right\} \simeq \mathbb{R}^{pq}$

on obtien bien : $\mathcal{O}(p,q) \overset{h}{\simeq} \mathcal{O}(p) \times \mathcal{O}(q) \times \mathbb{R}^{pq}$

Développement : Théorème Spectral - Version Calcul Différentiel

Leçons : 155 ; 158 ; 160 ; 170 ; 171 ; *203 ? ; 215 ? ; 208 ? ; 159 ?*

Référence : CVA - Page 107

ENONCÉ

Soit q une forme quadratique, de forme polaire φ sur un espace euclidien E de dimension n, muni du produit scalaire $< .,. >$.
Alors il existe une base orthonormée pour le produit scalaire, et orthogonale pour q.
C'est à dire, une base de E telle que $< e_i, e_j >= \delta_{i,j}$ et $\varphi(e_i, e_j) = 0$ si $i \neq j$.

Démonstration :

Montrons que q admet un maximum sur la sphére-unité

Soit $S = \{x \in E, < x, x >= 1\}$ la sphère-unité de E.

Si l'on fixe une base de E, on voit que la fonction $x \mapsto q(x)$ est une fonction polynomiale (homogène de degré 2) en les coefficients de x. Elle est donc continue (pour la topologie naturelle).

La sphère-unité étant compact, q possède un maximum sur S, noté λ, atteint en un certain $u \in S$.

Notons $q_\lambda(x) = \lambda. < x, x > -q(x)$

Montrons que q_λ est une forme quadratique positive

Comme q_λ est une combinaison linéaire de formes quadratiques, c'est une forme quadratique.
Sa forme polaire associée est $\varphi_\lambda(x, y) = \lambda < x, y > -\varphi(x, y)$
Elle est positive sur S par construction.
Soit $x \in E$ non nul. On peut écrire $x = \sqrt{< x, x >}.x_1$ avec $x_1 \in S$.
On en déduit que :

$$q_\lambda(x) = q_\lambda(\sqrt{< x, x >}.x_1) = \lambda. < x, x > . < x_1, x_1 > - < x, x > .q(x_1) =< x, x > .q_\lambda(x_1) \geqslant 0$$

Elle est donc bien positive sur E.

Calculons sa différentielle en $a \in E$

Comme q est une forme quadratique, c'est une fonction polynomiale, et est donc C^1.
Calculons la différentielle de q en $a \in E$. Soit $h \in$E.

$$q(a + h) = q(a) + 2.\varphi(h, a) + q(h)$$

On remarque que $2.\varphi(h, a)$ est linéaire en h.
On peut écrire que $h = ||h||.h_1$ avec $||h||| = \sqrt{< h, h >}$ et $h_1 \in S$. On obtient alors que :

$$\lim_{h\to 0} \frac{q(h)}{||h||} = \lim_{h\to 0} ||h||^2.\frac{q(h_1)}{||h||} = \lim_{h\to 0} ||h||.q(h_1) = 0$$

car q est majorée sur S. La différentielle de q en a est donnée par :

$$D_a(q)(h) = 2.\varphi(h,a)$$

De même, la différentielle du produit scalaire est :

$$D_a(<.,.>)(h) = 2. < h,a >$$

On en déduit donc que :

$$\begin{aligned} D_a(q_\lambda)(h) &= 2\lambda. < h,a > -2.\varphi(h,a) \\ &= 2.q(u). < h,a > -2.\varphi(h,a) \end{aligned}$$

Montrons que $(\mathbb{R}u)^\perp \subseteq (\mathbb{R}u)^{\perp_q}$

Comme q est positive sur E et que $q_\lambda(u) = 0$ par construction, on obtient que q_λ atteint son minimum en u. La différentielle de q_λ est s'annule donc en u, et donc :

$$2.\varphi(h,a) = 2.q(u). < h,a >$$

On en déduit donc que si $h \in (\mathbb{R}u)^\perp$, alors $< h,a >= 0$ et donc $\varphi(h,a) = 0$, et donc $h \in (\mathbb{R}u)^{\perp_q}$.

D'où l'inclusion anoncée.

Montrons enfin le résultat énoncé, par récurrence

Montrons par récurrence sur la dimension de E, notée n, qu'il existe une base orthonormée pour $< .,. >$ et orthogonale pour q.

C'est clair pour $n = 1$.

Supposons le résultat vrai pour $n - 1$.

Soit $e_n = u$ tel que construit précédemment, et H l'hyperplan $(\mathbb{R}u)^\perp$.

Par hypothèse de récurrence, il existe une base $(e_1, ..., e_{n-1})$ de H qui soit orthonormée pour $< .,. >|_H$ et orthogonale pour $q|_H$.

On remarque de plus que par construction, $||u|| = 1$.

On obtient donc que la base $(e_1, ..., e_n)$ est orthonormée pour $< .,. >$ et orthogonale pour q.

Ce qui est le résultat souhaité.