170

Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.

I Formes quadratiques et algèbre bilinéaire

A Lien entre formes bilinéaires et formes quadratiques Rom 15.1

Soit E un $\mathbb{K}$ ev de dimension finie n.

Définition 1 : Une forme bilinéaire sur E est une application $\varphi : E\times E \to \mathbb{K}$, $(x,y) \mapsto \varphi(x,y)$ telle que $\forall x,y \in E$, $z \mapsto \varphi(x,z)$ et $z \mapsto \varphi(z,y)$ sont linéaires. Elle est dite symétrique si $\varphi(y,x) = \varphi(x,y)$ et antisymétrique si $\varphi(y,x) = -\varphi(x,y)$.

Exemple 2 : Pour tout couple (l_1, l_2) de formes linéaires sur E, l'application $(x,y) \mapsto l_1(x) l_2(y)$ est une forme bilinéaire sur E.

Définition 3 : On note $\mathcal{L}_2(E)$, $S_2(E)$ et $A_2(E)$ les ev respectifs.

Définition 4 : On appelle forme quadratique sur E une application $q : E \to \mathbb{K}$ définie par : $\forall x \in E$, $q(x) = \varphi(x,x)$ où φ est une forme bilinéaire sur E. On note $Q(E)$ leur espace vectoriel.

Remarque 5 : Il n'y a pas unicité de la forme bilinéaire associée

Exemple 6 : Les formes bilinéaires $\varphi(x,y) = x_1y_1 + x_2y_2$ et $\psi(x,y) = x_1y_1 + x_1y_2 - x_2y_1 + x_2y_2$ définissent la même forme quadratique.

Théorème 7 : Si q est une forme quadratique sur E, il existe alors une unique forme bilinéaire symétrique φ telle que $q(x) = \varphi(x,x)$ $\forall x \in E$.

Corollaire 8 : $Q(E) \simeq S_2(E)$.

Définition 9 : dans le théorème 7 on dit que φ est la forme polaire de la forme quadratique q.

Proposition 10 : Soit $q \in Q(E)$ et φ sa forme polaire, alors on a $\forall x,y \in E$
$\varphi(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y)) = \frac{1}{4}(q(x+y) - q(x-y))$ et
$\forall (\lambda, x) \in \mathbb{K}\times E$, $q(\lambda x) = \lambda^2 q(x)$.

Corollaire 11 : Deux formes bilinéaires symétriques φ_1 et φ_2 sur E sont égales si et seulement si $\varphi_1(x,x) = \varphi_2(x,x)$ pour tout $x \in E$.

B Matrice associée à une forme quadratique Rom 15.1

Définition 12 : La matrice d'une forme bilinéaire φ dans la base B de E est la matrice carrée d'ordre n, $A = ((\varphi(e_i, e_j)))_{1\leq i,j\leq n}$.

Théorème 13 : Soient φ une forme bilinéaire sur E et A sa matrice dans la base B. Pour tous $x,y \in E$, on a $\varphi(x,y) = {}^tX A Y$.

Théorème 14 : Une application $\varphi : E\times E \to \mathbb{K}$ est une forme bilinéaire sur E si et seulement si il existe une matrice $A = ((a_{ij}))_{1\leq i,j\leq n}$ dans $\mathcal{M}_n(\mathbb{K})$ et des formes linéaires $l_1, \dots, l_n$ linéairement indépendantes telles que :
$\forall (x,y) \in E\times E$, $\varphi(x,y) = \sum_{1\leq i,j\leq n} a_{ij}\, l_i(x)\, l_j(y)$

Théorème 15 : Si $\varphi \in \mathcal{L}_2(E)$, φ est symétrique (resp antisymétrique) si et seulement si sa matrice dans une base quelconque B de E est symétrique (resp antisymétrique).

Corollaire 16 : $Q(E) \simeq S_2(E) \simeq S_n(\mathbb{K})$ donc $\dim(Q(E)) = \dim(S_2(E)) = \dim(S_n(E)) = \frac{n(n+1)}{2}$

Proposition 17 : Soient B_1 et B_2 deux bases de E et P la matrice de passage de B_1 à B_2. Si $A_1 = \mathrm{Mat}_{B_1}\varphi$, $A_2 = \mathrm{Mat}_{B_2}\varphi$, $\varphi \in \mathcal{L}_2(E)$ alors $A_2 = {}^tP A_1 P$.

Définition 18 : Le discriminant dans une base B de E de $\varphi \in \mathcal{L}_2(E)$ est $\Delta_B(\varphi) = \det(\mathrm{Mat}_B(\varphi))$.

Proposition 19 : Soient B_1 et B_2 deux bases de E et P la matrice de passage de B_1 à B_2. On a alors pour toute forme bilinéaire φ sur E, $\Delta_{B_2}(\varphi) = (\det(P))^2 \Delta_{B_1}(\varphi)$.

Définition 20 : Soit $q \in Q(E)$ de forme polaire φ et B base de E. Alors on a $\mathrm{Mat}_B(\varphi) = \mathrm{Mat}_B(q)$ et $\Delta_B(q) = \Delta_B(\varphi)$.

Proposition 21 : Soit $q \in Q(E)$ de forme polaire φ, B base de E et $A = \mathrm{Mat}_B(q)$. Alors $\forall x \in E$, $q(x) = {}^tX A X = \sum_{i=1}^{n} a_{ii} x_i^2 + 2\sum_{1\leq i<j\leq n} a_{ij} x_i x_j$ et $\forall (x,y) \in E^2$, $\varphi(x,y) = \langle AX, Y\rangle$.

II Outils pour étudier les formes quadratiques.

A Orthogonalité et isotropie Rom 15.2

Soit $q \in Q(E)$ de forme polaire φ.

Définition 22 : Deux vecteurs $x,y \in E$ sont dits orthogonaux relativement à φ si $\varphi(x,y) = 0$. Pour toute partie non vide X de E, l'orthogonal de X relativement à φ est $X^\perp = \{y \in E, \forall x \in X, \varphi(x,y) = 0\}$.

Exemple 23 : $\{0\}^\perp = E$ et $E^\perp = \{0\}$ pour le produit scalaire usuel sur $E = \mathbb{R}^2$.

Théorème 24 : Soit $X \subset Y \subset E$, alors $X^\perp$ est un sous espace de E et $X \subset (X^\perp)^\perp$ et $Y^\perp \subset X^\perp$.

Remarque 25 : En général $E^\perp \neq \{0\}$.

Exemple 26 : Pour la forme bilinéaire $\varphi(x,y) = x_1y_1 - x_2y_2$ on a $(\mathbb{R}^2)^\perp = \{(x_1,-x_1),\ x_1 \in \mathbb{R}\} \neq \{(0,0)\}$.

Définition 27 : On dit que $x \in E$ est isotrope relativement à φ s'il est orthogonal à lui-même, i.e $q(x)=0$. L'ensemble des vecteurs isotropes de E, relativement à φ, est le cône isotrope de φ.

Remarque 28 : Le cône isotrope de φ est donc le sous-ensemble de E :

$$C_\varphi = q^{-1}\{0\} = \{x \in E,\ q(x) = \varphi(x,x) = 0\}.$$

On dit aussi que C_φ est le cône isotrope de la forme quadratique q.

B Noyau et rang   Rom 15.2

Définition 29 : Le noyau de φ est l'orthogonal de E : $\ker\varphi = E^\perp$.

Lemme 30 : Le noyau de φ est inclus dans son cône isotrope.

Théorème 31 : Soit B base de E, $A = \mathrm{Mat}_B(\varphi)$ et $u \in \mathrm{End}(A)$ tel que $\mathrm{Mat}_B(u) = A$. Alors on a $\ker\varphi = \ker u$.

Définition 32 : On dit que $\varphi \in S_2(E)$ est non dégénérée si $\ker\varphi = \{0\}$.

Remarque 33 : φ est non dégénérée ssi pour toute base B de E, $\Delta_B(\varphi) \neq 0$.

Définition 34 : On dit que $q \in Q(E)$ est définie si $\forall x \in E\setminus\{0\}$ $q(x) \neq 0$.

Remarque 35 : q est définie si $C_\varphi = \{0\}$.

Proposition 36 : q est non dégénérée si et seulement si $\ker\varphi \subset C_\varphi$.

Définition 37 : Le rang de q est l'entier $rg(q) = n - \dim(\ker(q))$.

Remarque 38 : Le rang d'une forme quadratique est égal à celui de sa matrice dans une base quelconque.

Proposition 39 : q est non dégénérée $\Leftrightarrow rg(q) = n$.

Théorème 40 : Pour tout sev F de E, on a $\dim F + \dim F^\perp \geq \dim E$ avec égalité si et seulement si q est non dégénérée.
L'égalité $E = F \oplus F^\perp$ est réalisée si $q_{|F}$ est non dégénérée.

Théorème 41 : Si q non dégénérée et $C_\varphi \neq \{0\}$ alors il existe une base de E formée de vecteurs isotropes.

Per 6.2

C Groupe orthogonal associé à une forme quadratique   Gri 9.11 9.12

Proposition 42 : Soit $q \in Q(E)$ non dégénérée et $f \in \mathrm{End}(E)$. Alors $\exists!\, f^* \in \mathrm{End}(E)$ tel que : $\forall (x,y) \in E$, $\varphi(f(x),y) = \varphi(x, f^*(y))$.

Proposition 43 : Soit $q \in Q(E)$ non dégénérée et $f \in \mathrm{End}(E)$. On a équivalence entre :
i) $\forall x \in E$, $q(f(x)) = q(x)$;
ii) $\varphi(f(x), f(y)) = \varphi(x,y)$ $\forall x,y \in E$;
iii) $f^* \circ f = id$, en particulier f est bijectif.

Définition 44 : Le groupe orthogonal de q (non dégénérée) est $O(q) = \{f \in \mathrm{End}(E),\ f^*\circ f = id\}$ et le groupe spécial orthogonal est le groupe $O^+(q) = \{f \in O(q),\ \det f = 1\}$.

$\boxed{\text{Développement}}$ Le groupe $O(q)$ (q définie positive) est engendré par les réflexions orthogonales. Plus précisément, si $u \in O(q)$, u est produit d'au plus n réflexions.

Lemme 45 : Soit $n \geq 3$ et soient τ_1, τ_2 des réflexions. Il existe des renversements σ_1, σ_2 tels que $\tau_1\tau_2 = \sigma_1\sigma_2$.

Théorème 46 : Pour $n \geq 3$, $O^+(q)$ est engendré par les renversements. Précisément pour tout $u \in O^+(q)$, u est produit d'au plus n renversements.

III Réduction et classification des formes quadratiques.

A Réduction et méthode de Gauss   Gri 9.5 7.3

Définition 47 : Une base $\{e_i\}$ de E est dite orthogonale pour φ si $\varphi(e_i,e_j) = 0$ $\forall i \neq j$. Elle est dite orthonormée si $\varphi(e_i,e_j) = \delta_{ij}$.

Proposition 48 : $\{e_i\}$ est une base orthogonale ssi $M_B(q) = \begin{pmatrix} \varphi(e_1,e_1) & & 0 \\ & \ddots & \\ 0 & & \varphi(e_n,e_n) \end{pmatrix}$.
Dans ce cas $rg(q)$ est le nombre des $\varphi(e_i,e_i) \neq 0$.

Théorème 49 : Soit $q \in Q(E)$, $E \neq \{0\}$, alors il existe B une base orthogonale de E telle que si $x = \sum_{i=1}^n x_ie_i$, alors $q(x) = \sum_{i=1}^r a_ix_i^2$ où $a_i \in K$ et $r = rg\, q$.

Proposition 50 : Soit $q(x) = \sum a_{ij}x_ix_j$ (Méthode Gauss réduct° en carrés)
i) On ordonne selon la variable x_1
ii) On écrit les termes contenant x_1 comme le début d'un carré
iii) On obtient le carré d'une forme linéaire plus les termes qui ne contiennent pas x_1.
iv) On recommence l'opération sur les termes qui ne contiennent pas x_1.

Exemple 51 :

$$\varphi(x,x) = x_1^2 + 2x_2^2 + 5x_3^2 + 2x_1x_2 - 4x_2x_3 = (x_1+x_2)^2 + (x_2-2x_3)^2 + x_3^2$$

Proposition 52 : (Méthode de Gauss avec termes rectangles).
i) On choisit un terme rectangle à coefficient non nul $k x_ix_j$, $k \neq 0$
ii) On calcule les dérivées partielles q'_{x_i}, q'_{x_j} et on écrit $q(x) = \frac{1}{k} q'_{x_i} \cdot q'_{x_j}$ + termes complémentaires
iii) On écrit $\varphi_1\varphi_2 = \frac{1}{4}[(\varphi_1+\varphi_2)^2 - (\varphi_1-\varphi_2)^2]$
iv) On recommence selon la nature des termes restants

Exemple 53 : $q(x) = 5x_1x_2 + 6x_1x_3 + 3x_2x_3$
$= \frac{1}{20}(5x_1+5x_2+9x_3)^2 - \frac{1}{20}(5x_1+5x_2-3x_3)^2 - \frac{18}{5}x_3^2$.

B Classification et signature Rom 15.3

Théorème 54 : Si $A \in S_n(\mathbb{R})$ est de rang r, il existe $P \in GL_n(\mathbb{R})$ telle que ${}^tPAP$ soit diagonale de la forme $D = \begin{pmatrix} I_s & & \\ & -I_t & \\ & & 0_{n-r} \end{pmatrix}$ où $t+s = r$.

Théorème 55 : Il existe un unique couple (s,t) d'entiers naturels tel que pour toute base (e_i) de E orthogonale relativement à q, le nombre de vecteurs e_i tels que $q(e_i) > 0$ est égal à s et le nombre de vecteurs e_i tq $q(e_i) < 0$ est égal à t. De plus on a $s+t = rg(q)$.

Définition 56 : Le couple (s,t) d'entiers naturels défini par le théorème précédent est appelé signature de q et on le note $sgn(q)$.

Corollaire 57 : Une forme quadratique non nulle q est positive (resp définie positive) ssi sa signature est $(s,0)$ (resp $(n,0)$) où $s \in [\![1,n]\!]$.

Exemple 58 : pour q de l'exemple 53 on a $sgn(q) = (1,2)$.

Rom 15.6 13.6 13.7

IV Formes quadratiques sur un corps fini et loi de réciprocité quadratique.

On considère p nombre premier impair et $q = p^m$, $\mathbb{K} = \mathbb{F}_q$, $f \in Q(E)$ et φ sa forme polaire.

Lemme 59. il y a $\frac{q+1}{2}$ carrés dans $\mathbb{F}_q$.

Lemme 60 ; Pour $a,b,c \in \mathbb{F}_q$ $a,b \neq 0$, l'équation $ax^2+by^2 = c$ aux inconnues $x,y \in \mathbb{F}_q$ a au moins une solution.

Théorème 61 : Si $\alpha \in \mathbb{F}_q^*$ est un non carré fixé et φ une forme quadratique sur E de rang n compris entre 1 et m, il existe une base de E dans laquelle
$Mat_\beta(\varphi) = \begin{pmatrix} I_{n-1} & & \\ & s & \\ & & 0_{m-n} \end{pmatrix}$ avec $s \in \{1,\alpha\}$.

Corollaire 62 : Deux formes quadratiques non dégénérées φ et φ' sur E sont équivalentes ssi pour toute base B de E, $\frac{\Delta_B(\varphi')}{\Delta_B(\varphi)}$ est un carré dans $\mathbb{F}_q^*$.

Définition 63 : Pour tout $a \in \mathbb{F}_p^*$ le symbole de Legendre est l'entier :
$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 & \text{sinon.} \end{cases}$

Exemple 64 : $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Proposition 65 : i) Pour tout $a \in \mathbb{F}_p^*$ on a $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) [p]$.
ii) L'application $\begin{array}{rcl} \mathbb{F}_p^* & \to & \{-1,1\} \\ a & \mapsto & \left(\frac{a}{p}\right) \end{array}$ est l'unique morphisme de groupes non trivial de $\mathbb{F}_p^*$ sur $\{-1,1\}$.

Lemme 66 : Pour tout $a \in \mathbb{F}_p^*$, le nombre de solution de l'équation $ax^2 = 1$ est $\left(\frac{a}{p}\right) + 1 = \begin{cases} 2 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ 0 & \text{sinon.} \end{cases}$

$\boxed{\text{Développement}}$ (Loi de réciprocité quadratique)

Pour tout nombre premier impair $q \neq p$ on a :
$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Références :

- Rombaldi Mathématiques pour l'agrégation Rom
- Joseph Grifone Algèbre linéaire Gri
- Daniel Perrin Cours d'Algèbre Per