[PER] p 127

III - CLASSIFICATION

Déf 21 : Deux formes quadratiques sont équivalentes ($q \sim q'$) si $\exists u \in GL(E)$ tel que $q \circ u = q'$. Cela définit une relation d'équivalence.

Prop 22 : Si M est la matrice de q et M' celle de q' (dans une base B) alors $q \sim q' \iff \exists P \in GL_n(K), M' = {}^tPMP$

Déf 23 : Le discriminant $\delta(q)$ est $\det(M)$ modulo $(K^*)^2$. Cela ne dépend pas de la base choisie pour M.

Prop 24 : Si $q \sim q'$ alors $\text{rang}(q) = \text{rang}(q')$ et $\delta(q) = \delta(q')$

C-ex 25 : x^2+y^2 et $-x^2-y^2$ ne sont pas équivalentes sur $\mathbb{R}$ mais ont même rang et discriminant

Thm 26 : Si $K = \mathbb{C}$ et $\text{rang}(q) = r$ alors q est équivalente à $x \longmapsto x_1^2 + \dots + x_r^2$

Thm 27 : (Sylvester) Si $K = \mathbb{R}$ et q est de rang r, alors q est équivalente à

$$x \longmapsto \sum_{i=1}^{p} x_i^2 - \sum_{i=p+1}^{r} x_i^2 \quad \text{pour un } 0 \leq p \leq r$$

On dit que q est de signature $(p, r-p)$ et ce couple ne dépend que de q.

Ex 28 : Sur $K = \mathbb{R}$, et $q(x) = ax^2 + bxy + cy^2$ avec $a > 0$. $\Delta = b^2 - 4ac$ donne la signature :

- Si $\Delta < 0$, signature $(2,0)$
- Si $\Delta = 0$, signature $(1,0)$
- Si $\Delta > 0$, signature $(1,1)$

Lemme 29 : Soit $A_0 \in S_n(\mathbb{R}) \cap GL_n(\mathbb{R})$. Il existe V un voisinage ouvert de A_0 dans $S_n(\mathbb{R})$ et $\psi : V \to GL_n(\mathbb{R})$ ~~un C^1-difféomorphisme sur son image~~ tel que

$$\forall A \in V, \quad A = {}^t\psi(A) A_0 \psi(A)$$

Thm 30 (Lemme de Morse) Si $f : \Omega \to \mathbb{R}$ est de classe C^3 sur Ω (voisinage ouvert de 0) tel que $Df(0) = 0$ et $D^2f(0)$ est non dégénérée de signature $(p, n-p)$ alors il existe un C^1-difféo φ entre deux voisinages de 0 tels que

$$f(x) - f(0) = u_1^2 + \dots + u_p^2 - u_{p+1}^2 - \dots - u_n^2$$

où $u = \varphi(x)$.

DEVELOPPEMENT 1

Thm 31 : Si $K = \mathbb{F}_\ell$ où $\ell = \#\mathbb{F}_\ell < \infty$. Soit $\alpha \in \mathbb{F}_\ell^*$ qui n'est pas un carré dans $\mathbb{F}_\ell$, alors, si $r = \text{rang}(q)$ q est équivalente à $x \longmapsto x_1^2 + \dots + x_r^2$ ou à $x \longmapsto x_1^2 + \dots + x_{r-1}^2 + \alpha x_r^2$.

Application 32 : loi de réciprocité quadratique

Si p, q sont des nombres premiers impairs distincts alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

où $\left(\frac{x}{p}\right) = \begin{cases} 1 \text{ si } x \text{ est un carré modulo } p \\ 0 \text{ si } x = 0 \text{ modulo } p \\ -1 \text{ sinon} \end{cases}$

DEVELOPPEMENT 2

IV - ISOTROPIE

Déf 33 : $x \in E$ est isotrope si $q(x) = 0$

Le cône isotrope est $I(q) = \{x \in E \mid q(x) = 0\}$

Déf 34 : Un sous espace V est isotrope si $V \cap V^\perp \neq \{0\}$ c'est à dire $\exists x \in V - \{0\}, \forall y \in V, \varphi(x,y) = 0$ ce qui équivaut à $q|_V$ dégénérée.

Déf 35 : Un sous espace V est totalement isotrope si $V \subset V^\perp$, ce qui équivaut à $V \subset I(q)$.

Déf 36 : On note $\nu(q)$ la dimension maximale des sous espaces totalement isotropes pour q.

[ROU] p 354 et 209

[PER] p 123

/40

[GRI] p 413

Ex 37 : Si $K=\mathbb{R}$ et $q(x,y,z)=x^2+y^2-z^2$, $I(q)$ est un cône de $\mathbb{R}^3$ et $\nu(q)=1$.

Prop 38 : Soit q non dégénérée.

(i) $\nu(q) \leq \frac{n}{2}$

(ii) Si V est un sev non isotrope, $E = V \oplus V^\perp$

V - CONIQUES ET CONES ISOTROPES

Déf 39 : Une quadrique de $\mathbb{R}^n$ est une partie $\mathcal{C}$ de $\mathbb{R}^n$ d'équation $q(x)+l(x)+c=0$ où q est quadratique, l est linéaire, c constante.

Ex 40 : $\mathcal{C}_0 = \{(x,y) \in \mathbb{R}^2 \mid 3x^2+2y^2+2xy-4x-6=0\}$

Déf 41 : Etant donnée une quadrique d'équation $q(x)+l(x)+c=0$, la quadrique homogénéisée associée à cette équation est $Q(x,z)=q(x)+l(x)z+cz^2$ définie sur $\mathbb{R}^{n+1}$.

Remarque 42 : $\mathcal{C} = I(Q) \cap \{z=1\}$

- Si $n=2$, on parle de coniques
- selon $I(Q)$ et $I(q)$, on peut classifier les coniques.

Ex 43 : $x^2+y^2=1$ est l'équation d'un cercle de $\mathbb{R}^2$. La quadrique homogène associée est $Q(x,y,z)=x^2+y^2-z^2$ et $I(Q)$ est un cône de $\mathbb{R}^3$. Le cercle est l'intersection du plan $\{z=1\}$ avec le cône $I(Q)$.

Prop 44 : Classification affine des coniques en fonction de Q et q.

a) Si Q est de signature $(3,0)$ ou $(0,3)$

La conique est vide.

b) Si Q est de signature $(2,1)$ ou $(1,2)$

$I(q)$	conique
2 droites isotropes	hyperbole
1 droite isotrope	parabole
0 droite isotrope	ellipse

c) Si Q est de signature $(2,0)$ ou $(0,2)$

$I(q)$	conique
1 droite isotrope	$\emptyset$
0 droite isotrope	un point

d) Si Q est de signature $(1,1)$

$I(q)$	conique
$q=0$	droite
2 droites isotropes	2 droites sécantes
1 droite isotrope	2 droites parallèles

e) Si Q est de signature $(1,0)$ ou $(0,1)$

$I(q)$	conique
$q=0$	$\emptyset$
1 droite isotrope	droite

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

[Gou] p223

Cadre : K est un corps de caractéristique $\neq 2$. E est un K-espace vectoriel de dimension finie $n \geq 1$

I- FORMES BILINEAIRES SYMETRIQUES

Def 1 : Une forme bilinéaire symétrique est une application $\varphi : E \times E \longrightarrow K$ telle que $\forall x \in E$, $\varphi(x,\cdot)$ et $\varphi(\cdot,x)$ sont linéaires et $\forall x,y \in E$, $\varphi(x,y) = \varphi(y,x)$.

Ex 2 : • $(A,B) \longmapsto \mathrm{Tr}({}^tAB)$ est bilinéaire symétrique sur $M_n(K)$.

• Si $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ est C^2 alors $D^2f(a)$ est une forme bilinéaire symétrique appelée la Hessienne de f en a

Def 3 : Si φ est une forme bilinéaire symétrique sur E $q : E \longrightarrow K$, $q(x) = \varphi(x,x)$ est la forme quadratique associée à φ.

Prop 4 : φ est déterminée par les identités de polarisation

$$\varphi(x,y) = \frac{1}{2}\left[q(x+y) - q(x) - q(y)\right] = \frac{1}{2}\left[q(x)+q(y)-q(x-y)\right]$$
$$= \frac{1}{4}\left[q(x+y) - q(x-y)\right]$$

Remarque 5 : Cela définit un isomorphisme entre l'espace des formes quadratiques et celui des formes bilinéaires sym.

Prop 6 : Si $B = (e_1,\dots,e_n)$ est une base de E, la matrice de φ dans la base B est $M = (\varphi(e_i,e_j))_{ij}$. M est l'unique matrice telle que $\varphi(x,y) = {}^tXMY$ où X (resp. Y) est le vecteur coordonnées de x (resp. y) dans la base B. Réciproquement si M est symétrique $(X,Y) \mapsto {}^tXMY$ est bilinéaire symétrique sur K^n.

Ex 7 : $\begin{pmatrix} 3 & 1 & -2 \\ 1 & 2 & 0 \\ -2 & 0 & 0 \end{pmatrix}$ est la matrice dans la base canonique de $q(x,y,z) = 3x^2 + 2y^2 + 2xy - 4xz$

Prop 8 : Si B, B' sont des base de E, si M (resp. M') est la matrice de φ dans la base B (resp. B') et P la matrice de passage de B à B' alors $M' = {}^tPMP$

Déf 9 : $\mathrm{rang}\,\varphi = \mathrm{rang}\,M$ et $\mathrm{Ker}\,\varphi = \mathrm{Ker}\,M$

Déf 10 : φ est dégénérée si $\mathrm{Ker}\,\varphi \neq \{0\}$.

Prop 11 : $\mathrm{Ker}\,\varphi = \{x \in E \mid \forall y \in E,\ \varphi(x,y) = 0\}$

Déf 12 : • φ est définie si $\varphi(x,x) = 0 \Leftrightarrow x = 0$

• Si $K = \mathbb{R}$, φ est positive si $\forall x \in E$, $\varphi(x,x) \geq 0$

Appli 13 : Si $f : U \subset \mathbb{R}^n \to \mathbb{R}$ est C^2, $a \in U$ et $Df(a) = 0$ alors (i) $D^2f(a)$ définie positive $\Rightarrow$ a minimum local

(ii) a minimum local $\Rightarrow$ $D^2f(a)$ positive

[Gou] p227 [Rou] p371 [Gou] p227

II- ORTHOGONALITÉ

Déf 14 : • x et y orthogonaux $\Leftrightarrow \varphi(x,y) = 0$ noté $x \perp y$

• Si $A, B \subset E$, A orthogonal à $B \Leftrightarrow \forall x \in A, \forall y \in B,\ x \perp y$.

• Si $A \subset E$, $A^\perp = \{x \in E \mid \forall y \in A,\ \varphi(x,y) = 0\}$

Prop 15 : Si $A \subset B \subset E$ alors $A^\perp$ est un sous espace vectoriel et $\mathrm{Vect}(A)^\perp = A^\perp$, $A \subset A^{\perp\perp}$, $B^\perp \subset A^\perp$, $E^\perp = \mathrm{Ker}\,\varphi$

Prop 16 : Si F est un sous espace vectoriel de E alors

(i) $\dim F + \dim F^\perp = \dim E + \dim F \cap \mathrm{Ker}\,\varphi$

(ii) $F^{\perp\perp} = F + \mathrm{Ker}\,\varphi$

Déf 17 : Une base $(e_1,\dots,e_n)$ de E est orthogonale pour φ si $\forall i \neq j$, $\varphi(e_i,e_j) = 0$.

La matrice de φ dans une telle base est diagonale.

Thm 18 : Il existe une base orthogonale pour φ.

Thm 19 : (Algorithme de Gauss)

On se donne une forme quadratique $q(x) = \sum_{i \leq j} a_{ij} x_i x_j$ alors on peut écrire q comme combinaison linéaire de carrés de formes linéaires indépendantes.

Ex 20 : La forme quadratique $q(x,y,z) = 5xy + 6xz + 3yz$ s'écrit grace à l'algorithme de Gauss :

$$q(x,y,z) = \frac{3}{4}\left(x_1 + x_2 + \frac{2}{3}x_3\right)^2 - \frac{3}{4}\left(x_1 - x_2 - \frac{2}{3}x_3\right)^2 - \frac{2}{3}x_3^2$$

[DEU] Deheuvels, Formes quadratiques et groupes classiq
[GOU] Gourdon, Les maths en tête, algèbre
[GRI] Grifone, Algèbre Linéaire
[PER] Perrin, Cours d'algèbre
[ROU] Rouvière, Petit guide du calcul différentiel

Lemme de Morse

Mouzard - Morin

On commence par un lemme préliminaire.

Lemme. *Soit $A_0 \in GL_n(\mathbb{R}) \cap \mathscr{S}_n(\mathbb{R})$. Alors il existe un voisinage V de A_0 dans $\mathscr{S}_n(\mathbb{R})$ et une application $\psi : V \subset \mathscr{S}_n(\mathbb{R}) \to GL_n(\mathbb{R})$ de classe C^1 tels que $\forall A \in V, A = {}^t\phi(A)A_0\phi(A)$. Autrement dit, le changement de base des formes quadratiques dépend localement de manière C^1 de la forme quadratique.*

Démonstration : On pose

$$\begin{aligned} \varphi : GL_n(\mathbb{R}) &\to \mathscr{S}_n(\mathbb{R}) \\ P &\mapsto {}^tPA_0P. \end{aligned}$$

φ est de classe C^1 car polynomiale. On a $\varphi(I+H) - \varphi(I) = A_0H + {}^tHA_0 + \underset{\|h\|\to 0}{\mathcal{O}}(\|H\|^2)$. Donc $d\varphi_I H = A_0H + {}^tHA_0$. On va maitenant chercher à appliquer le théorème d'inversion locale, cependant $d\varphi_I$ n'est pas inversible :

$$\begin{aligned} d\varphi_I H = 0 \quad &\iff \quad A_0H = -{}^tHA_0 \\ &\iff \quad A_0H \in \mathscr{A}_n \end{aligned}$$

On va utiliser la décomposition suivante :

$$\mathscr{M}_n(\mathbb{R}) = \mathscr{S}_n(\mathbb{R}) \oplus \mathscr{A}_n(\mathbb{R}) = A_0\mathscr{S}_n(\mathbb{R}) \oplus A_0\mathscr{A}_n(\mathbb{R})$$

car A_0 est inversible. On considère $\varphi|_{A_0\mathscr{S}_n(\mathbb{R})}$: sa différentielle en I est inversible. D'après le théorème d'inversion locale, il existe un voisinage V de A_0 dans $\mathscr{S}_n(\mathbb{R})$ et $\phi : V \subset \mathscr{S}_n(\mathbb{R}) \to A_0\mathscr{S}_n(\mathbb{R}) \cap GL_n(\mathbb{R})$ qui réalise un C^1-difféomorphisme sur son image tels que

$$\forall A \in V, A = {}^t\psi(A)A_0\psi(A).$$

En particulier, $\psi : V \to GL_n(\mathbb{R})$ est de classe C^1.

□

Théorème. *Soient $U \subset \mathbb{R}^n$ un ouvert et $f : \mathbb{R}^n \to \mathbb{R}$ une fonction de classe C^3. On suppose que $D_0f = 0$ et que D_0^2f est non dégénérée de signature $(p, n-p)$. Alors il existe un C^1-difféomorphisme φ de $V \subset \mathbb{R}^n$ un voisinage de 0 dans $\mathbb{R}^n$ tel que $\varphi(0) = 0$ et $f(x) - f(0) = u_1^2 + \ldots + u_p^2 - u_{p+1}^2 - \ldots - u_n^2$ où $u = (u_1, \ldots, u_n) = \varphi(x)$.*

Démonstration : Par la formule de Taylor avec reste intégral, on a

$$f(x) - f(0) = \int_0^1 (1-t) D^2_{tx} f(x,x) \mathrm{d}t.$$

On pose $Q(x) = \displaystyle\int_0^1 (1-t) D^2_{tx} f \mathrm{d}t \in \mathscr{S}_n(\mathbb{R})$, ainsi $f(x) - f(0) = {}^t x Q(x) x$.
$Q(0) = \frac{1}{2} D^2_0 f$ est inversible car supposée non dégénérée. On peut alors appliquer le lemme : il existe un voisinage V de $Q(0)$ dans $\mathscr{S}_n(\mathbb{R})$ et $\psi : V \to GL_n(\mathbb{R})$ tels que

$$\forall A \in V, A = {}^t\psi(A) Q(0) \psi(A).$$

Or Q est continue en 0 donc il existe un voisinage U de 0 dans $\mathbb{R}^n$ tel que

$$\forall x \in U, Q(x) = {}^t\psi(Q(x)) Q(0) \psi(Q(x))$$

Enfin, $Q(0)$ est une forme quadratique de signature $(p, n-p)$ donc il existe $P \in GL_n(\mathbb{R})$ telle que $Q(0) = {}^t P \begin{pmatrix} I_p & 0 \\ 0 & I_{n-p} \end{pmatrix} P$. Alors on a

$$\forall x \in U, \quad f(x) - f(0) = {}^t(P\psi(Q(x))x) \begin{pmatrix} I_p & 0 \\ 0 & I_{n-p} \end{pmatrix} P\psi(Q(x))x = {}^t y \begin{pmatrix} I_p & 0 \\ 0 & I_{n-p} \end{pmatrix} y.$$

En posant $\varphi(x) := P\psi(Q(x))x$, il reste à montrer que φ vérifie bien les conditions annoncées. On a $\varphi(0) = 0$. Comme f est de classe C^3, on a que φ est de classe C^1 sur U. On va alors lui appliquer le théorème d'inversion locale. Soit $h \in U$. Alors

$$\varphi(h) - \varphi(0) = P\psi(Q(h))h = P\psi(Q(0))h + \underset{\|h\| \to 0}{\mathcal{O}}(\|h\|^2)$$

car $\psi \circ Q$ est C^1. Donc $d\varphi_0$ est inversible et le théorème d'inversion locale nous garantit l'existence du C^1 difféomorphisme annoncé.

□

Loi de réciprocité quadratique

Mouzard - Morin

Théorème. *Soient $p, q \geq 3$ deux nombres premiers. Alors* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ *avec la notation pour le symbole de Legendre :*

$$\left(\frac{x}{q}\right) = \begin{cases} 1 & si\ x \in \left(\mathbb{F}_q^\times\right)^2 \\ 0 & si\ x \equiv 0[q] \\ -1 & sinon \end{cases}.$$

Démonstration : Nous allons compter l'ensemble

$$X := \{(x_1, \ldots, x_p) \in \mathbb{F}_q^p | x_1^2 + \ldots + x_p^2 = 1\}$$

modulo p de deux manières différentes.
On remarque que $\mathbb{Z}/p\mathbb{Z}$ agit par permutation circulaire sur X : $(n, (x_1, \ldots, x_p)) \mapsto (x_{1+n}, \ldots, x_{p+n})$ où les indices sont pris modulo p. Soit $x \in X$.

· Cas 1 : $\exists i \neq j, x_i \neq x_j$.
Alors $|Orb(x)| = |\mathbb{Z}/p\mathbb{Z}| = p$ car le seul stabilisateur est $n = 0 \in \mathbb{Z}/p\mathbb{Z}$

· Cas 2 : $x_1 = \ldots = x_p$.
Alors $|Orb(x)| = 1$. La condition est alors $px^2 = 1$. Il y a exactement deux solutions si p est un carré modulo q, 0 sinon. C'est-à-dire $1 + \left(\frac{p}{q}\right)$.

Donc $|X| \equiv 1 + \left(\frac{p}{q}\right)[p]$.
On pose $d = \frac{p-1}{2}$ et $a = (-1)^d$. On considère maintenant l'ensemble

$$X' := \{(x_1, \ldots, x_p) \in \mathbb{F}_q^p \mid Q(x_1, \ldots, x_p) := 2x_1x_2 + \ldots + 2x_{p-2}x_{p-1} + ax_p^2 = 1\}.$$

La théorie des formes quadratiques nous dit que la matrice de Q dans une bonne base est I_p ou $\mathrm{diag}(1, \ldots, 1, \alpha)$ où $\alpha \in \mathbb{F}_q$ n'est pas un carré. Or le discriminant de Q est 1 par construction, qui est un carré dans $\mathbb{F}_q$. On en déduit que sa matrice est I_p dans une bonne base, et donc que $|X| = |X'|$.
Nous allons maintenant compter X' modulo p et en déduire le résultat. Soit $(x_1, \ldots, x_p) \in X'$.

· Cas 1 : $(x_1, x_3, \ldots, x_{p-2}) = (0, \ldots, 0)$.
La condition devient alors $ax_p^2 = 1$. Il y a $1 + \left(\frac{a}{q}\right)$ solutions pour x_p, et q^d pour $(x_2, \ldots, x_{p-1})$ ce qui donne $q^d\left(1 + \left(\frac{a}{q}\right)\right)$.

· Cas 2 : $(x_1, x_3, \ldots, x_{p-2}) \neq (0, \ldots, 0)$.
On considère alors $(x_1, x_3, \ldots, x_{p-2})$ fixés, et soit $x_p \in \mathbb{F}_q$ fixé. L'équation

devient celle d'un hyperplan affine dans un espace vectoriel de dimension d sur un corps de cardinal q, il y a q^{d-1} possibilités pour $(x_2, \ldots, x_{p-1})$. Il y a au total $q^{d-1}q(q^d-1)$ possibilités pour $(x_1, \ldots, x_p)$.

Donc $|X'| = q^d(1+\left(\frac{a}{q}\right))+q^d(q^d-1) = q^{p-1}+q^d\left(\frac{a}{q}\right)$. On regarde alors l'égalité entre $|X|$ et $|X'|$ modulo p :

$$1+\left(\frac{p}{q}\right) = q^{p-1}+q^d\left(\frac{a}{q}\right) \quad [p]$$

Or $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \quad [p]$. Donc

$$1+\left(\frac{p}{q}\right) = 1+q^{\frac{p-1}{2}}a^{\frac{q-1}{2}} \quad [p]$$

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \quad [p]$$

Or les termes en jeux valent $1, 0$ ou -1, on a donc l'égalité en tant qu'entier et non seulement modulo p.

□