Algèbre bilinéaire, formes quadratiques

Thomas Dedieu

Rentrée 2018, compilé le 26 août 2019

Avertissement. Ceci n'est pas un polycopié de cours. Ce texte est constitué de mes notes personnelles pour un cours de préparation à l'agrégation, grossièrement mises en forme. Néanmoins, si vous trouvez des erreurs il m'intéresse que vous me les communiquiez.

Dans tout ce cours, E est un espace vectoriel de dimension finie n sur un corps $\mathbf{k}$, supposé de caractéristique différente de 2 à partir du moment indiqué p. 5.

0 – Dualité

(0.1) Dual, bidual. $E^\vee$ (ou E^*) est le $\mathbf{k}$-ev des formes linéaires sur E.

On a donc $E^\vee = \mathcal{L}(E, \mathbf{k})$, et $E^\vee$ est de dimension n.

(0.1.1) Exercice important. Montrer que

$$\llcorner : e \in E \mapsto (\llcorner e : \ell \in E^\vee \mapsto \ell \llcorner e := \ell(e) \in \mathbf{k})$$

établit un isomorphisme canonique $E \cong (E^\vee)^\vee$. On peut préférer à la notation 'produit intérieur' la notation 'évaluation', $\mathrm{ev}_x : \ell \mapsto \ell(x)$.

(Ici on utilise de manière essentielle le fait que E est de dimension finie : on montre que $\llcorner$ est injective, et on conclut par un argument de dimension). [1]

(0.2) Base duale. Voici une formulation qui n'est pas intrinsèque. Étant donnée une base $(e_1, \ldots, e_n)$ de E, on a un système de coordonnées $(x_1, \ldots, x_n)$ sur E. L'espace $E^\vee$ des formes linéaires sur E est le $\mathbf{k}$-ev des polynômes *homogènes* de degré 1 en $x_1, \ldots, x_n$; la famille $(x_1, \ldots, x_n)$ en est une base.

Définition de la base duale. Remarquer que les $e_1^\vee, \ldots, e_n^\vee$ sont les $dx_1, \ldots, dx_n$ du calcul intégral.

(0.2.1) Attention. Si on se donne juste un vecteur $e \in E$ (tout seul), $e^\vee$ n'est pas défini (il faut tout une base).

(0.2.2) Si L est la colonne (!) des coordonnées de ℓ dans $\mathcal{B}^\vee$, la matrice de ℓ dans $\mathcal{B}$ et la base canonique de $\mathbf{k}$ est la ligne ${}^{\mathsf{T}}L$.

La base canonique de $\mathbf{k}$ étant plus que canonique, j'allège la notation $\mathrm{Mat}_{\mathcal{B},\mathcal{B}_{can}}$ en $\mathrm{Mat}_{\mathcal{B}}$.

(0.2.3) Lemme. $\ell = \ell(e_1).e_1^\vee + \cdots + \ell(e_n).e_n^\vee$.

(0.2.4) Changement de base. $\mathrm{Mat}(\mathcal{B}_F^\vee, \mathcal{B}_E^\vee) = {}^{\mathsf{T}}(\mathrm{Mat}(\mathcal{B}_E, \mathcal{B}_F))$ est la formule naturelle ; si on insiste pour avoir $\mathrm{Mat}(\mathcal{B}_E^\vee, \mathcal{B}_F^\vee)$, c'est ${}^{\mathsf{T}}(\mathrm{Mat}(\mathcal{B}_E, \mathcal{B}_F))^{-1}$.

Exemple. Soit E une droite engendrée par $e \neq 0$. Pour $\lambda \in \mathbf{k}^*$, $\lambda.e$ est une autre base de E. On a :

$$(\lambda e)^\vee = \frac{1}{\lambda} e^\vee.$$

En effet :

$$(\lambda e)^\vee(e) = \frac{1}{\lambda}(\lambda e)^\vee(\lambda e) = \frac{1}{\lambda} = \frac{1}{\lambda} e^\vee(e).$$

(0.2.5) Exercice. $(\mathcal{B}^\vee)^\vee \cong \mathcal{B}$ par l'isomorphisme de bidualité.

(0.3) Transposition. Pour $u \in \mathcal{L}(E, F)$, ${}^{\mathsf{T}}u \in \mathcal{L}(F^\vee, E^\vee)$ est

$$\ell \mapsto \ell \circ u.$$

1. sinon il faut rajouter des hypothèses de complétude, et se restreindre aux formes linéaires continues. Soit H un espace de Hilbert. L'inégalité de Cauchy–Schwartz assure que pour tout $x \in H$, la forme linéaire $\langle x, \cdot \rangle$ est continue. Le théorème de représentation de Riesz assure que la réciproque est vraie. (Ne pas confondre avec le théorème de convexité de Riesz).

(0.3.1) $\mathrm{Mat}_{\mathcal{B}_F^\vee,\mathcal{B}_E^\vee}({}^{\mathsf{T}}u) = {}^{\mathsf{T}}\big(\mathrm{Mat}_{\mathcal{B}_F,\mathcal{B}_E}(u)\big)$.
Preuve. Je conserve le système de notation de (0.2.2) : L est la colonne de ℓ dans $\mathcal{B}_F^\vee$. La matrice ligne de ${}^{\mathsf{T}}u(\ell)$ est

$$\mathrm{Mat}_{\mathcal{B}_E}\big({}^{\mathsf{T}}u(\ell)\big) = {}^{\mathsf{T}}L \times A,$$

donc ${}^{\mathsf{T}}u$ s'écrit matriciellement $L \mapsto {}^{\mathsf{T}}A \times L$. □
Exercice. Retrouver la formule de changement de base (0.2.4) à partir de (0.3.1).
(0.3.2) Exercice (abscons). ${}^{\mathsf{T}}({}^{\mathsf{T}}u) = u$ *via* les isomorphismes canoniques $(E^\vee)^\vee \cong E$.

(0.4) Orthogonalité. Définition. L'orthogonalité renverse les inclusions. $(A,B)^\perp = A^\perp \cap B^\perp$; $A^\perp + B^\perp \subseteq (A\cap B)^\perp$. $F \subseteq (F^\perp)^\perp$ *via* l'isomorphisme de bidualité.
(0.4.1) $\ker({}^{\mathsf{T}}u) = (\mathrm{im}(u))^\perp$; $\mathrm{im}({}^{\mathsf{T}}u) = (\ker u)^\perp$.
(0.4.2) $(E/F)^\vee \cong F^\perp$. ${}^{\mathsf{T}}\big(\pi : E \twoheadrightarrow E/F\big) = \big(\iota : F^\perp \hookrightarrow E^\vee\big)$.

(0.5) Dualité géométrique. On a une correspondance biunivoque entre les sev de dim r de $E^\vee$ et les sev de dim $c := n-r$ de E, donnée par $\Lambda \mapsto \Lambda^\perp$.

Cas particulier important : l'ensemble des hyperplans (vectoriels) de E s'identifie à l'ensemble des droites (vectorielles) de $E^\vee$. Voici un contexte dans lequel la géométrie projective surgit de manière naturelle.[2]

(0.5.1) Preuve. L'argument de dimension est inévitable, dans la mesure où cet énoncé ne fonctionne pas en dimension infinie (voir exemple (0.5.3)). Le truc à comprendre est que $\Lambda^\perp$ est un sev de E défini par un système d'équations linéaires. Ensuite, une bonne façon de comprendre la formule $\dim \Lambda^\perp = \dim E - \dim \Lambda$ est d'utiliser le pivot de Gauss. Une autre possibilité est de prendre $(\ell_1,\dots,\ell_r)$ base de Λ, de la compléter en une base de $E^\vee$, et de constater en utilisant la base duale que $\dim(\ell_1,\dots,\ell_r)^\perp = n-r$.

(0.5.2) Remarque. Caché là-dedans se trouve le fait que “rang = rang de la transposée”. En effet, considérons une matrice A. Le calcul de $\dim \Lambda^\perp$ nous dit que la dimension du noyau de A est n (nombre de colonnes) moins le rang des lignes de A. D'autre part, le théorème du rang nous dit que la dimension du noyau est aussi n moins le rang des colonnes de A.

(0.5.3) Application. En dimension finie, on a $A^\perp + B^\perp = (A\cap B)^\perp$ et $F = (F^\perp)^\perp$.
Exemple. En dimension infinie, prenant un peu d'avance sur la dualité par rapport à une forme quadratique, on peut considérer la forme bilinéaire non-dégénérée sur $\mathbf{k}[X]$ standard

$$\langle a_dX^d + \cdots + a_0, b_dX^d + \cdots + b_0\rangle = \sum a_ib_i,$$

et $F = \{P : P(1) = 0\}$. On vérifie que $F^\perp = \{0\}$ et donc $(F^\perp)^\perp = \mathbf{k}[X]$.

(0.5.4) Application. Calculer un système d'équation de $\mathrm{Vect}(u_1,\dots,u_r)$ connaissant les coordonnées de chaque u_i dans $\mathcal{B}$, sous l'hypothèse que les u_i sont linéairement indépendants. i) en trouvant un mineur non-nul dans la matrice des u_i ; ii) il est bon de parler du pivot dans ce contexte.

2. je ne résiste pas ! Ce contexte naturel est un cas particulier de celui fondamental des systèmes linéaires : les hyperplans de $\mathbf{k}^{n+1}$ -ou de $\mathbf{P}^n$!) forment un espace projectif.

Une fois qu'on a $A_r \in \mathrm{GL}_r(\mathbf{k})$,

$$\left(\begin{array}{c|c} & x_1 \\ A_r & \vdots \\ & x_r \\ \hline L_{r+1} & x_{r+1} \\ \vdots & \vdots \\ L_n & x_n \end{array}\right) \iff \forall i = 1, \ldots, n-r,\ \det \left(\begin{array}{c|c} & x_1 \\ A_r & \vdots \\ & x_r \\ \hline L_{r+i} & x_{r+i} \end{array}\right) = 0. \qquad (0.5.5)$$

En effet, on cherche les équations d'un espace de dimension r. Les équations du côté droit de (0.5.5) sont $n-r$ équations linéaires indépendantes vérifiées par les vecteurs de notre espace, il n'y en a pas d'autre.

On retrouve essentiellement la formule pour l'équation d'un plan dans $\mathbf{k}^3$ avec le produit vectoriel de deux vecteurs générateurs.

Un autre bon point pour la géométrie projective : si on la connaît, la méthode ci-dessus permet aussi d'écrire les équations des sous-espaces affines.

(0.5.6) Application. Savoir calculer la dimension d'une intersection d'hyperplans (rapport du jury).

1 – Définitions

(1.1) Polynômes homogènes de degré 2. On commence par la version non intrinsèque : une base de E étant donnée, une forme quadratique sur E est un polynôme homogène de degré 2 en les coordonnées $x_1, \ldots, x_n$.

Pour une définition sans coordonnée, il faut (?) voir les formes quadratiques comme des fonctions : une application

$$q : E \to \mathbf{k}$$

est une forme quadratique s'il existe Q forme bilinéaire (non nécessairement symétrique) telle que $q(x) = Q(x, x)$ pour tout $x \in E$; de manière équivalente, s'il existe $\ell_1, \ell'_1, \ldots, \ell_s, \ell'_s$ formes linéaires telles que

$$q = \textstyle\sum_{i=1}^{s} \ell_i \ell'_i. \tag{1.1.1}$$

Le point un peu gênant avec cette définition est qu'on voit les formes quadratiques comme des fonctions polynomiales, alors qu'on préférerait les voir comme des polynômes. En caractéristique $\neq 2$, on verra que ces deux objets s'identifient sans problème, même sur un corps fini.

En tout cas, la définition précédente fonctionne en toute caractéristique.

(1.1.2) Commentaire métaphysique. Malgré tout, formes bilinéaires et formes quadratiques, ce n'est pas tout-à-fait la même chose (accouplements *vs.* polynômes).

(1.2) Correspondance avec les formes bilinéaires symétriques. Si $\mathrm{char}(\mathbf{k}) \neq 2$, on a une correspondance biunivoque $\mathcal{Q}(E) \cong \mathrm{Sym}^2(E^\vee)$.

(1.2.1) Proposition. Pour tout $q \in \mathcal{Q}(E)$, il existe une et une seule forme bilinéaire symétrique P telle que $q(x) = P(x, x)$ pour tout $x \in E$; on l'appelle *forme polaire* de q.

Preuve (analyse-synthèse). On a nécessairement $2P(x, y) = q(x + y) - q(x) - q(y)$, et puisque $2 \neq 0$, ceci détermine un unique P possible. Il convient, car (i) il est bilinéaire symétrique puisque

$$P(x, y) = \sum_{1}^{s} \big(\ell_i(x)\ell'_i(y) + \ell_i(y)\ell'_i(x)\big)$$

(dans la notation de (1.1.1)), et (ii)

$$P(x, x) = \frac{1}{2}\big(q(2x) - 2q(x)\big) = q(x).$$

$\square$

(1.2.2) Corollaire. Puisque les formes bilinéaires s'identifient, une base étant choisie, à une matrice, la correspondance ci-dessus nous indique qu'au moins en caractéristique $\neq 2$, une forme quadratique s'identifie à ses coefficients ; autrement dit il n'y a pas lieu de distinguer entre polynôme et fonction polynomiale. *Cf.* [H2G2, Vol. I, Rmq. V.B.1.3].

(1.2.3) Problème avec la caractéristique 2. En caractéristique 2, $q(x, y) = xy$ provient de la forme bilinéaire $Q\big((x, y), (x', y')\big) = xy'$, mais il n'existe pas de forme bilinéaire symétrique donnant q :

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 2xy = 0.$$

(1.3) Exemple. Si $f : \mathbf{R}^n \to \mathbf{R}$ est une fonction de classe C^2, alors la Hessienne de f est une forme bilinéaire symétrique (Théorème de Schwarz).

À partir d'ici, on suppose $\mathrm{char}(\mathbf{k}) \neq 2$.

(1.4) Matrice d'une FQ dans une base ; elle est symétrique.
(1.4.1) Exemple. Matrices "antisymplectiques"

$$\begin{pmatrix} 0 & \mathrm{Id} \\ \mathrm{Id} & 0 \end{pmatrix}.$$

(1.4.2) $P(x, y) = {}^{\mathsf{T}}XAY$.
(1.4.3) Formules de changement de base.

(1.5) Définition de $\varphi \in \mathcal{L}(E, E^\vee)$ associée à q : $\varphi(x) := P(x, \bullet)$.
[Autrement dit, $\varphi = \lrcorner P : x \mapsto x \lrcorner P$.]
(1.5.1) Matrice dans une base ; s'obtient par (1.4.2).
(1.5.2) ${}^{\mathsf{T}}\varphi = \varphi$.
Attention, ça ne signifie pas que la matrice de φ dans n'importe quelle*s* base*s* est symétrique.

(1.6) Vocabulaire.
(1.6.1) vecteur isotrope : $x \in E$ tel que $q(x) = 0$;
cône (c'en est un !) isotrope : $\{x \in E : q(x) = 0\}$;
q anisotrope : $q^{-1}(0) = \{0\}$.
Pour $\mathbf{k} = \mathbf{R}$, q définie positive (resp. négative), noté $q \gg 0$ (resp. $\ll 0$) : $\forall x \in E,\ q(x) > 0$ (res. < 0).
(1.6.2) FQ non dégénérée : $\forall x \in E,\ \varphi(x) \neq 0$ ($\Leftrightarrow \varphi$ inversible) ;
$\operatorname{rg} q := \operatorname{rg} \varphi$;
$\operatorname{rad} q := \ker \varphi$.
(1.6.3) Pour F sev :
$\operatorname{rad} F := \operatorname{rad} q|_F$;
F non singulier (pour q) si $q|_F$ est non dégénérée ($\Leftrightarrow \operatorname{rad} F = \{0\}$) ;
F totalement singulier (ou totalement isotrope) pour q si $\operatorname{rad} F = F$.

(1.7) Morale. avoir des vecteurs isotropes ce n'est pas bien grave, ça arrive même à tout-le-monde sur $\mathbf{C}$ en dim $\geqslant 2$ (se voit à la main pour $x^2 + y^2$, puis par le théorème de classification par le rang en général). Être dégénéré est certainement plus embêtant.

(1.8) Dualité par rapport à une forme quadratique. Le *choix* d'une FQ non-dégénérée fournit un isomorphisme (non-canonique, même si on ne choisit pas de base) entre E et $E^\vee$. On y gagne que la dualité "reste dans E".

Par exemple, *dans le cas euclidien*, ceci attache à tout sous-espace F un supplémentaire préféré, *ossia* $F^\perp$.

(1.9) Adjonction par rapport à une FQ non dégénérée. Étant donnée q non dégénérée, on définit pour $f \in \mathcal{L}(E)$ un adjoint par la condition

$$\forall x, y \in E : \quad P(f(x), y) = P(x, f^*(y)).$$

On a la formule

$$f^* := \varphi^{-1} \circ {}^{\mathsf{T}}f \circ \varphi \in \mathcal{L}(E), \tag{1.9.1}$$

qui prouve au passage que notre définition est saine.

Preuve. Soit $x, y \in E$:

$$P\big(f(x), y\big) = \varphi \circ f(x)(y),$$

tandis que

$$P\big(x, f^*(y)\big) = \varphi(x)\big(f^*(y)\big) = {}^{\mathsf{T}}(f^*)\big(\varphi(x)\big)(y) = {}^{\mathsf{T}}(f^*) \circ \varphi(x)(y).$$

Ainsi,

$$\begin{aligned} &\forall x, y \in E : P(f(x), y) = P(x, f^*(y)) \\ \iff &\forall x \in E,\ \forall y \in E : \varphi \circ f(x)(y) = {}^{\mathsf{T}}f^* \circ \varphi(x)(y) \\ \iff &\forall x \in E : \varphi \circ f(x) = {}^{\mathsf{T}}f^* \circ \varphi(x) \\ \iff &\varphi \circ f = {}^{\mathsf{T}}f^* \circ \varphi. \end{aligned}$$

□

Si dans la preuve on préfère éviter d'écrire ${}^{\mathsf{T}}\varphi = \varphi$, il faut commencer par écrire

$$P(f(x), y) = P(x, f^*(y)) \Leftrightarrow P(y, f(x)) = P(f^*(y), x),$$

ce qui bien sûr revient essentiellement au même puisque c'est la symétrie de P qui indentifie φ à sa transposée.

1.1 – Orthogonalité

(1.10) Définitions. Pour tout $A \subset E$ (pas forcément sev), $A^\perp = ...$ qui lui est toujours un sev. $B \perp A$ signifie $B \subset A^\perp$, ou de manière équivalente $A \subset B^\perp$.

On note que c'est la version dans le cadre de la dualité par rapport à une forme quadratique (non dégénérée) de la dualité géométrique (0.5).

(1.11) Proposition. *Soit q forme quadratique non-dégénérée, F, F' sev.*

(i) $\dim F + \dim F^\perp = \dim E$.
(ii) $(F^\perp)^\perp = F$.
(iii) $(F \cap F')^\perp = F^\perp + F'^\perp$.
(iv) $(F + F')^\perp = F^\perp \cap F'^\perp$.

Le point (i) mérite qu'on s'y attarde un instant. Il n'implique nullement que F et $F^\perp$ sont en somme directe.

Pour le démontrer : soit $e_1, \ldots, e_p$ base de F, complétée en $\mathcal{B}$ base de E ;

$$x \in F^\perp \Leftrightarrow \forall i = 1, \ldots, p,\ P(e_i, x) = 0.$$

Notons $A = \mathrm{Mat}_{\mathcal{B}}(q)$. $F^\perp$ est défini par p équations linéaires, qui sont les p premières lignes de A. Elles sont indépendantes, puisque A est inversible. □

Attention. $F \perp G$ n'implique pas $F \cap G = \{0\}$, même si c'est vrai dans le cas euclidien. *Malgré tout*, ça fonctionne si F est non-singulier. En effet, dans ce cas $F \cap F^\perp = \{0\}$, et donc $F \perp G \Leftrightarrow G \subset F^\perp \Rightarrow G \cap F = \{0\}$.

(1.12) Lemme.. *Soit q forme quadratique (possiblement dégénérée), F, F' sev.*

(i) $\mathrm{rad}\, F = F \cap F^\perp$.
(ii) *F totalement singulier $\Leftrightarrow F \subset F^\perp$.*
(iii) *F non-singulier $\Leftrightarrow F \cap F^\perp = \{0\} \Leftrightarrow E = F \oplus F^\perp \Leftrightarrow F^\perp$ non-singulier.*

Preuve. Pour (i) et (ii) Il s'agit essentiellement de réécrire les définitions. (i) donne immédiatement F non-singulier $\Leftrightarrow F \cap F^{\perp} = \{0\}$, et donc F non-singulier $\Leftrightarrow F^{\perp}$ non-singulier. Enfin $E = F \oplus F^{\perp}$ implique tautologiquement $F \cap F^{\perp} = \{0\}$. Il reste donc seulement à voir la réciproque de cette dernière implication.

Si $F \cap F^{\perp} = \{0\}$, alors la somme $F + F^{\perp}$ est directe, et il suffit de montrer que $\dim(F) + \dim(F^{\perp}) \geqslant \dim(E)$. Cette inégalité s'obtient par le même raisonnement que dans la preuve du i Prop. (1.11) ci-dessus : $F^{\perp}$ est défini par $\dim(F)$ équations dans $E^{\vee}$, donc $\dim(F^{\perp}) \geqslant \dim(E^{\vee}) - \dim(F)$. □

(1.13) Corollaire. *Soit q forme quadratique, éventuellement dégénérée), et F sev. Si $q|_F$ est non-dégénérée, alors* $\dim F^{\perp} = n - \dim F$.

Il est bon de se rappeler que q non-dégénérée n'implique pas du tout $q|_F$ non-dégénérée.

2 – Complétion non singulière

(2.1) Théorème. *On suppose q non dégénérée, et on considère F sev de E. Pour toute donnée d'un supplémentaire G de $\operatorname{rad} F$ dans F,*

$$F = \operatorname{rad} F \oplus G, \tag{2.1.1}$$

et d'une base $(e_1, \dots, e_s)$ de $\operatorname{rad} F$, il existe $\bar{F}$ sev non singulier de E contenant F et décomposé en

$$F \subseteq \bar{F} = G \overset{\perp}{\oplus} \Pi_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} \Pi_s,$$

où chaque Π_i est un plan hyperbolique contenant e_i.

(2.1.2) Commençons par remarquer que dans une décomposition (2.1.1), (i) la somme directe est nécessairement orthogonale, puisque $\operatorname{rad} F = F \cap F^\perp$ est orthogonal à tout-le-monde dans F, et (ii) G est non singulier : pour tout x non nul dans G il existe $y \in F$ tel que $P(x,y) \neq 0$ (sinon x serait dans $\operatorname{rad} F$!), et cet y s'écrit $y' + y''$ selon la décomposition (2.1.1) ; alors $P(x,y') = 0$ puisque $y' \in \operatorname{rad} F$, et donc

$$P(x,y) = P(x,y'') \neq 0 \ \ :$$

$x \notin \operatorname{rad} G = G \cap G^\perp$. (Tout ceci est bien laborieux).
(2.1.3) Terminologie. Complétion non singulière ; plan hyperbolique.
(2.1.4) Écriture sous forme matricielle : un bloc inversible pour le supplémentaire de $\operatorname{rad} F$, et des blocs $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ pour les plans hyperboliques.

(2.1.5) Corollaire. (i) $\dim F + \dim(\operatorname{rad} F) \leqslant \dim E$.
(ii) F totalement singulier $\Rightarrow \dim F \leqslant \frac{1}{2} \dim E$.

(2.1.6) Exercice. S'il existe F totalement singulier de taille $\frac{1}{2}\dim E$, alors q est donnée dans une certaine base par une matrice "antisymplectique".

(2.2) Preuve. Par récurrence sur $s = \dim(\operatorname{rad} F)$.
(2.2.1) Il existe $e \in \big(G \oplus \operatorname{Vect}(e_1, \dots, e_{s-1})\big)^\perp$ tel que $P(e_s, e) = 1$.

Il suffit de prouver qu'il existe un tel e avec $P(e_s, e) \neq 0$. Or $\big(G \oplus \operatorname{Vect}(e_1, \dots, e_{s-1})\big)^\perp \cap e_s^\perp = F^\perp$ est de dimension $n - \dim F < \dim\big(G \oplus \operatorname{Vect}(e_1, \dots, e_{s-1})\big)^\perp = n - \dim F + 1$ puisque q est non dégénérée.
(2.2.2) Je trouve $\lambda \in \mathbf{k}$ tel que $q(e + \lambda e_s) = 0$, et puisque $P(e_s, e_s) = 0$ on a encore $P(e_s, e + \lambda e_s) = 1$. On pose $e'_s := e + \lambda e_s$ et $\Pi_s := \operatorname{Vect}(e_s, e'_s)$, en remarquant au passage que e'_s n'est pas colinéaire à e_s puisque $P(e_s, e'_s) \neq 0$.

Par construction $\Pi_s \perp \big(G \oplus \operatorname{Vect}(e_1, \dots, e_{s-1})\big)$, et donc ces deux sev sont en somme directe puisque Π_s est non singulier (Remarque (1.10)). Toujours puisque Π_s est non singulier, $\Pi_s^\perp$ aussi est non singulier, donc $q_{|\Pi_s^\perp}$ est non dégénérée. On conclut en appliquant l'hypothèse de récurrence à $G \oplus \operatorname{Vect}(e_1, \dots, e_{s-1})$ dans $\Pi_s^\perp$, après avoir vérifié que

$$\operatorname{rad}\big(G \oplus \operatorname{Vect}(e_1, \dots, e_{s-1})\big) = \operatorname{Vect}(e_1, \dots, e_{s-1}) \ \ :$$

$q|_G$ est non dégénérée, et $\operatorname{Vect}(e_1, \dots, e_{s-1})$ est dans le radical. □

(2.3) Lemme. q quelconque. Si x isotrope n'est pas dans $\operatorname{rad} q$, alors il suit de la preuve du théorème de complétion non singulière qu'il existe Π hyperbolique contenant x (en particulier, Π est non singulier).

(2.3.1) Exercice. Pour q quelconque, s'il existe un vecteur isotrope (non nul) en dehors du radical, alors il existe une base de vecteurs isotropes.

(2.4) Application : théorème de Witt. (Pas au programme 2018). *q non dégénérée. On considère deux sev F et F' tels qu'il existe une isométrie $u : (F, q_{|F}) \cong (F', q_{|F'})$. Alors u provient d'une isométrie de E tout entier.*
[preuve manuscrite dans les edit 2013–2014]

Revenir sur l'application à l'homogénéité des quadriques.

3 – Orthogonalisation et classification

3.1 – Formes normales et classification

(3.1) Proposition. Toute FQ possède une base orthogonale.

Preuve. Par récurrence, *sans* l'algorithme de Gauss. Si $q = 0$, c'est trivial ; sinon, il existe x non isotrope. Alors $x^\perp$ est un supplémentaire de $\mathbf{k}.x$ (par exemple parce que $\mathbf{k}.x$ est non singulier et par la Remarque (1.10)), auquel on applique l'hypothèse de récurrence. □

(3.2) Définition. q et q' sont équivalentes s'il existe $\phi \in \mathrm{GL}(E)$ tel que $q' = q \circ \phi$.

(3.2.1) Exercice. Montrer que ceci équivaut encore à chacune des deux conditions suivantes :

(i) pour toute base $\mathcal{B}$ de E, il existe $P \in \mathrm{GL}_n(\mathbf{k})$ (qui dépend de $\mathcal{B}$! au moins *a priori*) telle que
$$\mathrm{Mat}_{\mathcal{B}}\, q' = {}^{\mathsf{T}}P\,(\mathrm{Mat}_{\mathcal{B}}\, q)\, P\,;$$

(ii) il existe $\mathcal{B}$ et $\mathcal{B}'$ telles que
$$\mathrm{Mat}_{\mathcal{B}}\, q = \mathrm{Mat}_{\mathcal{B}'}\, q'.$$

(3.3) Théorème. Les FQ de $\mathbf{C}^n$ sont classifiées par le rang.

(3.4) Théorème (loi d'inertie de Sylvester)**.** On définit la signature d'une FQ q sur $\mathbf{R}^n$ comme étant le couple $\mathrm{sign}(q) = (a, b)$ où
$$a = \sup\bigl\{\dim(F) : q|_F \gg 0\bigr\}, \quad b = \circlearrowleft .$$

Théorème. Deux formes quadratiques q, q' sur $\mathbf{R}^n$ sont équivalentes si et seulement si $\mathrm{sign}(q) = \mathrm{sign}(q')$. De plus, l'ensemble des classes d'équivalences de formes quadratiques sur $\mathbf{R}^n$ est en bijection avec l'ensemble
$$\bigl\{(a,b) \in \mathbf{N}^2 : a + b \leqslant n\bigr\}.$$

(3.5) Classification sur Q. C'est un problème difficile d'arithmétique. C'est le but des quatre premiers chapitres du Cours d'Arithmétique de Serre. La stratégie est de commencer par classifier sur $\mathbf{Q}_p$ au moyen du symbole de Hilbert, puis de localiser sur tous les $\mathbf{Q}_p$.

(3.6) Classification sur $\mathbf{F}_q$, $q = p^r$, $p > 2$. ([H2G2, Vol. I, V.1.4] ; hors programme 2018, mais accessible). *Les FQ sur $\mathbf{F}_q$ sont classifiées par le rang et le discriminant réduit.*

NB : ceci est effectivement la classification sur tous les corps finis !

(3.6.1) Définition. Le discriminant réduit d'une forme quadratique q définie sur $\mathbf{k}$ est la classe du déterminant de “la” matrice de sa restriction à l'orthogonal du radical $(\mathrm{rad}\, q)^\perp$ modulo les carrés. On peut trouver plus confortable de formuler cette définition en termes de l'endomorphisme φ.

Preuve. Il y a exactement deux classes modulo les carrés dans $\mathbf{F}_q^*$: c'est la fameuse suite exacte de groupes
$$1 \to \{\pm 1\} \to \mathbf{F}_q^* \xrightarrow{x \mapsto x^2} \bigl(\mathbf{F}_q^*\bigr)^2 \to 1.$$
[démontrée pour $q = p$ premier dans *ibid.*, mais marche pour $q = p^r$ sans modification]. Soit donc $\zeta \in \mathbf{F}_q^*$ qui n'est pas un carré.

Le procédé d'orthogonalisation fournit une base dans laquelle la matrice de notre FQ est
$$\begin{pmatrix} \mathcal{E} & \\ & 0_{n-r} \end{pmatrix}, \quad \mathcal{E} = \mathrm{diag}(\varepsilon_1, \dots, \varepsilon_r),$$

où chaque ε_i est 0 ou ζ.

Mieux, puisque l'équation $ax^2+by^2 = 1$, $a, b \in \mathbf{F}_q^*$ admet au moins une solution dans $\mathbf{F}_q \times \mathbf{F}_q$ (lemme), on peut supposer $\varepsilon_1 = \cdots = \varepsilon_{r-1} = 1$. Sous cette hypothèse, ε_r est le discriminant réduit de notre forme quadratique. □

(3.6.2) Remarque. Le discriminant de la forme quadratique $ax^2+bxy+cy^2$ est la classe modulo les carrés du déterminant
$$\begin{vmatrix} a & b/2 \\ b/2 & c \end{vmatrix} = \frac{b^2-4ac}{4}.$$

(3.7) Écriture normale d'une forme bilinéaire alternée. *Soit B forme bilinéaire alternée sur un corps $\mathbf{k}$ de caractéristique $\neq 2$. Il existe une base dans laquelle la matrice de B est*
$$\begin{pmatrix} & \mathrm{Id}_p & \\ -\mathrm{Id}_p & & \\ & & 0_{n-2p} \end{pmatrix},$$
et $\mathrm{rg}(B) = 2p$.

Avant de procéder à la preuve, on admire la remarquable uniformité de cet énoncé, valable pour un corps $\mathbf{k}$ (de caractéristique $\neq 2\ldots$) arbitraire, en le comparant aux énoncés précédents valables pour les formes bilinéaires symétriques.

(3.7.1) D'ailleurs, question. Connaissez-vous des corps qui ne sont ni $\mathbf{Q}$ ni $\mathbf{R}$ ni $\mathbf{C}$ ni un corps fini ? la classification sur $\mathbf{k}(X)$ a certainement un intérêt du point de vue de la géométrie algébrique.

Preuve. Par récurrence sur la dimension, suivant la même stratégie que dans le cas symétrique. Si B est nulle, c'est terminé, et sinon il existe e, e' tels que $B(e, e') \neq 0$. On peut s'arranger pour que $B(e, e') = 1$. Puisque B est alternée et $\mathrm{char}(\mathbf{k}) \neq 2$, $B(e, e) = B(e', e') = 0$; ceci implique que les vecteurs e et e' sont linéairement indépendants,

Le plan $\Pi_e = \mathrm{Vect}(e, e')$ est non singulier, donc $\Pi_e^\perp$ est un supplémentaire, auquel on peut appliquer l'hypothèse de récurrence. Ensuite il s'agit juste d'ordonner les vecteurs comme il faut. □

3.2 – Algorithme de Gauss

(3.8) Lemme. $2uv = \dfrac{1}{2}\left[(u+v)^2 - (u-v)^2\right]$;

ceci permet d'orthogonaliser la FQ d'un plan hyperbolique, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 1/2 & 0 \\ 0 & -1/2 \end{pmatrix}$ correspondent à deux FQ équivalentes.

(3.9) Entrée et sortie de l'algorithme. On part de q donnée par sa matrice dans une certaine base $\mathcal{B}$. L'algorithme donne $\ell_1, \ldots, \ell_r$ formes linéaires indépendantes ($r = \mathrm{rg}\, q$) telles que
$$q = \alpha_1 \ell_1^2 + \cdots \alpha_r \ell_r^2 \tag{3.9.1}$$
plus la matrice dans les bases $\mathcal{B}$ et $\mathcal{B}_{\mathrm{can}}(\mathbf{k}^r)$ de $(\ell_1, \ldots, \ell_r) \in \mathcal{L}(E, \mathbf{k}^r)$ sous la forme
$$A = \begin{pmatrix} U_1 & * & & \cdots & * \\ & \ddots & \ddots & & \vdots \\ & & U_q & * \quad \cdots & * \end{pmatrix} \in \mathcal{M}_{r,n}(\mathbf{k}) \tag{3.9.2}$$
quitte à renuméroter les vecteurs de $\mathcal{B}$, où chaque U_i est l'un des deux blocs $\begin{pmatrix} 1 \end{pmatrix}$ ou $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

(3.10) Remarque [H2G2, Vol. I, V.1.3.2]**.** Il n'y a pas d'énoncé d'unicité, les ℓ_i ne sont pas uniquement déterminées, même pas à bricolage avec les α_i près.
Exemple :

$$a(x+by)^2 + b(x-ay)^2 = (a+b)x^2 + (a+b)aby^2.$$

Moralement, c'est le prix à payer pour la facilité déconcertante avec laquelle s'orthogonalisent les FQ : les FQ sont *toutes* orthogonalisables, et c'est un énoncé relativement élémentaire ; il faut comparer cette situation avec la diagonalisabilité des endomorphismes.

(3.11) L'algorithme : description et preuve. Montrons l'existence de formes linéaires ℓ_i vérifiant l'identité (3.9.1) par récurrence sur le nombre n de variables. Si $q = 0$ c'est immédiat, sinon il existe un coefficient $a_{ij} \neq 0$ et on est face à l'alternative suivante :

a) il existe i tel que $a_{ii} \neq 0$, et QARLVJPSQ [3] $i = 1$. On écrit

$$\begin{aligned} q &= a_{11}x_1^2 + 2a_{12}x_1x_2 + \cdots + 2a_{1n}x_1x_n + q(0, x_2, \ldots, x_n) \\ &= a_{11}\underbrace{\Big(x_1 + \frac{a_{21}}{a_{11}}x_2 + \cdots\Big)}_{=:\,\ell_1}{}^2 \underbrace{-\frac{1}{a_{11}}\Big((a_{21}x_2)^2 + \cdots\Big) + q(0, x_2, \ldots, x_n)}_{=:\,q_1(x_2,\ldots,x_n)}, \end{aligned} \tag{3.11.1}$$

et on conclut en appliquant HR à q_1 ;

$\neg$a) sinon, QARLVJPSQ $a_{12} \neq 0$. On écrit

$$\begin{aligned} q &= 2a_{12}x_1x_2 + 2a_{13}x_1x_3 + \cdots + 2a_{23}x_2x_3 + \cdots + q(0, 0, x_3, \ldots, x_n) \\ &= 2a_{12}\underbrace{\big(x_1 + \frac{a_{23}}{a_{12}}x_3 + \cdots\big)}_{=:\,'\ell_1}\underbrace{\big(x_2 + \frac{a_{13}}{a_{12}}x_3 + \cdots\big)}_{=:\,'\ell_2} \\ &\quad \underbrace{-2a_{12}\big(\frac{a_{23}}{a_{12}}x_3 + \cdots\big)\big(\frac{a_{13}}{a_{12}}x_3 + \cdots\big) + q(0, 0, x_3, \ldots, x_n)}_{=:\,q_{12}(x_3,\ldots,x_n)}, \end{aligned}$$

après quoi on conclut en remarquant

$$2a_{12}{}'\ell_1{}'\ell_2 = \frac{a_{12}}{2}\big(\underbrace{'\ell_1 + {}'\ell_2}_{=:\ell_1}\big)^2 - \frac{a_{12}}{2}\big(\underbrace{'\ell_1 - {}'\ell_2}_{=:\ell_2}\big)^2$$

et en appliquant HR à q_{12}.

Si on suit de près la preuve ci-dessus, on voit que la matrice de nos formes linéaires est de la forme (3.9.2). Ceci prouve leur indépendance linéaire, puisque l'on trouve sans grande peine un mineur de taille r non nul dans A.

(3.12) Application à la déduction d'une base orthogonale. On complète A en $\bar{A}$ carrée de taille n inversible en lui accolant (par en dessous) la matrice $\begin{pmatrix} 0 & \mathrm{Id}_{n-r} \end{pmatrix}$ (autrement dit, on pose $\ell_{r+1} = x_{r+1}, \ldots, \ell_n = x_n$).

La base duale $(\ell_1^\vee, \ldots, \ell_n^\vee)$ est orthogonale pour q. $\bar{A}$ est la matrice de $(\ell_1, \ldots, \ell_n) \in \mathcal{L}(E, \mathbf{k}^n)$ dans $\mathcal{B}$ et $\mathcal{B}_{\mathrm{can}}(\mathbf{k}^n)$, donc ${}^{\mathsf{T}}\bar{A}$ contient les colonnes des coordonnées de $\ell_1, \ldots, \ell_n$ dans $\mathcal{B}^\vee$: c'est la matrice de passage de $\mathcal{B}^\vee$ à $(\ell_1, \ldots, \ell_n)$. Ainsi $\bar{A}^{-1}$ est la matrice de passage de $\mathcal{B}$ dans une base orthogonale pour q.
Remarque. Il est facile d'inverser $\bar{A}$.

3. quitte à renuméroter les variables je peux supposer que

(3.13) Application à la factorisation de $\operatorname{Mat} q$**.** On fait l'hypothèse que chaque α_i possède une racine carrée (exemples de conditions suffisantes pour ça : (i) q réelle et définie positive ; (ii) $\mathbf{k}$ algébriquement clos). Alors, quitte à remplacer chaque ℓ_i par $\tilde{\ell}_i = \sqrt{\alpha_i}\ell_i$, on a $q = \tilde{\ell}_1^2 + \cdots \tilde{\ell}_r^2$. De manière correspondante, on obtient une matrice $\tilde{A}$ en multipliant la i-ème ligne de A par $\sqrt{\alpha_i}$ pour tout $i = 1, \ldots, r$. (Exercice : écrire ceci matriciellement).

Alors $\operatorname{Mat}_{\mathcal{B}} q = {}^{\mathsf{T}}\tilde{A}\,\tilde{A}$. En effet,

$$P(x, y) = \tilde{\ell}_1(x)\tilde{\ell}_1(y) + \cdots + \tilde{\ell}_r(x)\tilde{\ell}_r(y) = {}^{\mathsf{T}}(\tilde{A}X) \times \tilde{A}Y.$$

NB : i) inutile de déterminer la base orthogonale, connaître sa duale suffit ;
ii) $\tilde{A}$ n'a pas besoin d'être carrée.

(3.14) Décomposition de Cholesky. *Toute matrice symétrique réelle définie positive s'écrit de manière unique* ${}^{\mathsf{T}}T\,T$ *avec* T *triangulaire supérieure dont tous les coefficients diagonaux sont* > 0.

La condition sur les coefficients diagonaux est là pour assurer l'unicité. On voit en suivant la construction qu'il y a effectivement plusieurs factorisations possibles sinon.

Preuve. L'existence est un corollaire de (3.13). Dans ce cas, on est sûr de ne jamais avoir de bloc 2×2 sur la diagonale de A, car ceux-ci induisent des -1 dans l'écriture réduite de Sylvester. De même on est sûr de ne pas avoir à renuméroter pour avoir la forme triangulaire, car le coefficient devant x_i^2 ne fait que décroître au cours de l'algorithme.

Il vaut peut-être mieux se convaincre par une petite récurrence. On reprend celle de (3.9). Pour une FQ $\gg 0$, on est toujours dans le cas a) et on peut choisir le i qu'on veut puisque

$$a_{ii} = q(0, \ldots, i, \ldots, 0) > 0$$

pour $i = 1, \ldots, n$. Il s'agit de voir que la forme q_1 à laquelle on va appliquer HR est elle aussi définie positive. Par définition, on a pour tous $(x_2, \ldots, x_n) \in \mathbf{k}^{n-1}$ et $x_1 \in \mathbf{k}$

$$q_1(x_2, \ldots, x_n) = q(x_1, x_2, \ldots, x_n) - a_{11}\big(\ell_1(x_1, x_2, \ldots, x_n)\big)^2 \in \mathbf{k}[x_2, \ldots, x_n].$$

Puisque $\ell_1 = x_1 + \cdots$, on a pour tout $(x_2, \ldots, x_n) \in \mathbf{k}^{n-1}$

$$\ell_1\big(-\ell_1(0, x_2, \ldots, x_n), x_2, \ldots, x_n\big) = 0.$$

Ainsi, pour tout $(x_2, \ldots, x_n) \in \mathbf{k}^{n-1}$,

$$q_1(x_2, \ldots, x_n) = q\big(-\ell_1(0, x_2, \ldots, x_n), x_2, \ldots, x_n\big) > 0$$

donc q_1 est définie positive comme il fallait.

Au fond ce qui fait marcher le truc c'est que $q = \alpha_1\ell_1^2 + \cdots + \alpha_r\ell_r^2$ avec tous les $\alpha_i > 0$, et donc

$$q_1 = q - \alpha_1\ell_1^2 = \alpha_2\ell_2^2 + \cdots + \alpha_r\ell_r^2$$

est définie positive !

Pour l'unicité, si ${}^{\mathsf{T}}T_1T_1 = {}^{\mathsf{T}}T_2T_2$ alors ${}^{\mathsf{T}}T_2^{-1}\,{}^{\mathsf{T}}T_1 = T_2\,T_1^{-1}$. Cette matrice est à la fois triangulaire supérieure et inférieure, donc diagonale. D'autre part, elle est égale à son inverse, puisque

$${}^{\mathsf{T}}T_2^{-1}\,{}^{\mathsf{T}}T_1 = {}^{\mathsf{T}}(T_1T_2^{-1}) = {}^{\mathsf{T}}(T_2T_1^{-1})^{-1} = (T_2T_1^{-1})^{-1}$$

(pour la dernière égalité, on utilise la diagonalité qu'on vient d'établir). Ses coefficients diagonaux sont donc tous ± 1, et en fait tous $+1$ puisque strictement positifs. Finalement $T_2T_1^{-1} = \mathrm{Id}_n$, et l'unicité est prouvée. □

Si on préfère on peut imposer les coefficients diagonaux tous strictement négatifs, et ça marche tout pareil.

4 – Orthogonalisation simultanée

4.1 – Critère pour l'orthogonalisabilité simultanée

(4.1) Théorème. *On suppose q non dégénérée. Alors :*
q et q' simultanément orthogonalisables $\Leftrightarrow$ $\varphi^{-1}\varphi'$ diagonalisable.

(4.2) Remarque. Pour $\lambda \in \mathbf{k}$, $\ker(\lambda \mathrm{id} - \varphi^{-1}\varphi') = \ker(\lambda\varphi - \varphi')$ puisque φ injective, donc en pratique il est inutile (donc nuisible) d'inverser φ.

(4.3) Remarque. $\varphi^{-1}\varphi'$ est auto-adjoint relativement à q (et il n'aurait aucun sens de parler d'auto-adjonction relativement à q', cette dernière pouvant être dégénérée).
En effet, pour $x, y \in E$,

$$P\big(\varphi^{-1}\varphi'(x), y\big) = \varphi\big(\varphi^{-1}\varphi'(x)\big)(y) = \varphi'(x)(y) = \varphi'(y)(x) = P\big(x, \varphi^{-1}\varphi'(y)\big).$$

Variante :

$$(\varphi^{-1}\varphi')^* = \varphi^{-1\mathsf{T}}(\varphi^{-1}\varphi')\varphi = \varphi^{-1\mathsf{T}}(\varphi')^{\mathsf{T}}(\varphi^{-1})\varphi = \varphi^{-1}(\varphi')(\varphi^{-1})\varphi = \varphi^{-1}\varphi'.$$

□

(4.4) Attention. Hors du cadre euclidien, un endomorphisme auto-adjoint n'est pas nécessairement diagonalisable, *cf.* Exemple (4.10.3).

Preuve du Théorème (4.1). '$\Rightarrow$' est immédiat. Pour voir '$\Leftarrow$', on commence par constater que les sous-espaces propres sont en somme directe orthogonale relativement à q : pour $e_i \in E_{\lambda_i}$, $i = 1, 2$, $\lambda_1 \neq \lambda_2$, on a

$$\lambda_1\varphi(e_1)(e_2) = \varphi'(e_1)(e_2) = \varphi'(e_2)(e_1) = \lambda_2\varphi(e_2)(e_1),$$

et donc $\lambda_1 P(e_1, e_2) = \lambda_2 P(e_2, e_1)$ ce qui impose $P(e_1, e_2) = 0$ par symétrie (on a aussi utilisé la symétrie dans le petit calcul).

On en déduit qu'ils sont aussi orthogonaux relativement à q', par le suivant calcul : pour $e_1, e_2 \in E_{\lambda_1}, E_{\lambda_2}$,

$$P'(e_1, e_2) = \varphi'(e_1)(e_2) = \lambda_1\varphi(e_1)(e_2) = 0.$$

Ensuite on sait qu'il est possible d'orthogonaliser chaque $q_{|E_\lambda}$ (voire mieux dans certains cas...). C'est suffisant, puisque

$$E = E_{\lambda_1} \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} E_{\lambda_r}$$

et $q'|_{E_\lambda} = \lambda\, q|_{E_\lambda}$. □

4.2 – Applications aux pinceaux de quadriques complexes

(4.5) Nombre de quadriques dégénérées dans un pinceau. (Exercice [MG99, IV.3], à ne pas poser). On suppose toujours q non dégénérée, et pour une fois $\dim E = n+1$ (c'est pour la bonne cause). Montrer l'équivalence des deux propositions suivantes :

(i) l'ensemble des scalaires λ tels que la FQ $\lambda q - q'$ soit dégénérée a $n+1$ éléments ;
(ii) il existe $\mathcal{B}$ base de E et $\lambda_0, \ldots, \lambda_n$ deux à deux distincts tels que

$$q(x) = x_0^2 + x_1^2 + \cdots + x_n^2 \quad \text{et} \quad q'(x) = \lambda_0 x_0^2 + \lambda_1 x_1^2 + \cdots + \lambda_n x_n^2$$

$((x_0, \ldots, x_n) = \mathcal{B}^\vee)$.

(4.6) Nombre de points d'intersection de deux coniques. Si j'ai une conique dans $\mathbf{k}^2$ d'équation

$$a + 2bx + 2cy + dx^2 + 2exy + fy^2 = 0,$$

je lui associe la forme quadratique donnée par la matrice symétrique

$$\begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix}$$

(autrement dit, $q(x, y, t) = at^2 + 2bxt + 2cyt + dx^2 + 2exy + fy^2$). Les points de la conique correspondent aux droites isotropes de la forme quadratique (en fait, il y a un peu plus de ces derniers... les droites correspondant à des points affines sont celles avec un vecteur directeur $(x, y, 1)$).

Si j'ai deux coniques, je cherche à les orthogonaliser simultanément. Si j'y arrive, il est facile de calculer l'intersection de leurs cônes isotropes. On en déduit les points d'intersection des coniques de départ. Il y en a toujours 4, cas particulier du théorème de Bezout.

Moralité : le passage au projectif simplifie les choses, et transforme de l'affine moche en du linéaire joli !

4.3 – Le cas euclidien

(4.7) Corollaire. *Si q est définie positive, alors toute FQ q' est orthogonalisable en base orthonormée pour q.*

$\varphi^{-1}\varphi'$ étant auto-adjoint relativement à q, c'est une conséquence directe du Théorème (4.1) précèdent et du théorème suivant.

(4.8) Théorème. *Tout endomorphisme auto-adjoint relativement à une forme quadratique q définie positive est diagonalisable en base orthonormale pour q.*

(4.9) Remarque. L'hypothèse "q définie positive" sert à dire que les endomorphismes auto-adjoints sont ceux qui ont une matrice symétrique dans une base orthonormée pour q. Être bien attentif au lien entre matrices symétriques et endomorphismes auto-adjoints...

En général, la propriété vérifiée par la matrice d'un endomorphisme autoadjoint est donnée par la formule (1.9.1).

(4.10) Lemme. *En dimension $n \leqslant 2$, toute matrice symétrique réelle est diagonalisable.*

Preuve. C'est immédiat pour $n \leqslant 1$. Montrons donc que toute matrice

$$A = \begin{pmatrix} a & c \\ c & b \end{pmatrix}, \quad a, b, c \in \mathbf{R}$$

est diagonalisable. Le polynôme caractéristique est

$$\chi = (X - a)(X - b) - c^2. \tag{4.10.1}$$

Si $c = 0$, il est évident que A est diagonalisable, et sinon $c^2 > 0$, donc χ possède deux racines réelles distinctes (oui, même si $a = b$!). Pour le voir, on fait un dessin, puis on applique deux TVI entre $-\infty$ et a puis entre a et $+\infty$ pour respecter les normes européennes. □

(4.10.2) Remarque. On a seulement démontré “diagonalisable”, pas “diagonalisable en BON”. En fait, si les deux vap sont distinctes, toute base diagonalisante est orthogonale par l'argument du (4.1), et il est ensuite facile d'en déduire une base diagonalisante orthonormée. S'il y a une seule vap, la preuve montre que notre matrice est $\lambda \mathrm{Id}_2$, auquel cas le résultat est clair.

(4.10.3) Exemple. Si on autorise c à devenir complexe, on peut faire en sorte que χ comme en (4.10.1) ait seulement une racine double. Alors A possède une seule valeur propre, donc elle est diagonalisable ssi c'est une homothétie. On obtient ainsi une matrice symétrique complexe qui n'est pas diagonalisable.

Voici le bricolage : il faut avoir c^2 égal à la valeur minimale prise par $(x-a)(x-b)$. La dérivée s'annule en $(a+b)/2$ (milieu du segment $[a,b]$!), où le produit prend la valeur $-(a-b)^2/4$. Par exemple, le polynôme caractéristique de

$$\begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix}$$

est à racine double (d'ailleurs, c'est X^2), et cette matrice (qui n'est pas une homothétie) n'est pas diagonalisable.

(4.11) Lemme. *Soit u auto-adjoint relativement à $q \gg 0$. Pour tout F stable par u, $F^\perp$ est un supplémentaire stable. Les restrictions de u à F et $F^\perp$ sont auto-adjointes (relativement à $q|_F$ et $q|_{F^\perp}$ respectivement.*

On remarque au passage que la définie positivité se restreint bien, contrairement à la non dégénérescence : tout sous-espace d'un espace euclidien est encore euclidien. De même, on a toujours un orthogonal canonique (une fois la structure euclidienne choisie), en la personne de l'orthogonal. C'est un point agréable de la dualité par rapport à un produit scalaire euclidien vis-à-vis de la dualité vecteurs/formes linéaires.

Preuve du Théorème (4.8). Soit donc $q \gg 0$ et u auto-adjoint relativement à q. On veut montrer que u est diagonalisable en base orthonormée. On commence par remarquer qu'il suffit de diagonaliser en base orthogonale, puisqu'il est ensuite facile de déduire une BON diagonalisante (en multipliant chacun des vecteurs par le scalaire non nul adéquat).

On procède par récurrence sur $n = \dim E$. Pour cela, montrons que u possède un vecteur propre. Soit $R \in \mathbf{R}[X]$ facteur irréductible de μ, polynôme minimal de u, et $K_R = \ker R(u)$ (sev non réduit à $\{0\}$ par minimalité). Soit $x \in K_R - \{0\}$. Le polynôme minimal local en x, μ_x, divise R et est non constant, donc $\mu_x = R$. On a donc (notant comme d'habitude F_x le sous-espace cyclique associé à x)

$$1 \leqslant \dim F_x = \deg \mu_x = \deg R \leqslant 2,$$

la dernière inégalité étant donnée par le fait que R est un irréductible de $\mathbf{R}[X]$.

D'après le Lemme (4.10), u_{F_x} est diagonalisable en base orthonormée pour $q|_{F_x}$. En effet, il suit du Lemme (4.11) que u_{F_x} est auto-adjoint relativement à $q|_{F_x} \gg 0$, ce qui implique que sa matrice dans une BON est symétrique.

On conclut grace au Lemme (4.11) : $F_x^\perp$ est un supplémentaire de F_x stable par u, et puisque $u_{F_x^\perp}$ est auto-adjoint relativement à $q|_{F_x^\perp} \gg 0$ on peut lui appliquer l'hypothèse de récurrence. On conclut en remarquant que la concaténation de deux bases orthonormales pour $q|_{F_x}$ et $q|_{F_x^\perp}$ respectivement est une base orthonormale pour q. □

4.4 – Pour aller plus loin

(4.12) Théorème [Hodge–Pedoe, Book IV, Chap. XIII, §10, Thm. I]**.** *Soit q, q' deux formes quadratiques, q non-dégénérée. Soit A, A' deux matrices symétriques. Il existe une base dans* *laquelle les matrices de q et q' sont A et A' si et seulement si*

$$\mathrm{Mat}_{\mathcal{B}}(q') - X.\,\mathrm{Mat}_{\mathcal{B}}(q) \quad et \quad A' - X.A$$

sont équivalentes comme matrices à coefficients dans $\mathbf{k}[X]$.

(4.13) Corollaire [Hodge–Pedoe, Book IV, Chap. XIII, §10, Thm. II]**.** *Si les facteurs invariants de $\mathrm{Mat}_{\mathcal{B}}(q') - X.\,\mathrm{Mat}_{\mathcal{B}}(q)$ sont $(X-\lambda_1)^{e_1}, \ldots, (X-\lambda_r)^{e_r}$ (si $\mathbf{k}$ est algébriquement clos, c'est le cas général), alors il existe une base dans laquelle q et q' sont données par les matrices par blocs*

$$\begin{pmatrix} Q_{e_1} & & \\ & \ddots & \\ & & Q_{e_r} \end{pmatrix} \quad et \quad \begin{pmatrix} P_{e_1}(\lambda_1) & & \\ & \ddots & \\ & & P_{e_r}(\lambda_r) \end{pmatrix},$$

où

$$Q_e = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix} \quad et \quad P_e(\lambda) = \begin{pmatrix} & & & \lambda \\ & & \iddots & 1 \\ & \iddots & \iddots & \\ \lambda & 1 & & \end{pmatrix}$$

($e \times e$ toutes les deux).

(4.13.1) Remarque. Les matrices Q_e et P_e sont des blocs de Jordan, sauf qu'on s'est arrangé pour qu'elles soient symétriques !

(4.14) Exemple.
(4.14.1) On considère les deux formes quadratiques

$$q(x,y,z) = x^2 - yz \qquad \text{et} \qquad q'(x,y,z) = x^2 - yz + y^2.$$

Ce sont les équations des adhérences projectives des deux coniques affines $x^2 - y = 0$ et $x^2 - y + y^2 = 0$ qui se rencontrent en un seul point avec multiplicité 4 (l'origine de l'espace affine, ou le point projectif $(0:0:1)$).

Dans ce cas on trouve les facteurs invariants $X-1$ et $(X-1)^2$, donc on doit pouvoir mettre q et q' sous la forme

$$\begin{pmatrix} 1 & & \\ & 0 & 1 \\ & 1 & 0 \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} 1 & & \\ & 1 & 1 \\ & 1 & 0 \end{pmatrix}$$

respectivement. Et effectivement, on a

$$q(x,y,z) = \xi^2 + 2\eta\zeta \qquad \text{et} \qquad q'(x,y,z) = \xi^2 + \eta^2 + 2\eta\zeta$$

pour $\xi = x$, $\eta = y$ et $\zeta = -\frac{1}{2}z$.
(4.14.2) À présent on considère les deux formes quadratiques

$$q(x,y,z) = x^2 - yz \qquad \text{et} \qquad q''(x,y,z) = x^2 - yz + xy.$$

Elles correspondent aux deux coniques affines $x^2 - y = 0$ et $x^2 - y + xy = 0$ qui se rencontrent avec multiplicité 3 à l'origine.

Dans ce cas on trouve le facteur invariant $(X-1)^3$, donc on doit pouvoir mettre q et q'' sous la forme

$$\begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} & & 1 \\ & 1 & 1 \\ 1 & 1 & \end{pmatrix}$$

respectivement. Et effectivement, on a

$$q(x,y,z) = 2\xi\zeta + \eta^2 \qquad \text{et} \qquad q(x,y,z) = 2\xi\zeta + \eta^2 + 2\eta\zeta$$

pour $\xi = -z$, $\eta = x$ et $\zeta = \frac{1}{2}y$.

Il existe des énoncés de réduction pour le cas où les deux formes quadratiques sont dégénérées. Je ne les donne pas ici, ils se trouvent dans [Hodge–Pedoe].

Références

[Berger] Marcel Berger, *Géométrie*, CEDIC 1977, réédition Cassini.

[H2G2] Philippe Caldero et Jérôme Germoni, *(Nouvelles) Histoires hédonistes de groupes et de géométries*, Calvage & Mounet, (2017) 2015.

[Hodge–Pedoe] W. Hodge and D. Pedoe, *Methods of Algebraic Geometry*, Cambridge University Press, 1953.

[MG99] *Composition de mathématiques générales*, session de 1999, concours de l'agrégation externe de mathématiques.