Algèbre linéaire et géométrie pour le CAPES[1]

Olivier DEBARRE

[1]Version très préliminaire

Table des matières

CHAPITRE 1

Espaces vectoriels et applications linéaires

1. Définitions

Espace vectoriel, sous-espace vectoriel.

Exemples : $\mathbf{R}^n$, plan et droites dans $\mathbf{R}^3$.

Intersection de sous-espaces vectoriels, sous-espace vectoriel engendré par une partie S comme intersection des sous-espaces contenant S ou comme ensemble des combinaisons linéaires d'éléments de S.

Somme de sous-espaces vectoriels comme sous-espace vectoriel engendré par la réunion ou comme ensemble de sommes d'éléments de chaque sous-espace vectoriel.

Somme directe, exemples dans $\mathbf{R}^3$.

2. Applications linéaires

Définition, image, noyau (exemple avec équations dans $\mathbf{R}^3$). Exemples : symétries et projections.

3. Bases

Famille génératrice, libre ; base. Théorèmes fondamentaux sur l'existence des bases.

Formule du rang, formule de Grassmann.

CHAPITRE 2

Réduction des endomorphismes

Dans tout ce chapitre, u désigne un endomorphisme d'un espace vectoriel E non nul de dimension $n > 0$ sur un corps $\mathbf{k}$.

Le but de la théorie de la réduction des endomorphismes est de trouver une base de E dans laquelle la matrice de u soit « la plus simple possible ». Il y a bien sûr plusieurs façons de comprendre cette expression, et donc différents types de réduction.

Du point de vue matriciel, cela revient, étant donnée une matrice carrée M, à trouver une matrice inversible P telle que $P^{-1}MP$ soit « la plus simple possible ».

1. Sous-espaces stables

Un sous-espace vectoriel F de E est stable u si l'image par u de tout point de F est encore dans F. On écrit $u(F) \subset F$. C'est une notion très importante.

Si F est un sous-espace stable de E et que G est un supplémentaire de F dans E, c'est-à-dire que l'on a $E = F \oplus G$, la matrice de u dans une base de E constituée de la réunion d'une base $\mathscr{B}_F$ de F et d'une base $\mathscr{B}_G$ de G est « triangulaire supérieure par blocs », c'est-à-dire de la forme

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$$

où A est la matrice dans la base $\mathscr{B}_F$ de la restriction de u à F. La détermination d'un sous-espace stable est donc déjà le début d'une réduction de u.

Si on peut trouver un supplémentaire G qui est aussi stable par u (mais ce n'est pas toujours possible), on a $B = 0$ dans la matrice ci-dessus, qui est donc de la forme

$$\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}$$

On dit qu'elle est « diagonale par blocs ». On peut donc préciser l'objectif de la réduction : trouver une décomposition de E en somme directe de sous-espaces stables par u tels que la restriction de u à chacun de ces sous-espaces (correspondant à chacun des « blocs ») soit « la plus simple possible ».

Exercice 1. Trouver une droite de $\mathbf{R}^2$ stable par l'endomorphisme u défini par
$$u(x,y) = (x, x+y)$$
Admet-elle un supplémentaire stable ?

2. Sous-espaces propres et polynôme caractéristique

L'endomorphisme le plus simple est une homothétie. Suivant le principe ci-dessus, on cherche un sous-espace de E sur lequel u est une homothétie de rapport $\lambda \in \mathbf{k}$. Dans ce but, on définit, pour chaque $\lambda \in \mathbf{k}$, l'*espace propre* de u associé par
$$E_\lambda = \operatorname{Ker}(u - \lambda \operatorname{Id}_E)$$
C'est un sous-espace vectoriel stable de E sur lequel u est l'homothétie de rapport λ. Un élément de E_λ s'appelle un *vecteur propre* de u (pour la valeur propre λ). Pour des raisons techniques, on suppose souvent un vecteur propre non nul (de sorte que la valeur propre associée est bien déterminée). Les *valeurs propres* de u sont les éléments λ de $\mathbf{k}$ pour lesquels existe un vecteur propre (non nul). C'est le cas si et seulement si l'endomorphisme $u - \lambda \operatorname{Id}_E$ n'est pas injectif, ou encore pas bijectif, vu que l'on est en dimension finie. Les valeurs propres de u sont donc les racines dans $\mathbf{k}$ du *polynôme caractéristique*
$$\chi_u(X) = \operatorname{dét}(X \operatorname{Id}_E - u)$$
polynôme unitaire de degré n à coefficients dans $\mathbf{k}$. Pratiquement, on calcule donc les valeurs propres en cherchant les racines du polynôme caractéristique. Lorsque $\mathbf{k} = \mathbf{C}$, il existe toujours des valeurs propres (puisqu'on a supposé $n > 0$).

La *multiplicité* de la valeur propre λ est par définition sa multiplicité comme racine de χ_u.

Exercice 2. L'endomorphisme u de $\mathbf{R}^2$ défini par
$$u(x,y) = (y, -x)$$
a-t-il des valeurs propres ?

Les espaces propres sont en somme directe, mais leur somme n'est E que si u est diagonalisable. Par exemple, la seule valeur propre de la matrice carrée

$$U_s = \begin{pmatrix} 0 & 1 & 0 & \cdots & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 \end{pmatrix} \tag{1}$$

est 0, et l'espace propre associé est de dimension 1.

Exercice 3. Montrer que l'endomorphisme de $\mathbf{k}^n$ de matrice

$$\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$$

dans la base canonique est diagonalisable en déterminant ses valeurs propres et ses espaces propres.

3. Trigonalisation

On dit que u est *trigonalisable* s'il existe une base de E dans laquelle sa matrice est triangulaire supérieure.

Exercice 4. Montrer qu'il existe une base dans laquelle la matrice d'un endomorphisme trigonalisable est triangulaire inférieure.

Théorème 1. *Un endomorphisme est trigonalisable si et seulement si son polynôme caractéristique est scindé dans* $\mathbf{k}$.

En particulier, lorsque $\mathbf{k} = \mathbf{C}$, tout endomorphisme est trigonalisable.

Démonstration. On procède par récurrence sur la dimension n de E. Il existe par hypothèse une racine λ dans $\mathbf{k}$ du polynôme caractéristique, c'est-à-dire une valeur propre. Soit e un vecteur propre associé, soit E_1 la droite vectorielle engendrée par e et soit E_2 un supplémentaire de E_1 dans E. On est dans la situation évoquée plus haut : la matrice de u dans une base de E constituée de e et d'une base de E_2 est « triangulaire supérieure par blocs » du type

$$\begin{pmatrix} \lambda & B \\ 0 & D \end{pmatrix}$$

On peut appliquer l'hypothèse de récurrence à l'endomorphisme de E_2 de matrice D : dans une base convenable de E_2, sa matrice est triangulaire supérieure. Si on ajoute e à cette base, on obtient une base de E dans laquelle la matrice de u est triangulaire supérieure. $\square$

Exercice 5. Soit u un endomorphisme *nilpotent* de E, c'est-à-dire tel qu'il existe un entier $r > 0$ tel que $u^r = 0$.

(a) Montrer que u n'est pas injectif.

(b) Montrer qu'il existe une base de E dans laquelle la matrice de u est de la forme $\begin{pmatrix} 0 & B \\ 0 & D \end{pmatrix}$, où D est une matrice carrée d'ordre $n-1$.

(c) Montrer que la matrice D est nilpotente.

(d) Montrer par récurrence sur n qu'il existe une base dans laquelle la matrice de u est triangulaire supérieure avec des 0 sur la diagonale. Déterminer le polynôme caractéristique de u.

(e) Montrer $u^n = 0$.

4. Polynôme minimal

Si $P(X) = a_0 + a_1X + \cdots + a_rX^r$ est un polynôme à coefficients dans $\mathbf{k}$, on note $P(u)$ l'endomorphisme $a_0 \operatorname{Id}_E + a_1u + \cdots + a_ru^r$ de E. On définit ainsi un morphsime de $\mathbf{k}$-algèbres

$$\begin{array}{rccc} \varphi_u : & \mathbf{k}[X] & \longrightarrow & \operatorname{End}(E) \\ & P & \longmapsto & P(u) \end{array}$$

Cela signifie que l'on a $(P+Q)(u) = P(u) + Q(u)$ et $(PQ)(u) = P(u) \circ Q(u)$. L'espace vectoriel $\operatorname{End}(E)$ des endomorphismes de E étant de dimension finie n^2, la famille $\{\operatorname{Id}_E, u, u^2, \ldots, u^{n^2}\}$ est liée. Il existe donc un polynôme non nul P (de degré au plus n^2) tel que $P(u) = 0$. En d'autres termes, le morphisme φ_u n'est pas injectif. Son noyau est un idéal non nul de l'anneau principal $\mathbf{k}[X]$ donc est engendré par un polynôme unitaire uniquement déterminé, que l'on appelle le *polynôme minimal* de u, et que l'on notera μ_u. C'est le polynôme unitaire de plus petit degré qui annule u. Il est toujours de degré > 0 (car $E \neq 0$).

Exemples 1. (1) Le polynôme minimal de l'homothétie $\lambda \operatorname{Id}_E$ est $X - \lambda$; en particulier, le polynôme minimal de l'endomorphisme nul est X.

(2) On définit de façon analogue le polynôme minimal d'une matrice carrée M à coefficients dans $\mathbf{k}$. Notons que le polynôme minimal de M reste le polynôme minimal de la matrice M vue comme matrice à coefficients dans n'importe quel corps contenant $\mathbf{k}$. Cela résulte du fait que le degré du polynôme minimal est le rang de la famille $\{M^r\}_{r\in\mathbf{N}}$.

Exercice 6. Montrer que si u est nilpotent, son polynôme minimal est X^s, avec $s \leqslant n$ (utiliser l'exercice 5.(e)).

Lemme 1. *Les valeurs propres de u sont exactement les racines dans $\mathbf{k}$ de son polynôme minimal.*

Démonstration. Soit $\lambda \in \mathbf{k}$; en substituant u à X dans la division euclidienne $\mu_u(X) = Q(X)(X - \lambda) + \mu_u(\lambda)$, on obtient

$$0 = \mu_u(u) = Q(u) \circ (u - \lambda \operatorname{Id}_E) + \mu_u(\lambda) \operatorname{Id}_E \tag{2}$$

Si λ est valeur propre de u, on a $u(x) = \lambda x$ pour un vecteur propre (non nul) x. Si on applique l'égalité (2) à x, on obtient

$$0 = Q(u)\big((u - \lambda \operatorname{Id}_E)(x)\big) + \mu_u(\lambda)x = \mu_u(\lambda)x$$

de sorte que $\mu_u(\lambda) = 0$.

Inversement, si $\mu_u(\lambda) = 0$, on a $Q(u) \circ (u - \lambda \operatorname{Id}_E) = 0$ grâce à (2). Comme Q est non nul et de degré strictement inférieur à μ_u, on a $Q(u) \neq 0$, donc $u - \lambda \operatorname{Id}_E$ n'est pas bijectif : λ est bien valeur propre de u. □

Si u est diagonalisable, de valeurs propres distinctes $\lambda_1, \ldots, \lambda_r$, son polynôme minimal est

$$\mu_u(X) = (X - \lambda_1) \cdots (X - \lambda_r)$$

Il est donc scindé à racines simples. Nous verrons plus bas que la réciproque est vraie.

Exercice 7. Quels sont les endomorphismes nilpotents diagonalisables ?

5. Espaces caractéristiques

On suppose dans tout ce numéro que le polynôme minimal de u est *scindé* sur $\mathbf{k}$ (c'est le cas par exemple si $\mathbf{k} = \mathbf{C}$). Il se décompose donc en produit de facteurs linéaires

$$\mu_u(X) = \prod_{\lambda \in \mathbf{k}} (X - \lambda)^{q_\lambda} \qquad \text{avec } q_\lambda \in \mathbf{N}.$$

On définit alors l'*espace caractéristique* associé à λ par

$$E'_\lambda = \operatorname{Ker}(u - \lambda \operatorname{Id}_E)^{q_\lambda}$$

Il contient l'espace propre E_λ.

Lemme 2. *Si u et v sont des endomorphsimes qui commutent, le noyau et l'image de v sont stables par u.*

Démonstration. Si x est dans le noyau de v, on a $v(x) = 0$, donc $u(v(x)) = 0$. Comme u et v commutent, on a donc $v(u(x)) = 0$, ce qui signifie que $u(x)$ est dans le noyau de v. On a donc $u(\operatorname{Ker} v) \subset \operatorname{Ker}(v)$.

Si y est dans l'image de v, il existe x tel que $y = v(x)$. On a $u(y) = u(v(x)) = v(u(x))$, ce qui sgnifie que $u(y)$ est dans l'image de v. On a donc $u(\operatorname{Im} v) \subset \operatorname{Im}(v)$. □

Pour tout polynôme P, le noyau et l'image de $P(u)$ sont donc stables par u. En particulier, *les espaces caractéristiques sont stables par u.*

Lemme 3 (Lemme des noyaux). *Soient $P_1, \ldots, P_m$ des polynômes premiers entre eux deux à deux. On pose $P = P_1 \cdots P_m$.*

(1) *On a* $\operatorname{Ker} P(u) = \operatorname{Ker} P_1(u) \oplus \cdots \oplus \operatorname{Ker} P_m(u)$.
(2) *Les projections* $\operatorname{Ker} P(u) \to \operatorname{Ker} P_i(u) \subset \operatorname{Ker} P(u)$ *relatives à cette décomposition en somme directe sont des polynômes en u.*

Démonstration. On procède par récurrence sur m. Il suffit donc de traiter le cas $m = 2$. Le théorème de Bézout entraîne l'existence de polynômes A_1 et A_2 tels que

$$1 = A_1P_1 + A_2P_2$$

Si $x \in \operatorname{Ker} P_1(u) \cap \operatorname{Ker} P_2(u)$, on a $P_1(u)(x) = P_1(u)(x) = 0$, d'où

$$x = A_1(u)(x)P_1(u)(x) + A_2(u)(x)P_2(u)(x) = 0$$

D'autre part, $\operatorname{Ker} P_i(u)$ est contenu dans $\operatorname{Ker} P(u)$. Si $x \in \operatorname{Ker} P(u)$, on a

$$x = \underbrace{P_1(u)\big(A_1(u)(x)\big)}_{\in \operatorname{Ker} P_2(u)} + \underbrace{P_2(u)\big(A_2(u)(x)\big)}_{\in \operatorname{Ker} P_1(u)}$$

donc $E = \operatorname{Ker} P_1(u) + \operatorname{Ker} P_2(u)$. Ceci montre (1). De plus, la projection sur $\operatorname{Ker} P_1(u)$ est, sur $\operatorname{Ker} P(u)$, égale à $(A_2P_2)(u)$, et celle sur $\operatorname{Ker} P_2(u)$ à $(A_1P_1)(u)$, ce qui prouve (2). □

Comme, par définition, $\mu_u(u) = 0$, et que les polynômes $(X - \lambda)^{q_\lambda}$ sont premiers entre eux deux à deux, le lemme des noyaux entraîne que les espaces caractéristiques sont en somme directe, et que leur somme est E :

$$E = \operatorname{Ker} \mu_u(u) = \bigoplus_\lambda \operatorname{Ker}(u - \lambda \operatorname{Id}_E)^{q_\lambda} = \bigoplus_\lambda E'_\lambda$$

De plus, à une telle décomposition correspond pour chaque λ une projection $\pi_\lambda : E \to E$ d'image E'_λ qui est un polynôme en u, ce qui nous servira plus tard.

On a donc décomposé E en somme directe de sous-espaces vectoriels stables par u. En termes matriciels, cela signifie que dans une base constituée de la réunion de bases des espaces caractéristiques, la matrice de u est *diagonale par blocs.*

La structure de u sur chaque espace propre E_λ est particulièrement simple : c'est l'homothétie de rapport λ. Seulement, la somme des espaces propres n'est en général pas tout l'espace ; on ne peut donc décrire u complètement à l'aide des espaces propres.

Les espaces caractéristiques sont « plus gros » : leur somme est tout l'espace. En revanche, la structure de u sur un espace caractéristique E'_λ est plus compliquée : c'est la somme de l'homothétie de rapport λ et de l'endomorphisme *nilpotent* de E'_λ induit par $u - \lambda \operatorname{Id}_E$.

Le polynôme caractéristique de ce dernier est $X^{\dim(E'_\lambda)}$ (exerc. 5.(d)). Le polynôme caractéristique de la restriction de u à E'_λ est donc $(X - \lambda)^{\dim(E'_\lambda)}$. Comme on peut le voir en utilisant la matrice diagonale par blocs évoquée plus haut, le polynôme caractéristique de u est donc $\prod_\lambda (X - \lambda)^{\dim(E'_\lambda)}$. Par conséquent, *la dimension de l'espace caractéristique E'_λ est la multiplicité de la valeur propre λ.*

Enfin, le polynôme $X^{\dim(E'_\lambda)}$ annule la restriction de $u - \lambda \operatorname{Id}_E$ à E'_λ (exerc. 6), donc le polynôme $(X - \lambda)^{\dim(E'_\lambda)}$ annule la restriction de u à E'_λ, donc le polynôme

$\chi_u(X) = \prod_\lambda (X-\lambda)^{\dim(E'_\lambda)}$ annule u. On en déduit le théorème de Hamilton–Cayley : *le polynôme caractéristique est annulateur,* ou encore *le polynôme minimal divise le polynôme caractéristique*[1].

Proposition 1. *Les propriétés suivantes sont équivalentes :*
(i) *l'endomorphisme u est diagonalisable sur* $\mathbf{k}$ *;*
(ii) *il existe un polynôme non nul scindé à racines simples dans* $\mathbf{k}$ *qui annule u ;*
(iii) *le polynôme minimal de u est scindé à racines simples dans* $\mathbf{k}$ *;*
(iv) *pour chaque λ, on a $E_\lambda = E'_\lambda$.*

Démonstration. Il est clair que l'on a les implications (i)$\Longrightarrow$(ii)$\Longleftrightarrow$(iii)$\Longrightarrow$(iv). L'implication (iv)$\Longrightarrow$(i) résulte de l'égalité $E = \bigoplus_\lambda E'_\lambda$, conséquence du lemme des noyaux 3. $\square$

Exercice 8. Soit M une matrice inversible complexe et soit k un entier strictement positif tel que M^k soit diagonalisable. Montrer que M est diagonalisable.

---

[1]Rappelons que l'on a supposé pour la démonstration de ce résultat que le polynôme minimal de u est scindé ; cette hypothèse est inutile. On peut s'en convaincre en remarquant qu'il suffit de montrer ce théorème pour une matrice $M \in \mathscr{M}_n(\mathbf{k})$ et que l'on peut alors se placer dans un corps plus gros que $\mathbf{k}$ dans lequel μ_M est scindé (par exemple $\mathbf{C}$ si $\mathbf{k} = \mathbf{R}$; un tel corps existe toujours et s'appelle un « corps de décomposition » de μ_M). On peut aussi raisonner directement comme suit : posons $N = XI_n - M$. Les coefficients de la comatrice $\widetilde{N}$ sont des polynômes de degré $\leqslant n-1$; on peut donc l'écrire

$$\widetilde{N} = \sum_{j=0}^{n-1} X^j \widetilde{N}_j$$

où les $\widetilde{N}_j$ sont des matrices carrées à coefficients dans $\mathbf{k}$. On a

$$N\ {}^t\widetilde{N} = (\text{dét}\, N)\ I_n = P_M(X)\ I_n$$

qui s'écrit aussi

$$(XI_n - M)\ (\sum_{j=0}^{n-1} X^j \widetilde{N}_j) = P_M(X)\ I_n$$

Si on note $\chi_M(X) = \sum_{j=0}^n a_j X^j$ (avec $a_n = 1$), on obtient en identifiant les coefficients

$$M\widetilde{N}_0 = -a_0 I_n\ ,\quad \widetilde{N}_0 - M\widetilde{N}_1 = a_1 I_n\ ,\ \ldots\ ,\quad \widetilde{N}_{n-2} - M\widetilde{N}_{n-1} = a_{n-1} I_n\ ,\quad \widetilde{N}_{n-1} = a_n I_n = I_n\ .$$

On en déduit

$$\begin{aligned} \chi_M(M) &= \sum_{j=0}^n a_j M^j = \sum_{j=0}^n M^j (a_j I_n) \\ &= -M\widetilde{N}_0 + M(\widetilde{N}_0 - M\widetilde{N}_1) + \cdots + M^{n-1}(\widetilde{N}_{n-2} - M\widetilde{N}_{n-1}) + M^n \widetilde{N}_{n-1} = 0 \end{aligned}$$

(les termes se regroupent deux à deux et s'annulent).

6. Décomposition de Dunford

On décompose un endomorphisme en une partie « facile », car diagonalisable, et une partie nilpotente.

Proposition 2 (Décomposition de Dunford). *Supposons le polynôme minimal de u scindé. Il existe une décomposition*

$$u = d + v$$

unique telle que

(1) *d est diagonalisable ;*
(2) *v est nilpotent ;*
(3) *$dv = vd$.*

De plus, d et v sont des polynômes en u.

Démonstration. À la décomposition de E en somme directe des espaces caractéristiques E'_λ correspond pour chaque λ une projection $\pi_\lambda : E \to E$ d'image E'_λ dont on a déjà mentionné que c'est un polynôme en u. Comme $\sum \pi_\lambda = \mathrm{Id}_E$, on a

$$u = \sum u\pi_\lambda = \underbrace{\sum \lambda\pi_\lambda}_{d} + \underbrace{\sum (u - \lambda\,\mathrm{Id}_E)\pi_\lambda}_{v}$$

et on a toutes les propriétés cherchées.

Montrons l'unicité. Si l'on a une autre décomposition $u = d' + v'$ vérifiant les propriétés (1), (2) et (3), les endomorphismes d' et v' commutent à u, donc à tout polynôme en u, donc à d et v. Donc les endomorphismes diagonalisables d et d' diagonalisent dans une même base et $d - d' = v' - v$ est diagonalisable et nilpotent donc est nul (exerc. 7). □

Soit M une matrice carrée *réelle.* Même si son polynôme minimal n'est pas scindé dans $\mathbf{R}$, on peut considérer sa décomposition de Dunford complexe $M = D + V$. On a[2] $M = \bar{M} = \bar{D} + \bar{V}$ et les matrices $\bar{D}$ et $\bar{V}$ vérifient encore les propriétés (1), (2) et (3) . Par unicité, on a $\bar{D} = D$ et $\bar{V} = V$, donc D et V sont réelles.

De plus, si P est un polynôme complexe tel que $D = P(M)$, on a $D = \mathrm{Re}(D) = \mathrm{Re}(P(M)) = (\mathrm{Re}\, P)(M)$ et idem pour V. Les matrices D et V sont donc des polynômes *réels* en M. La matrice V est nilpotente, et la matrice D est diagonalisable *sur* $\mathbf{C}$.

Exercice 9. Soit $M = D + N$ la décomposition de Dunford d'une matrice carrée. À quelle condition M est-elle semblable à D ? Si M est inversible, montrer que D l'est aussi.

[2]C'est pour pouvoir prendre les conjugués qu'on raisonne avec des matrices plutôt que des endomorphismes.

Exercice 10. (a) On suppose $\mathbf{k} = \mathbf{C}$ et u *inversible.* Soit k un entier strictement positif. Montrer qu'il existe un polynôme $P \in \mathbf{C}[X]$ tel que $P(u)^k = u$ (on pourra d'abord traiter le cas $u = \lambda \operatorname{Id}_E + v$, avec $\lambda \neq 0$ et v nilpotent, en utilisant un développement en série entière de $\sqrt[k]{1+x}$).

(b) Montrer qu'il n'existe pas de matrice dont le carré vaut $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

CHAPITRE 3

Géométrie affine

1. Espaces et sous-espaces affines

Espace affine : ensemble E de points muni d'une règle qui à deux points A et B associe un vecteur $\overrightarrow{AB}$ dans un espace vectoriel $\overrightarrow{E}$ de façon à avoir la relation de Chasles et que pour chaque point A de E, l'application $M \mapsto \overrightarrow{AM}$ soit une bijection de E sur $\overrightarrow{E}$.

Notations : point $A + \overrightarrow{u}$, vecteur $B - A = \overrightarrow{AB}$.

La deuxième règle dit en essence que si l'on choisit une « origine » A, l'espace affine devient un espace vectoriel (on dit parfois que l'on vectorialise E en A).

Sous-espace affine (non vide).

Exemples : $\mathbf{R}^n$, plan et droites affines dans $\mathbf{R}^3$.

Intersection de sous-espaces affines, sous-espace affine engendré par une partie S *non vide* comme intersection des sous-espaces affines contenant S.

2. Applications affines

Définition : il existe un point A tel que l'application $\overrightarrow{AB} \mapsto \overrightarrow{f(A)f(B)}$ soit linéaire. Attention : pas de noyau ! Image et image réciproque (non vide) d'un espace affine. Exemples : symétries et projections affines.

Une application affine avec un point fixe peut s'étudier comme une application linéaire (en « vectorialisant » l'espace affine en ce point).

Proposition 3. *Pour qu'une application affine ait un unique point fixe, il faut et il suffit que l'application linéaire associée n'ait aucun vecteur fixe autre que* 0.

La condition signifie exactement que 1 n'est pas valeur propre de l'application linéaire associée.

Démonstration. Si f a un unique point fixe, on vectorialise E en ce point pour voir que $\overrightarrow{f}$ a la même propriété.

Inversement, on cherche les points fixes de f en écrivant, avec $O \in E$ quelconque,

$$f(A) = f(O) + \overrightarrow{f}(\overrightarrow{OA}) = A$$

c'est-à-dire $\overrightarrow{f}(\overrightarrow{OA}) - \overrightarrow{OA} = \overrightarrow{f(O)O}$. Par hypothèse, l'application $\overrightarrow{f} - \mathrm{Id}_E$ est injective, donc bijective. $\square$

3. Repères

Repère cartésien : un point plus une base de l'espace vectoriel associé (exemple : $(O, \overrightarrow{\imath}, \overrightarrow{\jmath}))$; coordonnées.

Points affinement indépendants : le sous-espace affine engendré est de dimension maximale, ou les vecteurs associés forment une partie libre.

Repère affine : $n+1$ points affinement indépendants.

Applications affines et repères : expression d'une application affine dans des repères cartésiens, une application affine est uniquement déterminée par ses valeurs sur les points d'un repère affine.

Représentations des sous-espaces affines : comme $A + \overrightarrow{F}$ (représentation paramétrique), en temps qu'image inverse d'un point par une application affine (équations cartésiennes). Exemple dans $\mathbf{R}^3$: les équations

$$\begin{cases} 2x + 3y - 5z &= 1 \\ -2x - 2y + 3z &= 0 \end{cases}$$

définissent la droite passant par $(-1, 1, 0)$ et dirigée par le vecteur $(-1, 4, 2)$.

Exercice 11. Conditions sur les coordonnées dans un repère cartésien pour que 3 points du plan soient alignés (ou plus généralement pour que $n+1$ points d'un espace affine de dimension n soient sur un hyperplan) : un déterminant est nul.

Si les points sont de coordonnées $A_j = (a_{j,k})_{1\leqslant k\leqslant n}$, la condition est qu'il existe $\lambda_1, \dots, \lambda_n, \lambda$ non tous nuls tels que

$$a_{j,1}\lambda_1 + \cdots + a_{j,n}\lambda_n + \lambda = 0$$

pour chaque j. Il faut donc que le déterminant de ce système soit nul.

4. Barycentres

4.1. Définition. Le barycentre du système de points pondérés $(A_1, a_1), \dots, (A_m, a_m)$ (avec $a = a_1 + \cdots + a_m \neq 0$) est l'unique point G qui vérifie

$$\overrightarrow{MG} = \frac{1}{a}\sum_{i=1}^{m} a_i \overrightarrow{MA_i}$$

pour un (ou pour tout) point M. En particulier, $\sum_{i=1}^{m} a_i\overrightarrow{GA_i} = 0$. Il est dans l'espace affine engendré par les A_i.

Associativité du barycentre. Notation

$$G = \sum_{i=1}^{m} \frac{a_i}{a} A_i$$

On peut donc considérer des sommes de points dans deux cas : la somme des coefficients vaut 0 (on obtient alors un vecteur), la somme des coefficients vaut 1 (on obtient alors un point). Le milieu d'un segment AB est donc $\frac{1}{2}A + \frac{1}{2}B$.

4.2. Applications affines et barycentres. Les applications affines « conservent les barycentres ». On peut même les caractériser par cette propriété.

PROPOSITION 4. *Soient E et F des espaces affines sur un corps avec au moins trois éléments. Une application $f : E \to F$ est affine si et seulement si l'image par f du barycentre de tout système de points pondérés $(A_1, a_1), \dots, (A_m, a_m)$ de poids total non nul est le barycentre du système de points pondérés $(f(A_1), a_1), \dots, (f(A_m), a_m)$.*

DÉMONSTRATION. Supposons f affine. Soit M un point de E. Le barycentre de $(A_1, a_1), \dots, (A_m, a_m)$ (avec $a = a_1 + \dots + a_m \neq 0$) est l'unique point G qui vérifie

$$\overrightarrow{MG} = \frac{1}{a} \sum_{i=1}^{m} a_i \overrightarrow{MA_i}$$

Prenons les images par l'application linéaire $\overrightarrow{f}$; on obtient

$$\overrightarrow{f(M)f(G)} = \frac{1}{a} \sum_{i=1}^{m} a_i \overrightarrow{f(M)f(A_i)}$$

ce qui prouve que $f(G)$ est le barycentre de $(f(A_1), a_1), \dots, (f(A_m), a_m)$.

Réciproquement, supposons simplement que pour tous points A et B de E, et tout $t \in \mathbf{R}$, l'image par f du barycentre de (A, a) et $(B, 1-a)$ soit le barycentre de $(f(A), a)$ et $(f(B), 1-a)$. On fixe un point O de E et on définit une application $\overrightarrow{f} : \overrightarrow{E} \to \overrightarrow{F}$ par

$$\overrightarrow{f}(\overrightarrow{OM}) = \overrightarrow{f(O)f(M)}$$

On vérifie ensuite

$$\overrightarrow{f}(a\overrightarrow{OA} + (1-a)\overrightarrow{OB}) = a\overrightarrow{f(O)f(A)} + (1-a)\overrightarrow{f(O)f(B)}$$

ce qui entraîne facilement que $\overrightarrow{f}$ est linéaire (il faut ici soit pouvoir diviser par 2, soit utiliser un élément du corps autre que 0 ou 1).

Voici la démonstration de Chambert–Loir. Fixons un point $O \in F$ et définissons une application $\overrightarrow{f} : \overrightarrow{E} \to \overrightarrow{F}$ par la formule $\overrightarrow{f}(\overrightarrow{OM}) = \overrightarrow{f(O)f(M)}$. Nous devons montrer que $\overrightarrow{f}$ est une application linéaire. Soit $\overrightarrow{u}$ et $\overrightarrow{v}$ des vecteurs de $\overrightarrow{E}$, soit A et $B \in E$ tels que $\overrightarrow{OA} = \overrightarrow{u}$ et $\overrightarrow{OB} = \overrightarrow{v}$. Soit a et b dans k et soit M l'unique point de E tel que $\overrightarrow{OM} = a\overrightarrow{u} + b\overrightarrow{v} = a\overrightarrow{OA} + b\overrightarrow{OB}$.

Plaçons nous dans le cas $a + b \neq 0$. Le point A_1 de E tel que $\overrightarrow{OA_1} = (a+b)\overrightarrow{OA}$ est barycentre de $((A, a+b), (O, 1-a-b))$; son image par f est donc le barycentre de $((f(A), a+b), (f(O), 1-a-b))$. On a ainsi $\overrightarrow{f(O)f(A_1)} = (a+b)\overrightarrow{f(O)f(A)}$, ce qui montre que $\overrightarrow{f}(\overrightarrow{OA_1}) = (a+b)\overrightarrow{f}(\overrightarrow{OA})$. De même, si B_1 est le point de E tel que $\overrightarrow{OB_1} = (a+b)\overrightarrow{OB}$, on a $\overrightarrow{f}(\overrightarrow{OB_1}) = (a+b)\overrightarrow{f}(\overrightarrow{OB})$. Le point M est le barycentre de $((A_1,a),(B_1,b))$; son image est ainsi le barycentre de $((f(A_1),a),(f(B_1),b))$ donc vérifie $\overrightarrow{f(O)f(M)} = \frac{a}{a+b}\overrightarrow{f(O)f(A_1)} + \frac{b}{a+b}\overrightarrow{f(O)f(B_1)}$. Par suite, on a

$$\overrightarrow{f}(a\overrightarrow{u} + b\overrightarrow{v}) = \overrightarrow{f(O)f(M)} = a\overrightarrow{f(O)f(A)} + b\overrightarrow{f(O)f(B)} = a\overrightarrow{f}(\overrightarrow{u}) + b\overrightarrow{f}(\overrightarrow{v})).$$

Si $a+b=0$, soit $\lambda \in k - \{0,1\}$ et soit C le point de E tel que $\overrightarrow{OC} = \lambda^{-1}\overrightarrow{OA}$. Comme précédemment, $\overrightarrow{f}(\lambda^{-1}\overrightarrow{u}) = \lambda^{-1}\overrightarrow{f}(\overrightarrow{u})$. Puisque $\lambda a + b \neq 0$, le premier cas entraîne que

$$\overrightarrow{f}(a\overrightarrow{u} + b\overrightarrow{v}) = \lambda a\overrightarrow{f}(\lambda^{-1}\overrightarrow{u}) + b\overrightarrow{f}(\overrightarrow{v}) = a\overrightarrow{f}(\overrightarrow{u}) + b\overrightarrow{f}(\overrightarrow{v}).$$

Cela conclut la démonstration de la linéarité de $\overrightarrow{f}$. L'application f est donc une application affine. □

4.3. Coordonnées barycentriques dans un repère affine. Définition, lien avec coordonnées cartésiennes :

$$\begin{aligned} & \text{M barycentre de } (A_0,x_0),\dots,(A_n,x_n) \\ \iff\ & x_0\overrightarrow{MA_0} + \cdots + x_n\overrightarrow{MA_n} = \overrightarrow{0} \\ \iff\ & x_0\overrightarrow{MA_0} + x_1(\overrightarrow{MA_0} + \overrightarrow{A_0A_1}) + \cdots + x_n(\overrightarrow{MA_0} + \overrightarrow{A_0A_n}) = \overrightarrow{0} \\ \iff\ & x\overrightarrow{A_0M} = x_1\overrightarrow{A_0A_1} + \cdots + x_n\overrightarrow{A_0A_n} \end{aligned}$$

On a donc

$$x_1,\dots,x_n \text{ coordonnées de } M \text{ dans le repère cartésien } (A_0,\overrightarrow{A_0A_1},\dots,\overrightarrow{A_0A_n})$$
$$\iff$$
$$x_0 = x - x_1 - \cdots - x_n, x_1,\dots,x_n \text{ coordonnées barycentriques de } M$$
$$\text{dans le repère affine } (A_0,\dots,A_n).$$

Exemple 2. Signe des coordonnées barycentriques selon la région du plan.

Exemple 3 (Équation d'un hyperplan affine). Dans un repère cartésien

$$\lambda_1 x_1 + \cdots + \lambda_n x_n + \lambda = 0$$

avec $\lambda_1,\dots,\lambda_n$ non tous nuls. C'est équivalent à $\lambda x_0 + (\lambda+\lambda_1)x_1 + \cdots + (\lambda+\lambda_n)x_n = 0$. En coordonnées barycentriques, l'équation est donc

$$\mu_0 x_0 + \cdots + \mu_n x_n = 0$$

avec $\mu_0,\dots,\mu_n$ non tous égaux.

Exemple 4 (Coordonnées barycentriques des points remarquables du triangle). Centre de gravité $(1,1,1)$.

Orthocentre $(\tan A, \tan B, \tan C)$.

Centre du cercle inscrit (a,b,c).

Centre du cercle circonscrit $(\sin 2A, \sin 2B, \sin 2C)$.

Exemple 5 (Points alignés dans le plan). C'est la condition $\begin{vmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \\ c_0 & c_1 & c_2 \end{vmatrix} = 0.$ Plus généralement, $n+1$ points dans un espace affine de dimension n.

4.4. Théorème de Menelaüs. Soient $A' \in [BC]$, $B' \in [CA]$ et $C' \in [AB]$, avec $A' \neq C$, $B' \neq A$, $C' \neq B$. Les points A', B' et C' sont alignés si et seulement si

$$\frac{\overline{A'B}}{\overline{A'C}} \cdot \frac{\overline{B'C}}{\overline{B'A}} \cdot \frac{\overline{C'A}}{\overline{C'B}} = 1$$

Par les barycentres : $A' = (0, a', a'')$, $B' = (b, 0, b'')$ et $C' = (c, c', 0)$, avec $\frac{a'}{a''} = -\frac{\overline{A'B}}{\overline{A'C}}$, $\frac{b}{b''} = -\frac{\overline{B'A}}{\overline{B'C}}$ et $\frac{c}{c'} = -\frac{\overline{C'A}}{\overline{C'B}}$. Ils sont alignés si et seulement si le déterminant est nul, c'est-à-dire $a''bc' + a'b''c = 0$.

Par le théorème de Thalès : si M est le point de rencontre de AC avec la parallèle à $A'B'$ passant par B, on a, si les points sont alignés,

$$\frac{\overline{C'B}}{\overline{C'A}} = \frac{\overline{B'M}}{\overline{B'A}} \qquad , \qquad \frac{\overline{CA'}}{\overline{A'B}} = \frac{\overline{CB'}}{\overline{B'M}}$$

La réciproque est moins pratique.

En utilisant des homothéties : soit $h_{A'}$ l'homothétie de centre A' qui envoie C sur B ; soit $h_{B'}$ l'homothétie de centre B' qui envoie A sur C ; soit $h_{C'}$ l'homothétie de centre C' qui envoie B sur A. La composée $h = h_{A'} \circ h_{B'} \circ h_{C'}$ est une homothétie affine qui laisse B invariant ; son rapport est le produit de l'énoncé. Si ce produit vaut 1, h est l'identité ; comme $M = h_{A'}^{-1}(C') = h_{A'}^{-1}(h(C')) = h_{B'}(C')$, les points M, C' et A' d'une part, M, C' et B' d'autre part, sont alignés, donc aussi A', B' et C'.

Réciproquement, si les points A', B' et C' sont alignés, $h(C')$ est sur la droite qui les joint. Si le produit ne vaut pas 1, h est une homothétie de centre B, qui est sur la droite joignant C' à $h(C')$, c'est-à-dire la droite $A'B'C'$, ce qui est absurde.

4.5. Théorème de Pappus.

5. Convexes

5.1. Définitions. Définition, contient tous les barycentres à coefficients positifs.

Intersection de convexes, enveloppe convexe d'une partie (intersection des convexes contenant la partie ou ensemble des barycentres à coefficients positifs).

5.2. Théorème de Carathéodory. Énoncé. Interprétation dans le plan.

Soit $A = \sum_{j=1}^{m} a_j A_j$ une décomposition minimale avec $a_j > 0$ et $\sum a_j = 1$. Si $m > n+1$, les vecteurs $A_2 - A_1, \ldots, A_m - A_1$ sont liés, donc

$$b_2(A_2 - A_1) + \cdots + b_m(A_m - A_1) = \overrightarrow{0}$$

Posons $b_1 = -(b_2 + \cdots + b_m)$. Alors $\sum_{j=1}^{m} b_j A_j = \overrightarrow{0}$ donc

$$A = \sum_{j=1}^{m} (a_j - tb_j) A_j$$

pour tout t. On choisit t de façon que $a_j - tb_j \geqslant 0$ pour tout j, avec égalité pour au moins un j, c'est-à-dire $t = \min\{a_j/b_j \mid b_j > 0\}$.

Corollaire 1. *L'enveloppe convexe d'une partie compacte de E est compacte.*

Exercice 12. Décrire l'enveloppe convexe dans $\mathbf{R}^2$ de la réunion d'une droite et d'un point non situé sur la droite.

On démontrera d'autres résultats sur les convexes dans un espace affine *euclidien* dans le § 1 du chap. 5.

CHAPITRE 4

Espaces vectoriels euclidiens

Nous n'avons jusqu'à présent fait intervenir que des relations d'incidence entre objets géométriques. Nous allons maintenant introduire celle de distance, via une norme.

1. Produit scalaire, norme

1.1. Définitions. Espace vectoriel euclidien, inégalité de Cauchy–Schwarz, norme, distance.

Attention : il existe des normes qui ne sont pas issues d'un produit scalaire, comme par exemple la norme

$$\|(x_1, \ldots, x_n)\|_1 = |x_1| + \cdots + |x_n|$$

sur $\mathbf{R}^n$. On peut montrer qu'une norme $\|\cdot\|$ est issue d'un produit scalaire si et seulement si elle satisfait l'égalité du parallèlogramme

$$\|x+y\|^2 + \|x-y\|^2 = 2(\|x\|^2 + \|y\|^2)$$

pour tous vecteurs x et y.

Produit scalaire canonique sur $\mathbf{R}^n$.

1.2. Barycentres. Le barycentre G des points pondérés $(A_1, a_1), \ldots, (A_m, a_m)$ (avec $a = a_1 + \cdots + a_m \neq 0$) peut aussi être caractérisé de façon métrique : c'est l'unique point où la fonction (appelée moment d'inertie de M par rapport au système de points pondérés $(A_1, a_1), \ldots, (A_m, a_m)$)

$$M \longmapsto \sum_{i=1}^{m} a_i \|\overrightarrow{MA_i}\|^2$$

atteint son extremum (maximum si $a < 0$, minimum si $a > 0$).

En effet, cette fonction f vérifie

$$f(M) = f(N) + 2\langle \overrightarrow{MN}, \sum_{i=1}^{m} a_i \overrightarrow{NA_i} \rangle + a\|\overrightarrow{MN}\|^2$$

donc $f(M) = f(G) + a\|\overrightarrow{MG}\|^2$.

EXEMPLE 6. Soient A, B et C des points non alignés du plan. Lignes de niveau de

$$M \longmapsto \langle \overrightarrow{MA}, \overrightarrow{MB} \rangle + \langle \overrightarrow{MB}, \overrightarrow{MC} \rangle + \langle \overrightarrow{MC}, \overrightarrow{MA} \rangle$$

On écrit

$$\langle \overrightarrow{MA}, \overrightarrow{MB} \rangle = \frac{1}{2}\Big(\|\overrightarrow{MA} - \overrightarrow{MB}\|^2 - \|\overrightarrow{MA}\|^2 - \|\overrightarrow{MB}\|^2 \Big) = \frac{1}{2}\Big(\|\overrightarrow{AB}\|^2 - \|\overrightarrow{MA}\|^2 - \|\overrightarrow{MB}\|^2 \Big)$$

Ce sont donc les lignes de niveaux de

$$M \longmapsto \|\overrightarrow{MA}\|^2 + \|\overrightarrow{MB}\|^2 + \|\overrightarrow{MC}\|^2$$

qui sont des cercles de centre l'isobarycentre de A, B et C.

1.3. Orthogonalité. Orthogonalité, sous-espaces vectoriels orthogonaux. Théorème de Pythagore.

Les formes linéaires sont toutes du type $x \mapsto \langle u, x \rangle$. Équation d'un hyperplan $\langle u, x \rangle = 0$.

Dimension de l'orthogonal, $E = V \oplus V^\perp$, $(V^\perp)^\perp = V$.

DÉMONSTRATION. On a $V \cap V^\perp = \{0\}$, donc $\dim(V^\perp) \leqslant \operatorname{codim}(V)$. Mais $V^\perp$ est défini comme le noyau de $E \to V^*$ donc est de dimension $\geqslant n - \dim(V)$. □

2. Bases orthogonales, bases orthonormées

2.1. Définition. Attention à la terminologie : pour le produit scalaire canonique de $\mathbf{R}^n$, la matrice A des composantes des vecteurs d'une base *orthonormée* est *orthogonale*, c'est-à-dire satisfait ${}^tA\,A = I_n$.

THÉORÈME 2 (Procédé d'orthonormalisation de Gram–Schmidt). *Soit* $(e_1, \dots, e_n)$ *une base d'un espace vectoriel euclidien E. Il existe une unique base orthonormée* $(f_1, \dots, f_n)$ *de E vérifiant la propriété suivante : pour tout* $m \in \{1, \dots, n\}$, *il existe des réels* $a_1, \dots, a_m$ *avec* $a_m > 0$ *tels que*

$$f_m = a_1 f_1 + \cdots + a_{m-1} f_{m-1} + a_m e_m$$

Interprétation matricielle : soit A la matrice des composantes des e_i dans la base canonique, c'est-à-dire la matrice de passage de la base canonique à la base (e_i). La matrice de passage T de la base (f_i) à la base (e_i) est triangulaire supérieure à coefficients diagonaux strictement positifs, et la matrice de passage O de la base canonique à la base (f_i) est orthogonale, comme matrice de passage d'une base orthonormée à une autre. On a $O = AT^{-1}$. On a ainsi montré que *toute matrice A inversible s'écrit de façon unique*

$$A = OT$$

où T est triangulaire supérieure à coefficients diagonaux strictement positifs et O est orthogonale.

Démonstration. On construit les f_i par récurrence. On pose $f_1 = e_1/\|e_1\|$. Les a_i sont déterminés pour $i < m$ par $0 = \langle f_m, f_i\rangle = a_i + a_m\langle e_m, f_i\rangle$, c'est-à-dire

$$f_m = a_m\Big(e_m - \sum_{i=1}^{m-1}\langle e_m, f_i\rangle f_i\Big)$$

et a_m par le fait que ce vecteur, non nul, doit être de norme 1. $\square$

3. Endomorphismes symétriques

Un endomorphisme u d'un espace vectoriel euclidien E est dit symétrique si

$$\langle u(x), y\rangle = \langle x, u(y)\rangle \qquad \text{pour tout } x \text{ et tout } y \text{ dans } E.$$

Un endomorphisme est symétrique si et seulement si sa matrice *dans une base orthonormée* est symétrique.

Exemple 7. Une projection orthogonale, une symétrie orthogonale sont des endomorphismes symétriques. Plus précisément, une symétrie (ou une projection) est un endomorphisme symétrique si et seulement si c'est une symétrie (ou une projection) orthogonale.

Le résultat principal de la théorie est le suivant.

Théorème 3. *Un endomorphisme symétrique est diagonalisable dans une base orthonormée.*

En termes matriciels, cela signifie que si M est une matrice symétrique *réelle,* il existe une matrice orthogonale P telle que $P^{-1}MP$ est diagonale.

Démonstration. On raisonne par récurrence sur la dimension et le point est de montrer qu'un endomorphisme symétrique d'un espace vectoriel réel (de dimension finie) a toujours (au moins) une valeur propre réelle, ou encore un vecteur propre. On cherche celui-ci de norme 1, c'est-à-dire dans la sphère unité $\mathbf{S}$ de E. Considérons la fonction

$$\begin{array}{rccc} f: & \mathbf{S} & \longrightarrow & \mathbf{R} \\ & x & \longmapsto & \langle u(x), x\rangle \end{array}$$

est continue. Comme $\mathbf{S}$ est compacte, f atteint son maximum en un point x_0 dont on va montrer que c'est un vecteur propre pour la valeur propre $\lambda = f(x_0) = \langle u(x_0), x_0\rangle$.

Soit x un vecteur unitaire qui est dans l'hyperplan $H = x_0^\perp$ orthogonal à x_0. Le vecteur $x_t = tx + \sqrt{1-t^2}x_0$ est encore dans $\mathbf{S}$ pour tout $t \in [-1,1]$; on a donc

$$\begin{aligned}
\langle u(x_0), x_0\rangle &= f(x_0) \\
&\geqslant f(x_t) \\
&= \langle tu(x) + \sqrt{1-t^2}u(x_0), tx + \sqrt{1-t^2}x_0\rangle \\
&= t^2\langle u(x), x\rangle + t\sqrt{1-t^2}\langle u(x), x_0\rangle \\
&\qquad\qquad + t\sqrt{1-t^2}\langle u(x_0), x\rangle + (1-t^2)\langle u(x_0), x_0\rangle
\end{aligned}$$

Comme u est symétrique, on a $\langle u(x), x_0\rangle = \langle u(x), x_0\rangle$; on obtient en réarrangeant

$$t^2\langle u(x_0), x_0\rangle \geqslant t^2\langle u(x), x\rangle + 2t\sqrt{1-t^2}\langle u(x_0), x\rangle$$

et en divisant par t si $t \neq 0$ et en faisant ensuite tendre t vers 0, on obtient $\langle u(x_0), x\rangle = 0$ (distinguer les cas $t > 0$ et $t < 0$). Le vecteur $u(x_0)$ est ainsi orthogonal à H, donc colinéaire à x_0 (parce que $H^\perp = \mathbf{k}x_0$), c'est-à-dire $u(x_0) = \lambda x_0$. Le vecteur x_0 est donc bien vecteur propre pour la valeur propre λ.

Vérifions que l'hyperplan H est stable par u. Si x est dans H, on a

$$\langle u(x), x_0\rangle = \langle x, u(x_0)\rangle = \lambda\langle x, x_0\rangle = 0$$

donc $u(x) \in H$. On a bien une décomposition $E = \mathbf{k}x_0 \oplus H$ en somme directe orthogonale de sous-espaces stables par u. On peut appliquer l'hypothèse de récurrence à la restriction de u à H, qui est encore un endomorphisme symétrique. Il existe une base orthonormée de H dans laquelle la matrice de cette restriction est diagonale ; si on lui ajoute x_0, on obtient une base orthonormée de E dans laquelle la matrice de u est diagonale. $\square$

Remarque 1. Il existe une autre démonstration plus courte du fait que les valeurs propres d'une matrice symétrique réelle, ou plus généralement d'une matrice M complexe *hermitienne*[1] sont réelles : soit λ une valeur propre (complexe) de M et X un vecteur propre (complexe non nul), de sorte que $MX = \lambda X$. On a

$$X^*MX = X^*(MX) = \lambda X^*X$$

En prenant les adjoints dans $MX = \lambda X$, on a, puisque $M^* = M$, $X^*M = \overline{\lambda}X^*$, d'où

$$X^*MX = (X^*M)X = \overline{\lambda}X^*X$$

Comme X^*X est un réel non nul, on obtient $\lambda = \overline{\lambda}$, de sorte que λ est bien réel.

[1] Cela signifie que l'adjointe M^*, c'est-à-dire la conjuguée de la transposée de M, est égale à M.

EXERCICE 13. La matrice symétrique $\begin{pmatrix} 2 & i \\ i & 0 \end{pmatrix}$ est-elle diagonalisable ?

4. Isométries

4.1. Définitions. Application linéaire qui conserve la norme (ou le produit scalaire). Elle est bijective, envoie une base orthonormée sur une base orthonormée. Sa matrice *dans une base orthonormée* est orthogonale. Elle est donc de déterminant 1 (déplacement) ou -1 (antidéplacement). Les isométries forment un groupe noté $O(E)$, les déplacements forment un groupe noté $O^+(E)$ ou $SO(E)$.

Une isométrie conserve aussi les volumes (tandis qu'une application linéaire les multiplie par la valeur absolue de son déterminant).

LEMME 4. *Soit f une isométrie de E. On a une décomposition*

$$E = \operatorname{Ker}(\mathrm{Id}_E - f) \overset{\perp}{\oplus} \operatorname{Im}(\mathrm{Id}_E - f)$$

en somme directe orthogonale.

DÉMONSTRATION. Si x est dans le noyau, on a

$$\langle x, y - f(y) \rangle = \langle x, y \rangle - \langle x, f(y) \rangle = \langle x, y \rangle - \langle f(x), f(y) \rangle = 0$$

le noyau et l'image sont donc orthogonaux. Comme la somme de leur dimension est la dimension de E (théorème du rang), leur somme est E. □

4.2. Symétries orthogonales, réflexions. Pour une réflexion (symétrie orthogonale par rapport à un hyperplan) :

$$s_H(x) = x - 2\frac{\langle x, e \rangle}{\langle e, e \rangle} e$$

où e est normal à H.

Une symétrie est une isométrie si et seulement si c'est une symétrie orthogonale.

Il résulte du lemme 4 qu'une isométrie est une réflexion si et seulement si l'ensemble de ses points fixes est un hyperplan.

THÉORÈME 4. *Toute isométrie est produit de réflexions.*

DÉMONSTRATION. Récurrence sur $p = \operatorname{codim}(F)$ où $F = \operatorname{Ker}(f - \mathrm{Id}_E)$. Soit $e \in E - F$. Par le lemme 4, l'hyperplan $H = (e - f(e))^\perp$ contient F, de sorte que tout point de F est fixe par $s_H \circ f(e) = e$. On a aussi $s_H \circ f(e) = e$. On en déduit que f est produit d'au plus p réflexions. □

5. Isométries du plan complexe

Notons $a = f(1)$, nombre complexe de module 1. On a $f(i) = ai$ ou $-ai$, donc $f(z) = az$ ou $f(z) = a\bar{z}$. Si $a = e^{i\theta}$, la matrice de f dans la base $(1, i)$ est

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \qquad \text{ou} \qquad S_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

Le groupe des déplacements du plan (les « rotations ») est donc commutatif. Dans une base orthonormée directe quelconque, la matrice d'une rotation reste la même (elle est changée en $R_{-\theta}$ dans une base indirecte).

Si f est un antidéplacement, c'est une réflexion : dans la base orthonormée $(e^{i\theta/2}, ie^{i\theta/2})$, sa matrice est $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

6. Isométries et déplacements de l'espace

Soit f une isométrie d'un espace vectoriel euclidien de dimension 3. Son polynôme caractéristique est de degré 3, donc admet une racine réelle, qui ne peut être que ± 1. Soit e_1 un vecteur propre unitaire. Son orthogonal est un plan stable par f, qui y induit donc une isométrie. Si cette isométrie est une rotation, sa matrice est du type R_θ ; si c'est une symétrie, sa matrice est, dans une base orthonormée convenable, du type $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Au total, la matrice de f dans une base orthonormée convenable est de l'un des types suivants :

- $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$ et f est un déplacement appelé *rotation* ;
- $\begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$ et f est un antidéplacement appelé *antirotation* (c'est une réflexion lorsque $\theta \equiv 0 \pmod{\pi}$).

L'opposé d'une antirotation est une rotation. Le nombre θ qui apparaît ci-dessus n'est déterminé que modulo 2π bien sûr, mais aussi seulement au signe près, même si l'espace est orienté. Pour avoir un nombre bien défini modulo 2π, il faut en général orienter l'axe de la rotation (ou de l'antirotation) et le plan orthogonal à cet axe. Il est souvent utile de se rappeler la formule :

$$\operatorname{tr}(f) = 2\cos\theta + \operatorname{dét}(f)$$

Une rotation d'angle π s'appelle un *demi-tour*. Sa matrice dans une base orthonormée convenable est $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$. C'est l'opposé de la réflexion par rapport au plan du demi-tour.

Exercices 14. 1) Toute rotation est composée de deux réflexions, donc de deux demi-tours (c'est un cas particulier du th. 4 ; utiliser l'astuce utile qu'en dimension 3, r est un demi-tour si et seulement si $-r$ est une réflexion).

2) Trouver l'axe et l'angle de la rotation de $\mathbf{R}^3$ de matrice $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ dans la base canonique.

7. Produit vectoriel

Espace euclidien orienté de dimension 3.
MA p. 108.

$$u \wedge (v \wedge w) = \langle u, w \rangle v - \langle u, v \rangle w$$

CHAPITRE 5

Espaces affines euclidiens

Un espace affine euclidien est un espace affine dirigé par un espace vectoriel euclidien. Distance de deux points.

1. Projection sur un convexe

1.1. Distance à un fermé. Soit K une partie non vide de E et soit a un point de E. On note

$$d(a, K) = \inf_{x \in K} \|a - x\|$$

Si K est compacte, la fonction continue $x \mapsto \|a - x\|$ atteint son minimum sur K en un point k (pas nécessairement unique) et $\|a - k\| = d(a, K)$. On dit que la distance de a à K est atteinte (en k).

Si K n'est que fermée, on prend un point k_0 de K et on note $r = \|a - k_0\|$ et $K_0 = K \cap B(a, r)$. On a $d(a, K) \leqslant r$ donc $d(a, K_0) = d(a, K)$ est atteinte en un point de K_0 (donc de K).

On a $d(a, K) = d(a, \overline{K})$ et $d(a, K) = 0$ si et seulement si $a \in \overline{K}$.

Exemple 8. Traiter l'exemple $K = S(a, r)$.

1.2. Théorème de Hahn–Banach. La discussion précédente est valable pour n'importe quelle norme. Ce qui suit nécessite d'avoir une norme euclidienne, c'est-à-dire provenant d'un produit scalaire.

Théorème 5. *Soit K une partie convexe fermée d'un espace vectoriel euclidien et soit a un point de E. La distance de $d(a, K)$ est atteinte en un unique point de K appelé projection de a sur K et noté $p_K(a)$. On a, pour tout k dans K,*

$$\langle k - p_K(a), a - p_K(a) \rangle \leqslant 0$$

En termes plus géométriques, l'hyperplan affine d'équation

$$\ell(x) = \langle x - p_K(a), a - p_K(a) \rangle = 0$$

définit deux demi-espaces fermés de E. Si a n'est pas dans K, il est dans l'intérieur de l'un de ces demi-espaces (défini par $\ell(x) > 0$) et K est contenu dans l'autre (défini par $\ell(x) \leqslant 0$).

Démonstration. Soient x et y deux points de K en lesquels la distance $d = d(a, K)$ est atteinte. On a

$$\|a - x + a - y\|^2 + \|(a - x) - (a - y)\|^2 = 2\|a - x\|^2 + 2\|a - y\|^2$$

Puisque $\frac{1}{2}(x + y)$ est dans K, on en déduit

$$\begin{aligned} 4d \leqslant 4\|a - \frac{1}{2}(x + y)\|^2 &= 2\|a - x\|^2 + 2\|a - y\|^2 - \|x - y\|^2 \\ &= 2d + 2d - \|x - y\|^2 \end{aligned}$$

d'où $x = y$. Ceci démontre l'unicité du point en lequel la distance est atteinte.

Soit k un point de K. On a, pour tout $t \in [0, 1]$,

$$\begin{aligned} d^2 &\leqslant \|a - (1 - t)x - tk\|^2 \\ &= \|a - x + t(x - k)\|^2 \\ &= \|a - x\|^2 + 2t\langle a - x, x - k\rangle + t^2\|x - k\|^2 \\ &= d^2 + 2t\langle a - x, x - k\rangle + t^2\|x - k\|^2 \end{aligned}$$

En simplifiant, en divisant par t, on obtient pour tout $t \in]0, 1]$

$$2\langle x - k, a - x\rangle + t\|x - k\|^2 \geqslant 0$$

d'où le résultat en faisant tendre t vers 0. □

Exercice 15. Lorsque F est un sous-espace affine de E, montrer que p_F est la projection orthogonale sur F.

Exercice 16. Soient a et b des points de E. Montrer que l'on a

$$\|p_K(a) - p_K(b)\| \leqslant \|a - b\|$$

En déduire que la fonction p_K est continue.

Exercice 17. Soient K_1 et K_2 des fermés disjoints de E, avec K_1 compact. Montrer qu'il existe un hyperplan affine de E définissant deux demi-espaces ouverts dont l'un contient K_1 et l'autre K_2.

1.3. Points extrémaux. On dit qu'un point x d'un convexe K est *extrémal* si x n'est intérieur à aucun segment non réduit à un point entièrement contenu dans K.

Exercice 18. Montrer que x est extrémal si et seulement si $K - \{x\}$ est convexe.

Un ouvert convexe n'a aucun point extrémal. Le convexe fermé E n'a aucun point extrémal. Points extrémaux d'une boule.

THÉORÈME 6. *Un compact convexe non vide a toujours un point extrémal.*

DÉMONSTRATION. On procède par récurrence sur la dimension n de E. Pour $n = 0$, il n'y a rien à montrer.

Soit K un compact convexe non vide. Soit $a \notin K$ et soit H l'hyperplan affine passant par $p_K(a)$ et orthogonal à $a - p_K(a)$. Tout point extrémal de $H \cap K$ est encore extrémal sur K. Il existe donc des points extrémaux. □

EXERCICE 19. Donner un exemple d'un compact convexe dont les points extrémaux ne forment pas un sous-ensemble fermé (on pourra considérer l'enveloppe convexe dans $\mathbf{R}^3$ du cercle $(x-1)^2+y^2-1 = z = 0$ et des points $(0, 0, \pm 1)$).

En fait, on a un résultat plus fort que nous ne démontrerons pas ici.

THÉORÈME 7 (Krein–Millman). *Un compact convexe est l'enveloppe convexe de ses points extrémaux.*

Exemple des polyèdres convexes, enveloppes convexes de leurs sommets.

2. Isométries affines

2.1. Définition, exemples. Application affine qui conserve les distances : l'application linéaire associée conserve la norme (ou le produit scalaire). Isométries positives ou négatives.

Translation $t_{\overrightarrow{u}}$, symétrie (affine) orthogonale par rapport à un sous-espace affine, réflexion affine (par raport à un hyperplan affine).

2.2. Les réflexions engendrent le groupe des isométries.

THÉORÈME 8. *Toute isométrie affine est produit de réflexions affines.*

DÉMONSTRATION. Soit x un point de E. Si $x = f(x)$, on vectorialise E en x et on applique le th. 4. Sinon, soit H l'hyperlan médiateur de x et $f(x)$; alors $s_h \circ f$ a un point fixe. □

EXEMPLE 9. Soit H un hyperplan affine orthogonal à $\overrightarrow{u}$. On a $t_{\overrightarrow{u}} = s_{H+\frac{1}{2}\overrightarrow{u}} \circ s_H$.

2.3. Décomposition des isométries affines.

THÉORÈME 9. *Toute isométrie affine f s'écrit de façon unique comme $f = g \circ t_{\overrightarrow{u}} = t_{\overrightarrow{u}} \circ g$ où g est une isométrie qui a un point fixe.*

L'intérêt est qu'une isométrie avec un point fixe peut s'étudier comme une isométrie vectorielle (en « vectorialisant » l'espace affine en ce point).

La démonstration montre que l'ensemble des points fixes de g est un sous-espace affine dirigé par $\operatorname{Ker}(\operatorname{Id}_{\overrightarrow{E}} - \overrightarrow{f})$ et que $\overrightarrow{u}$ est dans $\operatorname{Ker}(\operatorname{Id}_{\overrightarrow{E}} - \overrightarrow{f})$.

DÉMONSTRATION. On cherche donc un vecteur $\overrightarrow{u}$ tel que

- $g = t_{-\overrightarrow{u}} \circ f = f \circ t_{-\overrightarrow{u}}$, c'est-à-dire que l'on veut, pour tout M,

$$f(M) - \overrightarrow{u} = f(M - \overrightarrow{u}) = f(M) - \overrightarrow{f}(\overrightarrow{u})$$

  ou encore $\overrightarrow{u} \in \operatorname{Ker}(\operatorname{Id}_E - \overrightarrow{f})$;
- $t_{-\overrightarrow{u}} \circ f$ a un point fixe, c'est-à-dire que l'on cherche, ayant fixé un point quelconque O, un point A tel que $f(A) - \overrightarrow{u} = A$, ou encore

$$\overrightarrow{u} = f(A) - A = -(\operatorname{Id}_E - \overrightarrow{f})(\overrightarrow{OA}) + \overrightarrow{Of(O)}$$

  c'est-à-dire $\overrightarrow{u} - \overrightarrow{Of(O)} \in \operatorname{Im}(\operatorname{Id}_E - \overrightarrow{f})$.

Le théorème résulte du lemme 1, qui dit que l'on peut décomposer uniquement le vecteur $\overrightarrow{Of(O)}$ en

$$\overrightarrow{Of(O)} = \overrightarrow{u} + \left(\overrightarrow{Of(O)} - \overrightarrow{u}\right)$$

avec $\overrightarrow{u} \in \operatorname{Ker}(\operatorname{Id}_E - \overrightarrow{f})$ et $\overrightarrow{Of(O)} - \overrightarrow{u} \in \operatorname{Im}(\operatorname{Id}_E - \overrightarrow{f})$. □

2.4. Isométries laissant globalement invariante une partie non vide bornée.

THÉORÈME 10. *Soit S une partie non vide bornée d'un espace vectoriel euclidien E de dimension finie. Il existe une* unique *boule (fermée) de rayon minimal contenant S.*

DÉMONSTRATION. La partie S étant bornée, elle est contenue dans une certaine boule. Posons

$$r = \inf\{\rho \in \mathbf{R}^+ \mid \exists a \in E \quad S \subset B(a, \rho)\}$$

Il existe donc une suite (r_m) de réels positifs convergeant vers r et une suite (a_m) de points de E telles que $S \subset B(a_m, r_m)$. Soit x un point de S ; on a

$$\|x - a_m\| \leqslant r_m \qquad \text{pour tout } m \geqslant 0 \tag{3}$$

donc $\|a_m - a_0\| \leqslant r_m + r_0$. La suite (a_m) est donc bornée ; on peut en extraire une sous-suite qui converge vers un point a de E. On a alors, en passant à la limite dans (3),

$$\|x - a\| \leqslant r \qquad \text{pour tout } x \in S$$

soit encore $S \subset B(a, r)$. Nous avons montré qu'il existe une boule de rayon minimal contenant S.

Montrons que cette boule est unique. Supposons que l'on ait $S \subset B(b, r)$. On a alors, pour tout x dans S,

$$\|x - a\| \leqslant r \quad \text{et} \quad \|x - b\| \leqslant r$$

donc, par l'égalité du parallèlogramme,

$$\|x - \frac{1}{2}(a + b)\|^2 + \|\frac{1}{2}(a - b)\|^2 = \frac{1}{2}\|x - a\|^2 + \frac{1}{2}\|x - b\|^2 \leqslant r^2$$

En d'autres termes,

$$S \subset B\left(\frac{1}{2}(a + b), \sqrt{r^2 - \|\frac{1}{2}(a - b)\|^2}\right)$$

Comme r est minimal, on a $a = b$, ce qui montre l'unicité. □

COROLLAIRE 2. *Soit S une partie non vide bornée d'un espace vectoriel euclidien E. Il existe un point de E fixe par toutes les isométries de E laissant S globalement invariant.*

DÉMONSTRATION. Soit $B(a, r)$ l'unique boule de rayon minimal contenant S et soit u une isométrie de E laissant S globalement invariant, c'est-à-dire vérifiant $u(S) \subset S$. On a

$$S = u^{-1}(u(S)) \subset u^{-1}(S) \subset u^{-1}(B(a, r)) = B(u^{-1}(a), r)$$

Par unicité de la boule de rayon minimal contenant S, on en déduit $u^{-1}(a) = a$, donc $a = u(a)$. □

3. Isométries et déplacements du plan

Soit f un isométrie du plan complexe. On a vu dans le § 5 que l'isométrie vectorielle $\overrightarrow{f}$ s'écrit $z \mapsto az$ si elle est directe et $z \mapsto a\bar{z}$ si elle est indirecte, avec $|a| = 1$. Si b est l'affixe de $f(0)$, l'application f s'écrit donc $z \mapsto az + b$ si elle est directe et $z \mapsto a\bar{z} + b$ si elle est indirecte.

Dans le premier cas,

- soit $a \neq 1$, l'application linéaire $\overrightarrow{f}$ n'a pas de point fixe autre que l'origine, donc $\overrightarrow{u} = \overrightarrow{0}$ dans le th. 9 et f a un unique point fixe donc est une *rotation* ;
- soit $a = 1$ et f est une *translation.*

Dans le second cas, l'application $\overrightarrow{f}$ est une réflexion et f est une *symétrie glissée* : la composée d'une réflexion par rapport à une droite affine D et d'une translation par un vecteur de $\overrightarrow{D}$. Si ce vecteur n'est pas nul, la symétrie glissée n'a aucun point fixe.

On peut retrouver cela par le calcul.

Dans le cas direct $f(z) = az + b$ avec $a \neq 1$, l'unique point fixe de f est $\frac{b}{1-a}$.

Dans le cas indirect $f(z) = a\bar{z} + b$, avec $|a| = 1$, on choisit comme base orthonormée le couple $(e^{i\theta/2}, ie^{i\theta/2})$. En termes d'affixes, cela revient à poser $z = \exp(i\theta/2)u$. Si φ est l'expression de f dans la nouvelle base, on a alors, $f(z) = e^{i\theta/2}\varphi(u) = ae^{-i\theta/2}\bar{u} + b$, d'où

$$\varphi(u) = \bar{u} + be^{-i\theta/2}$$

Posons $\beta = be^{-i\theta/2}$ et $u_0 = \frac{i}{2}\operatorname{Im}(\beta)$. On a

$$\varphi(u_0 + u) = \overline{u_0 + u} + \beta = \bar{u} + (\beta - u_0) = \bar{u} + (\beta - 2u_0) + u_0$$

Cela montre que dans le repère cartésien $(u_0, \exp(i\theta/2), i\exp(i\theta/2))$, l'expression de f est donnée par $(x, y) \mapsto (x + t, -y)$, où $t = \beta - 2u_0 = \operatorname{Re}(\beta) \in \mathbf{R}$.

Exercice 20. Expliquer comment une rotation plane se décompose en la composée de deux réflexions (c'est un cas particulier du th. 8).

3.1. Angles.

3.1.1. *Angle orienté de vecteurs.* Étant donnés deux vecteurs unitaires du plan euclidien, il existe une unique rotation qui envoie l'un sur l'autre. On dit que deux paires (u, v) et (u', v') de vecteurs non nuls sont équivalentes s'il existe une rotation r telle que $r(\frac{u}{\|u\|}) = \frac{v}{\|v\|}$ et $r(\frac{u'}{\|u'\|}) = \frac{v'}{\|v'\|}$.

L'*angle orienté* de u et v est la classe d'équivalence de (u, v) ; on la note encore (u, v). On peut définir la *somme* de deux angles orientés (u, v) et (u', v') entre vecteurs que l'on peut supposer unitaires : si $v = r(u)$ et $v' = r'(u')$, on pose $(u, v) + (u', v') = (u'', r' \circ r(u''))$ où u'' est n'importe quel vecteur non nul. Cela munit l'ensemble des angles d'une structure de groupe. On a la relation de Chasles

$$(u, v) + (v, w) = (u, w)$$

À chaque rotation r, on peut associer l'angle $(u, r(u))$, qui ne dépend pas du vecteur non nul u choisi. Inversement, à chaque angle $\theta = (u, v)$ est associé l'unique rotation r_θ telle que $r_\theta(u) = v$; on l'appelle la rotation d'angle θ. On aura compris que cela définit un isomorphisme du groupe $SO(E)$ des rotations du plan sur le groupe des angles.

Comme $SO(E)$ est commutatif, une rotation r conserve les angles orientés :

$$(r(u), r(v)) = (u, v)$$

En revanche, une réflexion s les renverse :

$$(s(u), s(v)) = -(u, v)$$

On peut supposer u et v unitaires. Soit D la médiatrice de u et v, c'est-à-dire l'orthogonal de $u - v$. On a $u = \frac{1}{2}(u + v) + \frac{1}{2}(u - v)$ et ces deux vecteurs sont orthogonaux. On a donc

$$s_D(u) = \frac{1}{2}(u + v) - \frac{1}{2}(u - v) = v$$

et comme $s \circ s_D$ est une rotation,

$$(u, v) = (s \circ s_D(u), s \circ s_D(v)) = (s(v), s(u))$$

3.1.2. *Angle orienté de droites.* On peut aussi définir l'angle orienté de deux droites affines D et D', engendrées respectivement par des vecteurs unitaires u et u' comme l'angle (u, v). Comme on ne peut choisir u et v qu'au signe près, l'angle (D, D') n'est défini qu'à addition de l'angle plat près, c'est-à-dire modulo la relation d'équivalence qui identifie deux angles dont la différence est un angle plat. On remarque que $2(D, D')$ définit bien un angle orienté de vecteurs.

De nouveau, les rotations conservent les angles orientés de droites, tandis que les réflexions les renversent.

LEMME 5. *Soient D et D' des droites concourantes du plan affine euclidien. La composée $s_{D'} \circ s_D$ est la rotation d'angle $2(D, D')$ et de centre le point de rencontre de D et D'.*

DÉMONSTRATION. On vectorialise le plan affine en le point de concours de D et D'. La composée de deux symétries réflexions vectorielles est une rotation vectorielle, dont il s'agit de déterminer l'angle.

Soit u un vecteur unitaire de D et soit u' un vecteur unitaire de D'. L'angle cherché est

$$\begin{aligned}
(u, s_{D'} \circ s_D(u)) &= (u, s_{D'}(u)) \\
&= (u, u') + (u', s_{D'}(u)) \\
&= (u, u') + (s_{D'}(u'), s_{D'}(u)) \\
&= (u, u') - (u', u) \\
&= 2(u, u') \\
&= 2(D, D')
\end{aligned}$$

□

EXERCICE 21. Déterminer géométriquement le centre de la composée de deux rotations planes (MA, p. 73).

3.1.3. *Bissectrices.* Soient D et D' des droites affines concourantes en O, dirigées respectivement par des vecteurs unitaires u et u'. Les bissectrices de D et D' sont les droites dirigées par $u+u'$ et $u-u'$. Elles sont perpendiculaires. La seule donnée de D et D' ne permet pas de distinguer les deux bissectrices. Si Δ est l'une d'elles, on a

$$(D, \Delta) = (\Delta, D')$$

L'ensemble des points du plan équidistants de D et D' est la réunion de leurs deux bissectrices.

3.1.4. *Angle géométrique de vecteurs ou de droites.* On définit une (nouvelle) relation d'équivalence parmi les angles orientés de vecteurs en décrétant que (u, v) et (u', v') sont équivalents si et seulement si soit $(u', v') = (u, v)$, soit $(u', v') = (v, u)$. Un *angle géométrique de vecteurs* est une classe d'équivalence pour cette relation. On peut penser à un tel angle, encore noté (u, v), comme au secteur angulaire compris entre u et v (le point est que l'on ne distingue pas un côté de l'autre).

On procède de la même façon pour les angles géométriques de droites. Attention, ces angles ne forment pas un groupe (on ne peut pas les ajouter) !

3.2. Mesure des angles. On n'a pas eu besoin pour définir les angles orientés d'orienter le plan. En revanche, si on veut *mesurer* les angles orientés, il faut choisir une orientation, ce qui revient à fixer un sens positif de mesure. Dans une base orthonormée *directe*, on a vu que la matrice d'une rotation est toujours la même, à savoir

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

ce qui définit le réel θ de façon unique modulo 2π. On l'appelle *une mesure de l'angle orienté.* On a facilement

$$\cos\theta = \frac{\langle u, v\rangle}{\|u\|\|v\|}$$

mais ce nombre (qui ne dépend pas du choix d'une orientation) ne définit pas θ uniquement modulo 2π (θ et $-\theta$ ont le même cosinus).

Sans orientation, on ne peut pas faire la différence entre la mesure d'un angle orienté et celle de son opposé. En revanche, pour les angles *géométriques* de vecteurs, on peut définir une unique mesure dans $[0, \pi]$ par la formule ci-dessus (dans $[0, \frac{\pi}{2}]$ pour les angles géométriques de droites).

La situation est résumée dans le tableau suivant.

Angle	Mesure
orienté de deux vecteurs (classe d'équivalence de paires de vecteurs)	Sans orientation : dans $[0, \pi]$ Avec orientation : modulo 2π
orienté de deux droites (on identifie (u, v) et $(\pm u, \pm v)$)	Sans orientation : dans $[0, \frac{\pi}{2}]$ Avec orientation : modulo π
géométrique de deux vecteurs (on identifie (u, v) et (v, u))	Avec ou sans orientation : dans $[0, \pi]$
géométrique de deux droites (on identifie (u, v), (v, u) et $(\pm u, \pm v)$)	Avec ou sans orientation : dans $[0, \frac{\pi}{2}]$

Exercice 22. Puissance d'un point par rapport à un cercle. Ensemble des points dont le rapport des distances à deux points A et B est constant, ou tels que l'angle de droites (ou de demi-droites) (MA, MB) soit constant.

4. Similitudes

Définition 1. *(Similitudes vectorielles) Soit $\overrightarrow{E}$ un espace vectoriel euclidien. Un endomorphisme $\overrightarrow{f} : \overrightarrow{E} \to \overrightarrow{E}$ est une* similitude *s'il existe un réel $k > 0$ tel que*

$$\forall x \in \overrightarrow{E} \qquad \|\overrightarrow{f}(x)\| = k\|x\|$$

En d'autres termes, $\frac{1}{k}\overrightarrow{f}$ est une isométrie $\overrightarrow{u}$, ou encore $\overrightarrow{f} = \overrightarrow{h}_k \circ \overrightarrow{u}$, où $\overrightarrow{h}_k$ est l'isométrie de rapport k. Les similitudes de $\overrightarrow{E}$ forment un groupe : la composée d'une similitude de rapport k et d'une similitude de rapport k' est une similitude de rapport kk' ; l'inverse d'une similitude de rapport k est une similitude de rapport $1/k$.

Définition 2. *(Similitudes affines) Soit E un espace affine euclidien. Un bijection affine $f : E \to E$ est une* similitude *si l'endomorphisme associé de $\overrightarrow{E}$ est une similitude vectorielle. Cela revient à dire*

$$\forall A, B \in E \qquad \|\overrightarrow{f(A)f(B)}\| = k\|\overrightarrow{AB}\|$$

Les similitudes de E forment un groupe.

Exemples : isométries, homothétie $h_{A,k}$ de centre A et de rapport $k \neq 0$.

Une similitude est *directe* ou *indirecte* selon que son déterminant est positif ou négatif.

PROPOSITION 5. *Une similitude affine qui n'est pas une isométrie a un unique point fixe.*

DÉMONSTRATION. Soit A un point quelconque de E. On cherche un point O de E tel que $O = f(O)$, c'est-à-dire

$$\overrightarrow{f}(\overrightarrow{OA}) = \overrightarrow{f(O)f(A)} = \overrightarrow{Of(A)} = \overrightarrow{OA} + \overrightarrow{Af(A)}$$

ou encore

$$(\overrightarrow{f} - \mathrm{Id}_{\overrightarrow{E}})(\overrightarrow{OA}) = \overrightarrow{Af(A)}$$

Or les valeurs propres de $\overrightarrow{f}$ sont nécessairement de module le rapport k de f. Comme f n'est pas une isométrie, $k \neq 1$ et $\overrightarrow{f} - \mathrm{Id}_{\overrightarrow{E}}$ est inversible. Le point O est donc uniquement déterminé :

$$O = A + (\overrightarrow{f} - \mathrm{Id}_{\overrightarrow{E}})^{-1}(\overrightarrow{Af(A)})$$

□

5. Similitudes planes

Une similitude plane directe s'écrit

$$f = h_k \circ r_\theta$$

avec $k > 0$. On dit que θ est l'angle de la similitude (et k son rapport). Les similitudes directes conservent les angles orientés.

PROPOSITION 6. *Soit E un plan affine euclidien. Une bijection affine de E qui conserve les angles orientés est une similitude directe.*

DÉMONSTRATION. Quitte è composer la bijection f avec une translation, on peut supposer que f a un point fixe. On vectorialise en ce point. Soit u un vecteur unitaire. Il existe une similitude qui envoie $f(u)$ sur u ; quitte à composer f avec cette similitude, on peut supposer $f(u) = u$. Pour tout v non nul, on a $(u, v) = (f(u), f(v)) = (u, f(v))$ donc il existe un scalaire non nul t_v tel que $f(v) = t_v v$.

On a de même $f(u + v) = t_{u+v}(u + v)$ et $f(u + v) = f(u) + f(v) = u + t_v v$. Si (u, v) est libre, on en déduit $1 = t_{u+v} = t_v$, d'où $f(v) = v$. Si v est colinéaire à u, on a aussi directement $f(v) = v$ puisque $f(u) = u$.

Ceci montre que f est l'identité. □

En complexes, les similitudes directes sont toutes les applications

$$z \mapsto az + b$$

avec $a \neq 0$ (les similitudes indirectes sont du type $z \mapsto a\bar{z} + b$). Le rapport est $|a|$, l'angle est l'argument de a.

6. Homographies

Une homographie est une transformation du plan donnée en complexes par

$$z \longmapsto \frac{az+b}{cz+d}$$

où A, b, c et d sont des complexes vérifiant $ad-bc \neq 0$. Si $c \neq 0$, elle n'est pas définie en le point $-d/c$. Une similitude directe est une homographie.

Les homographies forment un groupe noté $PGL(2,\mathbf{C})$, isomorphe à $GL(2,\mathbf{C})/\mathbf{C}^*$.

PROPOSITION 7. *Le groupe $PGL(2,\mathbf{C})$ est engendré par les similitudes directes et l'application $z \mapsto \frac{1}{z}$.*

DÉMONSTRATION. Si $c \neq 0$, l'homographie $z \mapsto \frac{az+b}{cz+d}$ s'écrit

$$z \longmapsto \frac{a}{c} - \frac{ad-bc}{c}\frac{1}{cz+d}$$

Si $c = 0$, c'est une similitude directe. □

PROPOSITION 8. *Une homographie transforme toute droite ou cercle en une droite ou un cercle.*

DÉMONSTRATION. Comme une similitude directe transforme une droite en une droite et un cercle en un cercle, il suffit de montrer que l'homographie $h : z \mapsto \frac{1}{z}$ transforme une droite ne passant pas par 0 en un cercle passant par 0, une droite passant par 0 une droite passant par 0, et un cercle ne passant pas par 0 en un cercle ne passant pas par 0.

Une droite D ne passant pas par 0 peut se paramétrer par $t \mapsto a + tia$, avec a complexe non nul. On a

$$\left|\frac{1}{a+tia} - \frac{1}{2a}\right| = \frac{1}{2|a|}\left|\frac{1-ti}{1+ti}\right| = \frac{1}{2|a|}$$

L'image de D par h est donc le cercle de centre $\frac{1}{2a}$ et de rayon $\frac{1}{2|a|}$, passant par 0.

Une droite D passant par 0 peut se paramétrer par $t \mapsto ta$, avec a complexe non nul. Son image par h est la droite engendrée par le vecteur d'affixe $\frac{1}{a}$.

Un cercle C ne passant pas par 0 peut se paramétrer par $t \mapsto a(1+re^{it})$, avec a complexe non nul et $r \in]0,1[$. On a

$$\begin{aligned}
\left|\frac{1}{a(1+re^{it})} - \frac{1}{a(1-r^2)}\right| &= \frac{1}{|a|}\left|\frac{1-r^2-1-re^{it}}{(1+re^{it})(1-r^2)}\right| \\
&= \frac{r}{|a|(1-r^2)}\left|\frac{1+re^{-it}}{1+re^{it}}\right| \\
&= \frac{r}{|a|(1-r^2)}
\end{aligned}$$

L'image $h(C)$ est donc aussi un cercle ne passant pas par 0. □

Proposition 9. *Une homographie conserve les angles orientés.*

Démonstration. Attention, deux demi-droites concourantes en un point A sont en général envoyées par une homographie h sur deux arcs de cercle concourants de même extrémité $h(A)$. La proposition dit que l'angle orienté des deux demi-droites est égal à l'angle orienté des deux demi-tangentes en les deux arcs de cercle.

Comme une similitude directe conserve les angles orientés, il suffit de le vérifier pour l'homographie $h : z \mapsto \frac{1}{z}$. □

7. Isométries et déplacements de l'espace

Soit f une isométrie d'un espace affine euclidien E de dimension 3. En utilisant la classification des isométries de l'espace vectoriel $\overrightarrow{E}$ effectuée dans le § 6 du chap. 3, et le théorème de décomposition 9, on obtient :

- Soit $\overrightarrow{f}$ est l'identité et f est une translation. L'ensemble des points fixes de f est E si $f = \mathrm{Id}_E$, vide sinon.
- Soit $\overrightarrow{f}$ est une réflexion et f est une *symétrie glissée* par rapport à un plan P, c'est-à-dire la composée d'une réflexion affine et d'une translation par un vecteur parallèle à P. L'ensemble des points fixes de f est P si f est une symétrie, vide sinon.
- Soit $\overrightarrow{f}$ est une rotation et f est un *vissage,* c'est-à-dire la composée d'une rotation affine d'axe D et d'une translation par un vecteur parallèle à D. L'ensemble des points fixes de f est D si f est une rotation, vide sinon.
- soit f est une antirotation affine (avec un unique point fixe).

Dans l'espace, les demi-tours engendrent le groupe des déplacements. En effet, si f est un déplacement et si A est un point quelconque et si $A \neq f(A)$, la composée de f avec un demi-tour d'axe dans le plan médiateur de A et $f(A)$ laisse A fixe. En vectorialisant l'espace E en ce point, on se ramène au cas d'une rotation vectorielle, déjà traité dans l'exercice 14.1) du chap. 3.

PROPOSITION 10. *Deux déplacements de l'espace affine commutent si et seulement si on est dans l'un des cas suivants :*

- *l'un d'eux est l'identité ;*
- *leurs axes sont les mêmes ;*
- *ce sont des demi-tours d'axes (concourants) perpendiculaires.*

DÉMONSTRATION. Il n'est pas difficile de montrer que dans chacune des trois situations ci-dessus, les déplacements commutent.

Inversement, soient ρ_1 et ρ_2 des rotations affines différentes de l'identité et d'axes D_1 et D_2 distincts. On suppose $\rho_1\rho_2 = \rho_2\rho_1$. Soit A un point de D_1. On a $\rho_1(\rho_2(A)) = \rho_2(\rho_1(A)) = \rho_2(A)$: le point $\rho_2(A)$ est invariant par ρ_1 donc est sur D_1. La droite D_1 est donc globalement invariante par ρ_2. Un vecteur directeur $\overrightarrow{u}$ de D_1 est donc envoyé par $\overrightarrow{\rho_2}$ sur $\pm\overrightarrow{u}$. Mais 1 est valeur propre simple de $\overrightarrow{\rho_2}$, et D_1 ne peut être parallèle à D_2 (sinon ces deux droites seraient les mêmes) ; donc $\overrightarrow{\rho_2}(\overrightarrow{u}) = -\overrightarrow{u}$ et -1 est valeur propre de $\overrightarrow{\rho_2}$, qui est un demi-tour. De plus D_1 est perpendiculaire à D_2 et la rencontre.

On raisonne de même en échangeant les rôles de ρ_1 et ρ_2, ce qui prouve que ρ_1 est aussi un demi-tour. $\square$

CHAPITRE 6

Coniques et quadriques

1. Formes quadratiques

Le programme du CAPES ne considère que des formes quadratiques définies dans un espace euclidien. C'est un peu dommage. Je rappelle la définition générale. On suppose le corps $\mathbf{k}$ de caractéristique différente de 2.

Une application $q : E \to \mathbf{k}$ est une *forme quadratique* s'il existe une forme bilinéaire symétrique $B : E \times E \to \mathbf{k}$ telle que

$$q(x) = B(x, x) \qquad \text{pour tout } x \in E.$$

Une astuce classique permet de montrer que la forme B, si elle existe, est uniquement déterminée par q par la formule

$$B(x, y) = \frac{1}{2}\big(q(x + y) - q(x) - q(y)\big)$$

Lorsque E est de dimension finie n, une forme quadratique non nulle s'exprime, en fonction des coordonnées dans une base quelconque $\mathscr{B} = (e_i)$ de E, par un polynôme homogène de degré 2

$$q(x_1e_1 + \cdots + x_ne_n) = \sum_{1\leqslant i\leqslant j\leqslant n} a_{i,j}x_ix_j$$

En d'autres termes, la définition formelle ci-dessus permet de donner un sens à l'idée intuitive de polynôme homogène de degré 2 sans avoir recourt à un choix de base, c'est-à-dire à des coordonnées. En pratique cependant, une forme quadratique est le plus souvent donnée dans une base par un polynôme homogène de degré 2 en les coordonnées. Posons pour tout i et tout j

$$b_{i,i} = a_{i,i} \quad \text{et} \quad b_{i,i} = \frac{1}{2}(a_{i,j} + a_{j,i}) \ \text{ si } i \neq j.$$

On a encore

$$q(x_1e_1 + \cdots + x_ne_n) = \sum_{1\leqslant i,j\leqslant n} b_{i,j}x_ix_j$$

mais la matrice $(b_{i,j})$ est maintenant symétrique. On l'appelle la matrice de la forme quadratique q dans la base $\mathscr{B}$. Si X est la matrice colonne des coordonnées d'un vecteur x dans la base $\mathscr{B}$, on a

$$q(x) = {}^tXBX$$

Tout cela permet d'appliquer à l'étude des formes quadratiques des résultats sur les matrices. Cependant, une forme quadratique n'est pas un endomorphisme, et il faut prendre garde de ne pas confondre les deux. Par exemple, si P est la matrice de passage de $\mathscr{B}$ à une autre base $\mathscr{B}'$ de E, c'est-à-dire la matrice dont les colonnes sont formées des coordonnées des vecteurs de $\mathscr{B}'$ dans la base $\mathscr{B}$, la matrice de q dans la base $\mathscr{B}'$ est ${}^tPBP$.

Le premier résultat essentiel est qu'il existe toujours une base *orthogonale* pour q. Cela signifie simplement qu'il existe une base dans laquelle la matrice de q est diagonale, ou encore dans laquelle q s'écrit comme combinaison linéaire de carrés

$$q(x_1e_1 + \cdots + x_ne_n) = b_1x_1^2 + \cdots + b_nx_n^2 \tag{4}$$

On peut aussi dire que l'on a écrit q comme combinaison linéaire de carrés de formes linéaires indépendantes. On obtient ce résultat remarquable par exemple par l'algorithme de réduction de Gauss.

Il y a beaucoup de façons d'écrire une forme quadratique de cette façon, mais

- le nombre de formes linéaires (indépendantes) qui apparaissent est toujours le même : c'est le *rang* de la forme quadratique, égal aussi au rang de sa matrice dans n'importe quelle base ;
- *lorsque* $\mathbf{k} = \mathbf{R}$, le nombre de carrés qui apparaissent avec le signe $+$ et le nombre de carrés qui apparaissent avec le signe $-$ sont toujours les mêmes : on appelle ces deux nombres la *signature* de la forme quadratique.

Exercice 23. Écrire la forme quadratique

$$q(x_1, x_2, x_3) = x_1x_2 + x_2x_3 + x_3x_1$$

sur $\mathbf{R}^3$ comme combinaison linéaire de carrés de formes linéaires indépendantes. Quel est son rang ? Quelle est sa signature ?

Revenons enfin dans le cadre strict du programme : celui d'une forme quadratique définie sur un espace vectoriel euclidien E de dimension finie n. Le résultat principal (dit d'« orthogonalisation simultanée ») est qu'*il existe une base orthonormée de E orthogonale pour q,* ou encore, dans laquelle q s'écrit comme en (4).

La démonstration est immédiate lorsque l'on connaît le théorème 3 : la matrice B de q dans une base orthonormée quelconque de E est symétrique. Cette matrice est diagonalisable dans une base orthonormée $\mathscr{B}$; cela signifie qu'il existe une matrice *orthogonale* P telle que $P^{-1}BP$ soit diagonale. Mais $P^{-1} = {}^tP$, et ${}^tPBP$ est la matrice de q dans la base $\mathscr{B}$, qui est ainsi orthogonale pour q.

Il est important de bien comprendre la démonstration ci-dessus et en particulier de bien distinguer les différents sens du mot « orthogonal ».

Exercice 24. Dans l'espace euclidien $\mathbf{R}^3$, trouver une base orthonormée orthogonale pour la forme quadratique

$$q(x_1, x_2, x_3) = x_1x_2 + x_2x_3 + x_3x_1$$

2. Définition des quadriques

Le plus correct est de définir une quadrique par son équation. Soit E un espace affine réel. Un *polynôme de degré* 2 est une application $f : E \to \mathbf{R}$ telle qu'il existe un point O, une forme quadratique q *non nulle* sur $\overrightarrow{E}$, une forme linéaire ℓ sur $\overrightarrow{E}$ et une constante c telles que

$$\forall M \in E \qquad f(M) = q(\overrightarrow{OM}) + \ell(\overrightarrow{OM}) + c$$

Si on change le point O en O', la forme de f reste la même :

$$\begin{aligned} f(M) &= q(\overrightarrow{OO'} + \overrightarrow{O'M}) + \ell(\overrightarrow{OO'} + \overrightarrow{O'M}) + c \\ &= q(\overrightarrow{O'M}) + 2b(\overrightarrow{OO'}, \overrightarrow{O'M}) + \ell(\overrightarrow{O'M}) + q(\overrightarrow{OO'}) + \ell(\overrightarrow{OO'}) + c \end{aligned}$$

la forme linéaire ℓ et la constante c changent, mais pas la forme quadratique q.

Dans tout repère cartésien, f s'écrit donc comme un polynôme de degré 2 en 2 variables

$$f(x_1, \ldots, x_n) = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{i,j} x_i x_j + \sum_{1 \leqslant i \leqslant n} b_i x_i + c$$

dont la partie homogène de degré 2 est donnée par q.

On appelle *quadrique affine de E* la classe d'équivalence d'un polynôme de degré 2 pour la relation $f \sim g \Leftrightarrow f = tg$, avec $t \neq 0$ (on dit *conique* si E est de dimension 2). *L'image* de la quadrique f est

$$Q_f = \{M \in E \mid f(M) = 0\}$$

Elle peut être vide.

Il est clair que l'on a, en dimension 2, différentes « sortes » de coniques :

- $f(x, y) = x^2$; l'image est une droite « double », q est dégénérée ;
- $f(x, y) = xy$; l'image est réunion de deux droites, q est non dégénérée ;
- $f(x, y) = x^2 - y$; l'image est une parabole, q est dégénérée ;
- $f(x, y) = x^2 + y^2 - 1$; l'image est un cercle, q est non dégénérée.

On a envie de distinguer les deux dernières comme étant de « vraies » coniques. Il est clair que le fait que q soit ou non dégénérée n'a pas de rapport. Pour distinguer ces cas, on introduit l'homogénéisé de f : c'est la forme quadratique définie sur $\overrightarrow{E} \times \mathbf{R}$ par

$$Q(u, z) = q(u) + \ell(u)z + cz^2$$

Si on change de point O (donc ℓ et c changent), on obtient une forme quadratique équivalente à Q, donc de même rang. Dans les quatre cas précédents, cela donne :

- $Q(x,y,z) = x^2$; la forme quadratique Q est dégénérée ;
- $Q(x,y,z) = xy$; la forme quadratique Q est dégénérée ;
- $Q(x,y,z) = x^2 - yz$; la forme quadratique Q est non dégénérée ;
- $Q(x,y,z) = x^2 + y^2 - z^2$; la forme quadratique Q est non dégénérée.

DÉFINITION 3. *La quadrique f est* propre *si son homogénéisée Q est non dégénérée.*

DÉFINITION 4. *On dit que la quadrique f est* à centre *s'il existe un point* unique *Ω tel que*

$$f(M) = q(\overrightarrow{\Omega M}) + c$$

Le point Ω est alors un centre de symétrie pour l'image de f.

En d'autres termes, cela signifie que dans un repère cartésien d'origine Ω, la quadrique s'écrit

$$f(x_1, \dots, x_n) = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{i,j} x_i x_j + c$$

(on n'a plus de terme linéaire).

PROPOSITION 11. *La quadrique f est* à centre *si et seulement si la forme quadratique q est non dégénérée.*

La quadrique propre définie par $x_1^2 - x_2$ n'est donc pas à centre.

DÉMONSTRATION. On a vu que si l'on change l'origine O en Ω, le terme linéaire de f devient

$$M \longmapsto 2B(\overrightarrow{O\Omega}, \overrightarrow{\Omega M}) + \ell(\overrightarrow{\Omega M})$$

La forme bilinéaire B induit une application linéaire

$$\begin{array}{cccc} \Phi : & E & \longrightarrow & E^* \\ & x & \longmapsto & \big(y \mapsto B(y,x)\big) \end{array}$$

On veut donc $\Phi(2\overrightarrow{\Omega O}) = \ell$.

Si q (donc B) est non dégénérée, Φ est bijective, donc Ω existe et est unique. Réciproquement, si Ω existe et est unique, le noyau de Φ est réduit à $\{0\}$, donc Φ est injective, donc bijective, et B (donc q) est non dégénérée. □

Conseil pratique. Le centre peut être déterminé en résolvant le système de n équations linéaires

$$\frac{\partial f}{\partial x_1}(\Omega) = \cdots = \frac{\partial f}{\partial x_n}(\Omega) = 0$$

(pour qu'il n'y ait plus de terme linéaire). Si la quadrique est à centre, il y a une solution unique ; sinon, le système n'est pas Kramer, il y a une infinité de solutions, mais il n'y a pas de centre.

3. Classification euclidienne des coniques

Soit E un espace affine euclidien réel. Une quadrique propre à centre s'écrit, dans un repère orthonormé convenable d'origine le centre,

$$f(x_1, \ldots, x_n) = \alpha_1 x_1^2 + \cdots + \alpha_n x_n^2 + c$$

où $\alpha_1, \ldots, \alpha_n$ et c sont non nuls (puisque q et Q sont non dégénérées).

En particulier, dans un plan affine euclidien réel, une conique propre à centre d'image non vide s'écrit, dans un repère orthonormé convenable d'origine le centre,

- soit $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ (avec $a \geqslant b > 0$) ; c'est une ellipse, et un cercle si $a = b$;
- soit $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$ (avec $a \geqslant b > 0$) ; c'est une hyperbole, dite équilatère si $a = b$.

Une conique propre sans centre s'écrit, dans un repère orthonormé convenable,

- $y^2 = 2px$; c'est une parabole.

Une autre façon de comprendre cet énoncé est de dire que toute conique propre d'image non vide est image d'une des coniques du type précédent par une *isométrie* (on dit aussi qu'elles sont isométriques).

On dit que l'on a une classification *euclidienne* des coniques (propres). On peut en déduire leur classification *affine*. Soit

$$q(\overrightarrow{OM}) + \ell(\overrightarrow{OM}) + c$$

une conique propre. Elle s'écrit dans un repère convenable

- soit $x^2+y^2 = -1$; elle est vide et q est définie positive ou négative (c'est-à-dire que sa signature est $(+,+)$ ou $(-,-)$) ;
- soit $x^2 + y^2 = 1$; c'est une ellipse et q est définie positive ou négative (c'est-à-dire que sa signature est $(+,+)$ ou $(-,-)$) ;
- soit $x^2 - y^2 = 1$; c'est une hyperbole et q n'est pas définie (c'est-à-dire que sa signature est $(+,-)$) ;
- soit $y^2 = x$; c'est une parabole et q est dégénérée.

De nouveau, cela signifie qu'une conique propre est image par une transformation affine d'une des coniques ci-dessus.

Il est important de comprendre que l'on peut lire le type d'une conique sur son équation

$$f(M) = q(\overrightarrow{OM}) + \ell(\overrightarrow{OM}) + c = 0$$

dans n'importe quel repère. On suppose que la conique est propre, c'est-à-dire que la forme quadratique Q homogénéisée de f est non dégénérée. La conique est :

- vide si Q (donc aussi q) est définie ;
- une ellipse si q est définie (positive ou négative) mais pas Q ;
- une hyperbole si q est non dégénérée mais pas définie ;
- une parabole si q est dégénérée.

Exercice 25. Soit $(\overrightarrow{\imath}, \overrightarrow{\jmath})$ la base canonique de $\mathbf{R}^2$. Quelle est la nature de la conique définie dans le repère $(\overrightarrow{\imath}, \overrightarrow{\imath} + \overrightarrow{\jmath})$ par l'équation $y = x^2$? Déterminer son sommet.

Exemple 10. Exemple d'étude de la conique

$$f(x, y) = 2x^2 + xy + y^2 - 3x + y - 2$$

Détermination du type de la conique. La forme quadratique $Q(x, y, z) = 2x^2 + xy + y^2 - 3xz + yz - 2z^2$ peut se réduire par le processus de Gauss en

$$\begin{aligned} Q(x, y, z) &= 2\Big(x + \frac{1}{4}y - \frac{3}{4}z\Big)^2 - 2\Big(\frac{1}{4}y - \frac{3}{4}z\Big)^2 + y^2 + yz - 2z^2 \\ &= 2\Big(x + \frac{1}{4}y - \frac{3}{4}z\Big)^2 + \frac{7}{8}y^2 + \frac{7}{4}yz - \frac{25}{8}z^2 \\ &= 2\Big(x + \frac{1}{4}y - \frac{3}{4}z\Big)^2 + \frac{7}{8}(y+z)^2 - 4z^2 \end{aligned}$$

Elle est non dégénérée, donc la conique est propre. La forme quadratique $q(x, y) = 2x^2 + xy + y^2$ peut se réduire en $q(x, y) = 2(x + \frac{1}{4}y)^2 + \frac{7}{8}y^2$. Elle est définie ; comme Q ne l'est pas, on a une ellipse.

Détermination du centre. On pose $x = x' + x_0$ et $y = y' + y_0$. La conique devient

$$\begin{aligned} 2 &= 2(x' + x_0)^2 + (x' + x_0)(y' + y_0) + (y' + y_0)^2 - 3(x' + x_0) + (y' + y_0) \\ &= 2x'^2 + x'y' + y'^2 + x'(4x_0 + y_0 - 3) + y'(x_0 + 2y_0 + 1) \\ &\qquad + 2x_0^2 + x_0y_0 + y_0^2 - 3x_0 + y_0 \end{aligned}$$

On ne veut plus de terme linéaire, c'est-à-dire[1]

$$4x_0 + y_0 - 3 = x_0 + 2y_0 + 1 = 0$$

qui se résoud en $x_0 = 1$ et $y_0 = -1$. Ce sont les coordonnées du centre Ω. Si on place l'origine en Ω, la conique devient

$$2x'^2 + x'y' + y'^2 = 4$$

Détermination des axes. Il s'agit de trouver une base orthonormée qui soit orthogonale pour q. Il faut donc diagonaliser la matrice $\begin{pmatrix} 2 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}$. Les valeurs propres sont les racines du polynôme

$$\begin{vmatrix} X - 2 & -\frac{1}{2} \\ -\frac{1}{2} & X - 1 \end{vmatrix} = X^2 - 3X + \frac{7}{4}$$

[1] C'est exactement le système $\frac{\partial f}{\partial x}(x_0, y_0) = \frac{\partial f}{\partial y}(x_0, y_0) = 0$.

c'est-à-dire $\frac{1}{2}(3 \pm \sqrt{2})$. Des vecteurs propres sont $\overrightarrow{e}_\pm = (1, -1 \pm \sqrt{2})$. Ils sont bien orthogonaux et dirigent les axes de notre ellipse. Dans le repère orthonormé $\left(\Omega, \frac{1}{\|\overrightarrow{e}_+\|}\overrightarrow{e}_+, \frac{1}{\|\overrightarrow{e}_-\|}\overrightarrow{e}_-\right)$, la conique s'écrit

$$\frac{1}{2}(3+\sqrt{2})x''^2 + \frac{1}{2}(3-\sqrt{2})y''^2 = 4$$

Les demi-axes de l'ellipse sont donc $\sqrt{\frac{8}{3\pm\sqrt{2}}}$.

4. Classification euclidienne des quadriques

Dans un espace affine euclidien réel de dimension 3, une quadrique propre à centre d'image non vide s'écrit, dans un repère orthonormé convenable d'origine le centre,

- soit $\frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} = 1$, c'est un ellipsoïde ;
- soit $\frac{x^2}{a^2} + \frac{y^2}{b^2} - \frac{z^2}{c^2} = 1$, c'est un hyperboloïde à une nappe ;
- soit $\frac{x^2}{a^2} - \frac{y^2}{b^2} - \frac{z^2}{c^2} = 1$, c'est un hyperboloïde à deux nappes.

On obtient de même la classification affine : toute quadrique propre à centre s'écrit dans un repère convenable

- soit $x^2 + y^2 + z^2 = -1$, elle est vide ;
- soit $x^2 + y^2 + z^2 = 1$, c'est un ellipsoïde ;
- soit $x^2 + y^2 - z^2 = 1$, c'est un hyperboloïde à une nappe ;
- soit $x^2 - y^2 - z^2 = 1$, c'est un hyperboloïde à deux nappes.

De nouveau, le type de la quadrique peut se lire sur les signatures des formes quadratiques Q et q.

Exercice 26. Quelle est la nature de la quadrique définie par l'équation $xy + yz + zx = 1$ dans $\mathbf{R}^3$?

5. Coniques

5.1. Foyers et directrices.

Proposition 12. *Dans un plan affine euclidien E, on considère une conique propre d'image non vide C qui n'est pas un cercle. Il existe un point F, appelé* foyer*, une droite D ne contenant pas F, appelée* directrice*, et un réel $e > 0$, appelé* excentricité*, tels que*

$$C = \{M \in E \mid MF = ed(M, D)\}$$

La conique est une ellipse si $e < 1$, une parabole si $e = 1$, une hyperbole si $e > 1$.

Démonstration. On détermine explicitement l'équation de ce lieu en prenant $F = (c, 0)$ et D d'équation $x = h$. On obtient

$$(x - c)^2 + y^2 = e^2(x - h)^2$$

C'est donc bien une conique. Si $e = 1$, il n'y a pas de terme en x^2 ; si on prend $h = -c$ et on obtient $y^2 = 4cx$.

Si $e \neq 1$, on peut prendre $h = \frac{c}{e^2}$ et il n'y a pas de terme en x. On obtient

$$\frac{x^2}{c^2/e^2} + \frac{y^2}{(1 - e^2)c^2/e^2} = 1$$

Inversement, une conique propre qui n'est pas un cercle est de ce type. On a $a = \frac{c}{e}$, $h = \frac{a}{e}$ et :

- pour une ellipse, $c^2 = a^2 - b^2$;
- pour une hyperbole, $c^2 = a^2 + b^2$.

$\square$

Une parabole a un unique couple foyer-directrice (F, D), tandis que les ellipses et les hyperboles en ont deux. Une ellipse s'écrit

$$\{M \mid MF + MF' = 2\alpha\}, \text{ où } 2\alpha > FF'.$$

Une hyperbole s'écrit

$$\{M \mid |MF - MF'| = 2\alpha\}, \text{ où } 2\alpha < FF'.$$

Démonstration. L'ellipse est contenue dans la bande entre les deux directrices. Pour tout point M de cette ellipse, on a donc

$$MF + MF' = ed(M, D) + ed(M, D') = ed(D, D')$$

Inversement, on suppose $F = (c, 0)$ et $F' = (-c, 0)$. On a

$$\begin{aligned} MF'^2 + MF^2 &= 2(x^2 + y^2 + c^2) \\ MF'^2 - MF^2 &= 4cx \end{aligned}$$

On a donc

$$\begin{aligned} & MF + MF' = 2\alpha \\ \iff\ & MF' - MF = \frac{2c}{\alpha}x \\ \iff\ & MF = \alpha - \frac{c}{\alpha}x \quad \text{et} \quad MF' = \alpha + \frac{c}{\alpha}x \\ \iff\ & MF'^2 + MF^2 = \Big(\alpha - \frac{c}{\alpha}x\Big)^2 + \Big(\alpha + \frac{c}{\alpha}x\Big)^2 = 2\Big(\alpha^2 + \frac{c^2}{\alpha^2}x^2\Big) \end{aligned}$$

On obtient donc l'équation

$$(\alpha^2 - c^2)\Big(\frac{x^2}{\alpha^2} - 1\Big) + y^2 = 0$$

c'est-à-dire

$$\frac{x^2}{\alpha^2} + \frac{y^2}{\alpha^2 - c^2} = 1$$

qui est bien une ellipse. Réciproquement, toute ellipse peut se mettre sous cette forme.

Le cas de l'hyperbole est laissé en exercice. □

5.2. Représentation polaire. On prend pour origine de coordonnées polaires un foyer F et une origine angulaire perpendiculaire à la directrice correspondante, qui est à distance d de F. On a alors, pour un point M de coordonnées (r, θ),

$$MF = |\rho| \quad , \quad d(M, D) = |d - \rho\cos\theta|.$$

L'équation de la conique de foyer F, directrice D et excentricité e est alors $|\rho| = e|d - \rho\cos\theta|$. Comme les points de coordonnées (r, θ) et coordonnées $(-r, \theta + \pi)$ sont les mêmes, cette équation est équivalente à

$$\rho = \frac{ed}{1 + e\cos\theta}$$

Si $e = 1$ (parabole), on a une direction asymptotique pour $\theta = \pi$. Pour $e > 1$ (hyperbole), on a deux asymptotes correspondant à $\cos\theta = 1/e$. Pour $e \neq 1$, on a

$$d = a\frac{|1 - e^2|}{e}$$

5.3. Tangente et normale. Considérons un point $M = (x_0, y_0)$ d'une conique propre à centre C d'équation

$$\alpha x^2 + \beta y^2 = 1$$

et une droite D paramétrée par $t \mapsto (x_0 + tu, y_0 + tv)$ passant par M. Les points d'intersection de D avec C correspondent aux solutions de l'équation

$$1 = \alpha(x_0 + tu)^2 + \beta(y_0 + tv)^2$$

Ces solutions sont $t = 0$ (correspondant au point M) et

$$t_1 = -\frac{2(\alpha u x_0 + \beta v y_0)}{\alpha u^2 + \beta v^2} \tag{5}$$

On dit que D est *la tangente à C en M* si $t_1 = 0$. La droite D ne rencontre alors C qu'en M. L'équation de la tangente à C en M est donc

$$\alpha x_0 x + \beta y_0 y = 1$$

La *normale* à C en M est la perpendiculaire en M à la tangente.

La discussion précédente s'applique aussi aux paraboles par un calcul analogue. Elle est de toute façon un cas particulier de la situation plus générale d'une courbe plane définie par une équation (non nécessairement polynomiale) $f(x, y) = 0$. En un point (x_0, y_0) de cette courbe, la tangente à C est par définition la droite d'équation

$$(x - x_0)\frac{\partial f}{\partial x}(x_0, y_0) + (y - y_0)\frac{\partial f}{\partial y}(x_0, y_0) = 0$$

sous réserve que les dérivées partielles $\frac{\partial f}{\partial x}(x_0, y_0)$ et $\frac{\partial f}{\partial y}(x_0, y_0)$ ne soient pas toutes deux nulles (ce qui est toujours le cas pour une conique propre).

Proposition 13. *Soit C l'image (non vide) d'une conique propre qui n'est pas un cercle, soit F un foyer et soit D la directrice associée. Soit M un point de C ; on suppose que la perpendiculaire à MF en F rencontre D en un point P. La droite MP est la tangente à C en M.*

Démonstration. Soit N un point de PM autre que M. Soit N' sa projection sur D et soit N'' sa projection sur FP. Soit M' la projection de M sur D. On a

$$e = \frac{MF}{MM'} = \frac{NN''}{NN'} < \frac{NF}{NN'}$$

donc N n'est pas sur C. La droite PM ne rencontre donc C qu'en M : c'est la tangente à C en M. □

Corollaire 3. *Soit C l'image (non vide) d'une conique propre à centre, de foyers F et F' et soit M un point de C. La tangente à C en M est la bissectrice intérieure (resp. extérieure) de l'angle $\widehat{FMF'}$ si C est une hyperbole (resp. ellipse).*

Démonstration. Soit N la projection de M sur D et soit N' la projection de M sur D'. La tangente à C en M coupe D en P et D' en P'. On a

$$\frac{MF}{MF'} = \frac{eMN}{eMN'} = \frac{MP}{MP'}$$

Les triangles rectangles MFP et $MF'P'$ sont donc semblables. Les angles $\widehat{FMP}$ et $\widehat{F'MP'}$ sont donc égaux. □

Exercice 27. Énoncer et démontrer l'analogue du corollaire 3 pour les paraboles.

5.4. Paramétrisation des coniques. On peut paramétrer l'ellipse

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$$

par

$$t\mapsto(a\cos t, b\sin t)$$

De même, l'hyperbole

$$\frac{x^2}{a^2}-\frac{y^2}{b^2}=1$$

peut être paramétrée par

$$t\mapsto(\pm a\operatorname{ch} t, b\operatorname{sh} t)$$

(où $\operatorname{ch} t=\frac{1}{2}(e^t+e^{-t})$ et $\operatorname{sh} t=\frac{1}{2}(e^t-e^{-t})$).

Mais on peut utiliser la discussion précédente sur les sécantes à une conique pour obtenir des paramétrisations par des fractions rationnelles. Considérons le point $M=(-a,0)$ de l'ellipse

$$\frac{x^2}{a^2}\pm\frac{y^2}{b^2}=1$$

Comme on l'a vu plus haut, les points d'intersection de la droite D paramétrée par $t\mapsto(-a+t,tv)$ (et passant par M) avec C correspondent à $t=0$ (c'est le point M) et

$$t=\frac{2a}{1+\frac{a^2}{b^2}v^2}$$

On obtient la paramétrisation

$$v\mapsto(-a+\frac{2a}{1+\frac{a^2}{b^2}v^2}, v\,\frac{2a}{1+\frac{a^2}{b^2}v^2})$$

ou plus simplement, en prenant comme paramètre $u=av/b$,

$$v\mapsto(a\,\frac{1-u^2}{1+u^2}, b\,\frac{2u}{1+u^2})$$

EXERCICE 28. Obtenir une paramétrisation analogue pour les hyperboles.

6. Application à la résolution d'équations quadratiques dans Z

Quel rapport peut-il y avoir entre les coniques et les équations diophantiennes ? Le lien est le suivant. Supposons donnée une quadrique f à coefficients dans $\mathbf{Q}$, ou même plus généralement dans un corps $\mathbf{k}$ *de caractéristique différente de* 2. Si la forme quadratique q est non dégénérée, la quadrique f est à centre (la démonstration de la prop. 11 est valable sur tous les corps). En se plaçant dans un repère d'origine ce centre et d'axes dirigés par une base qui est *orthogonale* pour q, on peut supposer que f s'écrit

$$f(x_1,\dots,x_n) = \alpha_1 x_1^2 + \cdots + \alpha_n x_n^2 + c$$

où $\alpha_1,\dots,\alpha_n$ et c sont des éléments de $\mathbf{k}$ non nuls. Supposons connu un point $M_0 \in \mathbf{k}^n$ de l'image C de f (c'est-à-dire une solution dans $\mathbf{k}^n$ de l'équation $f(x_1,\dots,x_n) = 0$).

Si $M \in \mathbf{k}^n$ est un autre point de C, la droite M_0M est dirigée par un vecteur de $\mathbf{k}^n$. Inversement, si $\overrightarrow{u} \in \mathbf{k}^n$ n'est pas nul, la droite passant par M_0 et dirigée par $\overrightarrow{u}$ recoupe C en un autre point *à coordonnées dans* $\mathbf{k}^n$. Nous avons déjà démontré cela lorsque $n = 2$ en § 5.3 : la formule (5) montre que lorsque α, β, x_0, y_0, u et v sont dans $\mathbf{k}$, alors t_1 y est aussi. Cela se montre par un calcul analogue en général.

En résumé, cette construction permet de trouver *toutes* les solutions dans $\mathbf{k}^n$ de l'équation $f(x_1,\dots,x_n) = 0$ lorsqu'on en connaît une.

Exemple 11. *Trouver une infinité de solutions* entières *de l'équation*

$$2x^2 + xy + y^2 = 4z^2$$

Une solution évidente est $(0,0,0)$. On suppose donc que x, y et z ne sont pas tous nuls.

Si $z = 0$, on a $y \neq 0$ et $r = x/y$ est solution de $2r^2 + r + 1 = 0$, qui n'a pas de solution rationnelle. C'est donc impossible.

Donc $z \neq 0$. En divisant par z^2, on est ramené à chercher les solutions *rationnelles* de l'équation

$$2x^2 + xy + y^2 = 4$$

Une solution évidente est $(1,1)$. On cherche les autres sous la forme $(1+tu, 1+tv)$, avec u et v dans $\mathbf{Z}$. On obtient

$$\begin{aligned} 4 &= 2(1+tu)^2 + (1+tu)(1+tv) + (1+tv)^2 \\ &= 4 + t\big(5u + 3v + t(2u^2 + uv + v^2)\big) \end{aligned}$$

d'où

$$t_1 = -\frac{5u+3v}{2u^2+uv+v^2}$$

et

$$x = 1 - \frac{u(5u+3v)}{2u^2+uv+v^2} \qquad y = 1 - \frac{v(5u+3v)}{2u^2+uv+v^2}$$

On obtient les solutions de l'équation d'origine en réduisant x et y au même dénominateur. Des solutions sont par exemple données par

$$\begin{aligned} x &= 2u^2 + uv + v^2 - u(5u+3v) = -3u^2 - 2uv + v^2 \\ y &= 2u^2 + uv + v^2 - v(5u+3v) = 2u^2 - 4uv - 2v^2 \\ z &= 2u^2 + uv + v^2 \end{aligned}$$

Comment retrouve-t-on la solution $(1,1,1)$ (penser à la tangente) ?

Exercice 29. Trouver toutes les solutions entières de l'équation

$$2x^2+4xy+y^2+x=8$$

7. Quadriques sur un corps fini

Pourquoi s'arrêter en si bon chemin ? On a expliqué plus haut qu'une bonne partie de la théorie des quadriques s'applique sur un corps $\mathbf{k}$ quelconque de caractéristique différente de 2.

Considérons le cas où $\mathbf{k}$ est le corps $\mathbf{Z}/p\mathbf{Z}$, où p est un nombre premier *impair.*

Proposition 14. *L'image d'une quadrique à centre dans* $(\mathbf{Z}/p\mathbf{Z})^n$ *n'est jamais vide pour* $n \geqslant 2$.

Démonstration. On a vu que dans un repère affine convenable, la quadrique s'écrit

$$f(x_1,\dots,x_n)=\alpha_1x_1^2+\dots+\alpha_nx_n^2+c$$

où $\alpha_1,\dots,\alpha_n$ sont des éléments de $\mathbf{Z}/p\mathbf{Z}$ non nuls.

On va chercher des éléments x_1 et x_2 de $\mathbf{Z}/p\mathbf{Z}$ tels que

$$0=f(x_1,x_2,0,\dots,0)=\alpha_1x_1^2+\alpha_2x_2^2+c$$

On note $(\mathbf{Z}/p\mathbf{Z})^2$ l'ensemble des carrés de $\mathbf{Z}/p\mathbf{Z}$, c'est-à-dire l'image de l'application

$$\begin{array}{rccc}\varphi: & \mathbf{Z}/p\mathbf{Z} & \longrightarrow & \mathbf{Z}/p\mathbf{Z}\\ & x & \longmapsto & x^2\end{array}$$

Attention, $(\mathbf{Z}/p\mathbf{Z},\ \times\ )$ n'est pas un groupe, mais $((\mathbf{Z}/p\mathbf{Z})^*,\ \times\ )$ en est un ! Et $\varphi : (\mathbf{Z}/p\mathbf{Z})^* \to (\mathbf{Z}/p\mathbf{Z})^*$ est un morphisme de groupes. Son noyau est $\{x \in (\mathbf{Z}/p\mathbf{Z})^* \mid x^2=1\}$. Or dans un corps, le polynôme $x^2-1=(x-1)(x+1)$ a au plus deux racines, 1 et -1 (qui sont bien distinctes ici car la caractéristique est différente de 2). L'image $\varphi((\mathbf{Z}/p\mathbf{Z})^*)=((\mathbf{Z}/p\mathbf{Z})^*)^2$ est donc de cardinal

$$\frac{\mathrm{Card}(\mathbf{Z}/p\mathbf{Z})^*}{\mathrm{Card}(\mathrm{Ker}(\varphi))}=\frac{p-1}{2}$$

et $\mathrm{Card}(\mathbf{Z}/p\mathbf{Z})^2=\frac{p+1}{2}$. L'image de l'application injective

$$\begin{array}{ccc}(\mathbf{Z}/p\mathbf{Z})^2 & \longrightarrow & \mathbf{Z}/p\mathbf{Z}\\ x_1^2 & \longmapsto & -\frac{1}{\alpha_2}(\alpha_1x_1^2+c)\end{array}$$

est donc aussi de cardinal $\frac{p+1}{2}$. Comme $2\frac{p+1}{2}>p$, elle doit donc rencontrer $(\mathbf{Z}/p\mathbf{Z})^2$: ceci signifie qu'il existe $x_2 \in \mathbf{Z}/p\mathbf{Z}$ tel que $-\frac{1}{\alpha_2}(\alpha_1x_1^2+c)=x_2^2$, et termine la démonstration. $\square$

Une fois que l'on a une solution dans $(\mathbf{Z}/p\mathbf{Z})^n$ de l'équation $f(x_1, \ldots, x_n) = 0$ (attention, la démonstration de la proposition ne donne pas de *méthode* pour en trouver ; elle dit seulement qu'il en existe !), on obtient toutes les autres avec la méthode habituelle : couper la quadrique avec une droite passant par la solution.

Exemple 12. Résoudre la congruence

$$x^2 + xy + y^2 + x + 1 \equiv 0 \pmod 5$$

Olivier DEBARRE
Institut de Recherche Mathématique Avancée – UMR 7501
UFR de Mathématique et Informatique
7 rue René Descartes
Université Louis Pasteur
67084 Strasbourg Cedex – France

e-mail : debarre@math.u-strasbg.fr