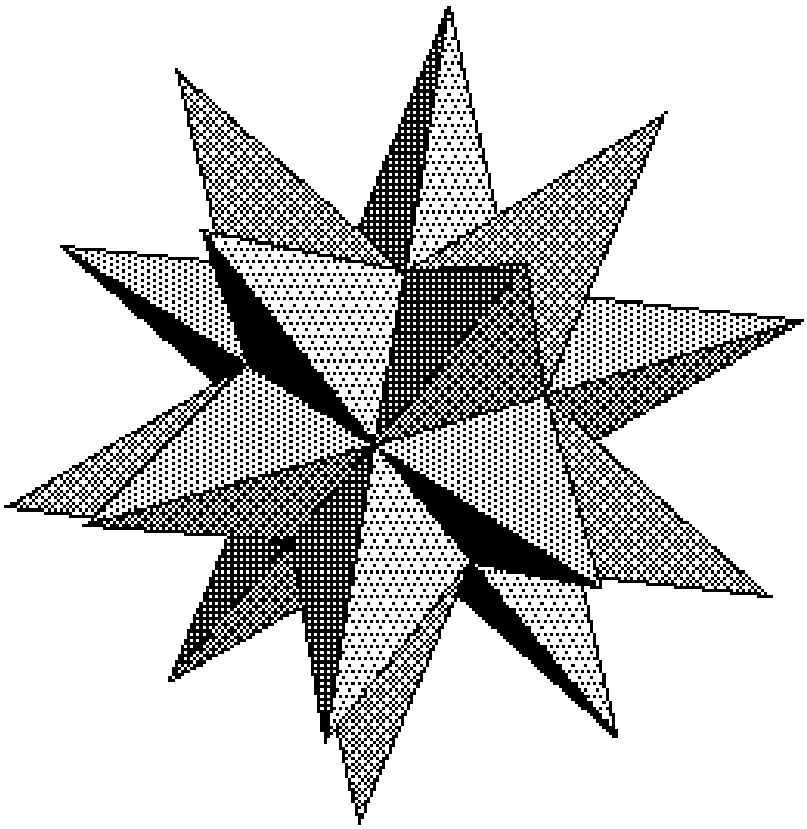
MAFPEN de La Réunion

Préparation à l'agrégation interne de mathématiques

Plans de leçons d'algèbre et de géométrie



Dominique TOURNÈS

juin 1994

BARYCENTRES ; APPLICATIONS

Remarques générales

• Le programme officiel est très sobre : “Barycentres”. On dispose donc d’une grande liberté. Il peut être tentant de faire une théorie savante en plongeant l’espace affine et son espace vectoriel associé dans un “espace universel”, mais il est sans doute préférable de se contenter d’une introduction naïve et de réserver la plus grande partie du temps aux applications.

• Ne pas oublier l’origine mécanique du barycentre. On trouvera un bon paragraphe à ce sujet dans AVEZ.

Plan

1. <u>Notion de barycentre</u>

a) Définitions et notations

On se place dans un espace affine réel E de dimension n. $(A_i)_{1\leq i\leq p}$ désigne une famille finie de points de E et $(\alpha_i)_{1\leq i\leq p}$ une famille de réels. On note $\alpha = \sum_{i=1}^{p} \alpha_i$.

• Si $\alpha = 0$, le vecteur $\sum_{i=1}^{p} \alpha_i \overrightarrow{OA_i}$ ne dépend pas de l’origine O, on le note $\sum_{i=1}^{p} \alpha_i A_i$.

• Si $\alpha \neq 0$, le point $O + \frac{1}{\alpha}\sum_{i=1}^{p} \alpha_i \overrightarrow{OA_i}$ ne dépend pas de l’origine O, on le note $\frac{1}{\alpha}\sum_{i=1}^{p} \alpha_i A_i$ et on l’appelle <u>barycentre</u> des <u>points massiques</u> (A_i, α_i).

b) Propriétés

• Commutativité

• Homogénéité (on peut donc se ramener à une masse totale égale à 1)

• Associativité (application : isobarycentre d’un triangle, point de concours des trois médianes et isobarycentre d’un tétraèdre, point de concours de sept droites remarquables)

• Construction du barycentre de deux points

2. <u>Caractérisation à l’aide du barycentre des objets de la géométrie affine</u>

Sous-espaces affines. Une partie F de E est un sous-espace affine ssi elle est stable par barycentration.

Convexité. Notions de segment, de partie convexe et d’enveloppe convexe. Une partie F de E est convexe ssi elle est stable par barycentration à coefficients positifs. L’enveloppe convexe d’une partie F de E est l’ensemble des barycentres à coefficients positifs des familles finies de points de F.

Repère affine. $(A_0, A_1, ..., A_n)$ est un repère affine ssi tout point M de E s’écrit de manière unique $M = \sum_{i=1}^{n} \alpha_i A_i$ avec $\alpha = 1$. Le (n+1)-uplet (α_i) est alors appelé famille des <u>coordonnées barycentriques</u> (normalisées) du point M dans le repère affine (A_i). Application : paramétrisation des sous-espaces affines.

Applications affines. Une application est affine ssi elle conserve les barycentres. Une application affine est entièrement déterminée par l’image d’un repère affine.

3. <u>Autres applications du barycentre</u>

a) Réduction des fonctions de Leibniz

• On appelle <u>fonction vectorielle de Leibniz</u> l'application $f : E \to \vec{E}, M \mapsto \sum_{i=1}^{p} \alpha_i \overrightarrow{MA_i}$.

$$\text{Si } \alpha = 0,\ f(M) = \sum_{i=1}^{p} \alpha_i A_i \text{ , si } \alpha \neq 0,\ f(M) = f(G) + \alpha \overrightarrow{MG}.$$

• On appelle <u>fonction scalaire de Leibniz</u> l'application $g : E \to \mathbf{R}, M \mapsto \sum_{i=1}^{p} \alpha_i MA_i^2$.

$$\text{Si } \alpha = 0,\ g(M) = g(O) + 2\overrightarrow{MO}.f(O) \text{, si } \alpha \neq 0,\ g(M) = g(G) + \alpha MG^2.$$

Applications : Lieux géométriques, problèmes d'optimisation.

b) Problèmes d'alignement et de concours (dans le plan)

• Trois points $M_1(x_1, y_1, z_1)$, $M_2(x_2, y_2, z_2)$ et $M_3(x_3, y_3, z_3)$, définis par des coordonnées barycentriques (normalisées ou non), sont alignés ssi $\begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix} = 0$.

• Une droite D a une équation de la forme ux + vy + wz = 0, avec u, v, w non égaux tous les trois. Une autre équation u'x + v'y + w'z = 0 de ce type représente la même droite ssi les triplets (u, v, w) et (u', v', w') sont proprotionnels. On dit que (u, v, w) est une famille de <u>coordonnées tangentielles</u> de D.

• Trois droites $D_1(u_1, v_1, w_1)$, $D_2(u_2, v_2, w_2)$ et $D_3(u_3, v_3, w_3)$, définies par des coordonnées tangentielles, sont concourantes ou parallèles ssi $\begin{vmatrix} u_1 & v_1 & w_1 \\ u_2 & v_2 & w_2 \\ u_3 & v_3 & w_3 \end{vmatrix} = 0$.

Applications : théorèmes de Menelaüs et de Ceva, théorème de Desargues, théorème de Pappus.

c) Théorèmes de Routh

Etant donnés un triangle ABC et des points X, Y, Z situés respectivement sur les côtés (BC), (CA), (AB) et distincts des sommets, on pose $\frac{\overline{BX}}{\overline{XC}} = \lambda$, $\frac{\overline{CY}}{\overline{YA}} = \mu$, $\frac{\overline{AZ}}{\overline{ZB}} = \nu$. On suppose que (BY) et (CZ) se coupent en L, (CZ) et (AX) en M, (AX) et (BY) en N. On note MNP l'aire algébrique d'un triangle orienté (M, N, P). Alors :

$$\frac{XYZ}{ABC} = \frac{\lambda\mu\nu + 1}{(\lambda+1)(\mu+1)(\nu+1)} \quad \text{et} \quad \frac{LMN}{ABC} = \frac{(\lambda\mu\nu - 1)^2}{(\lambda\mu + \lambda + 1)(\mu\nu + \mu + 1)(\nu\lambda + \nu + 1)}$$

Application : on retrouve les théorèmes de Menelaüs et de Ceva.

Bibliographie

AVEZ, *La leçon de géométrie à l'oral de l'agrégation*, Masson
TISSERON, *Géométries affine, projective et euclidienne*, Hermann

CERCLES DANS LE PLAN

Remarques générales

• Le programme est bref et assez vague : “En dimension 2 : cercles. Equation polaire d’un cercle passant par l’origine. Puissance d’un point par rapport à un cercle. Faisceaux linéaires de cercles.” Pourtant les cercles interviennent constamment en géométrie et les résultats sont innombrables : chacun pourra bâtir une leçon très personnelle.

• Attention : le paragraphe 4 (qu’on peut limiter aux similitudes) suppose connu le théorème fondamental de la géométrie affine.

Plan

1. Le cercle dans le plan

• Définition.
• Intersection d’un cercle et d’une droite, de deux cercles.
• Equation cartésienne, représentations paramétriques et équation complexe d’un cercle, équation polaire d’un cercle passant par l’origine.
• Lieu des points M tels que $\sum_{i=1}^{n} \alpha_i MA_i^2 = k$. Lieu des points M tels que $\frac{MA}{MB} = k$ *(cercles d’Appolonius).*

2. Condition de cocyclicité de quatre points

• Avec des angles de droites : A, B, C, D sont cocycliques ou alignés ssi $(AC, AD) = (BC, BD)$.

• Avec des nombres complexes : A, B, C, D sont cocycliques ou alignés ssi le birapport $\frac{d-a}{c-a} \Big/ \frac{d-b}{c-b}$ est réel.

• Avec des distances : A, B, C, D sont cocycliques ou alignés dans cet ordre ssi $AC.BD = AB.CD + AD.BC$. *(théorème de Ptolémée)*

Exercice 1 : *(Droite de Simson)*. L’ensemble des points qui se projettent en des points alignés sur les côtés d’un triangle est le cercle circonscrit.

Exercice 2 : Les cercles circonscrits aux quatre triangles d’un quadrilatère complet sont concourants.

3. Puissance d’un point par rapport à un cercle. Faisceaux de cercles

a) Puissance d’un point par rapport à un cercle

• On appelle puissance du point M par rapport au cercle Γ, de centre O, de rayon R et d’équation normale $x^2 + y^2 + ax + by + c = 0$, le nombre $P_\Gamma(M) = OM^2 - R^2 = x^2 + y^2 + ax + by + c$. Pour toute droite passant par M et rencontrant Γ en A et B (A = B si c’est une tangente), on a $P_\Gamma(M) = \overline{MA}.\overline{MB}$.

• Axe radical de deux cercles non concentriques ; construction. Centre radical de trois cercles dont les centres ne sont pas alignés.

Exercice 3 : *(Théorème de Pascal)*. Les côtés opposés d’un hexagone inscrit dans un cercle se coupent en trois points alignés.

Exercice 4 : Construire un cercle passant par deux points donnés et tangent à un cercle donné.

b) Faisceaux linéaires de cercles

• Etant donnés deux cercles distincts C_1 et C_2, d'équations normales $f_1(M) = 0$ et $f_2(M) = 0$, on appelle faisceau linéaire de cercles de base C_1 et C_2 l'ensemble des cercles d'équation normale $\lambda f_1(M) + (1 - \lambda) f_2(M) = 0$, avec $\lambda \in \mathbf{R}$. Remarque : deux cercles distincts quelconques du faisceau sont aussi des cercles de base du faisceau.

• *Description du faisceau F de cercles de base C_1 et C_2* :

1) Si C_1 et C_2 ont le même centre Ω, alors F est l'ensemble des cercles de centre Ω. On dit que F est un faisceau concentrique.

2) Supposons C_1 et C_2 non concentriques. Par un point M du plan, il passe un et un seul cercle de F si M n'appartient pas à l'axe radical de C_1 et C_2, tous les cercles de F si $M \in C_1 \cap C_2$, aucun cercle de F sinon.

- Si $C_1 \cap C_2 = \{A, B\}$, F est l'ensemble des cercles contenant A et B. On dit que F est le faisceau à points de base A et B.
- Si C_1 et C_2 ont une tangente commune D en A, F est l'ensemble des cercles tangents à D en A. On dit que F est un faisceau tangent.
- Si C_1 et C_2 sont disjoints, F contient exactement deux cercles points P et Q et les cercles de F sont centrés sur (PQ) \ ]PQ[. On dit que F est le faisceau à points limites P et Q.

4. Transformations conservant les cercles

a) Similitudes

Les bijections du plan dans lui-même qui transforment tout cercle en un cercle sont exactement les similitudes.

Exercice 5 : Construire un cercle passant par un point donné et tangent à deux droites données.

b) Inversions

On travaille désormais dans le plan conforme $\mathbf{C} \cup \{\infty\}$ et on appelle "cercle" soit un cercle de $\mathbf{C}$, soit la réunion d'une droite de $\mathbf{C}$ et du point à l'infini. L'inversion de pôle P et de puissance k ($k \neq 0$) est l'application i définie par $i(P) = \infty$, $i(\infty) = P$ et sinon $i(M) = M'$ où M' est le point de (PM) tel que $\overline{PM}.\overline{PM'} = k$.

Une inversion est une bijection involutive qui transforme tout cercle en un cercle.

c) Transformations circulaires

Les bijections du plan conforme dans lui-même qui transforment tout cercle en un cercle sont exactement les homographies $z \to \frac{az + b}{cz + d}$ et les antihomographies $z \to \frac{a\bar{z} + b}{c\bar{z} + d}$ ($ad - bc \neq 0$).

Bibliographie

RAMIS, DESCHAMPS et ODOUX, *Cours de mathématiques spéciales, tome 2*, Masson
BERGER, *Géométrie, tome 2*, CEDIC/Nathan
TISSERON, *Géométries affine, projective et euclidienne*, Hermann
LEHMANN et BKOUCHE, *Initiation à la géométrie*, PUF
COXETER, *Introduction to geometry*, Wiley

CHANGEMENTS DE BASE EN ALGÈBRE LINÉAIRE ; APPLICATIONS

Remarques générales

Thèmes du programme en rapport direct avec le sujet :
1) Effet d'un changement de base(s) sur la matrice d'une application linéaire. Matrices équivalentes. Caractérisation à l'aide du rang.
2) Matrices semblables. Réduction d'un endomorphisme en dimension finie. Diagonalisation. Trigonalisation.
3) Décomposition d'une forme quadratique en somme de carrés. Méthode de Gauss.

Plan

E et F sont des espaces vectoriels sur **K** = **R** ou **C**, de dimensions finies respectives n et p.

1. <u>Problème du changement de base</u>

Soient B = (e_i) et B' = (e'_i) deux bases de E. La matrice $\boxed{P = \left(e_i^*(e'_j)\right)}$ est appelée <u>matrice de passage</u> de B à B'. C'est la matrice de l'identité, considérée comme application de E muni de B' vers E muni de B ; c'est donc une matrice inversible, élément de $GL_n(\mathbf{K})$. Si un vecteur a pour coordonnées X dans B et X' dans B', on a la <u>formule de changement de base</u> $\boxed{X = P\,X'}$.

2. <u>Changement de bases et matrice d'une application linéaire</u>

a) Matrices équivalentes

• Soit f une application linéaire de E dans F, de matrice M lorsque E est muni d'une base B et F d'une base C, et de matrice M' lorsque E est muni d'une base B' et F d'une base C'.
Si P est la matrice de passage de B à B' et Q la matrice de passage de C à C', on a $\boxed{M' = Q^{-1}\,M\,P}$.

• On dit que deux matrices M et N, éléments de $M_{p,n}(\mathbf{K})$, sont <u>équivalentes</u> s'il existe $P \in GL_n(\mathbf{K})$ et $Q \in GL_p(\mathbf{K})$ telles que $N = Q^{-1}\,M\,P$. (Deux matrices rectangulaires sont équivalentes ssi elles peuvent représenter la même application linéaire.)

b) Caractérisation des classes d'équivalence

Toute matrice M de $M_{p,n}(K)$ est équivalente à une unique matrice de la forme $\left(\begin{array}{c|c} I_r & 0_{r,n-r} \\ \hline 0_{p-r,r} & 0_{p-r,n-r} \end{array}\right)$. L'entier r n'est autre que le rang de M. Deux matrices sont équivalentes ssi elles ont le même rang. Il y a inf(n, p) + 1 classes d'équivalence.

Calcul pratique **:** Le calcul du rang de M et l'obtention de bases dans lesquelles f a une matrice réduite peuvent se faire par opérations élémentaires sur les lignes et sur les colonnes de M.

3. <u>Changement de base et matrice d'un endomorphisme</u>

a) Matrices semblables

• Soit f un endomorphisme de E, de matrice M lorsque E est muni de la base B, de matrice M' lorsque E est muni de la base B'.
Si P est la matrice de passage de B à B', on a $\boxed{M' = P^{-1}\,M\,P}$.

• On dit que deux matrices M et N, éléments de $M_n(\mathbf{K})$, sont <u>semblables</u> s'il existe $P \in GL_n(\mathbf{K})$ telle que $N = P^{-1}\,M\,P$. (Deux matrices carrées sont semblables ssi elles peuvent représenter le même endomorphisme.)

• Les notions suivantes sont des invariants des classes de similitude : rang, déterminant, trace, polynôme caractéristique, polynôme minimal. Ces notions sont donc attachées intrinsèquement à f.

b) Réduction d'une matrice à la forme diagonale ou triangulaire

• La caractérisation complète des classes de similitude est hors de portée. On se contentera de donner les formes réduites usuelles : matrices diagonales ou triangulaires. On dit que f est diagonalisable (resp. trigonalisable) si M est semblable à une matrice diagonale (resp. triangulaire).

Théorèmes usuels de réduction :
• f est trigonalisable ssi son polynôme caractéristique est scindé.
• f est diagonalisable ssi son polynôme caractéristique est scindé et si, pour toute valeur propre, l'ordre de multiplicité de cette valeur propre est égal à la dimension du sous-espace propre correspondant.

c) Des applications en analyse

Étude des systèmes de suites récurrentes linéaires et des systèmes différentiels linéaires par changement de base.

4. Changement de base et matrice d'une forme quadratique

a) Matrices congruentes

• Soit q une forme quadratique sur E (il revient au même d'étudier la forme bilinéaire symétrique associée), de matrice M dans une base B, et de matrice M' dans une base B' (M et M' sont des matrices symétriques).
Si P est la matrice de passage de B à B', on a $M' = {}^tP\,M\,P$.

• On dit que deux matrices symétriques M et N, éléments de $M_n(K)$, sont congruentes s'il existe $P \in GL_n(\mathbf{K})$ telle que $N = {}^tP\,M\,P$. (Deux matrices symétriques sont congruentes ssi elles peuvent représenter la même forme quadratique.)

b) Caractérisation des classes de congruence

• Si **K** = **C**, toute matrice symétrique M de $M_n(\mathbf{K})$ est congruente à une unique matrice de la forme $\left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0_{n-r} \end{array}\right)$.
L'entier r n'est autre que le rang de M. Deux matrices de $M_n(\mathbf{C})$ sont congruentes ssi elles ont le même rang.
Il y a n + 1 classes de congruence.
• Si **K** = **R**, toute matrice symétrique M de $M_n(\mathbf{K})$ est congruente à une unique matrice de la forme $\left(\begin{array}{c|c|c} I_s & 0 & 0 \\ \hline 0 & -I_t & 0 \\ \hline 0 & 0 & 0_{n-s-t} \end{array}\right)$. Le couple d'entiers (s, t) est appelé signature de M. Deux matrices de $M_n(\mathbf{R})$ sont congruentes ssi elles ont la même signature. Il y a $\frac{(n+1)(n+2)}{2}$ classes de congruence.

Calcul pratique : Pour la détermination du rang, de la signature et d'une base dans laquelle q a une matrice réduite, on peut utiliser la méthode de Gauss.

c) Une application en géométrie

Classification affine des coniques et des quadriques.

Bibliographie

LANG, *Algèbre linéaire 1 et 2*, InterÉditions
RAMIS, DESCHAMPS et ODOUX, *Cours de mathématiques spéciales, tomes 1 et 2*, Masson

APPLICATIONS GÉOMÉTRIQUES DES NOMBRES COMPLEXES : ÉTUDE DE CONFIGURATIONS, DE TRANSFORMATIONS …

Remarques générales

• Nous donnons seulement un inventaire des questions qui peuvent être abordées. La leçon gagnera à être illustrée par quelques exercices substantiels.

• Il ne faut pas se contenter du programme de Terminale ! Étudier à l'aide des nombres complexes les inversions et les transformations circulaires permet d'élargir le plan de façon intéressante.

Plan

1. Principes de l'utilisation des nombres complexes en géométrie

• Soit P un plan affine euclidien orienté muni d'un repère orthonormé direct $(O, \vec{I}, \vec{J})$. L'application $P \to \mathbf{C}$, $M = O + x\vec{I} + y\vec{J} \mapsto z = x + iy$, est un isomorphisme d'espaces affines euclidiens orientés. On dit que z est l'affixe du point M et on note M(z). L'application associée $\vec{P} \to \mathbf{C}$, $\vec{u} = x\vec{I} + y\vec{J} \mapsto z = x + iy$, est un isomorphisme d'espaces vectoriels euclidiens orientés. On dit que z est l'affixe du vecteur $\vec{u}$ et on note $\vec{u}(z)$.

• Étant donnés deux vecteurs $\vec{u}_1(z_1)$ et $\vec{u}_2(z_2)$, leur produit scalaire s'exprime par $\vec{u}_1.\vec{u}_2 = \mathrm{Re}(z_1\bar{z}_2)$ et leur angle $(\vec{u}_1, \vec{u}_2)$ a pour mesure $\arg\left(\frac{z_2}{z_1}\right)$. (C'est justement l'existence de la fonction argument, isomorphisme de $(\mathbf{U}, \times)$ sur $(\mathbf{R}/2\pi\mathbf{Z}, +)$ qui permet de mesurer les angles !)

• Soit f : M ↦ M' une application de P dans P. f s'identifie à l'application z ↦ z' de **C** dans **C**, avec M(z) et M'(z'), appelée expression complexe de f.

2. Étude de configurations

a) Droites et cercles

• *Droites*

Toute droite a une équation complexe de la forme $\bar{a}z + a\bar{z} + b = 0$, avec $a \in \mathbf{C}^*$ et $b \in \mathbf{R}$. Réciproquement, toute équation de cette forme représente une droite, de vecteur normal a et passant par $-\frac{b}{2\bar{a}}$.

• *Condition d'alignement*

Trois points distincts A, B, C sont alignés ssi le rapport $\frac{c-a}{b-a}$ est réel.

• *Cercles*

Tout cercle a une équation complexe de la forme $z\bar{z} + \bar{a}z + a\bar{z} + b = 0$, avec $a \in \mathbf{C}$ et $b \in \mathbf{R}$. Réciproquement, toute équation de cette forme représente un cercle, de centre - a et de rayon $\sqrt{|a|^2 - b}$, ou l'ensemble vide.

• *Conditions de cocyclicité*

Quatre points distincts A, B, C, D sont cocycliques ou alignés ssi le birapport $\frac{d-a}{c-a} \Big/ \frac{d-b}{c-b}$ de leurs affixes est réel, ssi AB.CD ± AC.BD ± AD.BC = 0.

b) Polygones réguliers

Un polygone $A_1A_2\dots A_n$ (il est pratique d'indicer avec **Z**/n**Z**, de sorte que n + 1 = 1) est dit <u>régulier</u> lorsque tous ses côtés A_iA_{i+1} sont égaux et tous ses angles $\left(\overrightarrow{A_iA_{i-1}}, \overrightarrow{A_iA_{i+1}}\right)$ sont égaux. Pour étudier un tel polygone, on travaille dans le plan complexe en prenant pour origine l'isobarycentre O des A_i et en posant $a_1 = 1$.

• $A_1A_2\dots A_n$ est un polygone régulier ssi, pour tout i, $a_i = \xi^{i-1}$, où ξ est une racine primitive n-ème de l'unité. • Il y a $\frac{\varphi(n)}{2}$ polygones réguliers à n côtés (φ étant l'indicatrice d'Euler) dont un seul est convexe (les autres sont dits <u>étoilés</u>).

3. <u>Étude de transformations</u>

a) Similitudes

• La translation de vecteur $\vec{u}(b)$ a pour expression complexe z' = z + b. La rotation de centre $\Omega(\omega)$ et d'angle θ a pour expression complexe $z' = e^{i\theta}z + (1 - e^{i\theta})\omega$. Réciproquement, toute expression complexe z' = az + b, avec |a| = 1, représente une translation si a = 1, une rotation si $a \neq 1$.

• La réflexion d'axe D, d'équation $\bar{\alpha}z + \alpha\bar{z} + \beta = 0$ a pour expression complexe $z' = -\frac{\alpha\bar{z} + \beta}{\bar{\alpha}}$. Réciproquement, toute expression complexe z' = a $\bar{z}$ + b, avec |a| = 1, représente une réflexion si $a\bar{b} + b = 0$, une réflexion-translation si $a\bar{b} + b \neq 0$.

f est une similitude directe (resp. indirecte) ssi il existe des nombres complexes $a \neq 0$ et b tels que, pour tout nombre complexe z, f(z) = az + b (resp. $a\bar{z} + b$).

b) Inversions

On travaille désormais dans le plan conforme $\mathbf{C} \cup \{\infty\}$ et on appelle "cercle" soit un cercle de **C**, soit la réunion d'une droite de **C** et du point à l'infini. L'<u>inversion de pôle P et de puissance k</u> ($k \neq 0$) est l'application i définie par i(P) = ∞, i(∞) = P et sinon i(M) = M' où M' est le point de (PM) tel que $\overline{PM}.\overline{PM'} = k$. Son expression complexe est $z' = p + \frac{k}{\bar{z} - \bar{p}}$ (plus simplement $z' = \frac{k}{\bar{z}}$ si on prend le pôle pour origine).

Une inversion est une bijection involutive qui transforme tout cercle en un cercle.

c) Transformations circulaires

Les bijections du plan conforme dans lui-même qui transforment tout cercle en un cercle sont exactement les homographies $z \to \frac{az + b}{cz + d}$ et les antihomographies $z \to \frac{a\bar{z} + b}{c\bar{z} + d}$ (ad - bc $\neq$ 0).

Bibliographie

TISSERON, *Géométries affine, projective et euclidienne*, Hermann
BERGER, *Géométrie tome 2*, CEDIC/Fernand Nathan
AVEZ, *La leçon de géométrie à l'oral de l'agrégation*, Masson
ARNAUDIÈS et FRAYSSE, *Cours de mathématiques, tome 1*, Dunod

PROPRIÉTÉS DU CORPS DES NOMBRES COMPLEXES

Remarques générales

• “La leçon sur les nombres complexes ne saurait se réduire à munir l’ensemble des couples de réels d’une structure de corps : entre autres, le théorème de D’Alembert-Gauss est au programme, et on doit en connaître une démonstration.” (rapport du jury 1989)

• “Les leçons sur les nombres complexes restent d’un niveau insuffisant. Il faut dire que **C** est complet, même si c’est de l’analyse. Un candidat à l’agrégation doit avoir réfléchi sérieusement au problème de la mesure des angles, en particulier à la notion d’argument d’un nombre complexe, et ne peut se contenter de ce qu’en dit le programme de Terminale - a fortiori d’une ficelle qu’on enroule sur une poulie circulaire !” (rapport du jury 1990)

• Ces remarques précisent sans ambiguïté le cadre de la leçon. La structure de corps étant acquise, il s’agit de se consacrer aux thèmes suivants : topologie de **C**, notion d’argument d’un nombre complexe et applications en trigonométrie et géométrie (notamment mesure des angles), propriété de clôture algébrique et applications en analyse.

Plan

Introduction

On désigne par **C** le **R**-espace vectoriel $\mathbf{R}^2$, muni de la multiplication (x, y) (x’, y’) = (xx’ - yy’, xy’ + yx’). **C** est une **R**-algèbre de dimension 2, et un corps commutatif, dont les éléments sont appelés nombres complexes. **R** s’identifie à l’ensemble des nombres complexes de la forme (x, 0). Une base de **C** est (1, i), avec 1 = (1, 0) et i = (0, 1). On suppose connues les notions de partie réelle, partie imaginaire, conjugué et module.

1. Topologie de C

L’application $z \mapsto |z|$ est une norme sur **C**. Muni de cette norme, **C** est d’une part un plan euclidien, d’autre part une **R**-algèbre normée ayant les propriétés suivantes :

- Toute suite bornée admet au moins une valeur d’adhérence.
- Les parties compactes de **C** sont les parties fermées et bornées.
- **C** est complet.

2. Argument d’un nombre complexe

a) Nombres complexes de module 1

L’application $z \mapsto |z|$ est un homomorphisme du groupe multiplicatif $\mathbf{C}^*$ dans le groupe multiplicatif $\mathbf{R}_+^*$. Son noyau, noté **U**, est appelé groupe des nombres complexes de module 1.

L’application $z \mapsto \left(|z|, \frac{z}{|z|} \right)$ est un isomorphisme du groupe multiplicatif $\mathbf{C}^*$ sur le groupe produit $\mathbf{R}_+^* \times \mathbf{U}$.

b) Exponentielle complexe

Pour tout complexe z, la série $\sum \frac{z^n}{n!}$ est absolument convergente, donc convergente. Sa somme $\sum_{n=0}^{+\infty} \frac{z^n}{n!}$ est notée exp(z) ou e^z. L’application $z \mapsto \exp(z)$ est appelée exponentielle (complexe) et notée exp. On définit alors les fonctions cosinus (réel) et sinus (réel) par les formules d’Euler : $\cos x = \mathrm{Re}(e^{ix})$ et $\sin x = \mathrm{Im}(e^{ix})$.

Propriétés :
- exp est un homomorphisme du groupe ($\mathbf{C}$, +) dans le groupe ($\mathbf{C}^*$, $\times$).
- Pour tout complexe z, l'application f : $\mathbf{R} \to \mathbf{C}$, $t \mapsto e^{zt}$, est dérivable et f'(t) = z e^{zt}.
- cos 0 = 1 et cos admet au moins un zéro sur $\mathbf{R}_+$. On appelle nombre pi et on note π le double du plus petit zéro strictement positif de cos.

Théorème fondamental :

L'application $x \mapsto e^{ix}$ est un homomorphisme surjectif du groupe ($\mathbf{R}$, +) sur le groupe ($\mathbf{U}$, $\times$), de noyau $2\pi\mathbf{Z}$.

A partir des résultats précédents, on peut retrouver toutes les propriétés des fonctions usuelles cos, sin et tan introduites naïvement au lycée.

c) Argument d'un nombre complexe

L'isomorphisme de $\mathbf{U}$ sur le groupe quotient $\mathbf{R}/2\pi\mathbf{Z}$, qui résulte du théorème fondamental, est appelé argument et noté arg.

Par abus de langage, on appelle argument d'un nombre complexe z non nul et on note arg(z) l'argument de $\frac{z}{|z|}$.

L'unique représentant de arg(z) appartenant à $]-\pi, \pi]$ est appelé argument principal de z et noté Arg(z).

Si $z = x + iy \in \mathbf{U}\backslash\{-1\}$, on a $\mathrm{Arg}(z) = 2\tan^{-1}\frac{y}{1+x}$.

En résumé :

L'application $z \mapsto (|z|, \arg(z))$ est un isomorphisme du groupe ($\mathbf{C}^*$, $\times$) sur le groupe ($\mathbf{R}_+^*$, $\times$) $\times$ ($\mathbf{R}/2\pi\mathbf{Z}$, +).

d) Applications

- Formule de Moivre, linéarisation de $\cos^n x$, expression de cos nx comme polynôme en cos x (polynômes de Tchebycheff), diverses formules de trigonométrie.
- Racines n-ièmes d'un nombre complexe, groupe des racines n-ièmes de l'unité, racines primitives, polygones réguliers convexes et étoilés, polynômes cyclotomiques (théorème de Wedderburn).
- Mesure des angles dans un plan euclidien orienté, coordonnées polaires, expression complexe des similitudes, conditions de cocyclicité (théorème de Ptolémée).

3. Théorème de D'Alembert-Gauss

Théorème : **C** est algébriquement clos.

Conséquences :
- Les polynômes irréductibles de $\mathbf{C}[X]$ sont les polynômes du premier degré. Dans $\mathbf{R}[X]$, ce sont les polynômes du premier degré et les polynômes du second degré à discriminant strictement négatif.
- Toute matrice A de $M_n(\mathbf{C})$ est trigonalisable. Plus précisément, A est la somme commutative d'une matrice diagonalisable et d'une matrice nilpotente.

Applications :
De façon générale, l'intérêt du théorème de D'Alembert est de permettre de trouver les solutions réelles de problèmes réels en faisant des calculs intermédiaires dans $\mathbf{C}$. C'est le cas dans les situations suivantes :
- Equations algébriques du troisième et du quatrième degré.
- Décomposition des fractions rationnelles en éléments simples
- Systèmes différentiels linéaires d'ordre 1 et équations différentielles linéaires d'ordre n.
- Systèmes de suites à récurrence linéaire d'ordre 1 et suites à récurrence linéaire d'ordre n.

Bibliographie

LELONG-FERRAND et ARNAUDIÈS, *Cours de mathématiques*, Dunod
ARNAUDIÈS et FRAYSSE, *Cours de mathématiques*, Dunod
LEHNING, *Topologie*, Masson

DÉTERMINANTS ; APPLICATIONS

Remarques générales

Ne pas se perdre dans les définitions et propriétés des déterminants, consacrer la moitié du temps aux applications. Celles-ci étant fort nombreuses, on en développera quelques unes selon ses possibilités et on se contentera d'évoquer oralement les autres.

Plan

Soit E un espace vectoriel de dimension finie n sur un corps **K** commutatif de caractéristique nulle (en général **R** ou **C**). On note L(E) l'ensemble des endomorphismes de E et $M_n(\mathbf{K})$ l'ensemble des matrices carrées à coefficients dans **K**. On suppose connue la définition d'une forme n-linéaire alternée (ou, ce qui est équivalent en caractéristique nulle, antisymétrique).

1. Définition et propriétés des déterminants

a) Déterminant d'une famille de n vecteurs

Etant donnée une base B de E, il existe une unique forme n-linéaire alternée φ définie sur E telle que φ(B) = 1. On l'appelle déterminant dans la base B et on la note $\det_B$. Pour toute famille $(u_1, \ldots, u_n)$ de n vecteurs de E, on a

$$\boxed{\det_B(u_1,\ldots,u_n) = \sum_{\sigma\in S_n} \varepsilon(\sigma)\, x_{\sigma(1)1}\cdots x_{\sigma(n)n}},$$

où $(x_{ji})_{1\le j\le n}$ désigne la famille des coordonnées de u_i dans la base B. On écrit : $\det_B(u_1, \ldots, u_n) = \begin{vmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \cdots & x_{nn} \end{vmatrix}$.

Propriétés :

• Changement de base : si C est une autre base, on a $\boxed{\det_B = \det_B(C)\, \det_C}$.

• $\det_B(u_1, \ldots, u_n) = 0$ ssi la famille $(u_1, \ldots, u_n)$ est liée.

• Calcul pratique lorsque n = 2 ou n = 3 *(règle de Sarrus).*

b) Déterminant d'un endomorphisme

Etant donné un endomorphisme f de E, le scalaire $\det_B(f(B))$ ne dépend pas de la base B choisie. On l'appelle déterminant de f et on le note det f. Pour toute famille $(u_1, \ldots, u_n)$ de n vecteurs de E et toute base B, on a

$$\boxed{\det_B(f(u_1),\ldots,f(u_n)) = \det f \times \det_B(u_1,\ldots,u_n)}.$$

Propriétés :

• L'application det : (L(E), ∘) → (**K**, .) est un homomorphisme surjectif de monoïdes. $\boxed{\det f \neq 0 \text{ ssi } f \in \mathrm{GL}(E)}$.
L'application det : (GL(E), ∘) → (**K***, .) est un homomorphisme surjectif de groupes. Son noyau est un sous-groupe distingué de GL(E) appelé groupe spécial linéaire de E et noté SL(E).

• Une base B étant fixée, det f est un polynôme en les coordonnées des vecteurs de la famille f(B). En particulier, det est continue, GL(E) est ouvert, SL(E) est fermé, etc.

c) Déterminant d'une matrice

Etant donnée une matrice M de $M_n(\mathbf{K})$, on appelle déterminant de M et on note det M le déterminant de l'endomorphisme $X \mapsto MX$ de $\mathbf{K}^n$. Si f est un endomorphisme de E de matrice M dans une base B, det f = det M.

Les déterminants des sous-matrices carrées de M sont les mineurs de M. Le mineur d'ordre n - 1 obtenu en enlevant la ligne i et la colonne j se note $D_{ij}(M)$. Le nombre $(-1)^{i+j} D_{ij}(M)$ est le cofacteur d'indice (i, j). La matrice des cofacteurs est la comatrice de M et sa transposée la matrice complémentaire de M , notée $\tilde{M}$.

Propriétés :

• $\boxed{\det {}^tM = \det M}$. (On peut donc travailler sur les lignes au lieu de travailler sur les colonnes.)

• Développement par rapport à une ligne : posons $M = (a_{ij})$; pour tout i, on a : $\boxed{\det M = \sum_{k=1}^{n} (-1)^{i+k} a_{ik} D_{ik}(M)}$.

• M est inversible ssi $\det M \neq 0$. Dans ce cas : $\boxed{M^{-1} = \frac{1}{\det M} \tilde{M}}$.

2. <u>Applications</u>

a) Déterminant de Gram, calcul de la distance de deux sous-espaces

Soit E un espace affine, de direction $\vec{E}$. Le <u>déterminant de Gram</u> d'une famille $(\vec{u}_1, \ldots, \vec{u}_r)$ de vecteurs de $\vec{E}$ est le déterminant de la matrice $\left[(\vec{u}_i | \vec{u}_j)\right]_{1 \leq i, j \leq r}$; on le note $\text{Gram}(\vec{u}_1, \ldots, \vec{u}_r)$.

• $\boxed{\text{La famille } (\vec{u}_1, \ldots, \vec{u}_r) \text{ est libre ssi } \text{Gram}(\vec{u}_1, \ldots, \vec{u}_r) \neq 0}$.

• Soient F et G deux sous-espaces affines de E, A un point de F, B un point de G et $(\vec{u}_1, \ldots, \vec{u}_r)$ une base de $\vec{F} + \vec{G}$. La distance de F à G est donnée par : $\boxed{d^2(F, G) = \frac{\text{Gram}(\overrightarrow{AB}, \vec{u}_1, \ldots, \vec{u}_r)}{\text{Gram}(\vec{u}_1, \ldots, \vec{u}_r)}}$.

Cas particulier : distance d'un point M à un sous-espace affine F.

b) Condition de cocyclicité de quatre points (théorème de Ptolémée)

Soient M_1, M_2, M_3, M_4 quatre points distincts du plan. On note (x_i, y_i) les coordonnées de M_i et $d_{ij} = M_i M_j$. Les points M_1, M_2, M_3, M_4 sont cocycliques ou alignés ssi l'une des conditions équivalentes suivantes est vérifiée :

(i) $\begin{vmatrix} x_1^2 + y_1^2 & x_1 & y_1 & 1 \\ x_2^2 + y_2^2 & x_2 & y_2 & 1 \\ x_3^2 + y_3^2 & x_3 & y_3 & 1 \\ x_4^2 + y_4^2 & x_4 & y_4 & 1 \end{vmatrix} = 0$; (ii) $\begin{vmatrix} 0 & d_{12}^2 & d_{13}^2 & d_{14}^2 \\ d_{12}^2 & 0 & d_{23}^2 & d_{24}^2 \\ d_{13}^2 & d_{23}^2 & 0 & d_{34}^2 \\ d_{14}^2 & d_{24}^2 & d_{34}^2 & 0 \end{vmatrix} = 0$; (iii) $d_{12}d_{34} \pm d_{13}d_{24} \pm d_{14}d_{23} = 0$.

c) Points d'inflexion d'une courbe

Soit Γ la courbe d'équation $f(x, y) = 0$, où f est définie et de classe C^2 sur un ouvert de $\mathbf{R}^2$. Si un point régulier M de Γ est un point d'inflexion, alors ses coordonnées annulent le déterminant $\begin{vmatrix} 0 & f'_x & f'_y \\ f'_x & f''_{x^2} & f''_{xy} \\ f'_y & f''_{xy} & f''_{y^2} \end{vmatrix}$.

Application : une conique non dégénérée n'a pas de point d'inflexion.

d) Autres parties du programme où interviennent des déterminants (voir leçons correspondantes)

• Résolution des systèmes linéaires : déterminant principal, bordants, formules de Cramer.
• Réduction des endomorphismes : polynôme caractéristique.
• Formes quadratiques : discriminant (= déterminant de Gram d'une base), condition de positivité à l'aide des mineurs principaux, classification des coniques et quadriques.
• Problèmes d'incidence en géométrie affine, en coordonnées cartésiennes ou barycentriques.
• Orientation, produits mixte et vectoriel, calcul de distances, aires et volumes, propriétés métriques des courbes.
• Problèmes d'élimination : résultant (= déterminant de Sylvester), discriminant.
• Calcul différentiel : jacobien ; équations différentielles linéaires : wronskien.

Bibliographie

ARNAUDIÈS et FRAYSSE, *Cours de mathématiques*, Dunod
RAMIS, DESCHAMPS et ODOUX, *Cours de mathématiques spéciales*, Masson

L'ELLIPSE DANS LE PLAN AFFINE EUCLIDIEN

Remarques générales

• Cette leçon de synthèse est difficile car il faut organiser soi-même de manière cohérente les multiples résultats éparpillés dans la littérature.

• On a choisi ici de mettre en valeur les propriétés "affines" de l'ellipse, à partir de sa figure réduite qu'est le cercle. On peut aussi se consacrer aux propriétés différentielles et cinématiques de la courbe (courbure, développée, longueur d'un arc d'ellipse : fonctions elliptiques, mouvement des planètes, *etc*).

Plan

1. Notion d'ellipse

a) Théorème et définitions

Soit E une partie du plan. Les propriétés suivantes sont équivalentes :

(i) Il existe deux points distincts F et F' et un réel $a > \frac{FF'}{2}$ tels que E soit le lieu des points M vérifiant MF + MF' = 2a. *(Définition bifocale)*

(ii) Il existe un cercle C et un point F intérieur à C et distinct de son centre tels que E soit la médiatrice de C et de F. *(Définition par foyer et cercle directeur)*

(iii) Il existe une droite D, un point $F \notin D$ et un réel $e \in]0, 1[$ tels que E soit le lieu des points M vérifiant MF = e d(M, D). *(Définition par foyer et directrice)*

(iv) Il existe un repère orthonormé $(O, \vec{i}, \vec{j})$ et des réels a > b > 0 tels que E ait pour équation cartésienne $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$. *(Définition par équation réduite)*

Dans ce cas, on dit que E est une ellipse. A partir d'une étude précise des liens entre les quatre définitions, on définit les foyers, les cercles directeurs, les directrices, l'excentricité, le grand axe (ou axe focal), le petit axe, le centre, les sommets, le cercle principal, le cercle secondaire.

Si on pose $c = \frac{FF'}{2}$, on a $\boxed{e = \frac{c}{a} = \frac{\sqrt{a^2 - b^2}}{a}}$, et la directrice associée au foyer (c, 0) a pour équation $\boxed{x = \frac{a^2}{c}}$.

Un cercle peut être considéré comme une ellipse si on étend la définition (i) (prendre F = F'), la définition (ii) (prendre F au centre de C) ou la définition (iv) (prendre a = b). Par contre, ce n'est pas possible pour la définition (iii).

b) Symétries et construction de la courbe

• Le groupe des isométries de E est $\{id, s_O, s_1, s_2\}$, où s_O est la symétrie centrale de centre O, s_1 la réflexion d'axe $(O, \vec{i})$ et s_2 la réflexion d'axe $(O, \vec{j})$.
• Deux ellipses sont semblables ssi elles ont la même excentricité.
• L'intérieur de E est convexe.
• Les définitions (i), (ii) et (iii) permettent des constructions par points à la règle et au compas. La définition (i) permet aussi un tracé continu ("construction du jardinier"). On peut enfin, grâce à la définition (iv), se ramener à l'étude et à la représentation graphique d'une fonction numérique d'une variable réelle.

c) Equation cartésienne dans un repère orthonormé quelconque

Soit $(\Omega, \vec{I}, \vec{J})$ un repère orthonormé quelconque. E est une ellipse ssi E a une équation cartésienne de la forme $ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0$, avec $\begin{vmatrix} a & b \\ b & c \end{vmatrix} > 0$ et $a \times \begin{vmatrix} a & b & d \\ b & c & e \\ d & e & f \end{vmatrix} < 0$.

d) Equation polaire lorsque le foyer est à l'origine

Soit $(\Omega, \vec{I}, \vec{J})$ un repère orthonormé direct. E est une ellipse de foyer Ω ssi E a une équation polaire de la forme $\rho(1 + e\cos(\theta - \varphi)) = p$ avec $\varphi \in \mathbf{R}$, $e \in]0, 1[$ et $p > 0$. Dans ce cas, E a pour excentricité e et pour directrice la droite d'équation polaire $\rho\cos(\theta - \varphi) = p/e$.

2. <u>La figure réduite de l'ellipse : le cercle</u>

a) Effet d'une transformation affine sur une ellipse

• L'image d'une ellipse par une transformation affine est une ellipse. • Une ellipse est l'image de son cercle principal par l'affinité orthogonale d'axe l'axe focal et de rapport b/a. • Etant donnés une ellipse E et un cercle C, il existe une transformation affine f telle que f(C) = E.

b) Applications

• *Aire de l'ellipse :* L'aire de l'ellipse est πab.
• *Tangentes à l'ellipse :* Une ellipse admet une tangente en chacun de ses points $M_0(x_0, y_0)$, d'équation $\frac{x_0 x}{a^2} + \frac{y_0 y}{b^2} = 1$. Construction de cette tangente. Construction par tangentes de l'ellipse. Construction des tangentes menées à l'ellipse d'un point quelconque du plan.
• *Théorème de Pascal :* Les côtés opposés d'un hexagone inscrit dans une ellipse se coupent en trois points alignés.
• *Ellipse de Steiner :* Il existe une unique ellipse tangente aux trois côtés d'un triangle en leurs milieux.

3. <u>Propriétés angulaires de l'ellipse</u>

• *Propriété angulaire des tangentes :* La tangente en un point M d'une ellipse de foyers F et F' est la bissectrice extérieure de l'angle $\left(\overrightarrow{MF}, \overrightarrow{MF'}\right)$.

• *Théorème de l'angle pivotant :* Si M désigne le point d'intersection des tangentes à une ellipse de foyer F en deux points distincts A et B, la droite (FM) est la bissectrice intérieure de l'angle $\left(\overrightarrow{FA}, \overrightarrow{FB}\right)$. Si une troisième tangente à l'ellipse coupe les tangentes en A et B respectivement en S et T, l'angle de droites (FS, FT) ne dépend que de A et de B et vaut 1/2 $\left(\overrightarrow{FA}, \overrightarrow{FB}\right)$.

4. <u>L'ellipse dans l'espace</u>

• *L'ellipse en tant que section cylindrique :* La section d'un cylindre de révolution par un plan faisant avec l'axe du cylindre un angle $\varphi \in]0, \pi/2]$ est une ellipse d'excentricité $\cos\varphi$.

• *L'ellipse en tant que section conique :* La section d'un cône de révolution de sommet S et de demi-angle au sommet $\theta \in]0, \pi/2[$ par un plan ne passant pas par S et faisant avec l'axe du cône un angle $\varphi \in]\theta, \pi/2]$ est une ellipse d'excentricité $\frac{\cos\varphi}{\cos\theta}$.

Remarque : Toute ellipse est donc une perspective (cylindrique ou conique) de cercle. On pourra s'interroger en particulier sur la représentation en perspective cavalière (*ie* cylindrique) d'une sphère.

Bibliographie

RAMIS, DESCHAMPS et ODOUX, *Cours de mathématiques spéciales, tome 2*, Masson
LEHMANN et BKOUCHE, *Initiation à la géométrie*, PUF
AVEZ, *La leçon de géométrie à l'oral de l'agrégation*, Masson
DELTHEIL et CAIRE, *Géométrie et compléments*, Gabay
LEBOSSÉ et HÉMERY, *Géométrie, Classe de Mathématiques*, Gabay

ENDOMORPHISMES DIAGONALISABLES

Remarques générales

• "Pour certaines leçons, il peut être intéressant de détailler la solution d'un exercice, mais ceux de pure routine sont à proscrire (diagonalisation d'une matrice 3×3, ...)." (Rapport du jury 1989)

• "Le calcul des puissances d'une matrice se fait souvent plus efficacement à l'aide d'un polynôme annulateur qu'à l'aide d'une diagonalisation." (Rapport du jury 1990)

Plan

Introduction

Soient **K** l'un des corps **R** ou **C**, E un **K**-espace vectoriel de dimension finie n et u un endomorphisme de E. On note χ_u le polynôme caractéristique de u, μ_u son polynôme minimal, $m(\lambda)$ l'ordre de multiplicité d'une valeur propre λ de u et $E(\lambda)$ le sous-espace propre associé à λ On suppose connues les généralités concernant ces notions.

1. Endomorphismes diagonalisables

a) Définition et caractérisations

• On dit que u est diagonalisable s'il existe une base de E formée de vecteurs propres de u.

Exemples : Une homothétie et une dilatation sont diagonalisables, une transvection ne l'est pas.

• Les propriétés suivantes sont équivalentes :

(i) u est diagonalisable.
(ii) E est somme directe des sous-espaces propres de u.
(iii) χ_u est scindé et pour toute racine λ de χ_u, $\dim E(\lambda) = m(\lambda)$.
(iv) u annule un polynôme scindé dont toutes les racines sont simples.
(v) μ_u est scindé et n'a que des racines simples.

La seule implication délicate à démontrer est (v) $\Rightarrow$ (i), qui repose sur le lemme des noyaux.

Exercice : Si u et v sont diagonalisables et commutent, alors il existe une base dans laquelle u et v diagonalisent simultanément.

b) Point de vue matriciel

• Une matrice M de $M_n(\mathbf{K})$ s'identifie à l'endomorphisme u : $\mathbf{K}^n \to \mathbf{K}^n$, $X \mapsto MX$. On dit que M est diagonalisable si u est diagonalisable.

• Inversement, si $u \in L(E)$ a pour matrice M dans une base de E, on a les nouvelles caractérisations suivantes de la diagonalisabilité de u :

(vi) Il existe une base de E dans laquelle la matrice de u est diagonale.
(vii) M est semblable à une matrice diagonale.
(viii) M est diagonalisable.

Exercice : L'ensemble des matrices diagonalisables est dense dans $M_n(\mathbf{C})$. C'est faux dans $M_n(\mathbf{R})$.

c) Cas des endomorphismes symétriques ou hermitiens

• On suppose que **K** = **R**, que E est un espace euclidien et u un endomorphisme symétrique. Alors u est diagonalisable et il existe une base orthonormale de E formée de vecteurs propres de u.

• On suppose que **K** = **C**, que E est un espace hermitien et u un endomorphisme hermitien. Alors toutes les valeurs propres de u sont réelles, u est diagonalisable et il existe une base orthonormale de E formée de vecteurs propres de u.

> *Exercice :* Soit S une matrice symétrique positive. Démontrer qu'il existe une unique matrice symétrique positive R telle que $R^2 = S$.

2. Applications de la diagonalisation (à développer sur des exemples)

• Calcul des puissances et de l'exponentielle d'une matrice

• Etude de systèmes de suites à récurrence linéaire d'ordre 1 et de suites à récurrence linéaire d'ordre n

• Résolution de systèmes différentiels linéaires d'ordre 1 et d'équations différentielles linéaires d'ordre n

• Décomposition de formes quadratiques en somme de carrés et étude de coniques ou de quadriques

Bibliographie

CABANE et LEBOEUF, *Algèbre linéaire II, Matrices et réduction*, Ellipses
RAMIS, DESCHAMPS et ODOUX, *Cours de mathématiques spéciales, tomes 1 et 2,* Masson
ARNAUDIÈS et FRAYSSE, *Cours de mathématiques, tome 1 : Algèbre*, Dunod
MONIER, *Algèbre, tome 2*, Dunod

ENDOMORPHISMES D'UN ESPACE VECTORIEL DE DIMENSION FINIE

Remarques générales

• "S'il n'est pas exigé de connaître la démonstration de chacun des résultats cités dans le plan, on doit pouvoir en dire quelque chose ; citons quelques exemples de dialogues : —"Les éléments inversibles de L(E) forment un groupe noté GL(E)."—"Que savez-vous de GL(E) ?"—"C'est un groupe ...".” (Rapport du jury 1992)

• Il s'agit d'une leçon sur les endomorphismes, *pas sur les matrices*. Il faut donc énoncer tous les résultats du plan en termes d'endomorphismes, étant bien entendu qu'il faut savoir les traduire matriciellement et que d'autre part il est loisible d'adopter le point de vue matriciel pour les démonstrations.

Plan

Soit E un espace vectoriel de dimension finie n sur un corps **K** commutatif de caractéristique nulle (**R** ou **C** pour les propriétés topologiques). On note L(E) l'ensemble des endomorphismes de E. On suppose connues les généralités sur les espaces vectoriels de dimension finie et sur les applications linéaires en dimension finie, notamment la représentation matricielle.

1. Premières propriétés et exemples

a) Rang

Le rang d'un endomorphisme f de E, noté rg f, est la dimension de son image.
On rappelle la formule du rang : $\boxed{\dim E = \dim(\operatorname{Ker} f) + \operatorname{rg} f}$.
Deux endomorphismes f et g ont même rang ssi il existe des automorphismes α et β tels que $f = \alpha \circ g \circ \beta$. On dit que f et g sont équivalents.
S'il existe un automorphisme α tel que $f = \alpha \circ g \circ \alpha^{-1}$, on dit que f et g sont semblables. Il revient au même de dire qu'il existe des bases B et B' dans lesquelles f et g ont respectivement même matrice.

b) Déterminant

Soit f un endomorphisme de E. Il existe un unique réel λ tel que pour toute base B de E et toute famille $(x_1, \ldots, x_n)$ de vecteurs de E, on ait $\det_B(f(x_1),\cdots,f(x_n)) = \lambda \det_B(x_1,\cdots,x_n)$. λ est appelé déterminant de f et noté det f.
f est un automorphisme ssi $\det f \neq 0$.

c) Exemples

• *Homothéties, projections*

Les endomorphismes qui commutent avec tout endomorphisme sont exactement les homothéties.

• *Dilatations, transvections*
Soient H un hyperplan, D une droite supplémentaire de H et $\alpha \in \mathbf{K}^*$. L'application $E = H \oplus D \to E$, $x = y + z \mapsto y + \alpha z$, est appelée dilatation d'hyperplan H, de direction D et de rapport α.
Soient H un hyperplan, f une forme linéaire de noyau H et h un vecteur non nul de H. L'application $E \to E, x \mapsto x + f(x)h$, est appelée transvection d'hyperplan H et de direction **K**h.

Les automorphismes qui fixent chaque vecteur d'un hyperplan H sont exactement les dilatations et les transvections d'hyperplan H.

2. L'algèbre des endomorphismes

a) Propriétés algébriques

(L(E), +, .) est un **K**-espace vectoriel de dimension finie $(\dim E)^2$.
(L(E), +, ∘) est un anneau, en général ni commutatif, ni intègre.
(L(E), +, . , ∘) est une **K**-algèbre, appelée algèbre des endomorphismes de E.

b) Propriétés topologiques

E étant muni de sa topologie canonique d'espace vectoriel normé (en dimension finie, toutes les normes sont équivalentes), tous les endomorphismes de E sont continus. La relation $\|f\| = \mathrm{Sup}\{\|f(x)\| / x \in E \text{ et } \|x\| = 1\}$ définit une norme sur L(E), qui devient de ce fait une algèbre normée ($\|f \circ g\| \leq \|f\| \|g\|$) complète.
Le déterminant est une application continue de L(E) dans **K**.

Application : définition de l'exponentielle d'un endomorphisme.

3. Le groupe linéaire

a) Caractérisation des automorphismes

Pour un endomorphisme f de E, les propriétés suivantes sont équivalentes :		
(i) f est bijectif	(ii) f est injectif	(iii) f est surjectif
(iv) f est inversible à droite	(v) f est inversible à gauche	(vi) rg f = dim E

L'ensemble des automorphismes de E est un groupe, appelé groupe linéaire de E et noté GL(E). C'est le groupe des éléments inversibles de l'anneau L(E).

b) Propriétés algébriques

GL(E) opère fidèlement et transitivement sur l'ensemble des bases de E.
Le sous-groupe des automorphismes de déterminant 1 est appelé groupe spécial linéaire et noté SL(E).
Si dim E ≥ 2, GL(E) n'est pas commutatif, son centre est le groupe H(E) des homothéties de rapport non nul.
Dans le groupe GL(E), la relation de conjugaison n'est autre que la relation de similitude.

SL(E) est engendré par les transvections.	GL(E) est engendré par les dilatations.

Application : calcul du rang d'une matrice, calcul de l'inverse d'une matrice, résolution d'un système linéaire par opérations élémentaires sur les lignes et/ou les colonnes.

c) Propriétés topologiques

• GL(E) est un ouvert dense de L(E). L'application $GL(E) \to GL(E)$, $f \mapsto f^{-1}$, est continue. SL(E) est un fermé de L(E).
• Si **K** = **C**, GL(E) et SL(E) sont connexes par arcs. Si **K** = **R**, SL(E) est connexe par arcs mais GL(E) n'est pas connexe ; il a deux composantes connexes qui sont connexes par arcs : $GL^+(E) = \{f \in GL(E) / \det f > 0\}$ et $GL^-(E) = \{f \in GL(E) / \det f < 0\}$.

Bibliographie

ARNAUDIÈS et FRAYSSE, *Cours de mathématiques, tome 1 : algèbre*, Dunod
AVEZ, *La leçon de géométrie à l'oral de l'agrégation*, Masson
TISSERON, *Géométries affine, projective et euclidienne*, Hermann
TAUVEL, *Mathématiques générales pour l'agrégation*, Masson

ENDOMORPHISMES HERMITIENS EN DIMENSION FINIE

Remarques générales

• Programme : Endomorphismes hermitiens, matrices hermitiennes. Diagonalisation d'un endomorphisme hermitien dans une base orthonormale. Diagonalisation d'une matrice hermitienne au moyen d'une matrice unitaire.

• Cette leçon isolée n'a que peu de rapport avec le reste du programme, aussi il est difficile de présenter des applications intéressantes.

Plan

Introduction

Soit E un espace hermitien de dimension n. Le produit scalaire hermitien et la norme hermitienne sont notés respectivement $(x|y)$ et $\|x\|$.
On suppose connue la notion d'adjoint d'un endomorphisme u de E ; en dimension finie, cet adjoint existe et est unique : on le note u^* et on a $u^* = f^{-1}\circ{}^t u\circ f$, où f est la bijection semi-linéaire $x \mapsto (.\,|x)$ de E sur E^*.
On suppose également connus les résultats simples sur les automorphismes unitaires et le groupe unitaire.

1. Endomorphismes hermitiens

a) Définitions

On dit qu'un endomorphisme u de E est <u>hermitien</u> si $u^* = u$.
On dit qu'une matrice A de $M_n(\mathbf{C})$ est <u>hermitienne</u> si ${}^t\overline{A} = A$.

Liens entre ces deux définitions :
• Si u est un endomorphisme hermitien, alors dans toute base orthonormale de E la matrice de u est hermitienne.
• Si A est une matrice hermitienne, alors l'endomorphisme de $\mathbf{C}^n$ canoniquement associé à A est hermitien.

On note H l'ensemble des endomorphismes hermitiens ; c'est un $\mathbf{R}$-espace vectoriel de dimension n^2.
Tout endomorphisme u s'écrit de manière unique sous la forme $u = h_1 + i\,h_2$, avec h_1 et h_2 dans H.

b) Propriétés

• *Théorème fondamental :*

u est hermitien ssi toutes les valeurs propres de u sont réelles et s'il existe une base orthonormale de E formée de vecteurs propres de u.

• *Caractérisations des valeurs propres de u :* Si (e_i) est une base orthonormale de vecteurs propres associés aux valeurs propres $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ de u, alors pour tout i :

$$\lambda_i = (u(e_i)|e_i) = \sup\left\{\frac{(u(x)|x)}{\|x\|^2},\ x \neq 0 \text{ et } x \in \langle e_1, e_2, \ldots, e_{i-1}\rangle^{\perp}\right\} = \inf\left\{\frac{(u(x)|x)}{\|x\|^2},\ x \neq 0 \text{ et } x \in \langle e_1, e_2, \ldots, e_i\rangle\right\}.$$

• *Traduction matricielle :* A est une matrice hermitienne ssi il existe une matrice unitaire U (${}^t\overline{U} = U^{-1}$) et une matrice diagonale réelle D telles que $A = UDU^{-1}$.

> *Exercice :* Soient u et v deux endomorphismes hermitiens qui commutent. Montrer qu'on peut les diagonaliser dans une même base orthonormale.

2. Endomorphismes hermitiens positifs

a) Endomorphismes hermitiens positifs et définis positifs

On dit qu'un endomorphisme hermitien est positif (resp. défini positif) si toutes ses valeurs propres sont positives (resp. strictement positives). On note H^+ (resp. H^{++}) l'ensemble des endomorphismes hermitiens positifs (resp. définis positifs).

L'exponentielle induit un homéomorphisme de H sur H^{++}.

Exercice 1 : Si $u \in H^+$, il existe un unique $v \in H^+$ tel que $v^2 = u$.

Exercice 2 : Soient A et B deux matrices hermitiennes positives. Montrer que $0 \leq tr(AB) \leq tr(A)\,tr(B)$.

b) Décomposition polaire d'un endomorphisme

Soit u un endomorphisme de E. Alors :
(i) il existe un endomorphisme hermitien positif v et un endomorphisme unitaire w tels que $u = v \circ w$;
(ii) si de plus u est inversible, le couple (v, w) est unique et les applications $u \mapsto v$ et $u \mapsto w$ sont continues.

c) Décomposition de Choleski d'une matrice hermitienne positive

Soit M une matrice hermitienne positive. Il existe une matrice triangulaire supérieure T telle que $M = T^*T$.

Application 1 : Résolution du système linéaire MX = Y.

Application 2 : Inégalité de Hadamard. Si $A = (a_{ij}) \in M_n(\mathbf{C})$, on a $|\det(A)| \leq \left(\prod_{j=1}^{n} \left(\sum_{i=1}^{n} |a_{ij}|^2 \right) \right)^{1/2}$.

3. Application aux formes quadratiques hermitiennes

a) Lien entre endomorphismes hermitiens et formes quadratiques hermitiennes

Notons Q le **R**-espace vectoriel des formes quadratiques hermitiennes. L'application $u \mapsto [x \mapsto (x|u(x))]$ est un isomorphisme de H sur Q. L'endomorphisme hermitien u est positif (resp. défini positif) ssi la forme quadratique hermitienne associée est positive (resp. définie positive).

b) Orthogonalisation d'une forme quadratique hermitienne dans un espace hermitien

Soient E un espace hermitien et q une forme quadratique hermitienne sur E. Il existe une base orthonormale de E orthogonale pour q.

Application : Signature et décomposition en carrés d'une forme quadratique hermitienne (même si E n'est pas hermitien au départ et q donnée dans une base arbitraire).

c) Orthogonalisation simultanée de deux formes quadratiques hermitiennes

Soient E un **C**-espace vectoriel de dimension finie, q et q' deux formes quadratiques hermitiennes sur E, avec q définie positive. Il existe une base de E orthonormale pour q et orthogonale pour q'.

Bibliographie

TAUVEL, *Mathématiques générales pour l'agrégation*, Masson
RAMIS, DESCHAMPS et ODOUX, *Cours de mathématiques spéciales, tome 2*, Masson
MONIER, *Algèbre, tome 2*, Dunod

DIMENSION D'UN ESPACE VECTORIEL
RANG D'UNE APPLICATION LINÉAIRE

Remarques générales

• On se limitera au cas de la dimension finie, sur un corps **K** de caractéristique nulle. Les généralités sur les espaces vectoriels et les applications linéaires sont supposées connues.

• "... ainsi entend-on trop souvent parler de "la" base d'un espace vectoriel, de "la" base de vecteurs propres d'un endomorphisme, "du" supplémentaire d'un sous-espace, etc." (Rapport du jury 1991)

• Penser à présenter des exemples tirés d'autres parties du programme, notamment en analyse.

Plan

1. <u>Espaces vectoriels de dimension finie</u>

a) Notion de dimension

• Un espace vectoriel est <u>de type fini</u> s'il possède au moins une famille génératrice finie.

• *Théorème de la base incomplète*

Soient E un e.v. de type fini, G une famille génératrice de E et L une famille libre de E. Il existe une base B de E telle que $L \subset B \subset (L \cup G)$.

Conséquence : Tout e.v. de type fini admet au moins une base.

• *Théorème de la dimension finie*

Soit E un e.v. de type fini. Toutes les bases de E sont finies et ont le même nombre d'éléments.

• La <u>dimension</u> d'un e.v. E de type fini est le cardinal de l'une quelconque de ses bases. On note ce cardinal <u>dim E</u> et on dit que E est <u>de dimension finie</u>.

b) Conséquences

• Tout e.v. de dimension n est isomorphe à $\mathbf{K}^n$.

• Soit E un e.v. de dimension n et soit F une famille d'éléments de E. Les propriétés suivantes sont équivalentes :
(i) F est une base
(ii) F est une famille libre de n éléments
(iii) F est une famille génératrice de n éléments

• Tout sous-espace d'un e.v. de dimension finie admet au moins un supplémentaire.

c) Exemples

Exemple 1 : L'ensemble des suites (u_n) définies par la donnée de u_0, u_1, u_2 dans **C** et la relation de récurrence $u_{n+3} = 3u_{n+2} - 2u_n$ est un **C**-e.v. de dimension 3. En donner une base.

Exemple 2 : L'ensemble des solutions sur $]0, +\infty[$ de l'équation différentielle $x(x + 1)y'' + (x + 2)y' - y = 0$ est un **R**-e.v. de dimension 2. En donner une base.

Exemple 3 : $\mathbf{Q}[\sqrt[4]{2}]$ est un **Q**-e.v. de dimension 4. En donner une base.

d) Calcul sur les dimensions

Les e.v. que l'on peut construire à partir d'e.v. de dimension finie sont eux-mêmes de dimension finie et on a les formules suivantes :

• Sous-espace : $\boxed{\dim F \leq \dim E}$ • Somme : $\boxed{\dim (F + G) = \dim F + \dim G - \dim (F \cap G)}$

• Produit : $\boxed{\dim (E \times F) = \dim E + \dim F}$ • Extension de corps : $\boxed{\dim_K (E) = \dim_L (E) \times \dim_K (L)}$

• Quotient : $\boxed{\dim E / F = \dim E - \dim F}$ • Espace d'applications linéaires : $\boxed{\dim L(E, F) = \dim E \times \dim F}$

2. Rang d'une application linéaire

E et F désignent des e.v. de dimension finie et f une application linéaire de E dans F.

• Le rang d'une application linéaire est la dimension de son image. On note rg f. Le rang d'une famille de vecteurs d'un e.v. est la dimension du sous-espace engendré par cette famille.

• *Formule du rang :* $\boxed{\dim E = \dim (\operatorname{Ker} f) + \dim (\operatorname{Im} f)}$

Conséquence : Si dim E = dim F = n, les propriétés suivantes sont équivalentes :
(i) f est bijective (ii) f est injective
(iii) f est surjective (iv) rg f = n

Application : Toute **K**-algèbre intègre de dimension finie est un corps. Par exemple $\mathbf{Q}[\sqrt{2},\sqrt{3}]$.

3. Dualité en dimension finie

a) Bases duales

• Si E est un e.v. de dimension finie, son dual E^* est de même dimension finie. A toute base (e_i) de E, on associe une base (b_i^*) de E^*, appelée base duale de (e_i) et définie par les relations $b_i^*(b_j) = \delta_{ij}$.
• L'application $x \mapsto (f \mapsto f(x))$ est un isomorphisme (canonique) de E sur son bidual E^{**}.

b) Orthogonalité

Si E est un e.v. de dimension finie :
(i) Pour tout sous espace X de E, $(X^\perp)^\perp = X$.
(ii) Pour tout sous-espace Y de E^*, $(Y^\perp)^\perp = Y$.
(iii) $\dim X + \dim X^\perp = \dim E^* = \dim E = \dim Y + \dim Y^\perp$.

c) Transposée d'une application linéaire

Si E et F sont des e.v. de dimension finie :
(i) La transposition $f \mapsto {}^t f$ est une application linéaire bijective de L(E, F) sur $L(F^*, E^*)$.
(ii) Pour toute application linéaire f de E dans F, $\operatorname{rg} f = \operatorname{rg} {}^t f$.

Application : Polynômes d'interpolation de Lagrange.
E désigne l'espace vectoriel $\mathbf{K}_{n-1}[X]$. Etant donnés des éléments distincts $a_1, a_2, \ldots, a_n$ de **K**, on considère les formes linéaires $\varphi_i : P \mapsto P(a_i)$. Montrer que (φ_i) est une base de E^*. Expliciter la base (e_i) de E duale de (φ_i) et la décomposition d'un polynôme P quelconque suivant (e_i).

Bibliographie

RAMIS, DESCHAMPS et ODOUX, *Cours de mathématiques spéciales, tome 1*, Masson
CABANE et LEBOEUF, *Espaces vectoriels, polynômes,* Ellipses

FORMES QUADRATIQUES SUR UN ESPACE VECTORIEL EUCLIDIEN. APPLICATIONS GÉOMÉTRIQUES

Remarques générales

• "L'interprétation du sujet ne doit pas conduire au contresens : tel candidat ayant à traiter "formes quadratiques sur un espace vectoriel euclidien" a consacré plus des trois quarts de son temps aux espaces vectoriels euclidiens ...)." (Rapport du jury 1990)

• Les généralités sur les formes quadratiques sont supposées connues.

Plan

1. Formes quadratiques sur un espace vectoriel euclidien

On suppose connues les généralités sur les formes bilinéaires symétriques et les formes quadratiques.
Soit E un espace vectoriel euclidien de dimension n. Pour le produit scalaire et la norme de E, on utilise les notations (x|y) et ||x||.

a) Théorème fondamental

Si q est une forme quadratique sur E, il existe une base orthonormée de E qui est orthogonale pour q.

Premier point de vue : Si (e_i) est une telle base, indexée de sorte que $q(e_1) \geq q(e_2) \geq \ldots \geq q(e_n)$, alors pour tout i, on a $q(e_i) = \sup\left\{\frac{q(x)}{\|x\|^2},\ x \neq 0 \text{ et } x \in \langle e_1, e_2, \ldots, e_{i-1}\rangle^{\perp}\right\}$.

Deuxième point de vue : Si (e_i) est une telle base, (e_i) est une base de vecteurs propres pour l'endomorphisme $d^{-1} \circ d'$ de E, avec $d : E \to E^*,\ x \mapsto (.|x)$ et $d' : E \to E^*,\ x \mapsto \varphi(.|x)$, φ étant la forme polaire de q. De plus, pour tout i, la valeur propre associée à e_i est $q(e_i)$.

b) Conséquences

• Si u est un endomorphisme symétrique de E, u est diagonalisable dans une base orthonormée. Sa plus grande valeur propre est égale à $\sup_{x \neq 0} \frac{(u(x)|x)}{\|x\|^2}$.

• Toute matrice symétrique A est diagonalisable. Sa plus grande valeur propre est égale à $\sup_{X \neq 0} \frac{{}^tXAX}{{}^tXX}$.

• Si q est une forme quadratique sur un espace vectoriel E *quelconque* de dimension finie, et si b est une base *arbitraire* de E, alors la signature de q est (r, s), où r (resp. s) est le nombre de valeurs propres strictement positives (resp. strictement négatives) de la matrice symétrique A qui représente q dans b. De plus, en diagonalisant A, on obtient une décomposition en carrés de q.

• Si q et q' sont deux formes quadratiques sur un espace vectoriel E *quelconque* de dimension finie, et si q est définie positive, alors il existe une base de E orthonormale pour q et orthogonale pour q'. Dans la pratique, si q et q' sont représentées par des matrices A et B dans une base *arbitraire* b de E, la base cherchée s'obtient en diagonalisant la matrice $A^{-1}B$.

Exercice 1 : Trouver les extremums absolus de $\frac{2x^2 - 3y^2 + 2yz}{x^2 + 3y^2 + 3z^2 - 2yz}$ lorsque $(x, y, z) \in \mathbf{R}^3 \backslash \{(0, 0, 0)\}$.

Exercice 2 : Démontrer algébriquement que deux normes euclidiennes sur un espace vectoriel de dimension finie sont équivalentes.

Exercice 3 : Soit u un endomorphisme d'un espace euclidien E. Calculer ||u|| en fonction des valeurs propres de $u^* \circ u$.

2. Applications géométriques

a) Classification des coniques et des quadriques

Soit X un espace affine euclidien de direction E. On appelle quadrique euclidienne toute partie de X ayant dans un repère orthonormé une équation de la forme $\sum_{i,j} a_{ij}x_ix_j + \sum_i b_ix_i + c = 0$, avec A = (a_{ij}) symétrique et non nulle (c'est alors vrai dans tout repère orthonormé).

Si A est de rang r et si λ_1, ..., λ_r sont les valeurs propres non nulles de A, il existe une base orthonormée dans laquelle la quadrique a une équation de l'une des formes suivantes :

$$\boxed{\sum_{1\le i\le r} \lambda_i x_i^2 + \delta = 0 \quad \text{avec } \delta \in \mathbf{R}} \quad \text{ou} \quad \boxed{\sum_{1\le i\le r} \lambda_i x_i^2 + \beta x_n = 0 \quad \text{avec } \beta \in \mathbf{R}^*}.$$

Dans les cas usuels du plan (coniques) et de l'espace de dimension 3 (quadriques), on obtient la classification suivante en fonction de la signature de la forme quadratique, en ne mentionnant que les cas "intéressants" :

(2, 0) ou (0, 2)	ellipse
(1, 1)	hyperbole
(1, 0) ou (0, 1)	parabole

(3, 0) ou (0, 3)	ellipsoïde
(2, 1) ou (1, 2)	hyperboloïde à une ou deux nappes cône
(2, 0) ou (0, 2)	paraboloïde elliptique cylindre elliptique
(1, 1)	paraboloïde hyperbolique cylindre hyperbolique
(1, 0) ou (0, 1)	cylindre parabolique

b) Etude locale d'une surface

Soit S une surface d'équation z = f(x, y), où f est une application de classe C^2 sur un ouvert U de $\mathbf{R}^2$. Au voisinage d'un point a de U, on a la *formule de Taylor d'ordre 2 :*

$$\boxed{f(a + h) = f(a) + f'(a).h + \frac{1}{2} f''(a).(h, h) + o(\|h\|^2)}.$$

Le terme d'ordre 2 est une forme quadratique qui s'écrit $\frac{1}{2}\left(r\,h_1^2 + 2s\,h_1h_2 + t\,h_2^2\right)$, où l'on a posé

$$r = \frac{\partial^2 f}{\partial x^2}(a_1, a_2)\ ,\ s = \frac{\partial^2 f}{\partial x \partial y}(a_1, a_2)\ ,\ t = \frac{\partial^2 f}{\partial y^2}(a_1, a_2)\ .$$

Le paraboloïde d'équation $z = f(a) + f'(a).(x, y) + \frac{1}{2} f''(a).((x, y), (x, y))$ est appelé paraboloïde osculateur à S en a. Au voisinage de a, S "ressemble" à son paraboloïde osculateur et le signe de $rt - s^2$ permet de préciser la position de S par rapport à son plan tangent. Si $rt - s^2 > 0$ (resp. $rt - s^2 = 0$, resp. $rt - s^2 < 0$), on dit que a est un point elliptique (resp. parabolique, resp. hyperbolique). En un point elliptique, on a une disposition "en ballon" et en un point hyperbolique une disposition "en col" ; le cas d'un point parabolique est difficile et hors programme (voir ARNAUDIÈS et FRAYSSE).

Bibliographie

AVEZ, *La leçon de géométrie à l'oral de l'agrégation*, Masson
RAMIS, DESCHAMPS et ODOUX, *Cours de mathématiques spéciales, tomes 2 et 5,* Masson
TISSERON, *Géométries affine, projective et euclidienne*, Hermann
BERGER, *Géométrie, vol.4,* CEDIC/Fernand Nathan
ARNAUDIÈS et FRAYSSE, *Cours de mathématiques, tome 4*, Dunod
BALABANE, DUFLO, FRISCH et GUÉGAN, *Géométrie, maths en kit 1*, Vuibert

GROUPE DES PERMUTATIONS D'UN ENSEMBLE FINI ; APPLICATIONS

Remarques générales

• Programme :

- Permutations d'un ensemble fini, groupe symétrique
- Cycles, transpositions
- Décomposition d'une permutation en produit de cycles disjoints, en produit de transpositions
- Signature d'une permutation, groupe alterné

• L'exposé sur le groupe symétrique est standard et se trouve dans tous les traités d'algèbre. Le plus simple est de suivre le plan du programme. La difficulté est plutôt de réunir des illustrations et des applications issues de divers domaines.

Plan

1. Permutations d'un ensemble fini, groupe symétrique

• L'ensemble des permutations d'un ensemble fini E à n éléments est un groupe pour $\circ$, appelé groupe symétrique de E et noté S(E).
Lorsque E = {1, 2, ... , n}, on parle du groupe symétrique d'ordre n et on note S_n. Un élément σ de S_n se note $\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$.

• S_n est d'ordre n! ; pour $n \geq 3$, S_n n'est pas commutatif.

• Théorème de Cayley : Tout groupe fini d'ordre n est isomorphe à un sous-groupe de S_n.

2. Cycles, transpositions

• Une permutation σ est un cycle de longueur r (avec $r > 1$) s'il existe $i_1, i_2, \dots, i_r \in \{1, 2, \dots, n\}$ tels que $s(i_1) = i_2$, $s(i_2) = i_3$, … , $s(i_{r-1}) = i_r$, $s(i_r) = i_1$, et $\sigma(i) = i$ si $i \notin \{i_1, \dots, i_r\}$. On note $\sigma = (i_1\ i_2 \dots i_r)$.
Par convention, Id est un cycle de longueur 1 et on peut écrire Id = (1) = (2) = … = (n).

• Un cycle de longueur r est d'ordre r. Deux cycles disjoints commutent. L'ordre d'un produit de cycles disjoints est le PPCM des ordres des cycles.

Toute permutation se décompose de façon unique (à l'ordre près et à la présence près de cycles de longueur 1) en produit de cycles disjoints.

• Une transposition est un cycle de longueur 2.
Tout cycle est produit de transpositions : $(i_1\ i_2 \dots i_r) = (i_1\ i_r) \dots (i_1\ i_3)\ (i_1\ i_2)$.

S_n est engendré par les transpositions. (Mais la décomposition en produit de transpositions n'est pas unique !)

Exercices : 1) S_n est engendré : a) par (12) et (12...n) ; b) par (12), (13), ... , (1n) ; c) par (12), (23), ... , ((n-1)n).
2) Classes de conjugaison dans S_n.

3. Signature d'une permutation, groupe alterné

• Pour $\sigma \in S_n$, on appelle nombre d'inversions de σ le nombre $I(\sigma)$ des couples (i, j) tels que $i < j$ et $\sigma(i) > \sigma(j)$, et signature de σ le nombre $\varepsilon(\sigma) = (-1)^{I(\sigma)}$.
Exemple : pour un cyle σ de longueur r, $\varepsilon(\sigma) = (-1)^{r-1}$.

• Autres méthodes de calcul de la signature :

$$\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i}$$

$\varepsilon(\sigma) = (-1)^{n-p}$ où p est le nombre de cycles disjoints dans la décomposition de σ.

$\varepsilon(\sigma) = (-1)^{k}$ où k est le nombre de transpositions dans une décomposition de σ.

• La signature ε est un homomorphisme du groupe $(S_n, \circ)$ dans le groupe $(\{-1, 1\}, \times)$, surjectif si $n \geq 2$. Son noyau est un sous-groupe distingué de S_n, appelé groupe alterné d'ordre n et noté A_n.

Si $n \geq 2$, A_n est d'ordre $\frac{n!}{2}$; A_n est engendré par : a) les produits de deux transpositions ; b) les 3-cycles.

• Si $n \geq 5$, A_n est simple.

Comme A_n n'est pas commutatif pour $n \geq 5$, il en résulte que S_n n'est pas résoluble pour $n \geq 5$. Par contre, pour S_3 et S_4, on a les chaînes d'inclusions suivantes, où chaque sous-groupe est distingué dans le suivant et où les quotients successifs sont abéliens :
$\{Id\} \subset A_3 \subset S_3$
$\{Id\} \subset \{Id, (12)(34)\} \subset \{Id, (12)(34), (13)(24), (14)(23)\} \subset A_4 \subset S_4$

4. Exemples d'interventions des groupes symétriques (à développer)

• Définition de certaines notions : applications multilinéaires symétriques et antisymétriques, déterminants, polynômes et fonctions symétriques.

• Réalisations en géométrie : le groupe des isométries d'un triangle équilatéral est isomorphe à S_3 ; le groupe des isométries d'un tétraèdre régulier est isomorphe à S_4.

• Equations du troisième et du quatrième degrés : en lien avec la structure de S_3 et de S_4, les méthodes classiques reviennent à trouver une fonction des n racines prenant moins de n valeurs par permutation des racines, ce qui permet de se ramener à une équation de degré inférieur (la résolvante).
On peut utiliser $(x_1 + jx_2 + j^2x_3)^3$ pour le troisième degré et $x_1x_2 + x_3x_4$, ou $(x_1 + x_2)(x_3 + x_4)$, ou $(x_1 + x_2 - x_3 - x_4)^2$, pour le quatrième degré.

Bibliographie

ARNAUDIES et FRAYSSE, *Cours de mathématiques, tome 1 : algèbre*, Dunod
RAMIS, DESCHAMPS et ODOUX, *Cours de mathématiques spéciales, tome 1 : algèbre*, Masson
BOUVIER et RICHARD, *Groupes*, Hermann
JACOBSON, *Basic Algebra I*, Freeman

ISOMÉTRIES DE L'ESPACE AFFINE EUCLIDIEN DE DIMENSION 3 : FORMES RÉDUITES

Remarques générales

• Pour cette leçon assez délicate, nous ne donnons que l'essentiel. On trouvera des compléments et des exercices dans la bibliographie.

• Pour chaque type d'isométrie, prévoir un exemple montrant comment déterminer pratiquement ses éléments remarquables et … faire une figure !

Plan

E est un espace affine euclidien de dimension 3, de direction $\vec{E}$.

1. Etude résumée des isométries vectorielles

• Une application φ de $\vec{E}$ dans $\vec{E}$ est appelée isométrie (vectorielle) si elle vérifie une des propriétés équivalentes suivantes : (i) φ conserve le produit scalaire ; (ii) φ est linéaire et conserve la norme. φ est alors bijective et a pour déterminant 1 ou -1. Exemples : réflexion (symétrie orthogonale par rapport à un plan vectoriel), demi-tour (symétrie orthogonale par rapport à une droite vectorielle).

• L'ensemble des isométries, noté $O(\vec{E})$, est un sous-groupe de $GL(\vec{E})$ appelé groupe orthogonal de $\vec{E}$. On note $O^+(\vec{E})$ (resp. $O^-(\vec{E})$) le sous-groupe (resp. le sous-ensemble) des isométries de déterminant 1 (resp. -1).

• Si φ est une isométrie, il existe une droite $\vec{D}$ et un plan $\vec{P}$ orthogonaux, stables par φ, tels que la restriction de φ à $\vec{D}$ soit Id ou -Id et la restriction de φ à $\vec{P}$ soit une rotation vectorielle. $\vec{D}$ et $\vec{P}$ sont uniques lorsque φ est distinct de Id et -Id. Si $\varphi|_{\vec{D}} = \mathrm{Id}$, on dit que φ est une rotation (vectorielle) d'axe $\vec{D}$ et d'angle l'angle de $\varphi|_{\vec{P}}$. Si $\varphi|_{\vec{D}} = -\mathrm{Id}$, φ est le produit commutatif de la rotation d'axe $\vec{D}$ et d'angle l'angle de $\varphi|_{\vec{P}}$ et de la réflexion par rapport à $\vec{P}$; on dit alors que c'est une réflexion-rotation. L'espace étant orienté, si on désire mesurer l'angle de $\varphi|_{\vec{P}}$, on oriente conjointement $\vec{D}$ et $\vec{P}$ par le choix d'un vecteur unitaire de $\vec{D}$.

• $O(\vec{E})$ (resp. $O^+(\vec{E})$) est engendré par les réflexions (resp. les demi-tours).

2. Généralités sur les isométries affines

a) Définition et premières propriétés

• Une application f de E dans E est appelée isométrie (affine) si elle conserve la distance. Exemples : translation, réflexion (symétrie orthogonale par rapport à un plan affine), demi-tour (symétrie orthogonale par rapport à une droite affine).

• f est une isométrie ssi f est affine et $\vec{f} \in O(\vec{E})$. En particulier, une isométrie est bijective. Si $\vec{f} \in O^+(\vec{E})$, on dit que f est un déplacement, sinon un antidéplacement.

• L'ensemble des isométries est un groupe, noté Is(E). On note $Is^+(E)$ le sous-groupe des déplacements et $Is^-(E)$ le sous-ensemble des antidéplacements.

b) Décomposition canonique d'une isométrie

Une isométrie f s'écrit de manière unique f = t o g, où g est une isométrie ayant un ensemble non vide G de points fixes et où t est une translation de vecteur appartenant à $\vec{G}$. On a de plus f = g o t et $\vec{G} = \mathrm{Ker}(\vec{f} - \mathrm{Id})$. Enfin si f n'a pas de point fixe, on a dim G ≥ 1.

3. <u>Description des isométries affines</u>

a) Formes réduites

L'étude des isométries ayant au moins un point fixe se ramène à celle des isométries vectorielles. Par ailleurs, d'après le théorème précédent, une isométrie sans point fixe est soit une translation, soit la composée commutative d'une isométrie ayant au moins une droite de points fixes et d'une translation de vecteur parallèle au sous-espace des points fixes de l'isométrie précédente. D'où le tableau :

	avec point(s) fixe(s)	*sans point fixe*
déplacement	**ROTATION** Cas particulier : **IDENTITÉ**	**ROTATION-TRANSLATION** ou **VISSAGE** Produit commutatif d'une rotation et d'une translation de vecteur non nul parallèle à l'axe de rotation Cas particulier : **TRANSLATION**
antidéplacement	**RÉFLEXION-ROTATION** Produit commutatif d'une réflexion et d'une rotation d'axe perpendiculaire au plan de réflexion Cas particulier : **RÉFLEXION**	**RÉFLEXION-TRANSLATION** Produit commutatif d'une réflexion et d'une translation de vecteur non nul parallèle au plan de réflexion

b) Générateurs

Is(E) est engendré par les réflexions : toute isométrie est produit d'au plus 4 réflexions.
$Is^+(E)$ est engendré par les retournements : tout déplacement est produit d'au plus 2 demi-tours.

Bibliographie

TISSERON, *Géométries affine, projective et euclidienne*, Hermann
BERGER, *Géométrie tome 2*, CEDIC/Fernand Nathan
TAUVEL, *Mathématiques générales pour l'agrégation*, Masson
AVEZ, *La leçon de géométrie à l'oral de l'agrégation*, Masson

ISOMÉTRIES DU PLAN ; FORMES RÉDUITES ; APPLICATIONS

Remarques générales

• Pour gagner du temps, on suppose connue la classification des automorphismes orthogonaux.

• Le programme mentionne “Exemples de groupes d’isométries laissant stable une partie du plan”. Pour illustrer ce thème de façon ni trop banale, ni trop compliquée, un bon choix semble être l’étude des groupes de frises.

Plan

E est un plan affine euclidien. On suppose connue la classification des automorphismes orthogonaux de $\vec{E}$.

1. Généralités sur les isométries

a) Définition et premières propriétés

• Une application f de E dans E est appelée <u>isométrie</u> si elle conserve la distance. Exemples : translation, réflexion.

• f est une isométrie ssi f est affine et $\vec{f} \in O(\vec{E})$. En particulier, une isométrie est bijective. Si $\vec{f} \in O^+(\vec{E})$, on dit que f est un <u>déplacement</u>, sinon un <u>antidéplacement</u>.

• L’ensemble des isométries est un groupe, noté Is(E). On note $Is^+(E)$ le sous-groupe des déplacements et $Is^-(E)$ le sous-ensemble des antidéplacements.

b) Décomposition canonique d’une isométrie

Une isométrie f s’écrit de manière unique f = t o g, où g est une isométrie ayant un ensemble non vide G de points fixes et où t est une translation de vecteur appartenant à $\vec{G}$. On a de plus f = g o t et $\vec{G} = \mathrm{Ker}(\vec{f} - \mathrm{Id})$. Enfin si f n’a pas de point fixe, on a dim G ≥ 1.

2. Description des isométries planes

a) Formes réduites

L’étude des isométries ayant au moins un point fixe se ramène à celle des transformations orthogonales. Par ailleurs, d’après le théorème précédent, une isométrie sans point fixe est soit une translation, soit la composée commutative d’une réflexion et d’une translation de vecteur parallèle à l’axe de la réflexion. D’où le tableau :

	avec point(s) fixe(s)	sans point fixe
déplacement	ROTATION	TRANSLATION
antidéplacement	REFLEXION	REFLEXION-TRANSLATION

Conséquence : Toute isométrie plane est produit d’au plus trois réflexions. Les réflexions engendrent Is(E).

b) Expression complexe

Déplacements

La translation de vecteur $\vec{u}(b)$ a pour expression complexe z’ = z + b.

La rotation de centre Ω (ω) et d’angle θ a pour expression complexe $z' = e^{i\theta}z + (1 - e^{i\theta})\omega$.

Réciproquement, toute expression complexe z’ = az + b, avec |a| = 1, représente une translation si a = 1, une rotation si a ≠ 1.

Antidéplacements

La réflexion d’axe D d’équation $\bar{\alpha}z + \alpha\bar{z} + \beta = 0$ a pour expression complexe z’ = $\dfrac{-\alpha\bar{z} - \beta}{\bar{\alpha}}$.

Réciproquement, toute expression complexe $z' = a\bar{z} + b$, avec $|a| = 1$, représente une réflexion si $a\bar{b} + b = 0$, une réflexion-translation si $a\bar{b} + b \neq 0$.

3. Applications

a) Problèmes de construction

Quelques exemples : Construire un triangle équilatéral s'appuyant sur trois droites parallèles données. Construire un triangle connaissant ses médiatrices. Construire un polygone connaissant les milieux des côtés.

b) Problèmes d'optimisation

Problème de Fagnano : Inscrire dans un triangle ayant trois angles aigus un triangle de périmètre minimal.

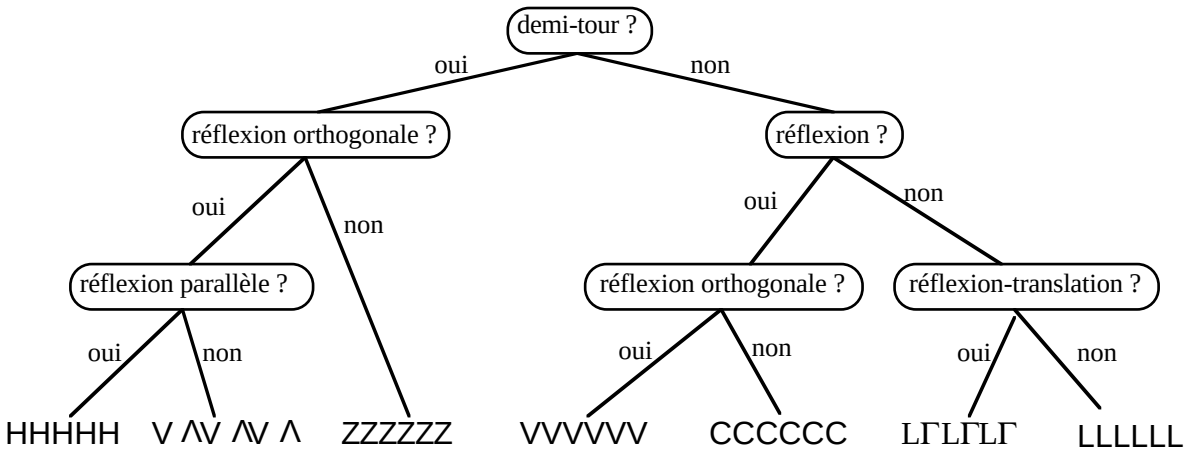
Problème de Steiner-Fermat-Toricelli : Soit ABC un triangle dont les trois angles sont $\leq 2\pi/3$. Trouver un point M tel que MA + MB + MC soit minimum.

c) Groupes de frises

Etant donné une partie F de E, l'ensemble G des isométries qui laissent F invariante est un sous-groupe de Is(E) appelé groupe de F. L'ensemble T des translations qui laissent F invariante est un sous-groupe de G, appelé groupe des translations de F. On dit que F est une frise si T est engendré par une translation non triviale. Dans la suite, on suppose que F est une frise et on désigne par t un générateur de T et par $\vec{v}$ son vecteur.

1) Une isométrie f de G\T est nécessairement de l'un des quatre types suivants : demi-tour, réflexion d'axe parallèle à $\vec{v}$, réflexion d'axe orthogonal à $\vec{v}$, réflexion-translation d'axe parallèle à $\vec{v}$.
2) Si G contient un demi-tour d, l'ensemble des demi-tours est d o T.
3) Si G contient une réflexion d'axe parallèle à $\vec{v}$, celle-ci est unique.
4) Si G contient une réflexion s d'axe orthogonal à $\vec{v}$, l'ensemble des réflexions de ce type est s o T.
5) Si G contient une réflexion-translation g d'axe parallèle à $\vec{v}$, l'ensemble des réflexions-translations est g o T.

On en déduit l'algorithme suivant de classification des frises. Au bout de chaque branche, on trouvera un dessin "prouvant" que ce cas se réalise effectivement. Voir TAUVEL pour la structure des groupes correspondants.



Bibliographie

AVEZ, *La leçon de géométrie à l'oral de l'agrégation*, Masson
TISSERON, *Géométries affine, projective et euclidienne*, Hermann
BERGER, *Géométrie tome 2,* CEDIC/Fernand Nathan
TAUVEL, *Mathématiques générales pour l'agrégation*, Masson

MATRICES CARRÉES INVERSIBLES

Remarques générales

Pour illustrer les différentes méthodes d'inversion d'une matrice, prévoir des calculs effectifs intéressants. "En algèbre linéaire, on fuira les exemples numériques indigents (les sempiternelles matrices 3×3...)" (rapport du jury 1990).

Plan

1. Définition et caractérisation des matrices carrées inversibles

• On dit que $A \in M_n(K)$ est inversible s'il existe $B \in M_n(K)$ telle que AB = BA = I. Dans ce cas, B est unique, s'appelle matrice inverse de A et se note A^{-1}.

• Pour $A \in M_n(K)$, les propriétés suivantes sont équivalentes :

(1) A est inversible
(2) A est inversible à gauche
(3) A est inversible à droite
(4) ${}^tA$ est inversible
(5) A est de rang n
(6) Le rang des vecteurs colonnes de A est égal à n
(7) Le rang des vecteurs lignes de A est égal à n
(8) $\det A \neq 0$

• Exemples :

Matrices élémentaires de dilatation $D_i(\alpha) = I + (\alpha - 1)E_{ii}$, avec $\alpha \neq 0$. Multiplier A à gauche (resp. à droite) par $D_i(\alpha)$ revient à multiplier par α la i-ème ligne (resp. colonne) de A. $\left[D_i(\alpha)\right]^{-1} = D_i\left(\frac{1}{\alpha}\right)$.

Matrices élémentaires de transvection $T_{ij}(\alpha) = I + \alpha E_{ij}$, avec $i \neq j$ et $\alpha \neq 0$. Multiplier A à gauche (resp. à droite) par $T_{ij}(\alpha)$ revient à ajouter à la i-ème ligne (resp. colonne) de A le produit par α de sa j-ème ligne (resp. colonne. $\left[T_{ij}(\alpha)\right]^{-1} = T_{ij}(-\alpha)$.

2. Propriétés de l'ensemble des matrices carrées inversibles

On note $GL_n(K)$ l'ensemble des matrices carrées inversibles d'ordre n, et $SL_n(K)$ le sous-ensemble des matrices de déterminant 1.

a) Propriétés algébriques

• $GL_n(K)$ est un groupe pour le produit des matrices, appelé groupe linéaire d'ordre n. $SL_n(K)$ est un sous-groupe distingué de $GL_n(K)$, appelé groupe spécial linéaire d'ordre n.

• Si $A \in GL_n(K)$, il existe des matrices élémentaires de transvection U_i telles que $A = U_1 \dots U_r D_n(\det A)$. Il en résulte que :

$GL_n(K)$ est engendré par les matrices élémentaires de dilatation et de transvection ;
$SL_n(K)$ est engendré par les matrices élémentaires de transvection.

b) Propriétés topologiques (K = R ou C)

• $M_n(K)$ étant un espace vectoriel de dimension finie, on le munit de la topologie canonique définie par l'une quelconque de ses normes. L'application $M_n(K) \to K$, $A \mapsto \det A$, est continue.

• $GL_n(K)$ est ouvert et dense dans $M_n(K)$. L'application $A \mapsto A^{-1}$, de $GL_n(K)$ dans lui-même, est continue.

• $SL_n(K)$ et $GL_n(\mathbf{C})$ sont connexes par arcs. $GL_n(\mathbf{R})$ n'est pas connexe ; il a deux composantes connexes, $GL_n^+(\mathbf{R})$ et $GL_n^-(\mathbf{R})$, qui sont connexes par arcs et homéomorphes.

3. Méthodes de calcul de l'inverse d'une matrice carrée inversible

a) Méthode de Cramer

$\boxed{A^{-1} = (\det A)^{-1}\tilde{A}}$, où $\tilde{A}$ est la matrice complémentaire de A (transposée de la matrice des cofacteurs). Cette méthode n'est praticable que si n = 2 ou n= 3.

b) Opérations élémentaires sur les lignes (ou sur les colonnes)

Par des opérations élémentaires sur les lignes, on peut transformer A en I. Les mêmes opérations élémentaires appliquées à I fournissent A^{-1}.

c) Résolution d'un système linéaire

Considérons A comme un automorphisme de K^n. Inverser A revient à résoudre le système AX = Y, où Y est un élément quelconque de K^n. On peut donc utiliser les différentes méthodes de résolution des systèmes linéaires (substitution, addition, ...).

d) Polynôme annulateur

Soit $P = a_nX^n + ... + a_0$ un élément de K[X] tel que $a_0 \neq 0$ et P(A) = 0 (un tel polynôme est un multiple du polynôme minimal de A). On a alors $\boxed{A^{-1} = -a_0^{-1}(a_nA^{n-1} + \cdots + a_1I)}$.

e) Méthode de réduction

Si A est diagonalisable ou trigonalisable, $A = PBP^{-1}$, avec B diagonale ou triangulaire. L'inversion de B est immédiate et on obtient $A^{-1} = PB^{-1}P^{-1}$. Cette méthode a un intérêt à condition que le calcul de P^{-1} soit beaucoup plus facile que celui de A^{-1}. C'est notamment le cas lorsque P est orthogonale ou unitaire.

f) Sous-algèbres de $M_n(K)$

Si A appartient à une sous-algèbre E de $M_n(K)$, alors A^{-1} appartient aussi à E, ce qui permet de chercher A^{-1} sous la même forme que A.

Bibliographie

CHAMBADAL et OVAERT, *Algèbre multilinéaire*, Dunod
OVAERT et VERLEY, *Algèbre vol. 1*, CEDIC/Fernand Nathan
TISSERON, *Géométries affine, projective et euclidienne*, Hermann

PROPRIÉTÉS ÉLÉMENTAIRES LIÉES À LA NOTION DE NOMBRE PREMIER

Remarques générales

• Par propriétés "élémentaires", il faut entendre celles qui n'utilisent pas la théorie des fonctions de variable complexe. Mais, même s'ils ne font pas partie du sujet, il faut au moins connaître les énoncés des deux beaux théorèmes suivants, qui précisent la répartition des nombres premiers :

- Théorème de Dirichlet : Toute suite arithmétique (an + b), avec a et b premiers entre eux, contient une infinité de nombres premiers.
- Théorème des nombres premiers (Hadamard, De La Vallée Poussin) : Si $\pi(x)$ désigne le nombre de nombres premiers inférieurs ou égaux à x, on a $\pi(x) \approx \frac{x}{\ln(x)}$.

• Ne pas négliger l'aspect algorithmique.

Plan

Introduction

Dans **Z**, on suppose connues la relation de divisibilité, les notions de pgcd et ppcm, les théorèmes de Gauss et de Bézout, ainsi que la théorie des congruences. On rappelle que les propriétés de divisibilité sont vraies "à association près" et donc qu'il suffit en général de travailler dans **N**.

1. Notion de nombre premier

• Définition : Entier naturel $p \geq 2$ dont les seuls diviseurs sont 1 et p.

• Théorème fondamental de l'arithmétique : Tout entier naturel non nul est de façon unique (à l'ordre près des facteurs) produit d'un nombre fini de nombres premiers. (En d'autres termes, **Z** est un anneau factoriel.)

• Théorème d'Euclide : L'ensemble des nombres premiers est infini.

Exercice 1 : Il existe une infinité de nombres premiers de la forme 4n + 3. Idem avec 6n + 5.

Exercice 2 : Notons $(p_i)_{i\geq 1}$ la suite des nombres premiers. La série $\sum_{i\geq 1} \frac{1}{p_i}$ est divergente.

2. Algorithmes et exemples

• Crible d'Eratosthène

• Test de primalité : $n \geq 2$ est premier ssi aucun entier a, avec $2 \leq a \leq \sqrt{n}$, ne divise n.

• Algorithme de décomposition d'un entier en facteurs premiers. Application au calcul du pgcd et du ppcm.

• Nombres de Fermat : Si a^m+1 est premier (avec $a \geq 2$ et $m \geq 1$), alors a est pair et m est une puissance de 2. En particulier, on appelle nombres de Fermat les entiers $F_n = 2^{2^n} + 1$, avec $n \geq 0$. A ce jour, on sait seulement que F_n est premier pour $n \leq 4$, puis composé pour $5 \leq n \leq 19$ et quelques autres valeurs isolées. Les nombres de Fermat interviennent dans le problème de la construction à la règle et au compas des polygones réguliers.

• Nombres de Mersenne : Si $a^m - 1$ est premier (avec $a \geq 2$ et $m \geq 2$), alors $a = 2$ et m est premier. On appelle nombres de Mersenne les entiers $M_n = 2^n - 1$, avec $n \geq 2$. A ce jour, on ne connaît que 28 valeurs de n pour lesquelles M_n est premier.

3. Nombres premiers et congruences

• Nombres premiers et anneaux $\mathbf{Z}/n\mathbf{Z}$: | n est premier ssi $\mathbf{Z}/n\mathbf{Z}$ est intègre ssi $\mathbf{Z}/n\mathbf{Z}$ est un corps. |

• Petit théorème de Fermat : | Si p est premier et si a n'est pas divisible par p, alors $a^{p-1} \equiv 1 [p]$. |

Il est facile de personnaliser l'exposé de ce théorème, puisqu'on en connaît plus de cent démonstrations !
Première méthode : On montre que $p \mid C_p^k$ pour tout $k \in \{1, \ldots, p-1\}$, puis par récurrence sur a, en utilisant la formule du binôme, que $a^p \equiv a [p]$.
Deuxième méthode : On travaille dans le groupe multiplicatif de $\mathbf{Z}/p\mathbf{Z}$.

Application : nouveau test de primalité. $n \geq 2$ est premier ssi $a^{n-1} \equiv 1 [n]$ pour tout a tel que $2 \leq a \leq \sqrt{n}$.

Exercice 3 : Calculer $3^{2^{32}}$ modulo $2^{32}+1$. En déduire que $2^{32}+1$ n'est pas premier.

Exercice 4 : On utilise le critère suivant pour vérifier la primalité : n est premier à 30, $2^{n-1} \equiv 1 [n]$ et $3^{n-1} \equiv 1 [n]$. Quelles sont les plus petites valeurs de n pour lesquelles ce critère est en défaut ?

Exercice 5 : Il existe une infinité de nombres premiers de la forme $4n + 1$.

Exercice 6 : Soit $n = p_1 p_2$, où p_1 et p_2 sont deux nombres premiers distincts, et soient α et β tels que $\alpha\beta \equiv 1 [\varphi(n)]$. Montrer que les applications $f : t \to t^\alpha$ et $g : t \to t^\beta$, de $\mathbf{Z}/n\mathbf{Z}$ dans lui-même, sont réciproques l'une de l'autre. (Ce résultat est utilisé en cryptographie : f sert pour le codage, g pour le décodage).

• Théorème de Wilson : | Soit $p \geq 2$. p est premier ssi $(p-1)! \equiv -1 [p]$. |

Bibliographie

HARDY and WRIGHT, *An introduction to the theory of numbers*, Oxford University Press
LEHNING et JAKUBOWICZ, *Mathématiques par l'informatique individuelle, tome 1 : le basic - arithmétique - cryptographie - équations*, Masson
ARNAUDIÈS et FRAYSSE, *Cours de mathématiques, tome 1 : algèbre*, Dunod

OPÉRATIONS ÉLÉMENTAIRES SUR LES LIGNES OU LES COLONNES D'UNE MATRICE. APPLICATIONS

Remarques générales

Les trois livres cités en bibliographie sont, chacun à sa manière, excellents pour préparer ce sujet ; ils contiennent d'autres applications que celles citées ici, ainsi que de nombreux exemples et exercices. Mettre au point quelques exemples numériques et, si possible, des algorithmes.

Plan

1. Opérations élémentaires sur les lignes d'une matrice

a) Principes généraux

• Soit M une matrice de $M_{n,p}(\mathbf{K})$, c'est-à-dire ayant n lignes et p colonnes. On va définir des opérations élémentaires sur les lignes de M, qui se traduisent par des multiplications à gauche par des matrices de $GL_n(\mathbf{K})$. Il est sous-entendu qu'on peut définir de façon analogue des opérations élémentaires sur les colonnes de M, se traduisant par des multiplications à droite par des matrices de $GL_p(\mathbf{K})$.

• Toute opération élémentaire transforme M en une matrice équivalente à M et donc conserve le rang.

b) Matrices de dilatation

• Soit $\alpha \neq 0$. On note $\boxed{L_i \to \alpha L_i}$ l'opération qui consiste à multiplier par α la i-ème ligne de M. Cela revient à multiplier M à gauche par $\boxed{D_i(\alpha) = I + (\alpha - 1)E_{ii}}$, appelée matrice élémentaire de dilatation.

• L'application $\alpha \mapsto D_i(\alpha)$ est un morphisme du groupe multiplicatif $\mathbf{K}^*$ dans le groupe $GL_n(\mathbf{K})$.

c) Matrices de transvection

• Soient $i \neq j$ et $\alpha \in \mathbf{K}$. On note $\boxed{L_i \to L_i + \alpha L_j}$ l'opération qui consiste à ajouter à la i-ème ligne de M le produit par α de sa j-ème ligne. Cela revient à multiplier M à gauche par $\boxed{T_{ij}(\alpha) = I + \alpha E_{ij}}$, appelée matrice élémentaire de transvection.

• L'application $\alpha \mapsto T_{ij}(\alpha)$ est un morphisme du groupe additif $\mathbf{K}$ dans le groupe $GL_n(\mathbf{K})$.

d) Matrices de transposition

• Soient $i \neq j$. On note $\boxed{L_i \leftrightarrow L_j}$ l'opération qui consiste à échanger la i-ème et la j-ème lignes de M. Cela revient à multiplier M à gauche par $\boxed{P_{(ij)} = I - E_{ii} - E_{jj} + E_{ij} + E_{ji}}$, appelée matrice de transposition. Cette opération, bien que pratique, n'est pas indispensable d'un point de vue théorique car $L_i \leftrightarrow L_j$ équivaut à la suite d'opérations : $L_i \to L_i + L_j$; $L_j \to L_j - L_i$; $L_i \to L_i + L_j$; $L_j \to -L_j$.

• Plus généralement, étant donnée une permutation σ de {1, 2, … , n}, on note P_σ la matrice $\left(\delta_{\sigma(i),j}\right)$, appelée matrice de permutation. Multiplier M à gauche par P_σ revient à faire agir la permutation σ sur les lignes de M. L'application $\sigma \mapsto P_\sigma$ est un morphisme du groupe symétrique S_n dans le groupe $GL_n(\mathbf{K})$.

2. <u>Applications</u>

a) Inversion d'une matrice carrée

Théorème : Soit M une matrice inversible de $M_n(\mathbf{K})$. Alors il existe des matrices élémentaires de transvection U_i telles que $M = U_1 U_2 \dots U_r D_n(\det M)$.

Conséquence 1 : Pour calculer pratiquement l'inverse de M, on effectue simultanément les mêmes opérations élémentaires sur les lignes de M et de I, jusqu'à ce que M soit transformée en I ; I est alors devenue M^{-1}.

Conséquence 2 : $GL_n(\mathbf{K})$ est engendré par les matrices élémentaires de dilatation et de transvection ; $SL_n(\mathbf{K})$ est engendré par les matrices élémentaires de transvection.

Conséquence 3 : Deux matrices A et B de $M_{n,p}(\mathbf{K})$ sont équivalentes ssi on peut passer de A à B par des opérations élémentaires sur les lignes *et* sur les colonnes.

b) Résolution d'un système linéaire

Théorème du pivot de Gauss : Soit M une matrice de rang r de $M_{n,p}(\mathbf{K})$. Par des opérations élémentaires sur les lignes, on peut transformer M en une matrice G échelonnée ayant r lignes non nulles.

Théorème du pivot de Hermite-Jordan : Soit M une matrice de rang r de $M_{n,p}(\mathbf{K})$. Par des opérations élémentaires sur les lignes, on peut transformer M en une matrice H échelonnée ayant r lignes non nulles, le premier élément non nul de chaque ligne non nulle étant 1 et tous les autres éléments de la colonne correspondante étant nuls.

A partir de l'un de ces théorèmes, on retrouve immédiatement tous les résultats théoriques concernant les systèmes linéaires et on dispose d'une méthode pratique de résolution.

c) Calcul du rang d'une matrice rectangulaire

Les opérations élémentaires conservant le rang, on peut effectuer des opérations élémentaires sur les lignes *et* les colonnes jusqu'à l'obtention d'une matrice échelonnée.

d) Calcul du déterminant d'une matrice carrée

On peut effectuer des opérations élémentaires sur les lignes *et* les colonnes jusqu'à l'obtention d'une matrice triangulaire, en tenant compte du fait que $\det D_i(\alpha) = \alpha$, $\det T_{ij}(\alpha) = 1$ et $\det P_\sigma = \varepsilon(\sigma)$.

Bibliographie

CABANE et LEBOEUF, *Matrices et réduction,* Ellipses
OVAERT et VERLEY, *Algèbre vol. 1*, CEDIC/Fernand Nathan
TISSERON, *Géométries affine, projective et euclidienne*, Hermann

GROUPES OPÉRANT SUR UN ENSEMBLE ; APPLICATIONS

Remarques générales

• Programme : "Groupe opérant sur un ensemble, orbites. Éléments conjugués, classes de conjugaison. Stabilisateur. Formule des classes."

• Ces notions ne révèlent leur intérêt qu'à travers des applications relativement difficiles. Éviter de réduire la leçon à un simple vocabulaire alourdissant des situations banales sans les éclairer.

Plan

1. Définitions et exemples

a) Groupe opérant sur un ensemble

• On dit qu'un groupe G opère sur un ensemble E s'il existe une application $G \times E \to E, (g, x) \mapsto g.x$, telle que

(i) $\forall x \in E \quad 1.x = x$;

(ii) $\forall (g_1, g_2) \in G^2 \quad \forall x \in E \quad (g_1 g_2).x = g_1.(g_2.x)$.

• Si G opère sur E, alors $g \mapsto (x \mapsto g.x)$ définit un homomorphisme T du groupe G dans le groupe S(E) des permutations de E. Réciproquement, si $T \in \mathrm{Hom}(G, S(E))$, alors G opère sur E par g.x = T(g) (x). Il y a donc une bijection entre l'ensemble des opérations de G sur E et l'ensemble Hom(G, S(E)).

• On dit que G opère fidèlement sur E si T est injective. Une opération fidèle permet de "réaliser" G comme sous-groupe de S(E).

b) Orbite et stabilisateur d'un élément

• La relation définie dans E par : $x \equiv y \Leftrightarrow \exists g \in G \quad y = g.x$, est une relation d'équivalence. Les classes d'équivalence sont appelées orbites. L'orbite de x est notée G.x.

• On dit que G opère transitivement sur E s'il n'y a qu'une orbite.

• Si x est un élément de E, l'ensemble $G_x = \{g \in G / g.x = x\}$ est un sous-groupe de G, appelé stabilisateur de x.

c) Exemples

• *Opérations d'un groupe sur lui-même* : Un groupe G opère sur lui-même par translation à gauche (g.x = gx) ou par conjugaison ($g.x = gxg^{-1}$).

• *Structure d'espace affine* : Soient V un espace vectoriel et E un ensemble non vide. On dit que E est un espace affine de direction V si le groupe additif de V opère fidèlement et transitivement sur E.

• *Angles de vecteurs (ou de demi-droites)* : Soient E un espace vectoriel euclidien et U l'ensemble de ses vecteurs unitaires. G = O(E) ou $O^+(E)$ opère dans U × U par $f.(\vec{u}, \vec{v}) = (f(\vec{u}), f(\vec{v}))$. L'orbite de $(\vec{u}, \vec{v})$ sous l'action de O(E) (resp. $O^+(E)$) est appelée angle non orienté (resp. angle orienté) de $(\vec{u}, \vec{v})$.
Remarque : Si dim E ≥ 3, les deux notions coïncident ; la distinction n'a d'intérêt qu'en dimension 2.

2. Formule des classes

a) Résultat préliminaire

Soit G un groupe opérant transitivement sur un ensemble E et soit x un élément de E. Alors E est en bijection avec le quotient G / G_x. Si de plus g est fini, alors E est fini et $\boxed{|E| = [G : G_x]}$.

b) Formule des classes

Soit G un groupe fini opérant sur un ensemble fini et soit $\{x_1, \dots, x_n\}$ un système de représentants des orbites. Alors :

$$\boxed{|E| = \sum_{i=1}^{n} \left[G : G_{x_i}\right]}.$$

c) Formule des classes de conjugaison d'un groupe fini

Soit G un groupe fini opérant sur lui-même par conjugaison et soit $\{x_1, \dots, x_n\}$ un système de représentant des orbites ayant au moins deux éléments. Alors, en notant C(G) le centre de G et C(x) le centralisateur d'un élément x de G, on a :

$$\boxed{|G| = |C(G)| + \sum_{i=1}^{n} \left[G : C(x_i)\right]}.$$

3. <u>Applications</u>

a) Théorème de Burnside

Si G est un groupe fini d'ordre p^k avec p premier et $k \geq 1$, alors $C(G) \neq \{1\}$.

b) Théorème de Cauchy

Soient G un groupe fini et p un diviseur premier de l'ordre de G. Alors G possède un élément d'ordre p.

c) Théorème de Wedderburn

Tout corps fini est commutatif.

d) Sous-groupes finis de $O^+(\mathbf{R}^3)$

Il existe au plus 6 types de sous-groupes finis de $O^+(\mathbf{R}^3)$, dont les caractéristiques sont données par le tableau suivant. Réciproquement, on peut montrer par un exemple que chacun de ces cas se produit effectivement.

Type	$\lvert G\rvert$	$\lvert G_{x_1}\rvert$	$\lvert G_{x_2}\rvert$	$\lvert G_{x_3}\rvert$	Exemple
I	1				{id}
II	n ($n \geq 2$)	n	n		rotations d'un polygone régulier à n côtés, d'axe perpendiculaire à son plan
III	2n ($n \geq 2$)	2	2	n	rotations d'un polygone régulier à n côtés
IV	12	2	3	3	rotations d'un tétraèdre
V	24	2	3	4	rotations d'un cube (ou d'un octaèdre)
VI	60	2	3	5	rotations d'un dodécaèdre (ou d'un icosaèdre)

Bibliographie

BOUVIER et RICHARD, *Groupes*, Hermann
BERGER, *Géométrie tome 1*, CEDIC/Fernand Nathan
FRENKEL, *Géométrie pour l'élève-professeur*, Hermann
TAUVEL, *Mathématiques générales pour l'agrégation*, Masson

ORIENTATION D'UN ESPACE VECTORIEL DE DIMENSION 3 ; PRODUIT MIXTE, PRODUIT VECTORIEL ; APPLICATIONS

Remarques générales

• Préparer un enchaînement cohérent pour définir et étudier de façon rigoureuse l'orientation, le produit mixte et le produit vectoriel. Éviter le style "physicien" !

• Si les résultats et applications sont nombreux, rien dans la leçon n'est vraiment difficile. La difficulté sera donc le choix de l'exposé : il faudra présenter plusieurs points du plan, mais lesquels ?

Plan

E est un espace affine euclidien de dimension 3, de direction $\vec{E}$.

1. Orientation

a) Orientation de E

Sur l'ensemble des bases de E, la relation définie par " $B \equiv B' \Leftrightarrow \det_B(B') > 0$ " est une relation d'équivalence. Il y a deux classes d'équivalence appelées orientations de E. Orienter E, c'est distinguer l'une de ces orientations (en général par le choix d'une base B). Les bases de même orientation que B sont dites positives ou directes, les autres négatives ou rétrogrades.
Remarque : tout ceci reste valable en dimension quelconque.

b) Orientation conjointe d'un plan et d'une droite orthogonaux de E

Soient P un plan et D une droite orthogonaux dans l'espace E orienté. Orienter P et D de façon conjointe, c'est choisir une base $(\vec{i}, \vec{j})$ de P et une base $(\vec{k})$ de D telles que $(\vec{i}, \vec{j}, \vec{k})$ soit une base directe de E. Il y a deux orientations conjointes, déterminées par les deux vecteurs unitaires de D.

2. Produit mixte, produit vectoriel

a) Produit mixte

• Soit B une base orthonormée directe. Le produit mixte de trois vecteurs $\vec{u}, \vec{v}, \vec{w}$ est par définition $\boxed{[\vec{u}, \vec{v}, \vec{w}] = \det_B(\vec{u}, \vec{v}, \vec{w})}$. ($[\vec{u}, \vec{v}, \vec{w}]$ ne dépend pas de B, mais seulement de l'orientation.)

• L'application $\vec{E} \times \vec{E} \times \vec{E} \to \mathbf{R}$, $(\vec{u}, \vec{v}, \vec{w}) \mapsto [\vec{u}, \vec{v}, \vec{w}]$ est une forme trilinéaire alternée qui vaut 1 pour les bases orthonormées directes. En particulier, $\boxed{[\vec{u}, \vec{v}, \vec{w}] = 0 \text{ ssi } \vec{u}, \vec{v}, \vec{w} \text{ sont coplanaires}}$.

b) Produit vectoriel

• Etant donnés deux vecteurs $\vec{u}$ et $\vec{v}$, il existe un unique vecteur $\vec{a}$ tel que, pour tout vecteur $\vec{w}$, $[\vec{u}, \vec{v}, \vec{w}] = \vec{a} \,.\, \vec{w}$. On dit que $\vec{a}$ est le produit vectoriel de $\vec{u}$ et $\vec{v}$; on le note $\vec{u} \wedge \vec{v}$. Ainsi, pour trois vecteurs quelconques, $\boxed{[\vec{u}, \vec{v}, \vec{w}] = (\vec{u} \wedge \vec{v}) \,.\, \vec{w}}$.

• L'application $\vec{E} \times \vec{E} \to \vec{E}$, $(\vec{u}, \vec{v}) \mapsto \vec{u} \wedge \vec{v}$ est une application trilinéaire alternée. On a de plus la propriété : $\boxed{\vec{u} \wedge \vec{v} = 0 \text{ ssi } \vec{u} \text{ et } \vec{v} \text{ colinéaires}}$.

• *Calcul du produit vectoriel* : Soit $\vec{P}$ un plan vectoriel contenant $\vec{u}$ et $\vec{v}$ (unique si $\vec{u}$ et $\vec{v}$ ne sont pas colinéaires), orienté par le choix d'un vecteur normal unitaire $\vec{k}$. Si dans $\vec{P}$, $(\vec{u}, \vec{v})$ désigne l'angle orienté de $\vec{u}$

et $\vec{v}$, et θ leur angle géométrique, on a $\boxed{\vec{u} \wedge \vec{v} = \|\vec{u}\| \|\vec{v}\| \sin(\vec{u}, \vec{v})\, \vec{k}}$ et $\boxed{\|\vec{u} \wedge \vec{v}\| = \|\vec{u}\| \|\vec{v}\| \sin\theta}$. On en déduit l'*identité de Lagrange* : $\boxed{(\vec{u}.\vec{v})^2 + \|\vec{u} \wedge \vec{v}\|^2 = \|\vec{u}\|^2 \|\vec{v}\|^2}$.

• *Expression analytique du produit vectoriel* : Dans une base orthonormée directe, si $\vec{u} = x\vec{i} + y\vec{j} + z\vec{k}$ et $\vec{v} = x'\vec{i} + y'\vec{j} + z'\vec{k}$, alors $\boxed{\vec{u} \wedge \vec{v} = \begin{vmatrix} y & y' \\ z & z' \end{vmatrix} \vec{i} + \begin{vmatrix} z & z' \\ x & x' \end{vmatrix} \vec{j} + \begin{vmatrix} x & x' \\ y & y' \end{vmatrix} \vec{k}}$.

• *Formule du double produit vectoriel* : $\boxed{\vec{u} \wedge (\vec{v} \wedge \vec{w}) = (\vec{u}.\vec{w})\vec{v} - (\vec{u}.\vec{v})\vec{w}}$.

3. <u>Applications</u> (à développer)

a) Problèmes d'incidence

• Caractérisations vectorielles du parallélisme, de l'orthogonalité, de l'alignement, de la coplanéité.
• Équation vectorielle d'une droite donnée par un point et un vecteur directeur, d'un plan donné par un point et deux vecteurs directeurs.

b) Calcul de distances, aires, volumes

• Distance d'un point à une droite, d'un point à un plan, de deux droites non parallèles.
• Aire d'un parallélogramme, d'un triangle.
• Volume d'un parallélépipède, d'un tétraèdre.

c) Le corps des quaternions

$\mathbf{H} = \mathbf{R} \times \vec{E}$ est un corps non commutatif, appelé corps des <u>quaternions</u>, pour les opérations définies par $(\alpha, \vec{u}) + (\beta, \vec{v}) = (\alpha + \beta, \vec{u} + \vec{v})$ et $(\alpha, \vec{u}) \times (\beta, \vec{v}) = (\alpha\beta - \vec{u}.\vec{v}, \alpha\vec{v} + \beta\vec{u} + \vec{u} \wedge \vec{v})$.

d) Etude des isométries

• Calcul de l'angle d'une rotation ou d'une rotation-réflexion.
• Expressions vectorielle et matricielle d'une rotation d'axe donné, défini par un point et un vecteur unitaire, et d'angle donné.
• Caractérisation des rotations vectorielles : ce sont les endomorphismes f non nuls tels que, pour tous vecteurs $\vec{u}$ et $\vec{v}$, $f(\vec{u} \wedge \vec{v}) = f(\vec{u}) \wedge f(\vec{v})$.

e) Propriétés métriques des courbes, cinématique

• Repère de Frenet, courbure, torsion.
• Repère mobile, vecteur rotation d'un repère orthonormal dépendant du temps, vitesse d'un point lié au repère ou mobile dans ce repère, accélération de Coriolis.

Bibliographie

RAMIS, DESCHAMPS et ODOUX, *Cours de mathématiques spéciales, tomes 2 et 5*, Masson
TISSERON, *Géométries affine, projective et euclidienne*, Hermann
MONIER, *Géométrie*, Dunod
LEHNING, *Analyse en dimension finie*, Masson

LA PARABOLE DANS LE PLAN AFFINE EUCLIDIEN

Remarques générales

Cette leçon de synthèse est difficile car il faut organiser soi-même de manière cohérente les multiples résultats éparpillés dans la littérature.

Plan

1. Notion de parabole

a) Théorème et définitions

Soit P une partie du plan. Les deux propriétés suivantes sont équivalentes :
(i) Il existe une droite D et un point $F \notin D$ tels que P soit la médiatrice de D et de F.
(ii) Il existe un repère orthonormé $(O, \vec{i}, \vec{j})$ et un réel $p > 0$ tels que P ait pour équation cartésienne $y^2 = 2px$.

Dans ce cas, D, F et p sont uniques et $(O, \vec{i}, -\vec{j})$ est le seul autre repère qui convienne. On dit que P est la parabole de directrice D, de foyer F, de paramètre p, de sommet O, d'axe $(O, \vec{i})$ et d'équation réduite $y^2 = 2px$. L'intérieur (resp. extérieur) de P est l'ensemble des points M tels que MF < d(M, D) (resp. MF > d(M, D)).

b) Equation cartésienne dans un repère orthonormé quelconque

Soit $(\Omega, \vec{I}, \vec{J})$ un repère orthonormé quelconque. P est une parabole ssi P a une équation cartésienne de la forme $ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0$, avec $\begin{vmatrix} a & b \\ b & c \end{vmatrix} = 0$ et $\begin{vmatrix} a & b & d \\ b & c & e \\ d & e & f \end{vmatrix} \neq 0$.

c) Equation polaire lorsque le foyer est à l'origine

Soit $(\Omega, \vec{I}, \vec{J})$ un repère orthonormé direct. P est une parabole de foyer Ω ssi P a une équation polaire de la forme $\rho(1 + \cos(\theta - \varphi)) = p$ avec $\varphi \in \mathbf{R}$ et $p > 0$. Dans ce cas, P a pour paramètre p et pour directrice la droite d'équation polaire $\rho \cos(\theta - \varphi) = p$.

2. Etude de la forme et construction de la courbe

a) Remarques diverses sur la forme de la courbe

• Le groupe des isométries de P est {id, s}, où s est la réflexion d'axe $(O, \vec{i})$.
• Une droite coupe P en 0, 1 ou 2 points.
• L'intérieur de P est convexe.
• Deux paraboles quelconques sont semblables. Elles sont isométriques ssi elles ont le même paramètre p.

b) Construction

1ère méthode : P est la réunion des courbes représentatives des fonctions $x \to \sqrt{2px}$ et $x \to -\sqrt{2px}$ (ou la courbe représentative de la fonction $y \to \frac{y^2}{2p}$).

2ème méthode : P est l'ensemble des centres des cercles tangents à D et passant par F, d'où une construction par points à la règle et au compas.

3. Autres propriétés

a) Propriétés différentielles de la courbe

• P admet en tout point M_0 (x_0, y_0) une tangente (aux divers sens du terme) d'équation $\boxed{yy_0 = p(x + x_0)}$.

• Courbure, centre de courbure, développée.
• Longueur d'un arc de parabole.
• Aire d'un segment de parabole (*Résultat d'Archimède* : "un segment quelconque compris par une droite et une parabole est égal à quatre fois le tiers d'un triangle qui a la même base et la même hauteur que le segment").

b) Propriétés géométriques des tangentes et normales

Soient M un point quelconque de P, H son projeté orthogonal sur D, K son projeté orthogonal sur (OF). La tangente en M coupe l'axe en T et la directrice en U ; la normale en M coupe l'axe en N. On a les propriétés géométriques suivantes :

1) (MT) est la médiatrice de [FH] et la bissectrice intérieure de $\widehat{FMH}$ (application : miroirs paraboliques).

2) $\widehat{MFU} = \pi/2$.

3) F est le milieu de [TN] et $\overline{KN} = p$.

Exercice 1 : De tout point M extérieur à P, on peut lui mener deux tangentes. En donner une construction. Elles sont perpendiculaires ssi M est sur D.

Exercice 2 : Les normales en trois points distincts A, B, C de P sont concourantes ssi le centre de gravité du triangle ABC est sur l'axe de P.

c) Théorème de l'angle pivotant

Si M désigne le point d'intersection de deux tangentes à P en deux points distincts A et B, la droite (FM) est la bissectrice intérieure de l'angle $(\overrightarrow{FA}, \overrightarrow{FB})$. Si une troisième tangente à P coupe les tangentes en A et B respectivement en S et T, l'angle de droites (FS, FT) ne dépend que de A et de B et vaut $\frac{1}{2}(\overrightarrow{FA}, \overrightarrow{FB})$.

Bibliographie

RAMIS, DESCHAMPS et ODOUX, *Cours de mathématiques spéciales, tome 2*, Masson
TRIGNAN, *Les coniques*, Vuibert
LEHMANN et BKOUCHE, *Initiation à la géométrie*, PUF
AVEZ, *La leçon de géométrie à l'oral de l'agrégation*, Masson

ILLUSTRATION DE LA NOTION DE PARTIE GÉNÉRATRICE D'UN GROUPE

Remarques générales

• Les généralités sur les groupes doivent être supposées connues, afin de ne pas perdre un temps précieux.

• Points du programme en rapport avec le sujet :

- Sous-groupe engendré par une partie
- Groupes cycliques. Ordre d'un élément
- Décomposition d'une permutation en produit de cycles disjoints, en produit de transpositions
- Groupe des racines n-ièmes de l'unité, générateurs (racines primitives)
- Les réflexions engendrent le groupe orthogonal O(E) ; les demi-tours engendrent SO(3)
- Les réflexions engendrent le groupe des isométries ; en dimension 3, les demi-tours engendrent le groupe des déplacements

• Le mot "illustration" est à comprendre en deux sens. Il s'agit bien sûr de donner des exemples de parties génératrices, mais aussi des exemples de ce à quoi elles peuvent servir en théorie des groupes. D'où un possible plan en deux parties.

Plan

1. Qu'est-ce qu'une partie génératrice d'un groupe ?

a) Définitions

Soient G un groupe, et E une partie de G.
On appelle sous-groupe de G engendré par E le plus petit (pour l'inclusion) sous-groupe de G contenant E. On le note $< E >$.

$$< E > = \bigcap_{\substack{H \text{ sous-groupe de } G \\ E \subset H}} H = \left\{ x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} \ / \ x_i \in E \text{ et } \alpha_i = \pm 1 \right\}$$

On dit que E est une partie génératrice de G si $< E > = G$.
On dit que G est de type fini s'il admet au moins une partie génératrice finie.

b) Exemples

• Groupes de type fini
Tout groupe fini est de type fini ; $\mathbf{Z}^2 = < (1,0) , (0,1) >$; **Q** n'est pas de type fini.
$G = \left\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$ est de type fini, mais le sous-groupe de G des matrices de la forme $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ n'est pas de type fini !

• Groupes monogènes
Tout groupe monogène est isomorphe à **Z** ou à $\mathbf{Z}/n\mathbf{Z}$. Tout sous-groupe d'un groupe monogène est monogène.

• Groupes symétriques et alternés
S_n est engendré par : les cycles ; les transpositions ; (12) et (12...n) ; (12), (13), ... , (1n) ; (12), (23), ... , ((n-1)n).
A_n est engendré par : les produits de deux transpositions ; les 3-cycles.

• Groupes de la géométrie
Soit E un **R**-espace vectoriel euclidien.
GL(E) est engendré par les dilatations ; SL(E) est engendré par les transvections.
O(E) est engendré par les réflexions ; pour dim E ≥ 3, SO(E) est engendré par les demi-tours.
On a des résultats analogues concernant le groupe affine et le groupe des isométries d'un espace affine euclidien.

2. A quoi sert une partie génératrice d'un groupe ?

a) Un homomorphisme de groupes f: G → H est entièrement déterminé si l'on connaît sa restriction à une partie génératrice de G

Exemple : Calcul de la signature d'une permutation à partir de sa décomposition en cycles.

b) Si un sous-groupe H de G contient une partie génératrice de G, alors H = G

Théorème 1 : Pour dim E = 3, SO(E) est simple.
(Soit G un sous-groupe distingué de SO(E) distinct de {Id}. On montre que G contient un retournement. Deux retournements quelconques étant conjugués, G contient tous les retournements. Comme les retournements engendrent SO(E), G = SO(E).)

Théorème 2 : Pour $n \geq 5$, A_n est simple.
(Même schéma : on montre que, si G est un sous-groupe distingué de A_n distinct de {Id}, G contient un 3-cycle, puis tous les 3-cycles.)

Théorème 3 : Sauf si n = 2 et si K est le corps à deux ou trois éléments, $SL_n(K)$ est égal à son groupe dérivé.
(Comme $SL_n(K)$ est engendré par les transvections, il suffit de montrer que toute transvection est un commutateur.)

c) Plus généralement, démontrer qu'une propriété concernant un ou plusieurs groupes est vraie revient, dans certains cas, à la vérifier pour des parties génératrices

Théorème : Soit H un sous-groupe d'un groupe fini G, avec G = < S > et H = < T >. H est distingué dans G si et seulement si, pour tout $s \in S$ et tout $t \in T$, $sts^{-1} \in H$.

Exemple : Pour montrer que {1, (12)(34), (13)(24), (14)(23)} = < (12)(34) , (13)(24) > est distingué dans S_4 = < (12) , (1234) >, il n'y a que 4 vérifications à faire au lieu de 96.

Attention, le théorème n'est plus valable si G est infini : prendre $G = \left\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$ et $H = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$.

Bibliographie

AVEZ, *La leçon de géométrie à l'oral de l'agrégation*, Masson
RAMIS, DESCHAMPS et ODOUX, *Cours de mathématiques spéciales, tome 1 : algèbre*, Masson
BOUVIER et RICHARD, *Groupes*, Hermann
TISSERON, *Géométries affine, projective et euclidienne*, Hermann
JACOBSON, *Basic Algebra I*, Freeman

PGCD ; THÉORÈME DE BÉZOUT. MÉTHODES DE CALCUL

Remarques générales

• Il faut traiter le cas des entiers et celui des polynômes. Pour éviter les répétitions, il est quasiment indispensable de présenter la théorie dans un cadre général (mais attention aux questions éventuelles du jury sur la théorie abstraite des anneaux …).

• Pour gagner du temps, ne rien mettre dans le plan à propos du PPCM (il y a une autre leçon pour ça). Par contre, on pourra évoquer oralement ses propriétés en parallèle avec celles du PGCD.

• L'aspect algorithmique est essentiel. Ne pas se limiter au calcul du PGCD ; il faut savoir calculer également les coefficients de Bézout. Sans méthode effective de calcul, ce beau théorème et ses nombreuses applications ne servent à rien !

Plan

Introduction

On suppose connues les notions d'anneau euclidien, principal et factoriel. On rappelle que tout anneau euclidien est principal, et que tout anneau principal est factoriel. En se plaçant dans un cadre général, on peut traiter simultanément les deux cas usuels que sont **Z** et **K**[X].

1. Définition du PGCD dans un anneau commutatif intègre

Soient A un anneau commutatif intègre et $(a_i)_{1\leq i\leq n}$ une famille finie d'éléments de A.
Un élément d de A est appelé un PGCD des a_i si d divise chaque a_i et si tout diviseur commun des a_i divise d.
S'il existe un PGCD d des a_i, alors l'ensemble des PGCD des a_i est la classe d'association de d. A association près, on peut donc parler du PGCD des a_i ; on note alors $\boxed{d = \mathrm{PGCD}(a_1, \dots, a_n) \text{ ou } d = \bigwedge_{i=1}^{n} a_i}$.

Remarque : Le PGCD n'existe pas toujours. Dans l'anneau $Z[i\sqrt{5}]$ (qui n'est pas factoriel), les éléments $x = 3^2 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ et $y = 6 + 3i\sqrt{5} = 3(2 + i\sqrt{5})$ n'ont pas de PGCD.

2. Existence et calcul du PGCD dans un anneau factoriel *(Dans cette partie, A est un anneau factoriel.)*

• Les a_i admettent toujours un PGCD. Dans le cas où les a_i sont non nuls, le PGCD s'exprime à partir des décompositions en éléments irréductibles des a_i. (Cette méthode de calcul est en pratique inutilisable.)

• On dit que les a_i sont premiers entre eux (dans leur ensemble) lorsque $\bigwedge_{i=1}^{n} a_i = 1$.

• Théorème de Gauss : $\boxed{\text{Si } a \mid bc \text{ et si } a \wedge b = 1, \text{ alors } a \mid c.}$

3. Cas d'un anneau principal : théorème de Bézout *(Dans cette partie, A est un anneau principal.)*

a) Théorème de Bézout

• Théorème : $\boxed{a_1A + a_2A + \dots + a_nA = \left(\bigwedge_{i=1}^{n} a_i\right)A}$

• Théorème de Bézout :

$\boxed{\begin{array}{l} \text{i) } \bigwedge_{i=1}^{n} a_i = 1 \text{ ssi il existe } u_1, \dots, u_n \text{ tels que } a_1u_1 + \dots + a_nu_n = 1. \\ \text{ii) Soit d un diviseur commun des } a_i. \ \bigwedge_{i=1}^{n} a_i = d \text{ ssi il existe } u_1, \dots, u_n \text{ tels que } a_1u_1 + \dots + a_nu_n = d. \end{array}}$

Pour le calcul des coefficients de Bézout u_i, voir partie 4.

b) Applications

• Autre preuve du théorème de Gauss. Eléments inversibles de $\mathbf{Z}/n\mathbf{Z}$; calcul de l'inverse.Théorème chinois.
• Décomposition des fractions rationnelles en éléments simples.
• Algèbre linéaire : lemme des noyaux, décomposition spectrale.

4. Cas d'un anneau euclidien : algorithme d'Euclide *(Dans cette partie, A est un anneau euclidien.)*

Comme PGCD(a, b, c) = PGCD(PGCD(a, b), c), il suffit de savoir calculer le PGCD de deux éléments a et b.

a) Algorithme d'Euclide

On pose $x_0 = a$, $x_1 = b$, $x_2 = x_0 - q_1x_1$, $x_3 = x_1 - q_2x_2$, … , $x_{n+1} = x_{n-1} - q_nx_n = 0$, où les q_i sont les quotients dans les divisions euclidiennes successives, jusqu'à ce qu'on obtienne un reste nul. On a alors :

$$PGCD(a, b) = PGCD(x_0, x_1) = PGCD(x_1, x_2) = \dots = PGCD(x_n, x_{n+1}) = PGCD(x_n, 0) = x_n.$$

Le passage de (x_{i-1}, x_i) à (x_i, x_{i+1}) peut s'écrire matriciellement $\begin{pmatrix} x_i \\ x_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} x_{i-1} \\ x_i \end{pmatrix}$. Finalement, on a :

$$\begin{pmatrix} a \wedge b \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

. Cet algorithme peut s'écrire aussi de manière récursive :

```
pour PGCD(a, b) faire
   si b = 0 alors a sinon PGCD(b, a mod b)
fin pour
```

Exercice 1 : Dans $\mathbf{K}[X]$, montrer que $(X^m - 1) \wedge (X^n - 1) = X^{m \wedge n} - 1$.
Exercice 2 : La suite de Fibonacci est définie par $F_0 = 0$, $F_1 = 1$ et $F_{n+1} = F_n + F_{n-1}$. Montrer que $F_m \wedge F_n = F_{m \wedge n}$.

b) Algorithme d'Euclide étendu

L'algorithme défini matriciellement par :

$$\begin{pmatrix} a \wedge b & u & v \\ 0 & \dots & \dots \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}$$

fournit, en plus du PGCD, des coefficients de Bézout, c'est-à-dire des nombres u et v tels que $a \wedge b = au + bv$.
Remarque : Dans le cas de $\mathbf{Z}$, cet algorithme fournit l'unique couple (u, v) tel que $|u| < |b|$ et $|v| < |a|$. Dans le cas de $\mathbf{K}[X]$, on obtient l'unique couple (u, v) tel que $\deg(u) < \deg(b)$ et $\deg(v) < \deg(a)$.

5. Une autre méthode de calcul du PGCD dans le cas des polynômes

• Soient P et Q deux polynômes non nuls de $\mathbf{K}[X]$. Le PGCD de P et Q est une combinaison linéaire non nulle de degré minimum de la famille $F = (P, XP, \dots, X^{n-1}P, Q, XQ, \dots, X^{m-1}Q)$, où $m = \deg(P)$ et $n = \deg(Q)$. Pratiquement, on écrit chaque élément de F dans la base $(X^{m+n-1}, X^{m+n-2}, \dots, X, 1)$ de $\mathbf{K}_{m+n-1}[X]$ et on échelonne le système obtenu par la méthode du pivot. La dernière ligne non nulle du tableau final fournit le PGCD. Les mêmes manipulations effectuées sur la matrice identique fournissent les coefficients de Bézout.

• Cette technique est à relier à la théorie de l'élimination et du résultant. Si K est algébriquement clos, on a :

P et Q ont une racine commune ssi $\deg(P \wedge Q) \geq 1$ ssi F est une famille liée.

Bibliographie

ARNAUDIÈS et FRAYSSE, *Cours de mathématiques, tome 1 : algèbre*, Dunod
LEHNING et JAKUBOWICZ, *Mathématiques par l'informatique individuelle, tome 1 : le basic - arithmétique - cryptographie - équations*, Masson
CABANE et LEBOEUF, *Espaces vectoriels, polynômes*, Ellipses
MONASSE, *Mathématiques et informatique*, Vuibert

RACINES D'UN POLYNÔME À UNE INDÉTERMINÉE SUR R OU C ; RELATIONS ENTRE LES COEFFICIENTS ET LES RACINES

Remarques générales

• Programme : Racines (ou zéros) d'un polynôme, ordre de multiplicité. Polynômes scindés. Equations algébriques. Relations entre les coefficients et les racines d'un polynôme scindé. Théorème de D'Alembert-Gauss ; polynômes irréductibles de $\mathbf{C}[X]$ et de $\mathbf{R}[X]$. Factorisation des polynômes dans $\mathbf{C}[X]$ et dans $\mathbf{R}[X]$. Exemples simples de problèmes d'élimination.

• "Les exercices sur les relations entre coefficients et racines d'un polynôme conduisent souvent à des débauches de calculs pouvant la plupart du temps être évités. Là encore l'arrière-plan théorique est souvent ignoré au profit d'une technique pas toujours maîtrisée." (rapport du jury 1990)

Plan

Introduction

K désigne l'un des corps **R** ou **C**. De nombreux problèmes se ramènent à la résolution d'une équation $P(x) = 0$, où $P \in \mathbf{K}[X]$, c'est-à-dire d'une <u>équation algébrique</u>. Le point de départ de la théorie est que, si $a \in \mathbf{K}$, la division euclidienne de P par $X - a$ s'écrit : $P = (X - a)Q + P(a)$.

1. Racines d'un polynôme

• On dit que a est une <u>racine</u> (ou un <u>zéro</u>) de P si $P(a) = 0$, ou de façon équivalente si $X - a \mid P$. Dans ce cas, le plus grand entier q tel que $(X - a)^q \mid P$ est appelé <u>ordre de multiplicité</u> de a.

• a est racine d'ordre q de P ssi $P(a) = P'(a) = \ldots = P^{(q-1)}(a) = 0$ et $P^{(q)}(a) \neq 0$.

• Si P a n racines distinctes, alors $\deg(P) \geq n$. Si P est de degré n, alors P a au plus n racines (comptées avec leur ordre de multiplicité). Une conséquence importante est qu'on peut identifier polynômes et fonctions polynômes.

• On dit que P est <u>scindé</u> si le nombre de racines de P (comptées avec leur ordre de multiplicité) est égal au degré de P.

Exercice 1 : L'équation $\frac{x^n}{n!} + \frac{x^{n-1}}{(n-1)!} + \cdots + \frac{x}{1!} + 1 = 0$ n'a pas de racine multiple.

Exercice 2 : Trouver un polynôme P tel que 1 soit racine d'ordre au moins n de P + 1 et -1 racine d'ordre au moins n de P - 1.

Exercice 3 : Interpolation de Lagrange. Polynômes prenant des valeurs données en n points donnés.

2. Relations entre coefficients et racines d'un polynôme scindé

• Soit $P = c_0X^n + c_1X^{n-1} + \ldots + c_n = c_0(X - a_1)(X - a_2) \ldots (X - a_n)$ un polynôme scindé. Pour $k = 1, 2, \ldots, n$, on a

$$(-1)^k \frac{c_k}{c_0} = \sigma_k(a_1, \ldots, a_n) = \sum_{i_1 < i_2 < \cdots < i_k} a_{i_1} a_{i_2} \cdots a_{i_k}$$

Les $\sigma_k : \mathbf{K}^n \to \mathbf{K}$ sont appelées <u>fonctions symétriques élémentaires</u>.

• Pour toute fonction polynôme symétrique $f : \mathbf{K}^n \to \mathbf{K}$, il existe une unique fonction polynôme g telle que $f = g(\sigma_1, \cdots, \sigma_n)$.

Exercice 4 : Soient $\theta \in \mathbf{R}$ et $n \in \mathbf{N}^*$. Calculer $\prod_{k=0}^{n-1} \sin\left(\theta + \frac{k\pi}{n}\right)$.

Exercice 5 : Résoudre dans **C** le système $x^2 + y^2 + z^2 = 0$, $x^4 + y^4 + z^4 = 0$, $x^5 + y^5 + z^5 = 0$.

3. Théorème fondamental de l'algèbre

• Théorème de D'Alembert-Gauss : **C** est algébriquement clos.

Ce théorème signifie que tout polynôme non constant de **C**[X] admet au moins une racine, ou de façon équivalente que tout polynôme de **C**[X] est scindé.

• Les polynômes irréductibles de **C**[X] sont les polynômes du premier degré. Ceux de **R**[X] sont les polynômes du premier degré et les polynômes du second degré sans racine réelle.

Exercice 6 : Décomposer $X^{10} + X^5 + 1$ en éléments irréductibles sur **C** et sur **R**.

4. Techniques de recherche des racines

Outre la recherche des racines multiples et l'exploitation des relations entre coefficients et racines, on peut s'appuyer sur les méthodes suivantes :

• Racines rationnelles d'un polynôme à coefficients rationnels.

• Polynômes du troisième degré (méthode de Cardan) et du quatrième degré (méthode de Ferrari).

• Equations réciproques.

• Après séparation des racines (**K** = **R**), calcul approché par dichotomie ou par la méthode de Newton.

Exercice 7 : Equation $x^5 - 1 = 0$. Lignes trigonométriques de $\frac{2\pi}{5}$. Construction du pentagone régulier.

Exercice 8 : Résoudre dans **C** l'équation $x^4 + \frac{7}{3}x^2 + 30x - \frac{100}{3} = 0$ (chercher une racine rationnelle puis utiliser les formules de Cardan).

Exercice 9 : Résoudre dans **C** l'équation $4x^4 - 85x^3 + 357x^2 - 340x + 64 = 0$ (se ramener à une équation réciproque).

5. Problèmes d'élimination

Dans cette partie, on suppose que **K** = **C** et on se donne deux polynômes P et Q, de degrés respectifs m et n.

• P et Q ont une racine commune ssi $\deg(P \wedge Q) \geq 1$ ssi la famille $(P, XP, \ldots, X^{n-1}P, Q, XQ, \ldots, X^{m-1}Q)$ est liée.

• On appelle résultant (ou déterminant de Sylvester) de P et Q, et on note R(P, Q), le déterminant de la famille précédente dans la base $(1, X, \ldots, X^{m+n-1})$ de $\mathbf{C}_{m+n-1}[X]$.

• P a une racine multiple ssi P et P' ont une racine commune. Le résultant de P et de P' s'appelle discriminant de P et se note $\Delta(P)$.

Exercice 10 : Eliminer x entre $x^3 - \lambda x^2 - q = 0$ et $x^3 - \lambda x - 3 = 0$.

Bibliographie

RAMIS, DESCHAMPS et ODOUX, *Cours de mathématiques spéciales, tome 1 : algèbre*, Masson
ARNAUDIÈS et FRAYSSE, *Cours de mathématiques, tome 1 : algèbre*, Dunod

SIMILITUDES PLANES
DIRECTES ET INDIRECTES : FORMES RÉDUITES

Remarques générales

• Ne pas se contenter du programme de Terminale, même augmenté des similitudes indirectes. Des exposés complets se trouvent dans FRENKEL, TISSERON et surtout dans BERGER.

• On suppose naturellement connue la description des isométries planes.

Plan

E est un plan affine euclidien.

1. Notion de similitude et propriétés générales

a) Définition et premières caractérisations

• Une application f non constante de E dans E est appelée similitude si elle conserve les rapports de distances, c'est-à-dire si $\frac{f(A)f(B)}{f(C)f(D)} = \frac{AB}{CD}$ chaque fois que les dénominateurs ne s'annulent pas.

• Pour qu'une application f de E dans E soit une similitude, il faut et il suffit qu'il existe un réel $k > 0$ tel que, pour tous points M et N, $f(M)f(N) = k\,MN$. k est appelé rapport de similitude.

• Pour qu'une application f de E dans E soit une similitude de rapport k, il faut et il suffit qu'elle soit le produit d'une homothétie de rapport k et d'une isométrie.

b) Conséquences

• L'ensemble des similitudes, noté Sim(E), est un sous-groupe du groupe affine qui contient le groupe des isométries et le groupe des homothéties-translations. Les similitudes de déterminant positif sont dites directes, leur ensemble, noté $Sim^+(E)$, est un sous-groupe de Sim(E). Les similitudes de déterminant négatif sont dites indirectes.

• Les similitudes transforment les droites en droites, les cercles en cercles, conservent les rapports de mesures algébriques, les rapports de distances, les barycentres, les angles non orientés, l'orthogonalité, le contact. Les similitudes directes conservent les angles orientés, les similitudes indirectes les changent en leurs opposés.

2. Description des similitudes planes

a) Formes réduites

Théorème : Une similitude de rapport différent de 1 admet un unique point fixe O et elle est de façon unique produit d'une homothétie de centre O et de rapport positif et d'une isométrie admettant O pour point fixe. De plus, cette décomposition est commutative.

Première preuve (topologique) : appliquer le théorème du point fixe à f si $k < 1$, à f^{-1} si $k > 1$.

Deuxième preuve (algébrique) : utiliser le fait que, 1 n'étant pas valeur propre de $\vec{f}$, $Id - \vec{f}$ est injective donc bijective puisqu'on est en dimension finie.

Conséquences :
Une similitude de rapport 1 est une isométrie et sa forme réduite est supposée connue. Soit donc f une similitude de rapport $k \neq 1$ et soit O son unique point fixe, appelé centre de similitude.
• Si f est directe, $f = h \circ r = r \circ h$, où h est l'homothétie de centre O et de rapport k et r une rotation de centre O. L'angle de r est appelé angle de similitude.
• Si f est indirecte, $f = h \circ s = s \circ h$, où h est l'homothétie de centre O et de rapport k et s une réflexion d'axe passant par O. L'axe de s est appelé axe de similitude.

b) Expression complexe

En fixant un repère orthonormé (et donc une orientation) de E, on identifie E à **C** et f à une application de **C** dans **C**.

Théorème : f est une similitude directe (resp. indirecte) ssi il existe des nombres complexes $a \neq 0$ et b tels que, pour tout nombre complexe z, $f(z) = az + b$ (resp. $a\bar{z} + b$).

3. <u>Caractérisations géométriques des similitudes</u>

Théorème : Soit f une bijection de E dans E. Les propriétés suivantes sont équivalentes :
(i) f est une similitude (ie conserve les rapports de distances)
(ii) f conserve les angles géométriques
(iii) f conserve l'orthogonalité
(iv) f transforme tout cercle en un cercle.

On prouve les implications (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (i). La dernière utilise le théorème fondamental de la géométrie affine, supposé connu (les transformations affines de E sont les bijections de E dans E qui conservent l'alignement).

4. <u>Compléments sous forme d'exercices</u>

a) Simple transitivité

• Soient quatre points A, B, A', B' avec $A \neq B$ et $A' \neq B'$. Montrer qu'il existe une unique similitude directe (resp. indirecte) f telle que f(A) = A' et f(B) = B'. Construire son centre (resp. son centre et son axe) lorsque ce n'est pas une isométrie.
• Soient A, B, A', B' quatre points distincts. Montrer que la similitude directe telle que $A \mapsto A'$ et $B \mapsto B'$ a même centre que la similitude directe telle que $A \mapsto B$ et $A' \mapsto B'$. En déduire que les cercles circonscrits aux quatre triangles d'un quadrilatère complet sont concourants.

b) Triangles semblables

Soient deux triangles ABC et A'B'C'. Montrer l'équivalence des propriétés suivantes (avec les notations usuelles) :

(i) Il existe une similitude f telle que f(A) = A', f(B) = B', f(C) = C'
(ii) $\hat{A} = \hat{A}'$, $\hat{B} = \hat{B}'$, $\hat{C} = \hat{C}'$
(iii) $\hat{A} = \hat{A}'$, $\frac{b'}{b} = \frac{c'}{c}$
(iv) $\frac{a'}{a} = \frac{b'}{b} = \frac{c'}{c}$.

c) Différentielle de l'inversion

Montrer que, en tout point, la différentielle d'une inversion est une similitude. En déduire qu'une inversion conserve les angles géométriques.

Bibliographie

TISSERON, *Géométries affine, projective et euclidienne*, Hermann
BERGER, *Géométrie tome 2*, CEDIC/Fernand Nathan
FRENKEL, *Géométrie pour l'élève-professeur*, Hermann
TAUVEL, *Mathématiques générales pour l'agrégation*, Masson
AVEZ, *La leçon de géométrie à l'oral de l'agrégation*, Masson

RÉSOLUTION D'UN SYSTÈME LINÉAIRE DE n ÉQUATIONS À p INCONNUES. MÉTHODES PRATIQUES DE RÉSOLUTION

Remarques générales

• Bien comprendre le titre : on attend une étude théorique puis *des* méthodes pratiques. Respecter les notations (*n* équations, *p* inconnues) même si le livre dont on s'inspire en emploie d'autres !

• Illustrer la théorie et les algorithmes par des exemples intéressants avec paramètres : "Les exercices de pure routine sont à proscrire (système de trois équations à trois inconnues, ...)" (rapport du jury 1989).

Plan

Introduction

K désigne **R** ou **C.** On suppose connue la théorie du rang. En particulier, le rang d'une matrice A est l'ordre maximum d'un mineur non nul, ou encore l'ordre d'un mineur non nul dont tous les bordants sont nuls.

1. Définitions et notations

• Un système linéaire de n équations à p inconnues x_1, ..., x_p dans K est un système de la forme $\boxed{\begin{cases} a_{11}x_1 + \cdots + a_{1p}x_p = b_1 \\ \vdots \\ a_{n1}x_1 + \cdots + a_{np}x_p = b_n \end{cases}}$, où $a_{ij} \in K$ et $b_i \in K$. On dit qu'il est compatible ssi il admet au moins une solution.

1ère interprétation : $\boxed{\sum_{j=1}^{p} x_j A_j = B}$, où $A_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix} \in K^n$ et $B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in K^n$.

2ème interprétation : $\boxed{AX = B}$, où $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \in K^p$ et $A = (A_1 \ \dots \ A_p) \in M_{n,p}(K)$.

• A est appelée matrice du système et s'identifie à l'application linéaire de K^p dans K^n ayant pour matrice A dans les bases canoniques. Son rang r est dit rang du système. A' = (A B) est appelée matrice élargie du système.

2. Résolution théorique

a) Premiers résultats

$\boxed{\text{Le système est compatible ssi A et A' ont même rang}}$ *(théorème de Kronecker-Capelli)*. Si le système est compatible, il admet au moins une solution X_0 et l'ensemble des solutions est alors $\boxed{X_0 + \text{Ker } A}$, sous-espace affine de K^p de dimension p - r.

b) Systèmes de Cramer

On dit que le système est un système de Cramer lorsque n = p = r. Un système de Cramer a une solution unique donnée par $\boxed{X = A^{-1}B}$ ou par $\boxed{\forall i \in \{1, \dots, n\} \quad x_i = \dfrac{\det(A_1, \dots, A_{i-1}, B, A_{i+1}, \dots, A_n)}{\det A}}$.

c) Cas général : théorème de Rouché-Fontené

Supposons le système compatible et soit P une sous-matrice carrée de A inversible et de rang r. Les équations correspondant aux lignes de P sont appelées équations principales ; les inconnues correspondant aux colonnes de P sont appelées inconnues principales.

Le système est équivalent au sous-système des équations principales et ce dernier est un système de Cramer par rapport aux inconnues principales.

3. Méthodes pratiques de résolution

a) Méthodes directes

Principe général : se ramener à un système triangulaire.

• Méthode de Gauss
Quitte à permuter les inconnues, on peut, au moyen d'opérations élémentaires sur les lignes du système AX = B, obtenir un système équivalent A'X = B', où A' est de la forme $\begin{pmatrix} 1 & * & \cdots & \cdots & \cdots & \cdots & * \\ 0 & 1 & * & & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & & \vdots \\ 0 & \cdots & 0 & 1 & * & \cdots & * \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \end{pmatrix}$.

Remarque 1 : Cette méthode permet de retrouver tous les résultats théoriques du paragraphe 2.
Remarque 2 : Il est préférable, afin de minimiser l'erreur de calcul, de choisir à chaque étape un pivot de module maximum (deux variantes : méthode du pivot partiel, méthode du pivot total).

• Méthode de Householder
Si $A \in GL_n(\mathbf{R})$, il existe P orthogonale et T triangulaire supérieure telles que A = PT. Le système AX = B est alors équivalent à $TX = {}^tPB$.

• Méthode de Choleski
Si A est réelle symétrique, définie positive, il existe S réelle triangulaire supérieure telle que $A = {}^tSS$. La résolution de AX = B se ramène à celle de deux systèmes triangulaires $^tSY = B$ et SX = Y.

Coût des méthodes directes : Pour A régulière d'ordre n, la méthode de Cramer nécessite environ $n^2.n!$ multiplications ; la méthode de Gauss $\frac{2n^3}{3}$ multiplications ; la méthode de Householder n^3 multiplications et 2n extractions de racines carrées ; la méthode de Choleski $\frac{n^3}{6}$ multiplications et n extractions de racines carrées.

b) Méthodes itératives

Principe général : On écrit A = M - N, avec M inversible et facile à inverser. Le système AX = B équivaut à $X = M^{-1}NX + M^{-1}B$. Si $\| M^{-1}N \| < 1$, le théorème du point fixe pour une application contractante dans un espace complet s'applique.

Une condition suffisante simple pour l'existence de telles matrices M et N est : $\boxed{\forall i \in \{1, \ldots, n\} \quad |a_{ii}| > \sum_{j \neq i} |a_{ij}|}$.

Principales méthodes itératives : méthode de Jacobi, méthode de Gauss-Seidel, méthode de relaxation.

Bibliographie

TAUVEL, *Mathématiques générales pour l'agrégation* , Masson
CABANE et LEBOEUF, *Matrices et réduction*, Ellipses
OVAERT et VERLEY, *Algèbre vol. 1*, CEDIC/Fernand Nathan
MONASSE, *Mathématique et informatique*, Vuibert

TRIGONALISATION DES ENDOMORPHISMES, SOUS-ESPACES CARACTÉRISTIQUES ; APPLICATIONS.

Remarques générales

Insister sur les applications. Prévoir des exemples intéressants : matrices réelles trigonalisables mais non diagonalisables ; matrices réelles non trigonalisables dans **R** et nécessitant un travail dans **C**.

Plan

Introduction

Soient **K** l'un des corps **R** ou **C**, E un **K**-espace vectoriel de dimension finie n et u un endomorphisme de E. On note χ_u le polynôme caractéristique de u et μ_u son polynôme minimal. On suppose connues les généralités concernant ces notions.

1. Endomorphismes trigonalisables

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

• Une matrice M de $M_n(\mathbf{K})$ s'identifie à l'endomorphisme u : $\mathbf{K}^n \to \mathbf{K}^n$, $X \mapsto MX$. On dit que M est trigonalisable si u est diagonalisable.

• Inversement, si $u \in L(E)$ a pour matrice M dans une base de E, u est trigonalisable ssi M est semblable à une matrice triangulaire supérieure, ssi M est trigonalisable.

• $\boxed{\text{u est trigonalisable ssi } \chi_u \text{ est scindé}}$. C'est toujours vrai lorsque K = C.

> *Exercice :* Soient u et v deux endomorphismes trigonalisables qui commutent. Montrer qu'on peut les trigonaliser dans la même base.

2. Sous-espaces caractéristiques, décomposition spectrale

Dans toute cette partie, on suppose que χ_u est scindé. On note $\chi_u = \prod_{i=1}^{k} (\lambda_i - X)^{m_i}$ et $\mu_u = \prod_{i=1}^{k} (X - \lambda_i)^{r_i}$, où les λ_i désignent les valeurs propres deux à deux distinctes de u.

a) Lemme des noyaux

Soient P_1, ..., P_k des polynômes de $\mathbf{K}[X]$ premiers entre eux deux à deux et $P = P_1P_2...P_k$. Alors $\boxed{\text{Ker } P(u) = \overset{k}{\underset{i=1}{\oplus}} \text{Ker } P_i(u)}$.

b) Sous-espaces caractéristiques

• $N(\lambda_i) = \text{Ker}(u - \lambda_i id)^{r_i}$ est appelé sous-espace caractéristique associé à la valeur propre λ_i.

• $\boxed{E = \overset{k}{\underset{i=1}{\oplus}} N(\lambda_i)}$, chaque $N(\lambda_i)$ est stable par u et $\boxed{\dim N(\lambda_i) = m_i}$. De plus, il existe une base de chaque $N(\lambda_i)$ telle que la matrice dans cette base de l'endomorphisme induit par u soit triangulaire supérieure. En définitive, il

existe une base de E dans laquelle la matrice de u est de la forme $\begin{pmatrix} T_1 & 0 & \cdots & 0 \\ 0 & T_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & T_k \end{pmatrix}$ avec $T_i = \begin{pmatrix} \lambda_i & * & \cdots & * \\ 0 & \lambda_i & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & \lambda_i \end{pmatrix}$.

c) Décomposition spectrale

u s'écrit de manière unique sous la forme u = d + n, avec d diagonalisable, n nilpotent et dn = nd.

Exercice : Soient $M \in GL_n(\mathbf{C})$ et $p \geq 2$. Montrer que si M est diagonalisable, alors toute matrice N telle que $N^p = M$ est encore diagonalisable.

2. Applications de la trigonalisation (à développer sur des exemples)

Dans les applications suivantes, on suppose que A = D + N, avec D diagonalisable et N nilpotente d'indice r.

a) Calcul des puissances et de l'exponentielle d'une matrice

$A^k = (D+N)^k = \sum_{i=0}^{r-1} C_k^i N^i D^{k-i}$ et $e^A = e^D e^N = e^D \sum_{i=1}^{r-1} \frac{N^i}{i!}$.

Si $D = P\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}P^{-1}$, alors $D^i = P\begin{pmatrix} \lambda_1^i & & 0 \\ & \ddots & \\ 0 & & \lambda_n^i \end{pmatrix}P^{-1}$ et $e^D = P\begin{pmatrix} e^{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & e^{\lambda_n} \end{pmatrix}P^{-1}$.

b) Etude de systèmes de suites à récurrence linéaire d'ordre 1 et de suites à récurrence linéaire d'ordre n

Si (U_p) est définie par U_0 et $U_{p+1} = AU_p$, alors $U_p = A^p U_0$.
Si (u_p) est définie par u_0, u_1, ..., u_{n-1} et $u_{p+n} = a_0u_p + a_1u_{p+1} + ... + a_{n-1}u_{p+n-1}$ on se ramène au cas précédent en posant $U_p = \begin{pmatrix} u_p \\ u_{p+1} \\ \vdots \\ u_{p+n-1} \end{pmatrix}$ et $A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ a_0 & a_1 & \cdots & \cdots & a_{n-1} \end{pmatrix}$.

c) Résolution de systèmes différentiels linéaires d'ordre 1 et d'équations différentielles linéaires d'ordre n

Le système différentiel X' = AX a pour solution générale $X = e^{tA}.C$, avec $C \in \mathbf{K}^n$.
L'équation différentielle $x^{(n)} = a_0x + a_1x' + \cdots + a_{n-1}x^{(n-1)}$ se ramène au cas précédent en posant $X = \begin{pmatrix} x, \\ x' \\ \vdots \\ x^{(n-1)} \end{pmatrix}$ et $A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ a_0 & a_1 & \cdots & \cdots & a_{n-1} \end{pmatrix}$.

Bibliographie

CABANE et LEBOEUF, *Algèbre linéaire II, Matrices et réduction*, Ellipses
RAMIS, DESCHAMPS et ODOUX, *Cours de mathématiques spéciales, tomes 1 et 2*, Masson
ARNAUDIÈS et FRAYSSE, *Cours de mathématiques, tome 1 : Algèbre*, Dunod