

118: Exemples d'utilisation de la notion de dimension en algèbre et géométrie

Pierre Lissy

March 3, 2010

E et F sont des espaces vectoriels sur un corps (commutatif) k , en général ils seront de dimension finie.

1 Techniques vectorielles en théorie des corps

1.1 Degré d'une extension de corps

Définition-proposition 1. Soit L une extension d'un corps K . Alors L est naturellement muni d'une structure de K – ev. On dit que cette extension est finie ssi la dimension de L est finie. Dimension de L sur K , noté $[L:K]$ est appelé degré de l'extension.

La première conséquence est la suivante.

Proposition 1. Soit k un corps fini. Il a un sous-corps premier $\mathbb{Z}/p\mathbb{Z}$. Alors nécessairement $|k| = p^n$.

Théorème 1 (base télescopique). $k \subset K \subset L$. Alors $[K:k][L:K] = [L:k]$, de plus il suffit de multiplier les bases.

1.2 Extension monogène

Définition 1. L'extension L est dit monogène ssi $L = K(\alpha)$. α est dit algébrique ssi le morphisme $T \mapsto P(\alpha)$ est non injectif, transcendant dans le cas contraire. Si il est algébrique, on appelle polynôme minimal μ_α le polynôme unitaire qui engendre l'idéal qu'est le noyau.

Théorème 2. On a les équivalences suivantes.

1. α algébrique
2. $K[\alpha] = K(\alpha)$
3. $\dim_K K[\alpha] < \infty$

Plus précisément dans ce cas, le polynôme P est irréductible sur $K[X]$ et la dimension de l'extension est exactement le degré du polynôme minimal.

Exemple 1. $\sqrt{2}$ est algébrique sur $\mathbb{Q}$, de polynôme minimal $X^2 - 2$. Donc l'extension $\mathbb{Q}[\sqrt{2}]$ est de dimension 2.

Exemple 2. [2]

1. Polynôme minimal de $\sqrt[3]{7} + \sqrt{2}$: $X^6 - 6X^4 - 14X^3 + 12X^2 - 84X + 41$
2. $i + j$: $X^4 + 2X^3 + 5X^2 + 4X + 1$
3. $j + \sqrt{3}$: $X^4 + 2X^3 - 3X^2 - 4X + 13$
4. $j\sqrt{2}$: $X^4 + 2X^2 + 4$

Théorème 3 (élément primitif). Soit K un corps de caractéristique nulle ou un corps fini. Toute extension finie est monogène.

1.3 Corps de rupture, de décomposition

Définition 2. Soit P un polynôme irréductible. Un corps de rupture est une extension L telle que $L = P(\alpha)$ avec $P(\alpha) = 0$ (P considéré dans $L[X]$)

Théorème 4. Il existe un corps de rupture, unique à isomorphisme de corps près. De plus, le degré de l'extension est égal au degré du polynôme minimal.

Définition 3. Corps de décomposition d'un polynôme: un corps contenant K tel que dans ce corps le polynôme est scindé, et minimum pour l'inclusion. Ce corps est une extension finie de degré inférieur à $n!$, n étant le degré du polynôme.

Théorème 5. Il existe un unique corps de déc à isom près.

On se réfère à [2]

Application 1. On a existence et unicité à isomorphisme près de l'existence du corps de cardinal $\mathbb{F}_q$. De plus, les techniques vectorielles nous donnent des infos supplémentaires:

1. Pour tout n il existe un polynôme irréductible sur $\mathbb{F}_p$. De plus, le corps de rupture de ce polynôme est $\mathbb{F}_{p^n}$
2. Tout corps de rupture sur un corps fini est en fait un corps de décomposition: si α est racine les autres racines sont les α^{p^i} .
3. Tout corps fini de cardinal p^n avec p premier est tel que ces sous-corps sont les $\mathbb{F}_{p^d}$ avec d divisant n . De même on trouverait les corps intermédiaires entre $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$.

1.4 Construction à la règle et au compas

Définition 4. Soit A un sous-ensemble du plan. On dit qu'un point M est constructible en un pas à partir de A ssi M est point d'intersection d'éléments du type suivant:

1. Droites affines passant par deux points de A .
2. Cercles centrés en un point de A et passant par un autre point de A .

Définition 5. . Un point est dit constructible ssi il existe une suite $A_1, \dots, A_n$ d'ensembles tels que

1. $A_0 = (0, 0), (1, 0)$
2. $M \in A_n$
3. $A_i = A_{i-1} \cup M_i$ où M_i est constructible en un pas à partir de A_{i-1} .

Un réel x est dit constructible ssi $(x, 0)$ l'est.

Théorème 6. Une condition nécessaire pour qu'un réel soit constructible est qu'il soit algébrique sur $\mathbb{Q}$ est que la dimension de l'extension soit une puissance de 2 (ie le degré du poly min est une puissance de 2)

Application 2. Impossibilité de la duplication du cube. Impossibilité de la trisection de l'angle. Impossibilité de la quadrature du cercle.

2 Utilisation en algèbre linéaire et bilinéaire

2.1 Raisonnements par récurrence en algèbre linéaire

La propriété essentielle est la suivante.

Théorème 7. Soit E un espace vectoriel de dimension finie. Soit F un sev de E . Alors F est encore de dimension finie. DE PLUS, si F est un sev strict la dimension est strictement plus petite.

Ce théorème permet de démontrer un certain nombre de propriétés en algèbre linéaire par réc sur la dimension de l'espace considéré.

Application 3. *Toute matrice sur un corps algébriquement clos est trigonalisable.*

Application 4. *Des endomorphismes trigonalisables qui commutent deux à deux sont co-trigonalisables. Idem diagonalisables.*

Application 5. *Un endomorphisme de trace nulle est tel qu'on peut trouver une base telle que la composante de $f(e_i)$ selon e_i soit nulle. Idem matrices*

Application 6. *[4] Par récurrence descendante sur la dimension, on a que deux sous-espaces de même dimension admettent un supplémentaire commun*

2.2 Raisonnements par récurrence en algèbre bilinéaire

On utilise le même théorème.

Application 7. *Il existe des BON dans un espace euclidien, hermitien, complétion d'une BON. Idem pour une forme quadratique, hermitienne. Existence de supplémentaires orthogonaux...*

Application 8. *Orthonormalisation de Schmidt*

Application 9. *Réduction des endomorphismes auto-adjoints, normaux.*

Application 10. *Une forme quadratique non dégénérée non définie réelle admet une base de vecteurs isotropes. Si B est une base et $\text{Tr}(M_B(\varphi)) = 0$ alors le cône isotrope contient une BON de vecteurs isotropes (fgn 3).*

Application 11. *Une forme quadratique est positive ssi on peut trouver des espaces vectoriels inclus les uns dans les autres de dimension $1, 2, \dots, n$ tels que le discriminant dans une base de la forme quadratique restreinte à chacun de ses sous-espaces soit positif.*

2.3 Classifications de classes de congruence, de classes d'équivalence

La notion de rang (et donc de dimension) permet de déterminer certaines orbites pour des actions de groupe (on utilise bien la notion pour un truc qui a rien à voir...)

Définition 6. *Deux matrices de $M_{n,m}(\mathbb{R})$ notée A et B sont équivalentes ssi il existe une matrice $P \in GL_n(K)$ et $Q \in GL_m(K)$ telles que $B = PAQ$. Deux endomorphismes $f \in L(E, F)$ et $g \in L(E, F)$ sont équivalents ssi il existe $u \in GL(E)$ et $v \in GL(F)$ tels que $f = vgu$. C'est équivalent de dire qu'on peut trouver deux couples de bases différentes (B_1, B_2) et (B'_1, B'_2) tels que $M_{B_1, B'_1}(f) = M_{B_2, B'_2}(g)$.*

Théorème 8. *Les matrices équivalentes sont celles de même rang. Les endomorphismes équivalents sont ceux de même rang.*

Définition 7. *Deux matrices A et B sont congruentes ssi il existe $P \in GL_n(\mathbb{R})$ tel que $A = {}^t PAP$. Deux formes quadratiques sont équivalentes ssi elles diffèrent d'un isomorphisme: $q' = q\alpha$. Deux formes quadratiques sont équivalentes ssi on peut trouver deux bases B et B' telles que $M_B(q) = M_{B'}(q)$.*

Rappel : signature d'une forme quadratique réelle: on peut le voir comme $(\dim F^+, \dim F^-)$ où F^+ et F^- sont orthogonaux positif négatif maximums.

Théorème 9. *Deux matrices complexes sont congrues ssi elles ont même rang. Deux formes quadratiques complexes sont équivalentes ssi elles ont même rang. Deux matrices réelles sont congrues ssi elles ont même signature. Deux formes quadratiques réelles sont équivalentes ssi elles ont même signature.*

3 Utilisation en géométrie affine

3.1 Equations d'un sous-espace vectoriel ou affine

Théorème 10. Soit p formes linéaires de E^* notées f_i . Alors $\dim \bigcap_{Ker(f_i)} = n - \text{rg}((f_i))$. Inversement, si F est un sev de E de dimension r alors il existe $n - r$ formes linéaires indépendantes (f_i) telles que $\bigcap_{Ker(f_i)} = F$.

Remarque 1. Ce théorème dit que si l'on se donne un sev de dimension r , alors ce sev peut être représenté comme la solution à $n-r$ équations linéaires indépendantes. C'est juste la traduction en terme d'équations d'autres résultats déjà vus.

Théorème 11. Soit F un sous-espace affine de dimension r , et soit x_0 un point de F , alors il existe $n - r$ formes linéaires indépendantes (f_i) telles que $\bigcap Ker(f_i) + x_0 = F$.

Application 12. Soit un espace vectoriel affine représenté par trois équations de la forme $\varphi_1(x) = b_1, \varphi_2(x) = b_2, \varphi_3(x) = b_3$. Alors

1. Soit les trois formes linéaires sont indépendantes et alors les 3 plans s'intersectent en un unique point, (ie la matrice des φ_i est inversible), que l'on peut facilement trouver en inversant une matrice.
2. Soit les trois formes linéaires sont linéairement dépendantes et leur rang est 2, par exemple $\varphi_3 = \lambda\varphi_1 + \mu\varphi_2$. Alors si $b_3 \neq \lambda b_1 + \mu b_2$ on a pas de solutions, sinon une droite solution.
3. Soit les trois formes linéaires sont linéairement dépendantes et le rang est 1, dans ce cas on a un hyperplan ou pas de solutions.

3.2

[5]

3.3

4 Utilisation en géométrie différentielle

4.1 sous-variétés

Définition 8. Soient V un sous-ensemble de $\mathbb{R}^n$, $a \in V$. et d un entier naturel. On dit que V est lisse en a , de dimension d , s'il existe un difféomorphisme F de classe C^1 d'un voisinage ouvert U de a dans $\mathbb{R}^n$, qui transforme V en un sous-espace vectoriel de dimension d , ie. $F(U \cap V) = V' \cap F(U)$ avec $V' = \mathbb{R}^d \times \{0\} \subset \mathbb{R}^n$. On dit que V est une sous-variété de dimension d de $\mathbb{R}^n$ si V est lisse de dimension d en chacun de ses points.

Remarque 2. On pourrait étendre aux sous-variétés de classe C^k de classe C^∞ .

Exemple 3. Le cône du second degré privé de 0 est une sous-variété de $\mathbb{R}^2$ de dimension 1.

Théorème 12. Soient U un ouvert de $\mathbb{R}^n$ et $f_1, \dots, f_p$ de U dans $\mathbb{R}$ des fonctions de classe C^1 . Soit V l'ensemble des points x tels que $x \in U$ et $f_1(x_1, \dots, x_n) = 0, \dots, f_p(x_1, \dots, x_n) = 0$. On suppose les différentielles indépendantes. Alors V est une sous-variété de dimension $n-p$ de $\mathbb{R}^n$.

Des exemples de non variété (pas lisse en 0)

Exemple 4. 1. $x^2 - y^2 = 0$

2. $x^3 + y^3 - 3xy = 0$

4.2 Théorème fondamental

Théorème 13. 1. V lisse en a , de dimension d

2. Pour tout a , il existe un voisinage de a et une submersion g à valeurs dans $\mathbb{R}^{n-p}$ telle que $U \cap M = g^{-1}(0)$;
3. Pour tout a , il existe un ouvert contenant A et autre ouvert de $\mathbb{R}^p$ contenant $(a_1, \dots, a_p)$ et une app C^∞ telle qu'après permutation des coordonnées $U \cap M$ soit le graphe.

Exemple 5. [3] L'ensemble des matrices de rang p est une sous-variété de $\mathbb{M}_n(\mathbb{R})$ de dimension $p(2n - p)$.

Théorème 14. Si V est lisse en a , de dimension d , ses vecteurs tangents en a forment un sous-espace vectoriel de dimension d , appelé espace vectoriel tangent en a à V . L'espace affine est le même mais passant par a .

Théorème 15. Dans une sous-variété définie implicitement, l'espace vectoriel tangent est défini par les équations $\sum \partial_j f_i(a) v_j = 0$ pour tout i entre 1 et p .

4.3 Les groupes classiques de l'algèbre linéaire

Théorème 16. [3]

1. $SL_n(\mathbb{R})$: espace tangent en Id est les matrices de traces nulles, variété de dimension $n^2 - 1$
2. $SL_n(\mathbb{C})$: espace tangent en Id est les matrices de traces nulles, variété de dimension $2(n^2 - 1)$
3. $O_n, SO_n(\mathbb{R})$: espace tangent en Id est les matrices telles que ${}^t M = -M$, variété de dimension $n(n - 1)/2$
4. $U_n(\mathbb{C})$: espace tangent en Id est les matrices telles que ${}^t \bar{M} = -M$, variété de dimension n^2

References

- [1] Perrin
- [2] Ortisz
- [3] Mneimé Testard
- [4] Gourdon
- [5] Lelong ferrand arnaudiès algèbre