Trace, formes quadratiques et extensions de corps

Yves Coudene 16/10/03

Ce document porte sur les notions de dimension d'espace vectoriel, extensions de corps, trace de matrices, polynôme minimal et caractéristique, théorème de Cayley-Hamilton, formes quadratiques, nombres irrationnels, déterminant de Vandermonde, déterminant de Gram.

On passe un certain temps en premier cycle à démontrer que tout espace vectoriel de dimension finie admet une base ; de même, on démontre que toute forme quadratique admet une base orthogonale. Cependant, à ce niveau du cours, tous les espaces vectoriels de dimension finie considérés arrivent avec une base naturelle, et toutes les formes quadratiques utilisées sont données dans une base orthogonale.

Au niveau du programme de l'agrégation, il existe essentiellement deux exemples d'espaces vectoriels de dimension finie pour lesquels il n'y a pas de base donnée à priori :
– Le premier est formé par les solutions d'une équation différentielle sur un intervalle borné. Sous des hypothèses ad hoc, le théorème de Cauchy-Lipschitz affirme que l'espace vectoriel des solutions est de dimension finie, mais il peut être difficile d'exhiber une base explicite de solutions. Cet espace vectoriel est muni d'une forme quadratique naturelle, $(f,g) \to \int fg$, qui ne fait référence à aucune base particulière.
– Le second exemple est de nature algébrique : considérons un corps L engendré par un nombre fini de nombres algébriques sur $\mathbf{Q}$. Ce corps est un espace vectoriel de dimension finie sur $\mathbf{Q}$. Les nombres algébriques qui ont permis de le définir ne forment pas une base de L en général. Il existe une forme quadratique naturelle sur L, qui est donnée par la trace : $(x,y) \to Trace_{L/\mathbf{Q}}(xy)$.

Dans ces deux exemples, il peut même être difficile de déterminer la dimension de l'espace vectoriel considéré. On va voir comment l'existence d'une forme quadratique peut aider à résoudre ce problème.

Définitions

Dans la suite, on s'intéresse au second exemple. Soit donc K un corps de carctéristique différente de 2, L une extension de dimension finie de K. Notons n la dimension de L en tant que K-espace vectoriel. Dans la suite, il peut être utile de faire intervenir une extension algébriquement close de K contenant L ; elle sera abusivement notée $\bar{K}$. On peut se restreindre à $K = \mathbf{Q}$ et $\bar{K} = \mathbf{C}$ si on veut.

Pour tout élément $y \in L$, on considère l'application K-linéaire donnée par :

$$\begin{array}{rccc} A_y : & L & \to & L \\ & x & \to & xy \end{array}$$

La *trace* de cette application linéaire est un élément de K qui est noté $tr_{L/K}(y)$, ou encore s'il n'y a pas d'ambiguité sur les corps considérés, $tr(y)$. On vérifie immédiatement que l'application $(x, y) \to tr(xy)$ est une application K-bilinéaire symétrique définie sur L.
Remarquons que si l'on se donne une base de L sur K, l'application qui associe à y la matrice de A_y dans cette base, réalise un plongement de L dans l'algèbre $M_n(K)$. Bien sûr, ce plongement n'est pas surjectif.

Voici une propriété des applications de la forme A_y, qui ne sont pas vraies pour toutes les applications K-linéaires :

Lemme : Le polynôme minimal P_m de A_y est irréductible. Le polynôme caractéristique P_c de A_y est égal à une puissance de son polynôme minimal.

Preuve :
Commençons par montrer que le polynôme minimal de A_y est irréductible sur K. Pour cela, rappelons que le polynôme minimal de y est le plus petit polynôme non nul P de $K[X]$ (au sens de la division) qui vérifie $P(y) = 0$. Ce polynôme est irréductible : s'il était le produit de deux polynômes non constants de $K[X]$, y serait racine d'un de ces deux polynômes, et donc P ne serait pas minimal. Maintenant le polynôme minimal de A_y est égal au polynôme minimal de y en vertu des deux relations : $P(A_y) = A_{P(y)}$ et $P(y) = P(A_y)1$.
L'anneau $K[X]$ étant factoriel, on peut décomposer P_c sous la forme d'un produit $P_c = (P_m)^l H$, avec l un entier et H un polynôme premier à P_m. Remarquons que H n'a pas de racines en commun avec P_m ; cela découle, par exemple, du théorème de Bezout. Si H est non constant, P_c aurait une racine dans $\bar{K}$ qui ne serait pas racine de P_m. C'est absurde car les racines de P_c sont les valeurs propres de A_y (dans $\bar{K}$) et ces valeurs propres sont toutes racines du polynôme minimal P_m.

Voici une conséquence de ce lemme : si $y \neq 0$, A_y ne peut pas être nilpotente. En effet, s'il existe un entier k tel que $(A_y)^k = 0$, le polynôme minimal de A_y divise X^k ; comme il est irréductible, il est égal à X, donc $A_y = 0$.
Autre conséquence : si la caractéristique de K est nulle, A_y est diagonalisable sur $\bar{K}$. De fait, en caractéristique 0 (plus généralement si le corps est parfait), les polynômes irréductibles ont leurs racines simples. Une matrice dont le polynôme minimal a ses racines simples est diagonalisable (sur $\bar{K}$).

Indépendance et trace

Voici comment utiliser la trace dans des questions d'indépendance linéaire.

Théorème :
On se donne $p_1, p_2, ...p_k$ des nombres premiers distincts. Alors les nombres réels $\sqrt{p_1}, \sqrt{p_2}, ...\sqrt{p_k}$ sont linéairement indépendants sur $\mathbf{Q}$.

Preuve :
Rappelons que si q est une forme bilinéaire symétrique définie sur un espace vectoriel L, et si $v_1, v_2, ..v_k$ sont des vecteurs de L, alors la famille des v_i est libre si le déterminant de la matrice de terme général $q(v_i, v_j)$ est non nul (une combinaison linéaire entre les v_i donne tout de suite une combinaison linéaire sur les colonnes de cette matrice). Un tel déterminant est appelé déterminant de Gram.

Ici, on considère comme $\mathbf{Q}$-espace vectoriel le corps engendré par les $\sqrt{p_i}$, et comme forme quadratique $(x, y) \to Tr_{L/\mathbf{Q}}(xy)$. Il faut donc calculer les traces $tr_{L/\mathbf{Q}}(\sqrt{p_i p_j})$.
– Si $i = j$, on a $tr(p_i) = p_i tr(1) = np_i$, où n est la dimension de L sur $\mathbf{Q}$.
– Si $i \neq j$, on remarque que le polynôme minimal de $\sqrt{p_i p_j}$ est égal à $X^2 - p_i p_j$. Son polynôme caractéristique est donc égal à $(X^2 - p_i p_j)^l$, pour un certain entier $l \in \mathbf{N}$. La trace de $\sqrt{p_i p_j}$ est égale au coefficient de X^{2l-1} dans ce polynôme, elle est donc nulle.

Par conséquent, la matrice de terme général $tr_{L/\mathbf{Q}}(\sqrt{p_i p_j})$ est diagonale, et ses termes diagonaux sont des entiers non nuls ; son déterminant est donc non nul. Les $\sqrt{p_1}, \sqrt{p_2}, ...\sqrt{p_k}$ sont linéairement indépendants sur $\mathbf{Q}$.

On peut calculer la dimension de $\mathbf{Q}[\sqrt{p_1}, ...\sqrt{p_k}]$; pour cela, on considère la famille des $\sqrt{\prod_{i\in I} p_i}$ où I est une partie quelconque de l'ensemble $\{1...k\}$. (on pose $\prod_{i\in I} p_i = 1$ si I est vide). Cette famille possède 2^k éléments ; l'espace vectoriel qu'elle engendre coincide avec $\mathbf{Q}[\sqrt{p_1}, ...\sqrt{p_k}]$. Il suffit de vérifier que c'est une famille libre, ce qui se fait comme plus haut, en considérant les traces. La dimension recherchée est donc égale à 2^k.

Non-dégénerescence de la trace

Suffit-il de calculer le déterminant de la matrice de terme général $tr(x_i x_j)$ pour savoir si la famille $\{x_1, ...x_k\}$ est libre ? Par exemple, si K est un sous-corps de $\mathbf{C}$, et si la forme quadratique associée à q est définie positive, La réponse est oui. Ceci provient du fait que la restriction d'une forme quadratique définie positive à un sous-espace vectoriel est encore définie positive.

Si la forme quadratique n'est pas positive, ce n'est plus forcément vrai. Dès l'instant où la forme admet un vecteur isotrope ($q(x, x) = 0$), on obtient un contre-exemple en considérant la famille libre composée de l'unique élément x, pour laquelle on a $det(q(x, x)) = 0$. Cependant, si la forme quadratique est non-dégénerée, on a tout de même le résultat suivant :

Pour toute base $\{x_1, ...x_n\}$, le déterminant $det(q(x_i, x_j))$ est non nul.

Ce résultat n'est pas difficile ; cf par exemple Ramis-Deschamps Tome 2 1.1.2 prop 2 cor I. Cette référence comporte d'autres informations sur les déterminants de la forme $det(q(x_i, x_j))$, appelés déterminants de Gram. Au final, on obtient le critère suivant :

soit q une forme bilinéaire symétrique non-dégénérée ; pour qu'une famille génératrice $\{x_1...x_n\}$ *soit une base, il faut et il suffit que* $det(q(x_i, x_j))$ *soit non nul.*

Dans le cas d'extensions de corps, il est facile de trouver des familles génératrices, si bien que la méthode présentée plus haut permet effectivement de determiner la dimension de l'extension, si la trace est non dégénérée :

Théorème : soit K un corps de caractéristique 0, et L une extension finie de K. Alors $(x, y) \to tr_{L/K}(xy)$ est une forme bilinéaire symétrique non dégénérée.

Première preuve :
Soit $y \in L$; on veut montrer que si pour tout $x \in L$, $tr(xy) = 0$, alors $y = 0$. En prenant $x = y^{p-1}$, $\forall p \geq 1$, on obtient $tr(A_y^p) = 0$, $\forall p \geq 1$.
Soient λ_i les valeurs propres de A_y dans $\bar{K}$, et n_i leurs multiplicités. On a : $tr(A_y^p) = 0 = \sum n_i \lambda_i^p$. Par conséquent, pour tout polynôme $P \in \bar{K}[X]$, on a :

$$\sum n_i P(\lambda_i) = nP(0)$$

En prenant $P(X) = \prod(X - \lambda_i)$, où le produit a lieu sur les valeurs propres de A_y non nulles, on obtient que le produit des valeurs propres non nulles est nul, une absurdité (on vient d'utiliser $n \neq 0$, ce qui est vrai car la caractéristique est nulle). Toutes les valeurs propres de A_y sont donc nulles, ce qui montre que le polynôme caractéristique de A_y est égal à X^n. On a donc $A_y^n = 0$ (par le théorème de Cayley-Hamilton), $y^n = A_y^n 1 = 0$, ce qui implique $y = 0$.

Remarque : en caractéristique 0, les polynômes symétriques élémentaires peuvent s'exprimer en fonction des sommes de puissances des racines ; il s'agit juste d'inverser les formules de Newton.

Seconde preuve :
sous la seule hypothèse de séparabilité, en utilisant le théorème de l'élément primitif : L'extension L est de la forme $L \simeq K[\theta]$, pour un certain $\theta \in L$.
Le polynôme minimal de A_θ est égal au polynôme minimal P_m de θ ; il est donc irréductible, et ses racines sont simples (dans $\bar{K}$; c'est la séparabilité). Il est de degré n, en vertu de l'isomorphisme $K[\theta] \simeq K[X]/P_m$. Comme il divise le polynôme caractéristique de A_θ, il est en fait égal à ce polynôme. On conclut que le polynôme caractéristique de A_θ a ses racines simples. Par conséquent les valeurs propres λ_i de A_θ sont de multiplicité 1.
Comme $1, \theta, \theta^2, ..., \theta^{n-1}$ forme une base de $K[\theta]$ sur K , il suffit de montrer que la

matrice $\Big(tr(\theta^i\theta^j)\Big)_{\substack{0\leq i\leq n-1\\0\leq j\leq n-1}}$ est non dégénérée, c'est-à -dire que son déterminant est non nul.

$$det\Big((tr(A_\theta^{i+j})\Big) = det\Big(\sum \lambda_k^{i+j}\Big) = det\Big(\sum \lambda_k^i\lambda_k^j\Big) = det({}^tBB) = det(B)^2$$

où $B = (\lambda_i^j)_{\substack{0\leq i\leq n-1\\0\leq j\leq n-1}}$.
Le déterminant de B est un déterminant de Vandermonde, qui peut être calculé explicitement : $detB = \prod_{i<j}(\lambda_i - \lambda_j) \neq 0$. Ceci termine la preuve.

Voici enfin un exemple d'extension pour laquelle la trace n'est pas définie positive : soit α une racine dans $\mathbf{C}$ de l'équation X^4+1 ($\alpha = e^{i\pi/4}$ par exemple) ; l'extension $\mathbf{Q}[\alpha]$ est de degré 4 sur $\mathbf{Q}$. Le polynôme minimal de α^2 est égal à X^2+1 , son polynôme caractéristique est donc égal à $(X^2+1)^2$. Par conséquent, la trace $tr_{\mathbf{Q}[\alpha]/\mathbf{Q}}(\alpha^2)$ est nulle. Le nombre α est un vecteur isotrope de la trace dans l'extension $\mathbf{Q}[\alpha]$.

Toutes ces considérations sont classiques en théorie de Galois. Voici deux références pour en savoir plus : Ian Stewart, *Galois Theory* et *Algebraic Theory of Numbers*.

Le document *"comptage de racines et signature de formes quadratiques"* , par Michel Coste, disponible sur le site, étudie plus en détail le rang de la forme quadratique associée à la trace, lorsque l'extension n'est pas séparable.