Étendre le corps

Daniel Ferrand
Juillet 2007

Non, non, il s'agit seulement de Mathématiques !

Précisement, étant données une extension de corps $K \to L$ et une matrice $A \in \mathbf{M}_{pq}(K)$, vue comme une application K-linéaire

$$A : K^q \longrightarrow K^p,$$

le problème est de déterminer les propriétés de l'application A qui sont transmises à l'application L-linéaire associée à la même matrice

$$A : L^q \longrightarrow L^p,$$

et, inversement, les propriétés de cette dernière qui s'imposent à l'application K-linéaire initiale. Ces questions sont familières pour l'extension $\mathbf{R} \subset \mathbf{C}$, mais un agrégatif peut aussi les rencontrer pour une extension finie de corps ($K \to K[X]/(P)$, avec P irréductible), ou pour une extension de corps finis, mais aussi pour l'extension transcendante $K \to K(X)$.

Comme le produit tensoriel (qui donne lieu à *l'extension du corps de base* $V \mapsto L \otimes_K V$) n'est plus au programme, nous ne parlerons pas d'applications linéaires de façon intrinsèque, mais uniquement par le biais de matrices, car pour ces dernières l'extension du corps de base est simplement l'inclusion d'anneaux évidente : $\mathbf{M}_{pq}(K) \subset \mathbf{M}_{pq}(L)$.

Il faut souligner que les *données* sont relatives au corps de base K, et que les énoncés comparent des *propriétés* sur K et sur L. On ne dira rien du « problème de descente » des applications, qui cherche des conditions sur une matrice à coefficients dans L, pour que ses coefficients soient, en fait, dans le sous-corps K. Pour l'extension $\mathbf{R} \subset \mathbf{C}$, la réponse est l'invariance par conjugaison. Une réponse dans le cas général obligerait à sortir du programme.

1.- Énoncés

Pour simplifier les énoncés on notera A_K la première application (celle qui est K-linéaire), et A_L la seconde.

On va montrer les équivalences suivantes :

1.1) A_K est injective $\iff$ A_L est injective.

1.1') A_K est surjective $\iff$ A_L est surjective.

Plus généralement, soit $B \in \mathbf{M}_{pr}(K)$ une autre matrice ; alors

1.2) Il existe une matrice $X \in \mathbf{M}_{rq}(K)$ telle que $A_K X = B_K$ si et seulement si il existe une matrice $Y \in \mathbf{M}_{rq}(L)$ telle que $A_L Y = B_L$.

1.3) $\operatorname{rang}(A_K) = \operatorname{rang}(A_L)$.

Les énoncés suivants portent sur les matrices carrées ; on suppose donc que $p = q$, et que A représente un endomorphisme de K^p ; on identifie aussi l'anneau des polynômes $K[X]$ à un sous-anneau de $L[X]$.

1.4) $\det(A_K) = \det(A_L)$; plus généralement, $\text{Pol.car}(A_K, X) = \text{Pol.car}(A_L, X)$.

1.5) $\text{Pol.min}(A_K, X) = \text{Pol.min}(A_L, X)$

Les équivalences précédentes découlent de raisonnements d'algèbre linéaire très élémentaires ; les suivantes sont plus profondes.

1.6) L'espace K^p est cyclique pour A_K si et seulement si L^p est cyclique pour A_L.

1.7) Considérons une seconde matrice de même format $A' \in \mathbf{M}_p(K)$. Alors A_K et A'_K sont semblables (i.e sont conjuguées par un élément de $\mathbf{GL}_p(K)$) si et seulement si A_L et A'_L sont semblables.

2.- Injectivité

Lemme 2.1 *Considérons une matrice $A \in \mathbf{M}_{pq}(K)$.*
i) A est injective si et seulement si il existe une matrice $B \in \mathbf{M}_{qp}(K)$ telle que

$$BA = I_q$$

ii) A est surjective si et seulement si il existe une matrice $C \in \mathbf{M}_{qp}(K)$ telle que

$$AC = I_p$$

iii) A est injective si et seulement si sa transposée ${}^tA$ est surjective.

La relation $BA = I_q$ implique visiblement que l'application K-linéaire $A : K^q \longrightarrow K^p$ est injective. Réciproquement, si A est injective, cette application établit un isomorphisme entre K^q et $\text{Im}(A)$, et le choix d'un supplémentaire V de $\text{Im}(A)$ dans K^p, permet de construire l'application

$$B : K^p = \text{Im}(A) \oplus V \longrightarrow K^q,$$

qui est l'inverse de A sur $\text{Im}(A)$, et est nulle sur V ; on a bien $BA = I_q$.

De même, si $AC = I_p$ alors A est surjective, et si, réciproquement, l'application A est surjective, on peut choisir p éléments dans K^q dont les images par A forment la base canonique de K^p ; d'où une application $C : K^p \longrightarrow K^q$ telle que $AC = I_p$.

La propriété *iii)* découle des deux premières et du fait que la transposition renverse l'ordre des facteurs d'un produit.

2.2. L'implication : A_L injective $\Rightarrow$ A_K injective.

Elle se voit sur le diagramme commutatif

$$\begin{array}{ccc} K^q & \xrightarrow{A_K} & K^p \\ \downarrow & & \downarrow \\ L^q & \xrightarrow[A_L]{} & L^p \end{array}$$

dont les flèches verticales sont les injections canoniques.

2.3. L'implication : A_K injective $\Rightarrow$ A_L injective.

La démonstration repose sur l'égalité de 2.1.*i)* : si A_K est injective, il existe B telle que $B_K A_K = I$; ce produit de matrices donne aussi $B_L A_L = I$, donc A_L est injective.

2.4. **Attention !** Il est en général faux que q vecteurs de L^p, qui sont linéairement indépendants sur K, le soient aussi sur L ; par exemple, $\{1, i\} \subset \mathbf{C}$ est une partie qui est libre sur $\mathbf{R}$ et pas sur $\mathbf{C}$. Dans le langage qui précède, cela signifie qu'une application K-linéaire injective $K^q \to L^p$ (celle associée aux q vecteurs K-libres), ne se factorise en général pas en

$$\begin{array}{ccc} K^q & \longrightarrow & K^p \\ & \searrow & \downarrow \text{can.} \\ & & L^p \end{array}$$

où la flèche verticale désigne l'inclusion canonique.

3. Surjectivité

Pour démontrer l'équivalence (1.1'), on peut se ramener par transposition à l'énoncé analogue sur l'injectivité, en utilisant la partie *iii)* du lemme.

Mais on peut aussi utiliser une rétraction K-linéaire de $K \to L$: plus précisement, choisissons un sous-K-espace V supplémentaire de K dans L, de sorte que l'on a une décomposition $L = K \oplus V$; on définit alors une application K-linéaire

$$t : L \longrightarrow K$$

en posant $t(x) = x$ si $x \in K$, et, par exemple, $t(x) = 0$ si $x \in V$; bien entendu, cette application ne respecte pas les produits. On prolonge t en une application K-linéaire $\mathbf{M}_{rq}(L) \to \mathbf{M}_{rq}(K)$. Pour l'extension $\mathbf{R} \subset \mathbf{C}$, on peut prendre pour t la partie réelle.

Démontrons alors (1.2) (ce qui entraînera (1.1') qui en est un cas particulier) ; l'implication directe $\Rightarrow$ est évidente ; supposons, inversement, qu'il existe une matrice $Y \in \mathbf{M}_{rq}(L)$ telle que $A_L Y = B_L$. Cette égalité se déploie en pr égalités de la forme

$$a_{i1}y_{1j} + a_{i2}y_{2j} + \cdots + a_{iq}y_{qj} = b_{ij}.$$

Les y_{kj} sont dans L ; en prenant l'image par l'application K-linéaire t (qui est l'identité sur K), on trouve

$$a_{i1}t(y_{1j}) + a_{i2}t(y_{2j}) + \cdots + a_{iq}t(y_{qj}) = b_{ij}.$$

Cela s'écrit aussi $A_K t(Y) = B_K$.

4. Égalité des rangs

Soit r le rang de la matrice A_K ; en choisissant une base de l'espace $\mathrm{Im}(A_K) \subset K^p$, on peut décomposer la matrice A en le produit $A = BC$,

$$K^q \xrightarrow{C} K^r \xrightarrow{B} K^p,$$

où la matrice B_K représente une application injective, et C_K une application surjective. D'après (1.1) et (1.1'), l'application B_L est injective, et C_L est surjective ; par suite, la décomposition $A_L = B_L C_L$ montre que B_L induit un isomorphisme L-linéaire de L^r sur $\mathrm{lm}(A_L)$. D'où l'égalité des rangs.

Cette égalité peut se déduire aussi du critère portant sur le format maximum d'un mineur inversible extrait de A ; mais ce serait utiliser une théorie bien compliquée pour un résultat aussi simple.

5. Égalité des polynômes

L'égalité des déterminants et des polynômes caractéristiques (1.4) est mise pour mémoire ; elle provient de ce que le déterminant est une expression polynomiale (compliquée, certes, mais polynomiale) en les coefficients de la matrice.

Soit $P(X) \in K[X]$ le polynôme minimal de A_K ; il est caractérisé par le fait que l'application

$$K[X]/(P) \longrightarrow \mathbf{M}_p(K), \quad X \mapsto A_K,$$

est bien définie (i.e $P(A) = 0$), et est injective. En posant $r = \deg(P)$, l'espace de gauche admet pour base les classes $\{1, x, \ldots, x^{r-1}\}$, et celui de droite a une base canonique à p^2 éléments ; cette application s'exprime donc, sur ces bases, par une matrice $M \in \mathbf{M}_{p^2,r}$ (qu'il n'est pas question d'expliciter !) ; l'application

$$L[X]/(P) \longrightarrow \mathbf{M}_p(L), \quad X \mapsto A_L,$$

est donnée par la même matrice ; c'est M_L. D'après (1.1), M_L est injective, donc P est le polynôme minimal de A_L.

6. Espaces cycliques et similitude

Les énoncés (1.6) et (1.7) reposent sur des théorèmes difficiles : le premier dit que l'espace K^p est cyclique pour un endomorphisme A_K si et seulement si le polynôme minimal de A_K est égal à son polynôme caractéristique (rappelons que cela utilise l'existence d'un élément dont le polynôme annulateur est égal au polynôme minimal) ; comme les polynômes minimal et caractéristique sont conservés par extension du corps de base, il en est de même de la cyclicité, d'où (1.6).

Venons-en à la similitude (1.7). Il est évident que si A_K et A'_K sont semblables, alors A_L et A'_L le sont. La réciproque utilise la théorie des invariants de similitude : il existe une unique suite de polynômes unitaires de $K[X]$, $(P_1, P_2, \ldots, P_s)$ telle que P_i divise P_{i+1} pour $i < s$, pour laquelle il existe une décomposition en somme directe

$$K^p = E_1 \oplus E_2 \oplus \cdots \oplus E_s$$

où chaque E_i est stable et cyclique pour A_K, et de polynôme minimal P_i.

Une telle décomposition en sous-espaces stables cycliques se transporte de K^p à L^p, si bien que la suite $(P_1, P_2, \ldots, P_s)$ donne les invariants de similitudes de A_L en vertu de l'unicité de cette suite ; il est alors clair que A_K et A'_K sont semblables si et seulement si A_L et A'_L sont semblables.

Il faut souligner qu'une égalité de la forme $A'_L = Q.A_L.Q^{-1}$, avec $Q \in \mathbf{GL}_p(L)$, ne permet pas de trouver directement une matrice $P \in \mathbf{GL}_p(K)$ qui conjugue A_K et A'_K ; il faut le long détour de la théorie des invariants de similitude pour pouvoir en affirmer l'existence ; cependant, lorsque K est un corps infini, un argument de densité permet de contourner cette théorie ; le voici, quelque peu résumé : soit $V \subset \mathbf{M}_p(K)$ le K-espace vectoriel formé des matrices P telles que

$$P.A_K = A'_K.P.$$

Il faut voir que V contient une matrice inversible, c'est-à-dire que l'application polynomiale

$$\det{}_V : V \longrightarrow K$$

est non nulle, et, en particulier que $V \neq 0$. Le terme : "application polynomiale" signifie ceci : si on choisit une base $(v_1, \ldots, v_n)$ de V, tout élément de cet espace est de la forme $x = \sum x_i v_i$ et on peut écrire

$$\det(x) = \det(x_1 v_1 + \cdots + x_n v_n) = P(x_1, \ldots, x_n)$$

où P est un polynôme homogène de degré p en ces n variables. Admettons que le sous-L-espace $W \subset \mathbf{M}_p(L)$ engendré par V soit *égal* à l'espace des matrices $Q \in \mathbf{M}_p(L)$ telles que $Q.A_L = A'_L.Q$ (C'est un bon exercice pour vérifier si on a compris 1.1) et 1.2) !). Par hypothèse, l'application polynomiale

$$\det{}_W \, : \, W \longrightarrow L$$

est non nulle ; comme elle s'exprime, relativement à une base choisie dans V, par la même formule que $\det_V$, ce dernier polynôme $P(X_1, \ldots, X_n)$ est lui aussi non nul ; mais, sur un corps infini, un tel polynôme non nul prend une valeur non nulle sur K^n.