Changement de corps en algèbre linéaire

But :

Dans tout le texte, K désigne un corps et L une extension de K.

On va étudier les problèmes :

1. Soit K un corps,  un polynôme. Peut-on trouver une extension L de K dans laquelle *P* admet au moins une racine ? Dans laquelle *P* est scindé ?
2. En changeant de corps, change t’on les propriétés d’une matrice ?
   1. R-similitude et C-similitude

Théorème :

Deux matrices réelles *A*, *B* sont R-semblables si et seulement si elles sont C-semblables.

Démonstration :

Si  où , alors *A* et *B* sont C-semblables car .

Réciproquement, supposons que  où .

On peut écrire  où  et  sont réelles (pas forcément inversibles).

Comme , on a  et .

Si l’une des deux matrices réelles est inversible, on peut conclure.

Sinon, il existe  tel que  est inversible (réelle), et on peut encore conclure.

En effet,  est une fonction polynomiale réelle, et n’est pas nulle car , donc elle prend des valeurs non nulles sur R.

* 1. Invariance du rang

Théorème :

On a  et le rang d’une matrice  est le même que l’on considère que *A* est à coefficients dans K ou dans L.

Ainsi, le rang d’une matrice à coefficients dans K peut s’obtenir aussi bien à l’aide d’opérations élémentaires à coefficients dans K que dans L.

Démonstration :

On note *r* le rang de *A* sur K. On a alors  avec  et  donc le rang de *A* sur L est aussi *r*.

Corollaire :

Soit  un système de *n* équations à *p* inconnues à coefficients dans K de rang *r*.

Si  est une base de l’espace des solutions dans K, c’en est aussi une de l’espace des solutions dans L.

Démonstration :

Les  sont aussi des solutions à coefficients dans L et la matrice *P* représentant  dans la base canonique de  est aussi celle qui représente  dans la base canonique de . *P* est donc de rang  sur L. Autrement dit,  est libre dans le L-ev  ; c’est donc une base de l’espace des solutions de  dans  puisque cet espace est aussi de dimension  car le rang de *A* est le même sur K et L.

* 1. Invariance du polynôme caractéristique et du polynôme minimal

Théorème :

On a  et les polynômes caractéristique et minimal de  sont les mêmes que l’on considère que *A* est à coefficients dans K ou dans L.

Démonstration :

Pour le polynôme caractéristique, c’est évident…

Soit  le polynôme minimal de *A* sur K et *M* son polynôme minimal sur L. On a , donc *M* divise *m* dans .

Par ailleurs, si *d* est le degré de *m*, la famille  est libre dans le K-ev , donc la matrice  qui représente cette famille dans la base canonique est de rang *d*. Mais *P* représente aussi la famille  dans la base canonique de  (les deux bases sont constituées des mêmes matrices ). La propriété d’invariance du rang montre alors que le rang de *P* sur L est aussi *d* donc que  est libre dans le L-ev , et donc *A* n’a pas de polynôme annulateur non nul dans , ce qui impose  et donc 

* 1. Extension du I.

Théorème :

Si K est infini, deux matrices  de  semblables sur L sont semblables sur K.

L’autre sens est toujours aussi évident.

Démonstration :

Supposons *A* et *B* L-semblables. Alors le système  est un système de  équations à coefficients dans K d’inconnues les coordonnées  de *P* dans la base canonique. Comme ce système est représenté par une matrice à coefficients dans K (dépendants des coefficients de *A* et *B*), le rang est le même que l’on regarde les solutions  ou dans .

Soit  une base de solutions du système  dans . La matrice qui représente  dans la base canonique de  est de rang *N* donc la matrice qui représente  dans la base canonique de  aussi. Ainsi,  est un système libre de solutions de  dans . Comme le système est de rang *N*, c’en est une base.

Autrement dit, toute solution  de  s’écrit  avec .

Or, ce système a une solution inversible donc la fonction polynomiale  n’est pas la fonction nulle sur , ce qui veut dire que  est somme de termes  (où  car s’exprimant à l’aide des ) dont au moins l’un est non nul. On conclut en utilisant le lemme :

Lemme :

Si  est un polynôme non nul et si K est infini, alors la fonction polynomiale  n’est pas identiquement nulle.

En effet, montrons le résultat par récurrence sur *N*:

Le cas  est connu pour K infini.

Soit , supposons la propriété vraie pour . Soit . On écrit alors  avec . L’un au moins des  est non nul.

Donc, par hypothèse de récurrence, on peut fixer  tel que  ne soit pas le polynôme nul ; alors, comme K est infini, il existe *x* tel que , et dans ce cas  ce qui achève la récurrence.

Ainsi, pour en revenir au théorème, le lemme montre que  a une solution inversible, disons  où 

Donc  pour une matrice .

* 1. Construction de corps

Théorème :

Soit K un corps, et . Alors il existe une extension L de degré fini de K dans laquelle *P* est scindé.

Démonstration :

Par récurrence (forte) sur  où *m* est la somme des multiplicités des racines de *P* dans K.

Pour , *P* est scindé sur K, donc  convient.

Soit , supposons la propriété vraie pour tout corps K et tout  et soit  tel que . Soit *R* un facteur irréductible de *P* de degré . Alors l’anneau quotient  est un corps, et c’est une extension de dimension *r* de K, dont  est une K-base. En plus, on a  dans L donc  est racine de *P*.

Ainsi, sur L, *P* a une racine de plus et on peut appliquer l’hypothèse de récurrence à  : on peut trouver une extension finie M de L, donc aussi de K dans laquelle *P* est scindé.

* 1. Applications
  + Pour toute matrice , il existe L, extension finie de K, dans laquelle *A* est trigonalisable.
  + Le polynôme minimal d’une matrice  divise son polynôme caractéristique (Cayley–Hamilton) ; de plus, les deux ont les mêmes facteurs irréductibles dans .

Démonstration :

Soit *R* un facteur irréductible de  dans  et L une extension finie de K dans laquelle *R* est scindé. Si *a* est une racine de *R*, on a alors , donc *a* est une valeur propre de *A* dans L (car  est aussi le polynôme minimal de *A* sur L) et *a* est donc une racine de . Ainsi, *R* et  ne sont pas premiers entre eux dans  (on ne peut pas écrire une relation de Bézout puisque ) donc *R*, qui est irréductible, divise .

D’où le résultat.

* + Soit . On suppose que  a une solution non nulle à coefficients réels positifs. Alors il a une solution non nulle à coefficients dans N.

Démonstration :

Quitte à supprimer des colonnes de *M*, on peut supposer que  a une solution à coefficients strictement positifs.

Soit  une base de solutions rationnelles de . Selon le corollaire du II,  est aussi une base de l’espace des solutions réelles de . Par hypothèse, il existe donc des réels  tels que  est à coefficients strictement positifs. Prenons pour tout  une suite  de rationnels tendant vers . Pour *n* assez grand, , qui tend vers *X*, est un vecteur rationnel à coefficients strictement positifs. En multipliant par un dénominateur commun des , on obtient une solution non nulle à coefficients dans N.