Chapitre 8 : Changement de corps en algèbre linéaire

But :
Dans tout le texte, $\mathbb{K}$ désigne un corps et $\mathbb{L}$ une extension de $\mathbb{K}$.
On va étudier les problèmes :
(1) Soit $\mathbb{K}$ un corps, $P\in\mathbb{K}[X]$ un polynôme. Peut-on trouver une extension $\mathbb{L}$ de $\mathbb{K}$ 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 ?

I $\mathbb{R}$-similitude et $\mathbb{C}$-similitude

Théorème :
Deux matrices réelles A, B sont $\mathbb{R}$-semblables si et seulement si elles sont $\mathbb{C}$-semblables.

Démonstration :
Si $A=PBP^{-1}$ où $P\in GL_n(\mathbb{R})$, alors A et B sont $\mathbb{C}$-semblables car $GL_n(\mathbb{R})\subset GL_n(\mathbb{C})$.
Réciproquement, supposons que $A=PBP^{-1}$ où $P\in GL_n(\mathbb{C})$.
On peut écrire $P=P_1+iP_2$ où P_1 et P_2 sont réelles (pas forcément inversibles).
Comme $A(P_1+iP_2)=B(P_1+iP_2)$, on a $AP_1=BP_1$ et $AP_2=BP_2$.
Si l'une des deux matrices réelles est inversible, on peut conclure.
Sinon, il existe $x\in\mathbb{R}$ tel que P_1+xP_2 est inversible (réelle), et on peut encore conclure.
En effet, $f(x)=\det(P_1+xP_2)$ est une fonction polynomiale réelle, et n'est pas nulle car $f(i)=\det(P)\neq 0$, donc elle prend des valeurs non nulles sur $\mathbb{R}$.

II Invariance du rang

Théorème :
On a $M_{n,p}(\mathbb{K})\subset M_{n,p}(\mathbb{L})$ et le rang d'une matrice $A\in M_{n,p}(\mathbb{K})$ est le même que l'on considère que A est à coefficients dans $\mathbb{K}$ ou dans $\mathbb{L}$.

Ainsi, le rang d'une matrice à coefficients dans $\mathbb{K}$ peut s'obtenir aussi bien à l'aide d'opérations élémentaires à coefficients dans $\mathbb{K}$ que dans $\mathbb{L}$.

Démonstration :
On note r le rang de A sur $\mathbb{K}$. On a alors $A=PJ_rQ$ avec $P\in GL_n(\mathbb{K})\subset GL_n(\mathbb{L})$ et $Q\in GL_p(\mathbb{K})\subset GL_p(\mathbb{L})$ donc le rang de A sur $\mathbb{L}$ est aussi r.

Corollaire :
Soit $AX=0$ un système de n équations à p inconnues à coefficients dans $\mathbb{K}$ de rang r.
Si $(X_1,\dots X_{p-r})\in\mathbb{K}^p$ est une base de l'espace des solutions dans $\mathbb{K}$, c'en est aussi une de l'espace des solutions dans $\mathbb{L}$.

Démonstration :

Les X_i sont aussi des solutions à coefficients dans $\mathbb{L}$ et la matrice P représentant $(X_1,\dots X_{p-r})$ dans la base canonique de $\mathbb{L}^p$ est aussi celle qui représente $(X_1,\dots X_{p-r})$ dans la base canonique de $\mathbb{K}^p$. P est donc de rang $p-r$ sur $\mathbb{L}$. Autrement dit, $(X_1,\dots X_{p-r})$ est libre dans le $\mathbb{L}$-ev $\mathbb{L}^p$; c'est donc une base de l'espace des solutions de $AX=0$ dans $\mathbb{L}^p$ puisque cet espace est aussi de dimension $p-r$ car le rang de A est le même sur $\mathbb{K}$ et $\mathbb{L}$.

III Invariance du polynôme caractéristique et du polynôme minimal

Théorème :

On a $M_n(\mathbb{K})\subset M_n(\mathbb{L})$ et les polynômes caractéristique et minimal de $A\in M_n(\mathbb{K})$ sont les mêmes que l'on considère que A est à coefficients dans $\mathbb{K}$ ou dans $\mathbb{L}$.

Démonstration :

Pour le polynôme caractéristique, c'est évident…

Soit $m\in\mathbb{K}[X]\subset\mathbb{L}[X]$ le polynôme minimal de A sur $\mathbb{K}$ et M son polynôme minimal sur $\mathbb{L}$. On a $\tilde{m}(A)=0$, donc M divise m dans $\mathbb{L}[X]$.

Par ailleurs, si d est le degré de m, la famille $(I_n,A,\dots A^{d-1})$ est libre dans le $\mathbb{K}$-ev $M_n(\mathbb{K})$, donc la matrice $P\in M_{n^2,d}(\mathbb{K})$ qui représente cette famille dans la base canonique est de rang d. Mais P représente aussi la famille $(I_n,A,\dots A^{d-1})$ dans la base canonique de $M_n(\mathbb{L})$ (les deux bases sont constituées des mêmes matrices $E_{i,j}$). La propriété d'invariance du rang montre alors que le rang de P sur $\mathbb{L}$ est aussi d donc que $(I_n,A,\dots A^{d-1})$ est libre dans le $\mathbb{L}$-ev $M_n(\mathbb{L})$, et donc A n'a pas de polynôme annulateur non nul dans $\mathbb{L}_{d-1}[X]$, ce qui impose $\deg M=d$ et donc $M=m$

IV Extension du I.

Théorème :

Si $\mathbb{K}$ est infini, deux matrices A,B de $M_n(\mathbb{K})$ semblables sur $\mathbb{L}$ sont semblables sur $\mathbb{K}$.

L'autre sens est toujours aussi évident.

Démonstration :

Supposons A et B $\mathbb{L}$-semblables. Alors le système $AP=PB$ est un système de N^2 équations à coefficients dans $\mathbb{K}$ d'inconnues les coordonnées $(P_{i,j})$ de P dans la base canonique. Comme ce système est représenté par une matrice à coefficients dans $\mathbb{K}$ (dépendants des coefficients de A et B), le rang est le même que l'on regarde les solutions $P\in M_n(\mathbb{K})$ ou dans $M_n(\mathbb{L})$.

Soit $P_1,\dots P_N$ une base de solutions du système $AP=PB$ dans $M_n(\mathbb{K})$. La matrice qui représente $(P_1,\dots P_N)$ dans la base canonique de $M_n(\mathbb{K})$ est de rang N donc la matrice qui représente $(P_1,\dots P_N)$ dans la base canonique de $M_n(\mathbb{L})$ aussi. Ainsi, $(P_1,\dots P_N)$ est un système libre de solutions de $AP=PB$ dans $M_n(\mathbb{L})$. Comme le système est de rang N, c'en est une base.

Autrement dit, toute solution $P \in M_n(\mathbb{L})$ de $AP = PB$ s'écrit $P = \sum_{i=1}^{N} x_i P_i$ avec $x_i \in \mathbb{L}$.

Or, ce système a une solution inversible donc la fonction polynomiale $f(x_1,\dots x_N) = \det\left(\sum_{i=1}^{N} x_i P_i\right)$ n'est pas la fonction nulle sur $\mathbb{L}^N$, ce qui veut dire que $f(x_1,\dots x_N)$ est somme de termes $a x_1^{n_1} \dots x_N^{n_N}$ (où $a \in \mathbb{K}$ car s'exprimant à l'aide des P_j) dont au moins l'un est non nul. On conclut en utilisant le lemme :

Lemme :

Si $f \in \mathbb{K}[X_1,\dots X_n]$ est un polynôme non nul et si $\mathbb{K}$ est infini, alors la fonction polynomiale $\widetilde{f} : \mathbb{K}^N \to \mathbb{K}$ n'est pas identiquement nulle.

En effet, montrons le résultat par récurrence sur N :

Le cas $N = 1$ est connu pour $\mathbb{K}$ infini.

Soit $N \geq 2$, supposons la propriété vraie pour $N-1$. Soit $f \in \mathbb{K}[X_1,\dots X_n]$. On écrit alors $f = \sum_{i=1}^{d} P_i X_N^i$ avec $P_i \in \mathbb{K}[X_1,\dots X_{N-1}]$. L'un au moins des P_i est non nul.

Donc, par hypothèse de récurrence, on peut fixer $a = (a_1,\dots a_{n-1})$ tel que $\sum_{i=1}^{d} P_i(a) X_N^i$ ne soit pas le polynôme nul ; alors, comme $\mathbb{K}$ est infini, il existe x tel que $\sum_{i=1}^{d} P_i(a) x^i \neq 0$, et dans ce cas $f(a_1,\dots a_{n-1}, x) \neq 0$ ce qui achève la récurrence.

Ainsi, pour en revenir au théorème, le lemme montre que $AP = PB$ a une solution inversible, disons $P = \sum_{i=1}^{N} x_i P_i$ où $\forall i \in [\![1,n]\!], x_i \in \mathbb{K}$

Donc $A = PBP^{-1}$ pour une matrice $P \in GL_n(\mathbb{K})$.

V Construction de corps

Théorème :

Soit $\mathbb{K}$ un corps, et $P \in \mathbb{K}[X]$. Alors il existe une extension $\mathbb{L}$ de degré fini de $\mathbb{K}$ dans laquelle P est scindé.

Démonstration :

Par récurrence (forte) sur $d = \deg P - m$ où m est la somme des multiplicités des racines de P dans $\mathbb{K}$.

Pour $d = 0$, P est scindé sur $\mathbb{K}$, donc $\mathbb{L} = \mathbb{K}$ convient.

Soit $d \geq 1$, supposons la propriété vraie pour tout corps $\mathbb{K}$ et tout $d' < d$ et soit $P \in \mathbb{K}[X]$ tel que $d = \deg P - m$. Soit R un facteur irréductible de P de degré $r \geq 2$. Alors l'anneau quotient $\mathbb{L} = \mathbb{K}[X]/(R.\mathbb{K}[X])$ est un corps, et c'est une extension de dimension r de $\mathbb{K}$, dont $1, \overline{X}, \dots \overline{X}^{r-1}$ est une $\mathbb{K}$-base. En plus, on a $\overline{P} = 0$ dans $\mathbb{L}$ donc $\overline{X}$ est racine de P.

Ainsi, sur $\mathbb{L}$, P a une racine de plus et on peut appliquer l'hypothèse de récurrence à $P \in \mathbb{L}[X]$: on peut trouver une extension finie $\mathbb{M}$ de $\mathbb{L}$, donc aussi de $\mathbb{K}$ dans laquelle P est scindé.

VI Applications

- Pour toute matrice $A \in M_n(\mathbb{K})$, il existe $\mathbb{L}$, extension finie de $\mathbb{K}$, dans laquelle A est trigonalisable.

- Le polynôme minimal d'une matrice $A \in M_n(\mathbb{K})$ divise son polynôme caractéristique (Cayley–Hamilton) ; de plus, les deux ont les mêmes facteurs irréductibles dans $\mathbb{K}[X]$.

Démonstration :

Soit R un facteur irréductible de $\min_A$ dans $\mathbb{K}[X]$ et $\mathbb{L}$ une extension finie de $\mathbb{K}$ dans laquelle R est scindé. Si a est une racine de R, on a alors $\min_A(a) = 0$, donc a est une valeur propre de A dans $\mathbb{L}$ (car $\min_A$ est aussi le polynôme minimal de A sur $\mathbb{L}$) et a est donc une racine de χ_A. Ainsi, R et χ_A ne sont pas premiers entre eux dans $\mathbb{K}[X]$ (on ne peut pas écrire une relation de Bézout puisque $R(a) = \chi_A(a) = 0$) donc R, qui est irréductible, divise χ_A.

D'où le résultat.

- Soit $M \in M_{n,p}(\mathbb{Z})$. On suppose que $MX = 0$ a une solution non nulle à coefficients réels positifs. Alors il a une solution non nulle à coefficients dans $\mathbb{N}$.

Démonstration :

Quitte à supprimer des colonnes de M, on peut supposer que $MX = 0$ a une solution à coefficients strictement positifs.

Soit $V_1,\dots V_N \in \mathbb{Q}^p$ une base de solutions rationnelles de $MX = 0$. Selon le corollaire du **II**, $V_1,\dots V_N \in \mathbb{Q}^p$ est aussi une base de l'espace des solutions réelles de $MX = 0$. Par hypothèse, il existe donc des réels $x_1,\dots x_N$ tels que $X = \sum_{i=1}^{N} x_i V_i$ est à coefficients strictement positifs. Prenons pour tout $i \in [\![1, n]\!]$ une suite $(r_i(n))_{n\in\mathbb{N}}$ de rationnels tendant vers x_i. Pour n assez grand, $\sum_{i=1}^{N} r_i(n) V_i$, qui tend vers X, est un vecteur rationnel à coefficients strictement positifs. En multipliant par un dénominateur commun des $r_i(n)$, on obtient une solution non nulle à coefficients dans $\mathbb{N}$.