

Algebre Lineaire II

David Wiedemann

Table des matières

1	Polynomes	3
1.1	Division avec reste	5
1.2	Factorisation des polynomes sur un corps	6
1.3	Factorisation des polynomes sur un corps	7
1.4	Diviseurs Communs le plus grand	7
1.5	Factorisation en elements irreductibles	9
2	Valeurs et Vecteurs Propres	10
3	Le polynome caracteristique	12
3.1	Theoreme de Cayley-Hamilton	14

List of Theorems

1	Definition (Centre d'un anneau)	3
2	Definition (Diviseurs de 0)	3
3	Definition (Anneau integre)	3
1	Theorème	3
4	Definition (Polynome)	3
2	Theorème	3
5	Definition (Degre d'un polynome)	4
3	Theorème	4
4	Theorème	4
5	Theorème	5
6	Corollaire	5
7	Theorème	5
6	Definition (Diviseurs de polynomes)	6
7	Definition (Racine)	6
8	Theorème	6
8	Definition (Multiplicite d'une racine)	7
9	Theorème (Theoreme fondamental de l'algebre)	7

9	Definition (Polynome irréductible)	7
10	Theorème	7
11	Theorème	7
10	Definition (Polynome Unitaire)	7
11	Definition (Diviseur Commun)	8
12	Theorème	8
12	Definition (PGCD)	8
13	Theorème (Algorithme d'Euclide)	8
14	Theorème	9
15	Theorème (La factorisation est unique)	9
16	Corollaire	10
13	Definition (Vecteur propre)	10
17	Lemme	10
14	Definition	10
18	Corollaire	11
15	Definition (Matrices semblables)	11
16	Definition (Sous-espace propre)	11
19	Lemme	11
20	Corollaire	12
17	Definition (Multiplicite algebrique)	13
21	Proposition	13
22	Theorème (Theoreme de diagonalisation)	13
23	Theorème (Evaluation d'une matrice dans un polynome)	14
24	Theorème (Cayley-Hamilton)	14
18	Definition (Polynome minimal)	14
25	Corollaire	15

1 Polynomes

Definition 1 (Centre d'un anneau)

Le centre $Z(R)$ est l'ensemble des elements x satisfaisant

$$\{x \in R \mid ra = ar \forall a \in R\}$$

Definition 2 (Diviseurs de 0)

a est un element non nul d'un anneau R satisfaisant qu'il existe $b \in R$ tel que $ab = 0$ ou $ba = 0$.

Definition 3 (Anneau integre)

Si un anneau est commutatif et n'a pas de diviseurs de 0, alors l'anneau est integre.

Theorème 1

Soit R un anneau, alors il existe un anneau $S \supseteq R$ (R est un sous-anneau) et $\exists x \in S \setminus R$ tel que

- $ax = xa, \forall a \in R$
- Si $a_0 + \dots + a_n x^n = 0$ et $a_i \in R \forall i$ alors $a_i = 0 \forall i$

Cet x est appele indeterminee ou variable.

Definition 4 (Polynome)

Un polynomer sur R est une expression de la forme

$$p(x) = a_0 + \dots + a_n x^n$$

ou a_i est le i -eme coefficient de $p(x)$.

$R[x]$ est l'ensemble des polynomes sur R .

Theorème 2

$R[X]$ est un sous-anneau. R est sans diviseurs de 0 $\Rightarrow R[X]$ est sans diviseurs de 0.

De meme, si R est commutatif, $R[x]$ aussi.

Preuve

Soit $f(x) = \sum a_i x_i, g(x) = \sum b_i x^i$ de degre n resp. m .

$$f(x) + g(x) = \sum_{i=1}^{\max(m,n)} (a_i + b_i) x^i$$

De meme, on a

$$f(x) \cdot g(x) = a_0 b_0 + \dots = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) x^k$$

Donc $R[X]$ est stable pour $+$, \cdot et donc immédiatement pour $-$, donc $R[X]$ est un sous-anneau de S .

Soient $f(x), g(x) \neq 0$ et $n = \max\{i : a_i = 0\}$, le $m + n$ -ième coefficient de $f(x)g(x)$ est $a_n b_m$ et donc si R est intègre, $R[x]$ l'est aussi. \square

Définition 5 (Degré d'un polynôme)

Soit $f(x) = a_0 + \dots \in R[X]$, $f(x) \neq 0$. On définit

$$\deg(f) = \max\{i : a_i \neq 0\}$$

Ce dernier terme s'appelle le coefficient dominant de f , de plus on définit

$$f(x) = 0 : \deg(f) = -\infty$$

Si $\deg(f) = 0$, alors f est une constante.

Théorème 3

Soit R un anneau, $f, g \in R[X] \neq 0$ tel que au moins un de leur coefficients dominants de f ou de g ne sont pas des diviseurs de 0. Alors $\deg(f \cdot g) = \deg(f) + \deg(g)$

Preuve

Soit $f(x) = a_0 + \dots, g(x) = b_0 + \dots, \deg f = n, \deg g = m$. Le $n + m$ ième coefficient de $f \cdot g = a_n \cdot b_m \neq 0$ \square

Soit $p(x) \in R[x]$, ce polynôme induit une application $f_p : R \rightarrow R$, on écrit aussi $p(r)$

Théorème 4

Soit K un corps et $r_0, r_1, \dots, r_n \in K$ des éléments distincts et soient $g_0, \dots, g_n \in K$.

Il existe un seul polynôme $f \in K[x]$ tel que

1. $\deg f \leq n$
2. $f(r_i) = g_i$

Preuve

On cherche a_0, \dots, a_n tel que

$$a_0 + a_1 r_i + \dots + a_n r_i^n = g_i$$

Donc, on cherche

$$\begin{pmatrix} 1 & r_0 & \dots & r_0^n \\ \vdots & \dots & \dots & \dots \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \dots \end{pmatrix} = \begin{pmatrix} g_0 \\ \dots \end{pmatrix}$$

Il faut donc montrer que la matrice ci-dessus a un déterminant non nul.

On le montre par induction sur n .

Dans le cas $n = 0$, le déterminant vaut trivialement 1. Dans le cas $n > 0$, on a

$$\det \begin{pmatrix} 1 & 0 & \dots \\ 1(r_1 - r_0) & \dots & \\ \dots & \ddots & \\ 1(r_n - r_0) & \dots & \end{pmatrix} = (r_1 - r_0)(r_2 - r_0) \dots \det(V(r_1, \dots, r_n)) \neq 0 \quad \square$$

Lecture 2: Polynomes

Wed 24 Feb

Theorème 5

Soit K un corps fini de caractéristique q , alors $K \supseteq \mathbb{Z}_q$.

De plus K est un espace vectoriel de \mathbb{Z}_q de dimension finie.

Corollaire 6

Soit K un corps infini. Deux polynomes sont égaux si et seulement si leurs évaluations sont les memes.

Preuve

Une direction est triviale.

L'autre suit immédiatement du theoreme 1.6 □

1.1 Division avec reste

Theorème 7

Soit R un anneau, $f, g \in R[x]$, $g \neq 0$ et soit le coefficient de $g \in R^*$

Il existe $q, r \in R[x]$ uniques tel que

1. $f(x) = q(x)g(x) + r(x)$
2. $\deg r < \deg g$

Preuve

Si $\deg f < \deg g$, on a fini.

Soit donc $\deg f \geq \deg g$, donc

$$f(x) = a_0 + \dots + a_n x^n$$

et

$$g(x) = b_0 + \dots + b_m x^m$$

et b_m^{-1} existe.

On procede par induction sur n .

Si $n = m$:

On note que

$$f(x) - \frac{a_n}{b_m}g(x)$$

est un polynome de degre $< n$ Si $n > m$:

On note que

$$f(x) - \frac{a_n}{b_m}x^{n-m}g(x)$$

est un polynome de degre $< n$.

Par hypothese d'induction il existe $q(x), r(x)$ tel que

- $f(x) - \frac{a_n}{b_m}x^{n-m}g(x) + r(x)$
- $\deg r < \deg g$

et donc on a fini de montrer l'existence.

Supposons maintenant qu'il existe r' et q' satisfaisant les memes proprietes que q et g , alors on a

$$q(x)g(x) + r(x) = q'(x)g(x) + r'(x)$$

Donc

$$r' \neq r \text{ et } q' \neq q$$

□

en comparant les degre, on a une contradiction.

1.2 Factorisation des polynomes sur un corps

Definition 6 (Diviseurs de polynomes)

Soit $q(x) \in K[x]$.

q divise f si il existe $g(x)$ tel que

$$q(x)g(x) = f(x)$$

On dit que q est un diviseur de f , on ecrit $q(x)|f(x)$

Definition 7 (Racine)

Soit $p(x) \in K[x]$, et soit $\alpha \in K$ tel que $p(\alpha) = 0$

Theorème 8

Soit $f(x) \in K[x] \setminus \{0\}$, alors $\alpha \in K$ est une racine de f si et seulement si $(x - \alpha)|f(x)$

Preuve

Si $(x - \alpha)q(x) = f(x)$, alors on a fini.

sinon, la division de $f(x)$ par $x - \alpha$ avec reste donne

$$f(x) = q(x)(x - \alpha) + r \text{ ou } r \in K$$

Si $r \neq 0$, alors $f(\alpha) = q(\alpha)(\alpha - \alpha) + r = r \neq 0$ et donc $(x - \alpha)|f(x)$

□

Definition 8 (Multiplicite d'une racine)

La multiplicite d'une racine α de $p(x) \in K[x]$ est le plus grand $i \geq 1$ tel que

$$(x - \alpha)^i | p(x)$$

Theorème 9 (Theoreme fondamental de l'algebre)

Tout polynome $p(x) \in \mathbb{C}[x] \setminus \{0\}$ de degre ≥ 1 possede une racine complexe.

Lecture 3: Factorisation des polynomes sur un corps

Tue 02 Mar

1.3 Factorisation des polynomes sur un corps

Soit K un corps.

Definition 9 (Polynome irreductible)

Un polynome $p(x) \in K[x] \setminus \{0\}$ est irreductible si

- $\deg p \geq 1$
- si $p(x) = f(x) \cdot g(x)$, alors $\deg f = 0$ ou $\deg g = 0$.

Theorème 10

Un polynome de degre 2 sur $K[x]$ est irreductible si et seulement si le polynome ne possede pas de racines.

1.4 Diviseurs Communs le plus grand**Theorème 11**

Soient $f(x), g(x) \in K[x]$ pas tous les deux nuls.

On considere l'ensemble $I = \{u \cdot f + v \cdot g : u, v \in K[x]\}$.

Il existe un polynome $d(x) \in K[x]$ satisfaisant

$$I = \{h \cdot d : h \in K[x]\}$$

Preuve

Soit $a \in I \setminus \{0\}$ de degre minimal.

L'ensemble $\{h \cdot d : h \in K[x]\}$ est clairement un sous-ensemble de I .

Il reste a montrer l'inclusion inverse.

Si d ne divise pas $uf + vg$, la division avec reste donne

$$uf + vg = qd + r \iff r = uf + vg - qd = (u - qu')f + (v - qv')g$$

Or le reste est non nul, mais le reste est de degre inferieur a $\deg d$. \nrightarrow □

Definition 10 (Polynome Unitaire)

Un polynome $f(x) \in K[x]$ dont le coeff. dominant = 1 est un polynome unitaire.

Definition 11 (Diviseur Commun)

Soient $f, g \in K[x]$ non-nuls.

Un diviseur commun de f et g est un polynome qui divise f et g .

Theorème 12

Soient $f, g \in K[x]$ non-nuls.

Soit $d \in K[x]$ comme dans le theoreme precedent.

- d est un diviseur commun de f et g .
- Chaque diviseur commun de f et g est un diviseur de d .
- Si d est unitaire, alors d est unique.

Preuve

- $f \in I \Rightarrow \exists h$ tel que $hd = f \iff d|f$ et $g \in I \Rightarrow d|g$
- Soit $d' \in K[x]$ tq $d'|f, d'|g$, on veut montrer que $d'|d$.

$$f = f'd', g = g'd'$$

des que $d \in I$, il existe $u, v \in K[x]$ tel que

$$d = uf + vg = uf'd' + vg'd' = (uf' + vg')d' \Rightarrow d'|d \quad \square$$

- Soit $d' \in I$ tel que $I = \{hd' | h \in K[x]\}$.
Soient d, d' unitaires.
 $d|d'$ et $d'|d$, donc ils sont les memes a un facteur pres.

Definition 12 (PGCD)

L'unique polynome unitaire $d \in K[x]$ qui satisfait les conditions ci-dessus est appele le plus grand commun diviseur de f et g .

Theorème 13 (Algorithme d'Euclide)

Soient f_0, f_1 non nuls et

$$\deg f_0 \geq \deg f_1$$

On cherche $\gcd(f_0, f_1)$ Si $f_1 = 0$, alors $\gcd = f_0$.

Si $f_1 \neq 0$ On pose

$$f_0 = q_1 f_1 + f_2$$

Soit $h \in K[x] : h|f_0$ et $h|f_1 \Rightarrow h|f_2$ Et donc on pose $\gcd(f_0, f_1) = \gcd(f_1, f_2)$ On repete jusqu'a trouver un f_k nul.

Grace a l'algorithme d'Euclide, on peut aussi trouver $u, v \in K[x]$ tel que $uf_0 + vf_1 = \gcd(f_0, f_1)$.

En effet, on a

$$\begin{pmatrix} f_i \\ f_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} f_{i-1} \\ f_i \end{pmatrix}$$

et donc en appliquant cette matrice plusieurs fois, on trouve une dépendance linéaire entre f_{k-1} et f_k

Et donc le $\gcd(f_0, f_1) = \frac{1}{\text{coeff dominant de } f_{k-1}}(uf_0 + vf_1)$

Lecture 4: Polynomes 2

Wed 03 Mar

1.5 Factorisation en éléments irréductibles

Un polynome $p(x)$ est irréductible si le degré de p est ≥ 1 , $p(x) \neq 0$.

Si $h|p$, alors $h = a$ ou $h = a \cdot p$.

Tout $f(x) \in K[x]$ se laisse factoriser

$$f(x) = a \prod_i p_i(x), p_i(x) \text{ irréductibles, unitaires}$$

Est-ce que cette factorisation est unique ?

Theorème 14

Soit $p(x) \in K[x] \setminus \{0\}$ irréductible et supposons que $p|f_1(x) \dots f_k(x)$, alors il existe i tel que $p(x)|f_i(x)$

Preuve

Par récurrence, il suffit de démontrer l'assertion pour $k = 2$.

Supposons que $p|f \cdot g$, $f, g \in K[x] \setminus \{0\}$.

Si $p \nmid f$, alors $\gcd(p, f) = 1$. Donc, il existe $u, v \in K[x]$ tel que $up + vf = 1$, donc on a

$$upg + vfg = g \Rightarrow p|upg + vfg \Rightarrow p|g \quad \square$$

Theorème 15 (La factorisation est unique)

La factorisation est unique à l'ordre près des p_i .

Preuve

Soit $f(x) = a \prod p_i(x)$ et $f(x) = a \prod q_j(x)$ une autre factorisation en éléments irréductibles.

Par récurrence sur k .

Si $k = 1$, alors

$$ap_1(x) = aq_1(x) \dots q_l(x)$$

Et donc $q_1(x) = p_1(x)$, car p_1 est irréductible. Si $k > 1$,

$$ap_1(x) \dots p_k(x) = aq_1(x) \dots q_l(x)$$

Grace au theoreme ci-dessus, $p_1|q_j$ pour un certain $j \iff p_1 = q_j$. Et donc on obtient

$$p_2(x) \dots = q_1(x) \dots q_l(x) \quad \square$$

Par récurrence, cette factorisation existe et est la même à l'ordre près.

Corollaire 16

Soit $f(x) \in K[x] \setminus \{0\}$ et $\alpha_1 \dots$ des racines de f de multiplicité k_1, \dots, k_l respectivement.

Alors il existe $g(x) \in K[x]$ tel que

$$f(x) = g(x) \prod (x - \alpha_i)^{k_i}$$

Preuve

Exercice □

2 Valeurs et Vecteurs Propres

Definition 13 (Vecteur propre)

Soit V un espace vectoriel sur K et f un endomorphisme sur V .

Un vecteur propre de f associé à la valeur propre $\lambda \in K$ est un vecteur $v \neq 0$ satisfaisant

$$f(v) = \lambda v$$

Lemme 17

Soit $B = \{v_1, \dots, v_n\}$ une base de V et $A \in K^{n \times n}$ la matrice de l'endomorphisme f relatif à B .

La matrice A est une matrice diagonale

$$A = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{pmatrix}$$

$\iff v_i$ est un vecteur propre associé à la valeur propre λ_i .

Preuve

On a

$$[f(v_i)]_B = Ae_i = \lambda_i e_i$$

Donc v_i est un vecteur propre associé à λ_i .

Dans l'autre sens, les arguments sont similaires. □

Definition 14

Un endomorphisme f sur un espace vectoriel de dimension finie est appelé diagonalisable s'il existe une base tel que $\{v_1, \dots\}$ de V composée de vecteurs propres.

Lecture 5: Vecteurs/Valeurs Propres

Tue 09 Mar

Corollaire 18

Soit $f : V \rightarrow V$ un endomorphisme et $\{v_1, \dots, v_n\}$ une base de V .
 Alors f est diagonalisable si et seulement si il existe une matrice inversible $P \in K^{n \times n}$ tel que $P^{-1}A_BP$ est diagonale.

Preuve

f est diagonalisable $\iff \exists B' = \{w_1, \dots\}$ tel que $A_{B'}$ est diagonale.

Mais $A_{B'} = P^{-1}A_BP$

□

Definition 15 (Matrices semblables)

$A, B \in K^{n \times n}$ sont semblables s'il existe $P \in K^{n \times n}$ inversible tel que

$$P^{-1}AP = B$$

Donc si f est diagonalisable, la matrice de f est semblable a une matrice diagonale.

Definition 16 (Sous-espace propre)

Soit $f : V \rightarrow V$ un endomorphisme et λ une valeur propre de f , alors

$$E_\lambda = \ker(f - \lambda \cdot \text{Id})$$

est l'espace propre de f associe a λ .

$\dim E_\lambda$ est la multiplicite geometrique de λ .

Lemme 19

Soit $f : V \rightarrow V$ un endomorphisme et v_1, \dots, v_r des vecteurs propres associes aux valeurs propres $\lambda_1, \dots, \lambda_r$ distinctes.
 Alors $\{v_1, \dots, v_r\}$ est un ensemble libre.

Preuve

$r = 1$ est evident.

Pour $r = 2$:

Supposons que v_1, v_2 sont lineairement dependants, alors il existe $\exists \alpha_1, \alpha_2 \in K \setminus \{0\}$ tel que

$$\alpha_1 v_1 + \alpha_2 v_2 = 0$$

Spg $\lambda_2 \neq 0$, en appliquant f , on trouve

$$0 = \alpha_1 f(v_1) + \alpha_2 f(v_2)$$

$$0 = \alpha_1 \frac{\lambda_1}{\lambda_2} v_1 + \alpha_2 v_2$$

$$0 = \alpha_1 \left(1 - \frac{\lambda_1}{\lambda_2}\right) v_2$$

Pour $r > 2$

Supposons l'assertion est fausse et soit $r > 2$ minimal tel que v_1, \dots, v_r sont

lin. dependants.. Soit

$$\alpha_1 v_1 + \dots = 0$$

avec $\alpha_i \neq 0 \forall i$, alors

$$0 = \alpha_1 \frac{\lambda_1}{\lambda_r} v_1 + \dots + \alpha_r v_r$$

En soustrayant les deux egalites, on trouve

$$0 = \alpha_1 \left(1 - \frac{\lambda_1}{\lambda_r}\right) v_1 + \dots$$

□

Ce qui contredit la minimalite.

Corollaire 20

Soit $f : V \rightarrow V$ un endomorphisme de V sur K et $\dim V = n$.

Soient λ_1, \dots , les valeurs propres differentes de f .

Soit $n_1 \dots$ les multiplicites geometriques respectives.

Soient $B_i = \{v_1^{(i)}, \dots, v_{n_i}^{(i)}\}$ des bases de E_{λ_i} , alors

$$\bigcup_i B_i$$

est un ensemble libre.

f est diagonalisable $\iff n_1 + \dots + n_r = n$

Preuve

Soit

$$\sum_{i=1}^r \sum_{j=1}^{n_i} \alpha_{ij} v_j^{(i)} = 0$$

□

Montrons que $\alpha_{ij} = 0 \forall i, j$ "Immediat" par lemme d'avant.

On remarque immediatement que si $\sum n_i = n$, les vecteurs propres forment une base.

A l'inverse, soit f diagonalisable, cad il existe une base B de V composee de vecteurs propres. Soit $m_i = |B \cap E_{\lambda_i}|$, donc m_i est le nombre de vecteurs dans B associe a λ_i .

Clairement $\sum m_i = n$, mais $m_i \leq n_i \leq \dim E_{\lambda_i}$, donc $\sum n_i = n$.

Lecture 7: Polynome caracteristique

Wed 10 Mar

3 Le polynome caracteristique

Soit A une matrice $n \times n$, $\lambda \in K$ est une valeur propre de l'endomorphisme defini par A si et seulement si $\ker(A - \lambda \text{Id}) \supsetneq \{0\}$. On note

$$\det(A - \lambda I) = \sum_{\pi \in S_n} \text{sgn}(\pi) \prod_{i=1}^n (A - \lambda \text{Id})_{i\pi(i)}$$

On observe que λ est une valeur propre de f si et seulement si λ est une racine de p_A .

Soit $f : V \rightarrow V$ un endomorphisme, $B = \{v_1, \dots\}$ une base de V . Le polynome caractéristique de f est donné par

$$\det(A_B - \lambda \text{Id})$$

Cette définition fait du sens, car le changement de base n'influence pas la valeur du déterminant.

Definition 17 (Multiplicité algébrique)

La multiplicité algébrique d'une valeur propre est la multiplicité comme racine du polynome caractéristique.

Proposition 21

Soit f un endomorphisme de $V \rightarrow V$.

Soit $\lambda \in K$ une valeur propre.

La multiplicité géométrique de λ est au plus la multiplicité algébrique.

Preuve

Soit $\{v_1, \dots, v_r\}$ une base de E_λ , on complète cette base en une base de V avec $\{w_1, \dots, w_{n-r}\}$. Dans cette base, la représentation de la matrice de $A - \lambda \text{Id}$ implique que

$$\det(A - x \text{Id}) = (\lambda - x)^r \det C \quad \square$$

et donc r est au plus la multiplicité algébrique.

Théorème 22 (Théorème de diagonalisation)

Soit V un espace vectoriel sur K de dimension n , $f : V \rightarrow V$ un endomorphisme, $\lambda_1, \dots \in K$ les valeurs propres distinctes, alors f est diagonalisable si et seulement si

- $p_f(x) = (-1)^n \prod_{i=1}^r (x - \lambda_i)^{g_i}$
- $\dim E_{\lambda_i} = g_i$ pour tout i

Preuve

Soit f diagonalisable et soit $B = \{v_1, \dots\}$ une base composée de vecteurs propres. A_B est une matrice diagonale, alors $p_f(x) = \det(A_B - x \text{Id}) = (-1)^n \prod (\lambda_i - x)^{g_i}$. De plus $\dim(\ker(A_B - \lambda_i \text{Id})) = g_i$

Soient m_i les multiplicités géométriques des valeurs propres. car

$$\deg(p_f) = n$$

on a fini. \square

Lecture 7: Cayley-Hamilton

Tue 16 Mar

3.1 Theoreme de Cayley-Hamilton

Theorème 23 (Evaluation d'une matrice dans un polynome)

Soit $p(x) = a_0 + \dots + a_n x^n \in K[x]$ Pour $A \in K^{n \times n}$, on definit

$$p(A) = a_0 \text{Id} + \dots + a_n A^n$$

Theorème 24 (Cayley-Hamilton)

Soit $A \in K^{n \times n}$ et $p(\lambda) \in K[\lambda]$ le polynome caracteristique de A , alors
 $p(A) = 0 \in K^{n \times n}$

Preuve

Supposons d'abord que $A \in K^{n \times n}$ est diagonalisable.

Alors $\exists \{v_1, \dots\}$ une base composee de vecteurs propres de A .

Considerons

$$\begin{aligned} p(A) \cdot v_i &= a_0 v_i + a_1 A v_i + \dots \\ &= a_0 v_i + a_1 \lambda_i v_i + \dots \\ &= p(\lambda_i) v_i = 0 \end{aligned}$$

Supposons donc que A n'est pas diagonalisable.

Notons que

$$\text{Id} = \frac{\text{cof}(A - \lambda \text{Id})^T}{\det(A - \lambda \text{Id})} \cdot (A - \lambda \text{Id})$$

Alors

$$a_0 + a_1 \lambda \text{Id} + \dots = \text{cof}(A - \lambda \text{Id})^T \cdot (A - \lambda \text{Id})$$

$$\text{cof}(A - \lambda \text{Id})^T \cdot (A - \lambda \text{Id}) = B_0 A + \sum_{i=1}^{n-1} \lambda^i (B_i A - B_{i-1}) - \lambda_n B_{n-1}$$

Ce qui implique

$$\begin{aligned} a_0 \text{Id} &= B_0 A \\ a_i \text{Id} &= B_i A - B_{i-1} \text{ pour } i \in \{1, \dots, n-1\} \\ a_n \text{Id} &= -B_{n-1} \end{aligned}$$

On multiplie chacune de ces equations par A^i et on les additionne. On trouve alors

$$p(A) = 0 \quad \square$$

Definition 18 (Polynome minimal)

Le polynome unitaire de degre minimal parmi ceux, qui annullent la matrice $A \in K^{n \times n}$ est appele le polynome minimal de A .

Preuve

Ce polynome est unique.

Supposons qu'il existe q, p des polynomes qui annullent A . Alors

$$p \nmid q \text{ et } q \nmid p$$

Donc

$$p = qq' + r$$

ou $r \neq 0, \deg r < \deg p$, donc

$$0 = p(A) = r(A) + q'(A)q(A) = r(A)$$

Donc p n'est pas de degre minimal \nmid .

□

Corollaire 25

Soit $A \in K^{n \times n}$

- *A^k est combinaison lineaire de $\text{Id}, A, \dots, A^{n-1}$ pour tout $k \in \mathbb{N}$*
- *A inversible, alors A^{-1} s'ecrit comme combinaison lineaire de $\text{Id}, A, \dots, A^{n-1}$*

Preuve

- *Pour $k \in 0, \dots, n-1$ clair.*

Soit $k \geq n : x^k = q(x)p_A(x) + r(x)$, on evalue

$$A^k = q(A)p_A(A) + r(A) = r(A)$$

et r est de degre $n-1$.

—

$$\det A \neq 0$$

□

Donc il suffit de reformuler $p(A) = 0$.