Mathématiques

Algèbre Semestre 2

Eric Charpentier

Table des matières

Première partie

Polynôme

1 Polynôme formel

Définition. Soit $\mathbb{K}$ un corps ($\mathbb{R}$ ou $\mathbb{C}$). On appelle polynôme (formel) sur $\mathbb{K}$, en une indéterminé X, toute expression formelle de la forme : $\sum_{k\geq 0} a_k X^k$ où $a_k \in \mathbb{K} (k \in \mathbb{N})$ tous nuls pour k assez grand, avec les règles de manipulations suivantes :

- Additions : $\sum_{k\geq 0} a_k X^k + \sum_{k\geq 0} b_k X^k = \sum_{k\geq 0} (a_k + b_k) X^k$
- Produits : $\lambda \in \mathbb{K} \Rightarrow \lambda \sum_{k\geq 0} a_k X^k = \sum_{k\geq 0} \lambda . a_k X^k$
- Produits de polynômes : $\sum_{k\geq 0} a_k X^k . \sum_{k\geq 0} b_k X^k = \sum_{k\geq 0} c_k X^k$ où $c_k = \sum_{j=0}^{k} (a_j . b_{k-j})$

Démonstration. $\sum_{k\geq 0} a_k X^k . \sum_{l\geq 0} b_l X^l = \sum_{k\geq 0} \sum_{l\geq 0} a_k b_l X^{k+l} = \sum_{m\geq 0} \sum_{k=0}^{m} a_k b_{m_k} X^m$ où $m = l + n$ □

Remarques.

- On identifie X^0 au nombre $1 \in \mathbb{K}$. Donc le polynôme $a_0 X^0$ est identifié au nombre $a_0 \in \mathbb{K} : a_0 X^0 = a_0$.
- On note $X = X^1$
- On note 0 le polynôme $\sum_{k\geq 0} 0 X^k$ ("polynôme nul")
- La règle de multiplication des polynômes montre que $X^i X^j = X^{i+j}$ et $X^i = X.X...X$

2 Anneau commutatif unitaire

Proposition et définition. Soit $\mathbb{K}[X]$ l'ensemble des polynômes sur $\mathbb{K}$ de l'indéterminée X. Alors : $\mathbb{K}[X]$ est un anneau commutatif unitaire (ou unifère) intègre.

- $(\mathbb{K}[X], +)$ est un groupe commutatif, i.e.
  - L'addition est associative : $\forall A, B, C \in \mathbb{K}[X] : A + (B + C) = (A + B) + C$
  - Il existe un élément neutre pour l'addition à savoir le polynôme nul : $\forall A \in \mathbb{K}[X], A + 0 = 0 + A = A$
  - Il existe un opposé, pour tout $A \in \mathbb{K}[X]$, il existe un opposé, $-A$.
- L'anneau ($\mathbb{K}[X]$,+,X) est commutatif, i.e. le produit est commutatif : $AB = BA$
- L'anneau ($\mathbb{K}[X]$, +,X) est unitaire (ou unifère) i.e. il existe un élément neutre pour X, appelé polynôme unitaire (qui est en fait $X^n = 1$) : $1A = A1 = A$ ($\forall A \in \mathbb{K}[X]$)
- L'anneau $\mathbb{K}[X]$ est intègre, i.e. $AB = 0 \Rightarrow A = 0$ ou $B = 0$

Preuve de l'intégrité. Soit $A = \sum_{k\geq 0} a_k X^k, B = \sum_{k\geq 0} b_k X^k$ deux polynômes non nuls.
Soient k_a et k_b le plus grand k tel que $a_k \neq 0$ et $b_k \neq 0$.
On a donc $A = a_0 X^0 + ... + a_{k_A} X^{k_A}$ et $B = b_0 X^0 + ... + b_{k_B} X^{k_B}$.
Ainsi $AB = a_0 b_0 X^0 + ... + a_{k_A} b_{k_B} X^{k_A + k_B} \neq 0$.

Si on appelle degré de a_iX^i le nombre i, on peut écrire : $A = a_{k_A}X^{k_A} +$ termes de degrés $< k_A$ et $B = b_{k_B}X^{k_B} +$ termes de degrés $< k_B$ et $AB = a_{k_A}b_{k_B}X^{k_A+k_B} +$ termes de degrés $< k_A + k_B$

3 Précisions sur le degrés

Définition.

- $deg(a_iX^i)$ si $a_i \neq 0$ (définition du degrés dans un monôme normal, i.e. d'un polynôme de la forme $a_iX^i, a_i \neq 0$)
- $A \neq 0 : A = a_0X^0 + a_1X^1 + a_dX^d$ avec d le plus grand k tel que $a_k \neq 0$. Alors le degrés $A = d$.

Proposition. Soient A, B deux polynômes $\neq 0$, alors :

- $deg(AB) = deg(A) + deg(B)$
- $deg(A + B) \leq max(deg(A), deg(B))$.
- Si $deg(A) = deg(B)$ notant $A = cd(A)X^{deg(A)}+$ monômes de degrés moindres.
  Et $B = cd(B)X^{deg(B)}+$ monômes de degrés moindres.
  Où $deg(A) = deg(B)$
  En notant cd le coefficient dominant on a donc :
  - Si $cd(A) + cd(B) \neq 0$, alors $deg(A + B) = deg(A) = deg(B)$
  - Si $cd(A) = cd(B) = 0$, alors $deg(A + B) < deg(A) = deg(B)$

Démonstration.

- On l'a fait en justifiant que $\mathbb{K}[X]$ est intègre : $A = cd(A)X^{deg(A)}+$ monômes de degrés moindres et $B = cd(B)X^{deg(B)}+$ monômes de degrés moindres. D'où $AB = cd(A)cd(B)X^{deg(A)+deg(B)}$ donc
$$deg(AB) = deg(A) + deg(B)$$
- $A + B = cd(A)X^{deg(A)} +$ termes de degrés $<$deg(A) $+ cd(B)X^{deg(B)}+$ termes de degrés $<$ B. Donc si deg(B) $<$ deg(A) : $A + B = cd(A)X^{deg(A)}+$ termes de degrés $<$ A donc $deg(A + B) = deg(B) = max(deg(A), deg(B))$

□

Définition.

$$deg(0) = -\infty$$

Démonstration. On veut que la proposition précédente reste vraie pour le polynôme nul :
$deg(0) = deg(0A) = deg(0) + deg(A) \forall deg(A) \in \mathbb{N}(A \neq 0)$
Donc $deg(0) = \pm\infty$
De plus $deg(0 + A) = max(deg(0), deg(A)) \forall A \neq 0$
Donc $deg(0) \leq deg(A), \forall deg(A) \in \mathbb{N}$: donc $deg(0) \leq 0$
Donc $deg(0) = -\infty$

□

Et on vérifie qu'on a bien $deg(0 \times 0) = -\infty = deg(0) + deg(0)$

et $deg(0 + 0) = -\infty = max(deg(0), deg(0))$

La proposition reste vraie si l'un des polynômes est nul même si les deux le sont.

4 Division euclidienne

Proposition et définition. Soient $A, B \in \mathbb{K}[X] \text{avec} B \neq 0$. Alors il existe un unique couple $(Q, R) \in \mathbb{K}[X] \times \mathbb{K}[X]$ tel que : $A = BQ + R$ et $deg(R) < deg(B)$. C'est la division euclidienne de A par B : Q est le quotient, R est le reste.

Démonstration. **Existence.** Il existe un polynôme tel que $deg(A - BQ) = min(deg(A - BS) : S \in \mathbb{K}[X])$.

Posons $R = A - BQ$ et prouvons que $deg(R) < deg(B)$, i.e. $deg(A - BQ) < deg(B)$.

Supposons que $deg(A - BQ) \geq deg(B)$

Écrivons $B = b_d X^d + \text{monômes de degrés moindres}(\alpha)$ où $d = deg(B)(b_d \neq 0)$: donc $b_d = cd(B)$ et $A - BQ = u_{d+m}X^{d+m} + \alpha$ où $m \geq 0$ et $u_{d+m} = cd(A - BQ) \neq 0$ car $deg(A - BQ) \geq d$.

Alors : $A - BQ - \frac{u_{d+m}}{b_d}X^m B = A - BQ - \frac{u_{d+m}}{b_d}X^m(b_d X^d + \alpha < d) = u_{d+m}X^{d+m} + \alpha < (d + m) - \frac{u_{d+m}}{b_d}b_d X^{m+d} + \alpha < (d + m) = \alpha < (d + m) = deg(A - BQ)$

et donc : $\underbrace{deg(A - BQ - \frac{u_{d+m}}{b_d}X^m B)}_{A-BQ'} < deg(A - BQ)$.

où $Q' = Q + \frac{u_{d+m}}{b_d}X^m = Q + \frac{u_{d+m}X^{d+m}}{b_d X^d} = Q + \frac{A - BQ}{td(B)}$ où td est le terme dominant.

Ainsi il existe un polynôme Q' tel que $deg(A - BQ') < deg(A - BQ)$, ce qui contredit le choix de Q ($deg(A - BQ)$ minimal !). Cela prouve, par l'absurde, qu'on n'a pas $deg(A - BQ) \geq deg(B)$ et donc que $deg(A - BQ) < deg(B)$

Unicité. Supposons que : $A = BQ + R, deg(R) < deg(B)$ et $A = BQ' + R', deg(R') < deg(B)$.

Alors : $BQ + R = BQ' + R'$ donc $B(Q - Q') = R - R'$ et donc : $deg(B(Q - Q')) = deg(R' - R)$

d'où : $deg(B) + deg(Q - Q') = deg(R' - R) \leq max(deg(R'), deg(-R)) < deg(B) \Rightarrow deg(Q - Q') < 0 \Rightarrow Q - Q' = 0 \Rightarrow Q' = Q$

Et alors : $BQ + R = BQ' + R' = BQ + R' \Rightarrow R' = R$

□

Algorithme de division euclidienne.

Entrée : $Q = 0, R = 0$

Boucle : Tant que $deg(R) \geq deg(B)$:

faire :

$Q = Q + \frac{td(R)}{td(B)}$

$R = R - \frac{td(R)}{td(B)}B$

Sortie :

si $deg(R) < deg(B)$

sortir (Q,R)

A chaque itération dans la boucle, $deg(R)$ diminue strictement car $R - \frac{td(R)}{td(B)} = cd(R)X^{deg(R)}$+monômes de degrés $<$
$deg(R) - \frac{cd(R)X^{deg(R)}}{cd(B)X^{deg(B)}}(cd(B)X^{deg(B)} + \text{monômes de degrés} < deg(B))$
$= (cd(R)X^{deg(R)} + \text{monômes de degrés} < deg(R)) - (cd(R)X^{deg(R)} + \text{monômes de degrés} < deg(B) + deg(R) - deg(B))$
= somme de monômes de degrés $< deg(R)$
Donc l'algorithme se termine après après un nombre fini d'itérations ($\leq deg(A) + 1$).

5 Plus Grand Commun Diviseur

Proposition et définition. Soient A,B deux polynômes de $\mathbb{K}[X]$ non tous deux nuls. Il existe un unique polynôme D **unitaire** (i.e. $cd(D) = 1$) tel que : $A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$ où $\forall P \in \mathbb{K}[X], P\mathbb{K}[X] = (PQ : Q \in \mathbb{K}[X])$
Et donc $A\mathbb{K}[X] + B\mathbb{K}[X] = AU + BV : U \in \mathbb{K}[X], V \in \mathbb{K}[X]$.
Ce polynôme D est appelé le PGCD unitaire de A et B. Il est caractérisé par :

1. $D|A \text{et} D|B$
2. $\forall P$, si $P|A$ et $P|B$ alors $P|D$
3. D est unitaire.

Les polynômes qui vérifient 1 et 2 sont les kD , $k \in \mathbb{K}/(0)$.

Démonstration. Soit $C \in A\mathbb{K}[X] + B\mathbb{K}[X]$ non nuls et de degré minimal, il en existe puisque A, B ne sont pas tous les deux nuls. Soit :
$A = A.1 + B.0 \in A\mathbb{K}[X] + B\mathbb{K}[X]$
$B = A.0 + B.1 \in A\mathbb{K}[X] + B\mathbb{K}[X]$
Soit $F \in A\mathbb{K}[X] + B\mathbb{K}[X]$: faisons la division euclidienne de F par C :
$F = CQ + R, deg(R) < deg(C)$
Mais : $F = AU + BV$ et $C = AU_C + BV_C$ ainsi $F - CQ = A(U - U_cQ) + B(V - V_cQ)$ ($C \in A\mathbb{K}[X] + B\mathbb{K}[X]$)
On a donc : $R \in A\mathbb{K}[X] + B\mathbb{K}[X]$ et $deg(R) < deg(C)$
D'où $R = 0$ car C est de degrés minimal.
Donc $F = CQ \in C\mathbb{K}[X]$.($\forall F \in A\mathbb{K}[X] + B\mathbb{K}[X]$).
Et donc : $A\mathbb{K}[X] + B\mathbb{K}[X] \subset C\mathbb{K}[X]$
Réciproquement : $C = AU_C + BV_C \Rightarrow \forall Q \in \mathbb{K}[X], CQ = AU_CQ + BV_CQ \in A\mathbb{K}[X] + B\mathbb{K}[X]$
$\Rightarrow C\mathbb{K}[X] \subset A\mathbb{K}[X] + B\mathbb{K}[X]$ Donc : $A\mathbb{K}[X] + B\mathbb{K}[X] = C\mathbb{K}[X]$
Clairement : $C\mathbb{K}[X] = \frac{C}{cd(C)}\mathbb{K}[X]$
Car : $CQ = \frac{C}{cd(C)}cd(C)Q$
Posant : $D = \frac{C}{cd(C)}$

On a donc D unitaire : $C = cd(C)X^{deg(C)} \Rightarrow \dfrac{C}{cd(C)} = 1X^{deg(C)}$ (Il est donc unitaire) et $A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$

Montrons que D vérifie 1,2 et 3(évident) :

$A, B \in A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X] \Rightarrow D|A \text{et} D|B \Rightarrow 1$

Si $P|A$ et $P|B$, alors $A = PS, B = PT$

Donc $\forall U, V : AU + BV = P(SU + TV)$

Mais $D \in A\mathbb{K}[X] + B\mathbb{K}[X] \text{donc} \exists U, V$ tel que $D = AU + BV = P(SU + TV)$

Et donc : $P|D$: ce qui prouve 2. Donc D vérifie 1,2 et 3.

Maintenant, soit E un polynôme vérifiant 1 et 2 : montrons que $E = kD, k \in \mathbb{K}/(0)$ où E vérifie 3 alors $k = 1$ (et donc $E = D$).

E vérifie 1 $\Leftrightarrow E|A \text{et} E|B \Rightarrow E|D$

E vérifie 2 $\Leftrightarrow$ tout polynôme divisant A et B divise $E \Rightarrow D|E$

$D|E : E = DQ$ et $E|D : D = EQ' \Rightarrow D = DQQ' \Rightarrow deg(D) = deg(D) + deg(Q) + deg(Q') \Rightarrow deg(Q) = deg(Q') = 0$

Donc $Q = cte = k$ et $D = DQQ' \Rightarrow QQ' \Rightarrow QQ' = 1 \Rightarrow Q' = Q^{-1} = k^{-1}$

Ainsi : $E = DQ = kD, k \in \mathbb{K}/(0)$

Enfin : $cd(E) = kcd(D) = k$: donc E vérifie 3 $\Leftrightarrow k = 1 \Leftrightarrow E = D$. □

6 Plus Petit Commun Multiple

Proposition et définition. Soient $A, B \in \mathbb{K}[X]$ tous deux non nuls.

Il existe un unique $M \in \mathbb{K}[X]$ unitaire tel que $A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X]$. On l'appelle le PPCM de A, B.

Il est caractérisé par :

1. $A|M$ et $B|M$
2. $\forall P \in \mathbb{K}[X], (A|P \text{ et } B|P) \Rightarrow M|P$
3. M est unitaire

Tout P vérifiant 1,2 est de la forme kM , $k \in \mathbb{K}[X]/(0)$ et on dit que c'est un PPCM de A, B.

Démonstration. $AB \in A\mathbb{K}[X] \cap B\mathbb{K}[X]$

Car $AB \in A\mathbb{K}[X], AB = BA \in B\mathbb{K}[X]$ Mais $AB \neq 0$ car $A \neq 0, B \neq 0$ (et car $\mathbb{K}[X]$ est intègre)

Donc : $A\mathbb{K}[X] \cap B\mathbb{K}[X] \neq \{0\}$.

Soit donc $C \in A\mathbb{K}[X] \cap B\mathbb{K}[X]$ non nul et de degré minimal.

Soit $F \in A\mathbb{K}[X] \cap B\mathbb{K}[X]$: faisons la division euclidienne.

$F = QC + R, deg(R) < deg(C)$.

$F \in A\mathbb{K}[X], C \in A\mathbb{K}[X] \Rightarrow QC \in A\mathbb{K}[X], \text{donc} F - QC \in A\mathbb{K}[X]$.

De même : $F - QC \in B\mathbb{K}[X]$.

Donc : $R \in A\mathbb{K}[X] \cap B\mathbb{K}[X]$.

Mais $deg(R) < deg(C)$. Donc $R = 0$ (par le choix de C).

Donc $F = CQ \in C\mathbb{K}[X](\forall F \in A\mathbb{K}[X] \cap B\mathbb{K}[X])$.

Et donc : $A\mathbb{K}[X] \cap B\mathbb{K}[X] \subset C\mathbb{K}[X]$.

Réciproquement : $C \in A\mathbb{K}[X] \cap B\mathbb{K}[X] \Rightarrow C = AU = BV$.

$\Rightarrow \forall Q \in \mathbb{K}[X], CQ = AQU \in A\mathbb{K}[X] = BQV \in B\mathbb{K}[X](\Rightarrow CQ \in A\mathbb{K}[X] \cap B\mathbb{K}[X])$.

$\Rightarrow C\mathbb{K}[X] \subset A\mathbb{K}[X] \cap B\mathbb{K}[X]$.

Posons $M = \dfrac{C}{cd(C)}$: alors M est unitaire et $A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X]$

Montrons que M vérifie 1,2 et 3(évident).

$M \in A\mathbb{K}[X] \cap B\mathbb{K}[X] \Rightarrow A|M$ et $B|M$ donc 1 est évident !

M vérifie 2 $\Leftrightarrow (\forall F, A|F$ et $B|F \Rightarrow M|F) \Leftrightarrow (\forall F, F \in A\mathbb{K}[X] \cap B\mathbb{K}[X] \Rightarrow F \in M\mathbb{K}[X])$

Évident puisque $A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X]$.

Donc M vérifie 1,2 et 3.

Enfin, soit E vérifiant 1,2, montrons que $E = kM, k \in /(0)$ et que si E vérifie 3, alors $E = M$.

E vérifie 1 $\Leftrightarrow A|E$ et $B|E \Leftrightarrow E \in A\mathbb{K}[X] \cap B\mathbb{K}[X]$

$\Leftrightarrow E \in M\mathbb{K}[X]$

$\Leftrightarrow M|E$

E vérifie 2 $\Leftrightarrow$ (tout F tel que $A|F$ et $B|F$ vérifie $E|F) \Rightarrow E|M$ car M vérifie 1.

Donc $E|M$ et $M|E$ d'où (comme précédemment) : $E = kM, k \in \mathbb{K}/(0)$

De plus : $cd(E) = kcd(M) = k$ donc E vérifiant 3 $\Leftrightarrow k = 1 \Leftrightarrow E = M$.

Ce qui montre que 1,2 et 3 caractérise M. □

7 Lien entre PGCD et PPCM

Proposition et définition. Soient A, B tous deux non nuls. Soit $D = PGCD(A, B)$ leur PGCD est unitaire. Soit $M = PPCM(A, B)$ leur PPCM est unitaire. Alors :

$$DM = \frac{A}{cd(A)} \cdot \frac{B}{cd(B)}$$

Démonstration. Voir plus tard □

Algorithme d'Euclide. D se calcule par l'algorithme d'Euclide. $A = BQ_1 + R_1, degR_1 < degB$

Les diviseurs communs à A et B sont les diviseurs communs à B et $A - BQ_1 = R_1$

Puis : $B = Q_2R_1 + R_2, degR_2 < degR_1$ On a de même : $PGCD(B, R_1) = PGCD(R_1, R_2)$ etc... Cette succession de divisions ne peut pas se poursuivre indéfiniment puisque les degrés des restes décroissent strictement : $deg(B) > deg(R_1) > deg(R_2) > ...$

Et toute séquence strictement décroissante dans $\mathbb{N} \cup \{-\infty\}$ se termine. Or, tant que le reste est différent 0, on peut continuer l'algorithme. Donc quand l'algorithme se termine c'est qu'on est arrivé à un reste nul :

$R_{n-2} = Q_nR_{n-1} + R_n$ avec $R_n \neq 0$ dernier reste non nul.

$R_{n-1} = Q_{n+1}R_n + 0$

Alors : $D = PGCD(A,B) = PGCD(B,R_1) = PGCD(R_1,R_2) = ... = PGCD(R_{n-1},R_n) = PGCD(R_n,0) = \frac{R_n}{cd(R_n)}$ (le plus grand diviseur unitaire de R_n).
Donc le $PGCD(A,B)$ est le dernier reste unitaire non nul dans l'algorithme d'Euclide rendu unitaire.

Exemple.

$A = X^5 - X^4 + 2X^3 + 1$

$B = X^5 + X^4 + 2X^2 - 1$

$A = B - 2(X^4 - X^3 + X^2 - 1) = B - 2R_1$ On peut schtroumpfer le facteur -2

$B = (X+2)R_1 - X^3 + X + 1 = (X+2)R_1 - R_2$

$R_1 = (X-1)R_2 - 0$

Donc $PGCD(A,B) = D = X^3 + X + 1$

Comme pour les entiers, on peut remonter le flot des divisions pour trouver des polynômes (U_0, V_0) tel que $D = AU_0 + BV_0$ (c'est ce qu'on appelle l'algorithme d'Euclide étendu). Dans l'exemple ci-dessus :

$D = X^3 + X + 1 = (X^5 + X^4 + 2X^2 - 1) - (X+2)(X^4 - X^3 + X^2 - 1)$

$= B - (X+2)(-0.5)(A - B)$

$= \frac{1}{2}(X+2)A + (1 - \frac{1}{2}(X+2))B$

$= \frac{1}{2}(X+2)A - \frac{1}{2}XB$

D'où la solution $U_0 = \frac{1}{2}(X+2)$ et $V_0 = -\frac{1}{2}X$

Pour l'équation $AU + BV = D$ (on verra plus tard comment en déduire toutes les solutions (U,V)...)

8 Premier entre eux

Définition. Deux polynômes A, B (nous tous deux nuls) sont dits premiers entre eux si $PGCD(A,B) = 1$.

Proposition. A et B sont premiers entre eux si et seulement si $\exists U, V \in \mathbb{K}[X]$ tel que $AU + BV = 1$ (condition de Bézout).

Démonstration. A et B sont premiers entre eux : $\Leftrightarrow PGCD(A,B) = 1 \Leftrightarrow A\mathbb{K}[X] + B\mathbb{K}[X] = \mathbb{K}[X]$
$\Leftrightarrow 1 \in A\mathbb{K}[X] + B\mathbb{K}[X] \Rightarrow$ car $1 \in \mathbb{K}[X] \Leftarrow$ car si $1 \in A\mathbb{K}[X] + B\mathbb{K}[X]$, tous ses multiples y sont aussi. □

9 Lemme de Gauss

Proposition. Soient $A, B, C \in \mathbb{K}[X]$ si $C|AB$ et C et B sont premiers entre eux alors $C|A$ ‘

Démonstration. C et B sont premiers entre eux $\Leftrightarrow \exists U, V$ tel que $1 = CU + BV$
$\Rightarrow A = CUA + ABV \Rightarrow A \in C\mathbb{K}[X]$ Car CUA et ABV appartient à $C\mathbb{K}[X]$. □

Proposition. Soient $A, B \in \mathbb{K}[X]$ non tous deux nuls.

Soit D leur PGCD (unitaire). Soient U_0, V_0 tel que $D = AU_0 + BV_0$

(ceux obtenus par exemple par l'algorithme d'Euclide étendu).

Alors la solution générale $(U, V) \in \mathbb{K}[X]X\mathbb{K}[X]$ de l'équation $AU + BV = D$ est donnée par :

$U = U_0 + \frac{B}{D}S$

$V = V_0 - \frac{A}{D}S$

Démonstration. $D = AU_0 + BV_0 = AU + BV$

$\Rightarrow A(U - U_0) = B(V_0 - V) \Rightarrow \frac{A}{D}(U - U_0) = \frac{B}{D}(V_0 - V)$

Donc $\frac{B}{D}|\frac{A}{D}(U - U_0)$. Mais $\frac{B}{D}$ est premier avec $\frac{A}{D}$ (d'après Bézout)

Donc d'après le lemme de Gauss : $\frac{B}{D}|U - U_0$

On pose : $U - U_0 = \frac{B}{D}S$

i.e. $U = U_0 + \frac{B}{D}S$

On reporte dans : $\frac{A}{D}(U - U_0) = \frac{B}{D}(V_0 - V)$

On obtient : $\frac{A}{D}\frac{B}{D}S = \frac{B}{D}(V_0 - V)$.

L'un au moins des polynômes A, B est différent de 0 (par hypothèse). Quitte à les échanger, on peut supposer que c'est le cas de B : on peut donc simplifier par $\frac{B}{D}$ et on obtient : $V_0 - V = \frac{A}{D}S$, i.e. $V = V_0 - \frac{A}{D}S$. Cela prouve que toute solution (U, V) de $AU + BV = D$ est de la forme $U = U_0 + \frac{B}{D}S$ et $V = V_0 - \frac{A}{D}S$ où $S \in \mathbb{K}[X]$.

Et en fait n'importe quel $S \in \mathbb{K}[X]$ donne une solution (U, V) puisque si $U = U_0 + \frac{B}{D}S$ et $V = V_0 - \frac{A}{D}S$ alors $AU + BV = AU_0 + BV_0 + A\frac{B}{D}S - B\frac{A}{D}S = D$ □

10 Décomposition en éléments simple

Proposition - formule de Taylor pour les polynômes. Soit $P \in \mathbb{K}[X]$, soit $a \in \mathbb{K}$ $P(X + a) = P_a(X)$ est un polynôme

Si $P(X) = c_nX^n + c_{n-1}X^{n-1} + ... + c_1X + c_0$

On obtient : $P(X + a) = c_n(X + a)^n + c_{n-1}(X + a)^{n-1} + ... + c_1(X + a) + c_0$

$= c_nX^n + c'_{n-1}X^{n-1} + ... + c'_1X + c'_0$

La formule de Taylor évite ce calcul et donne directement les coefficients :

$$P(a + X) = \sum_{j \geq 0} \frac{p^{(j)}(a)}{j!}(X - a)^j$$

où $p' = p^{(1)}$... sont les dérivées successives de P, définis par :

$(X^k)' = kX^{k-1}$ et $(X^k)^{(j)} = ... = \frac{k!}{(k-j)!}X^{k-j}$ si $j \leq k$ et 0 si $j > k$

Démonstration. On peut considérer $P(X - a)$ comme un polynôme en $X - a$:

$P(X) = \sum_{k\geq 0} \lambda_k (X-a)^k$

Il s'agit de vérifier que $\lambda_k = \dfrac{p^{(k)}(a)}{k!}$

On sait que, par récurrence, $\forall j \geq 0$ et $\forall k \geq 0$:

$((X-a)^k)^{(j)} = \dfrac{k!}{(k-j)!}(X-a)^{k-j}$ si $j \leq k$

Vrai pour $j=0$: $((X-a)^k)^{(0)} = (X-a)^k = \dfrac{k!}{(k-0)!}(X-a)^{k-0}$

alors $((X-a)^k)^{(j+1)} = \dfrac{k!}{(k-j)!}((X-a)^{k-j})'$

$= \dfrac{k!}{(k-j)!}(k-j)(X-a)^{k-j-1} = \dfrac{k!}{(k-j-1)!}(X-a)^{k-j-1}$ si $j \leq k-1$ et 0 si $j=k$.

Appliquons cela à $P(X)$:

$P(X) = \sum_{k\geq 0} \lambda_k (X-a)^k$

$\Rightarrow p^{(j)}(X) = \sum_{k\geq 0} \lambda_k ((X-a)^k)^{(j)}$

$= \sum_{k\geq j} \lambda_k \dfrac{k!}{(k-j)!}(X-a)^{k-j} = \lambda_j . \dfrac{j!}{0!} + \sum_{k\geq j+1} \lambda_k \dfrac{k!}{(k-j)!}(X-a)^{k-j}$

Et donc :$P^{(j)}(a) = \lambda_j j!$ c'est à dire $\lambda_j = \dfrac{P^{(j)}(a)}{j!}$. C'est bien le coefficient de la formule de Taylor.

□

11 Racines

Définition. Soit $P(X) \in \mathbb{K}[X]$. Soit $a \in \mathbb{K}[X]$. En substituant a à X on obtient un élément de $\mathbb{K}$, qui sert $P(a)$. On dit que a est une **racine** de P si $P(a) = 0$.

Proposition. Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$ Alors : a est racine de P. $\Leftrightarrow X-a | P(X)$

Démonstration. $P(X) = Q(X)(X-a) + R$ où $R = P(a)$ (voir TD). Donc $X-a|P(X) \Leftrightarrow P(a) = 0$ □

Définition. Soient $P \in \mathbb{K}[X], a \in \mathbb{K}$. On dit que a est une racine d'ordre m de P (où $m \in \mathbb{N}^*$) si $(X-a)^m | P(X)$ et $(X-a)^{m+1}$ ne divise pas $P(X)$

I.e $(X-a)^m$ est la plus grand puissance de $X-a$ et divise $P(X)$.

Proposition. Soient $P \in \mathbb{K}[X], a \in \mathbb{K}$ les assertions suivantes sont équivalentes.

1. a est racine d'ordre m de P.
2. $P^{(k)}(a) = 0$ pour $0 \leq k \leq m$ et $P^{(m)}(a) \neq 0$.
3. a est racine de P et racine d'ordre $m-1$ de P' si $m-1 \geq 1$. Et si $m=1$ a est racine de P et n'est pas racine de P'.

Démonstration. Par la formule de Taylor :

$$P(X) = \sum_{k=0}^{m-1} \frac{P^{(k)}(x)}{k!}(X-a)^k + (X-a)^m . \sum_{k\geq 0} \frac{P^{(k)}(a)}{k!}(X-a)^{k-m} = R(X) + (X-a)^m . Q(X)$$

Cela montre que dans la division euclidienne de $P(X)$ par $(X-a)$, le quotient est $Q(X)$ et le reste est $R(X)$.
Donc $(X-a)^m|P(X) \Leftrightarrow R(X)=0$
$\Leftrightarrow P^{(k)}(a)=0, 0\leq k\leq m-1$
Donc : $((X-a)^m|P(X)$et $(X-a)^{m+1}$ ne divise pas $P(X))$
$\Leftrightarrow (P^{(k)}(a)=0, \leq k\leq m-1$ et $P^{(m)}(a)\neq 0)$. Cela prouve que (1) $\Leftrightarrow$ (2)
Enfin il est clair que (2) $\Leftrightarrow$ (3). Puisque (3) $\Leftrightarrow P(a)=0$ et $(P')^{(k)}(a)=0 \Leftrightarrow P^{(k+1)}(a)=0, 0\leq k\leq m-2$ et $(P')^{m-1}(a)\neq 0$
$\Leftrightarrow P^{(k)}(a)=0, 0\leq k\leq m-1$ et $P^{(m)}(a)\neq 0$. □

12 Réduction de polynômes

Définition. On dit qu'un polynôme $A\in\mathbb{K}[X]$ **non constant** est irréductible (sur $\mathbb{K}$) s'il n'existe pas de décomposition $A=BC$ avec $deg(B)<deg(A)$ et $deg(C)<deg(A)$
$A=BC$ avec $deg(B)<deg(A)$ et $deg(C)<deg(A)$
$\Leftrightarrow A=BC$ avec $0<deg(B)<deg(A)$
$\Leftrightarrow A=BC$ avec $0<deg(C)<deg(A)$

Exemple. Tout polynôme de degré 1 est irréductible. En effet, on peut l'écrire $A(X)=cd(A)(X-a)$ et il est clair qu'on ne peut pas avoir $A=BC$ avec $deg(B)<1$ et $deg(C)<1$ car on avait $B=cte$ et $C=cte$ donc $A=cte$.

$X^2+1\in\in\mathbb{R}[X]$ est irréductible sur $\mathbb{R}$. En effet, si on avait $X^2+1=B(X)C(X)$ où $deg(B)<2$ et $deg(C)<2$.
Donc $0<deg(B)<2$ et $0<deg(C)<2$ (puisque $deg(B)+deg(C)=2$) donc $deg(B)=deg(C)=1$
On pourrait donc écrire : $X^2+1=\lambda(X-a).\mu(X-b)$ avec $\lambda\mu=1$ donc
$X^2+1=(X-a)(X-b)$
Et a,b seraient des racines (réelles) de X^2+1 **impossible !** Mais X^2+1 n'est pas irréductible sur $\mathbb{C}$ puisque $(X^2+1)=(X-i)(X+i)$

X^4+1 n'est pas irréductible sur $\mathbb{R}$ (bien que sans racine réelle...) car : $X^4+1=(X^2+1)^2-2X^2=(X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1)$ Les deux polynômes sont irréductibles sur $\mathbb{R}$.

Lemme. Si $P\in\mathbb{K}[X]$ est irréductible (sur $\mathbb{K}$) et ne divise pas $A\in\mathbb{K}[X]$, alors P est premier avec A.

Démonstration. Soit $D=PGCD(P,A), D|P$ et P est irréductible donc on n'a pas $0<deg(D)<deg(P)$
Donc $deg(D)=0$ ou $deg(D)=deg(P)$ donc $D=1$ puisque D est unitaire et $P=kD$ puisque $D|P$ exclu car P serait un PGCD de P et A et donc P diviserait A. Donc $D=1$, i.e. P et A sont premiers entre eux. □

Proposition, lemme d'Euclide. Si $P\in\mathbb{K}[X]$ est irréductible et $P|AB$ et P ne divise pas A alors $P|B$.

Démonstration. P est irréductible et P ne divise pas A donc (lemme précédent) P est premier avec A donc (Gauss) $P|B$.
Faux si P n'est pas irréductible. Par exemple : $(X-1)(X-2)|(X-1)^2(X-2)(X-3)$ et $(X-1)(X-2)$ ne

divis pas $(X-1)^2$

Mais $(X-1)(X-2)$ ne divise pas $(X-2)(X-3)$. □

13 Arithmétique des polynômes

Théorème fondamental de l'arithmétique des polynômes. Tout polynôme $A \in \mathbb{K}[X]$ non nul s'écrit d'une façon unique sous la forme :

$$A = cd(A) \prod_{P \in \Im} P^{v_P(A)}$$

$\Im$ est l'ensemble des polynômes irréductibles unitaires de $\mathbb{K}[X], \forall P \in \Im, v_P(A) \in \mathbb{N}$, et $P \in \Im, v_{p(A)} \neq 0$ est fini (donc le produit $\prod_{P \in \Im} P^{v_P(A)}$ est en fait un produit fini.)

C'est la décomposition de A en facteurs irréductibles dans $\mathbb{K}[X]$. $v_p(A)$ s'appelle la **valuation** de A en P.

Démonstration.

Existence. $\frac{A}{cd(A)}$ est un polynôme unitaire non nul. S'il est irréductible, c'est terminé : $\frac{A}{cd(A)} = P_0 \in \Im = \prod_{P \in \Im} P^{v_P(A)}$ où $v_P(A) = 1$si $P = P_0$ et 0 si $P \neq P_0$.

Si $\frac{A}{cd(A)}$ n'est ni constant ni irréductible, on peut l'écrire : $\frac{A}{cd(A)} = BC$ avec B, C unitaires tel que $deg(B) < deg(A), deg(C) < deg(A)$.

On raisonne par récurrence, on peut supposer que :

$B = \prod_{P \in \Im} P^{v_P(B)}, C = \prod_{P \in \Im} P^{v_P(C)}$.

Un polynôme de degré 1 est irréductible donc le théorème s'y applique : ce qui amorce la récurrence.

On a donc : $\frac{A}{cd(A)} = BC = \prod_{P \in \Im} P^{v_p(B)} P^{v_p(C)}$ et la décomposition existe, avec $v_p(A) = v_p(B) + v_p(C)$.

Unicité. Supposons que $\prod_{P \in \Im} P^{n_P} = \prod_{P \in \Im} P^{m_P}$ avec $m_P, n_P \in \mathbb{N}$ (nuls sauf un nombre fini d'entre eux).

Il s'agit de montrer que $n_P = m_P, \forall P \in \Im$. Supposons que ce ne soit pas le cas : il existe $P_0 \in \Im$ tel que $n_{P_0} \neq m_{P_0}$. Quitte à échanger les notations n_P, m_P, on peut supposer que $n_{p_0} > m_{p_0}$. Alors :

$P_0^{n_{P_0}} \prod_{P \in \Im} P^{n_P} = P_0^{m_{P_0}} \prod_{P \in \Im} P^{m_P}$.

i.e. $P_0^{n_{P_0} - m_{P_0}} \prod_{P \in \Im} P^{n_P} = \prod_{P \in \Im} P^{m_P}$.

où $n_{P_0} - m_{P_0} > 0$ donc P_0 divise le premier membre de l'égalité. Mais il ne divise pas le second membre, car sinon, d'après le lemme d'Euclide, il diviserait l'un des facteurs $P \in \Im / \{P_0\}$, ce qui est impossible puisque P_0 et P sont irréductibles, unitaire et distincts. ($[P_0 | P$ et P irréductible$] \Rightarrow P = kP_0$ où $k \in \mathbb{K}$ et alors $[P_0, P$ unitaire$] \Rightarrow k = 1$, et donc $P = P_0 \notin \Im / \{P_0\}$. On a donc une contradiction d'où l'unité.

□

Corollaire. Soient $A, B \in \mathbb{K}[X]$ non constants. Donc : $A = cd(A) \prod_{P \in \Im} P^{v_p(A)}, B = cd(B) \prod_{P \in \Im} P^{v_P(B)}$ Alors :

1. $A|B \Leftrightarrow v_P(A) \leq v_P(B), \forall P \in \Im$.

2. $PGCD(A,B) = \prod_{P\in\Im} p^{min(v_P(A),v_P(B))}$.
3. $PPCM(A,B) = \prod_{P\in\Im} p^{max(v_P(A),v_P(B))}$.
4. $PGCD(A,B)PPCM(A,B) = \dfrac{AB}{cd(A)cd(B)}$.

Démonstration. 1. $A|B \Leftrightarrow \exists Q \in \mathbb{K}$ tel que $B = AQ (Q \neq 0$ car $B \neq 0)$

i.e. tel que $\prod_{P\in\Im} P^{v_P(B)} = \prod_{P\in\Im} P^{v_P(A)} \prod_{P\in\Im} P^{v_P(Q)}$.

i.e. tel que $\forall P \in \Im, v_P(B) = v_P(A) + v_P(Q)$.

i.e. que $v_P(B) \geq v_P(A) \forall P \in \Im$.

Réciproque si $v_P(B) \geq v_P(A) \forall P \in \Im$ on peut écrire $v_P(B) = v_P(A) + n_P$ avec $n_P \in \mathbb{N}$ (nul, comme $v_p(A), v_p(B)$, sauf pour un nombre fini de P) et on peut poser $Q = \prod_{P\in\Im} P^{n_P}$, donc $n_P = v_P(Q)$ et on remonte les équivalences précédentes jusqu'à $B = AQ$.

2. $D = PGCD(A,B)$ est le plus grand diviseur (unitaire) de A et B :

$\forall P \in \Im : v_P(D) \leq v_P(A)$ et $v_P(D) \leq v_P(B)$ car $D|A$ et $D|B$

donc :$\forall P \in \Im, v_P(D) \leq min(v_P(A), v_P(B))$.

Et il faut le plus grand D vérifiant cela.

Donc $v_P(D) = min(v_P(A), v_P(B))$.

3. $M = PPCM(A,B)$ est le plus petit multiple de A, B (avec $v_P(M)$ minimal : donc $v_P(M) = max(v_P(a), v_P(B))$)

i.e $\forall P \in \Im, v_P(M) \geq v_P(A)$ et $v_P(M) \geq V_p(B)$

i.e. $\forall P \in \Im, v_p(M) \geq max(v_P(A), v_P(B))$

4. $PGCD(A,B)PPCM(A,B) = \prod_{P\in\Im} P^{min(v_P(A),v_P(B))+max(v_P(A),v_P(B))}$

$= \prod_{P\in\Im} P^{v_P(A)+v_P(B)} = \prod_{P\in\Im} P^{v_P(A)} \prod_{P\in\Im} P^{v_P(B)} = \dfrac{A}{cd(A)} . \dfrac{B}{cd(B)}$.

□

Autre corollaire du théorème. Soit $A \in \mathbb{K}[X]$ non nul.

$A = cd(A). \prod_{P\in\Im} P^{v_P(A)} \prod_{P\in\Im} P^{v_P(A)} = \prod (X - a_i)^{m_i} Q$

$\prod_{P\in\Im} P^{v_P(A)}, degP = 1$ et $\prod_{P\in\Im} P^{v_P(A)} = Q, degP > 1$

Où les a_i sont les racines de A et $m_i = v_{X-a}(A)$ leurs multiplicités. Et Q est un polynôme sous racines dans $\mathbb{K}$

En particulier :

$$\sum m_i \leq deg(A)$$

"La somme des multiplicités des racines d'un polynômes est inférieur au degrés de ce polynôme".

Théorème de d'Alembert.

1. Dans $\mathbb{C}[X]$ les polynômes unitaires irréductibles sont les $X-a, a\in\mathbb{C}$. Donc tout polynômes $A\in\mathbb{C}[X]$ non constant s'écrit : $A(X)=cd(A).\prod_{P\in\Im}(X-a_i)^{m_i}$. En particulier , il a $deg(A)$ racines (comptées avec leur multiplicité $\sum m_i=deg(A)$).
2. Dans $\mathbb{R}[X]$ les polynômes sont unitaires sont les $X-a$ où $a\in\mathbb{R}$ et les X^2+bX+c où $b,c\in\mathbb{R}$ avec $b^2-4c<0$. Donc tout $A\in\mathbb{R}[X]$ non constant s'écrit : $A(X)=cd(A)\prod_{P\in\Im}(X-a_i)^{m_i}.\prod_{P\in\Im}(X^2+b_jX+c_j)^{n_i}$.

Démonstration. 1. (Dans $\mathbb{C}$) : admis (hors programme)

2. (Dans $\mathbb{R}$) : Soit $A(X)\in\mathbb{R}[X]\subset\mathbb{C}[X]$,de degré$\geq 1$
On peut appliquer le (1).
Dans $\mathbb{C}[X]A(X)=cd(A)\prod(X-a_i)^m, a_i\in\mathbb{C}$
Donc :$A(X)=cd(A)\prod(X-a_i)^{m_i}.\prod(X-a_j)^{m_j}$
Mais comme $A(X)\in\mathbb{R}[X]$, si z est une racine complexe de A, $\overline{z}$ en est une aussi, avec la même multiplicité. En effet :
$A(X)=c_NX^N+...+c_1X+c_0, c_k\in\mathbb{R}$
$A(Z)=0\Leftrightarrow c_Nz^N+...+c_1z+c_0=0$
$\Leftrightarrow \overline{c_N}\overline{z}^N+...+\overline{c_1}+\overline{z}+\overline{c_0}=0$
$\Leftrightarrow c_N\overline{z}^N+...+c_1\overline{z}+c_0=0(c_krels)$
$\Leftrightarrow A(\overline{z})=0$
De même $A^{(j)}(z)=0,(0\leq j\leq m-1)\Leftrightarrow A^{(j)}(\overline{z})=0$ et $A^{(m)}(z)\neq 0\Leftrightarrow A^{(m)}(\overline{z})\neq 0$
Cela justifie que : z est racine de A de multiplicité m si et seulement si $\overline{z}$ est racine de A de multiplicité m
Donc, dans $\prod(X-a_j)^{m_j}$ les sommes peuvent se regrouper par paires de conjuguées de même multiplicités.
$\prod(X-z_j)^{m_j}(X-\overline{z}_j)^{m_j}$
$=\prod[(X-z_j)(X-\overline{z}_j)]^{m_j}$
$\prod[x^2-(2\Re(z_j))X+|z_j|^2]^{m_j}$
$=\prod(X^2+b_j.X+c_j)^{m_j}$
où $b_j=-2\Re(z_j)\in\mathbb{R}, c_j=|z_j|^2\in\mathbb{R}$, et $b_j^2-4c_j<0$ puisque les racines $z_j,\overline{z}_j$ ne sont pas réelle.

□

Exemples typiques. **(voir correction des ds et des dst)** X^m-1 et X^m+1, il faut distinguer les cas : n pair et n impair.

Le cas pair. — $X^{2m}-1=(X-1)(X+1)\prod_{k=1}^{m-1}(X-e^{i\pi\frac{k}{m}})(X-e^{-i\pi\frac{k}{m}})$ dans $\mathbb{C}[X]$
— $X^{2m}-1=(X-1)(X+1)\prod_{k=1}^{m-1}(X^2-2cos(\frac{\pi k}{m})X+1)\text{dans}\mathbb{R}[X]$
— $X^{2m}+1=\prod_{k=0}^{m-1}(X-e^{i\pi\frac{2k+1}{2m}})(X-e^{-i\pi\frac{2k+1}{2m}}),\text{dans}\mathbb{C}[X].$
— $X^{2m}+1=\prod_{k=0}^{m-1}X^2-2cos(\frac{2k+1}{2m}\pi)X+1),\text{dans}\mathbb{R}[X]$

Preuve. Sur le cercle trigonométrique $z^{2m}=1=e^{2\pi ik}\Leftrightarrow z=e^{\frac{\pi ik}{m}}=e^{i\pi\frac{k}{m}},k\in\mathbb{Z}$

$X^{2m}+1=$facteurs complexes.
$z^{2m}=-1=e^{i\pi+2ki\pi}=e^{(2k+1)i\pi}\Rightarrow z=e^{\frac{(2k+1)i\pi}{2m}},k\in\mathbb{Z}$

Exemple. $m=1: X^2+1=(X-e^{i\frac{\pi}{2}})(X-e^{-i\frac{\pi}{2}})=(X-i)(X+i)$ dans $\mathbb{C}[X]$
$=X^2+1$ (irréductible) dans $\mathbb{R}[X]$
$m=2: X^4+1=(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)$ dans $\mathbb{R}[X]$

Le cas impair. — $X^{2m+1}-1=(X-1)\prod_{k=1}^{m}(X-e^{\frac{2\pi ik}{2m+1}})(X-e^{-\frac{2\pi ik}{2m+1}})\text{dans}\mathbb{C}[X]$

— $X^{2m+1}-1=(X-1)\prod_{k=1}^{m}(X^2-2cos(\frac{2\pi k}{2m+1})X+1)\text{dans}\mathbb{R}[X]$

— $X^{2m+1}+1=(X+1)\prod_{k=0}^{m-1}(X-e^{i\pi\frac{2k+1}{2m+1}})(X-e^{-i\pi\frac{2k+1}{2m+1}}),\text{dans}\mathbb{C}[X]$

— $X^{2m+1}+1=(X+1)\prod_{k=0}^{m-1}(X^2-2cos(\frac{2k+1}{2m+1}\pi)X+1),\text{dans }\mathbb{R}[X]$

Preuve. $X^{2m+1}-1=(X-1).$facteurs non réels

$z^{2m+1}=1=e^{2\pi ik}\Leftrightarrow z=e^{\frac{2\pi ik}{2m+1}},k\in\mathbb{Z}$

$X^{2m+1}+1=(X+1).$facteurs non réels

$z^{2m+1}=-1=e^{(2k+1)i\pi}\Leftrightarrow z=e^{\frac{(2k+1)i\pi}{2m+1}},k\in\mathbb{Z}$

14 Formules de Viète

Pour terminer ce chapitre sur les polynômes, voici les formules de Viète qui expriment les coefficients d'un polynômes en fonction de ses racines.

Théorème. Soit $A\in\mathbb{K}[X]$ est un polynômes de degré $n\geq 1$. On suppose qu'il est scindé dans $\mathbb{K}[X]$, c'est à dire que

$$A(X)=cd(A)\prod_{i=1}^{n}(X-x_i),x_i\in\mathbb{K}$$

Écrivons :$A(X)=a_nX^n+a_{n-1}X^{n-1}+...+a_1X+a_0$ Alors :

$-\frac{a_{n-1}}{a_n}=\sum_{i=1}^{n}x_i$

$+\frac{a_{n-2}}{a_n}=\sum_{1\leq i\leq j\leq n}^{n}x_ix_j$

$-\frac{a_{n-3}}{a_n}=\sum_{1\leq i\leq j\leq k\leq n}^{n}x_ix_jx_k$

$(-1)^n\frac{a_0}{a_n}=x_1...x_n$

Démonstration. Comme dans l'exemple, on écrit :

$A(X)=a_nX^n+a_{n-1}X^{n-1}+...+a_1X+a_0$

$=a_n(X-x_1)(X-x_2)...(X-x_n)$

$=a_n[X^n-(x_1+...+x_n)X^{n-1}+(\sum_{1\leq i\leq j\leq n}x_ix_j)X^{n-2}+...+(-1)^nx_1...x_n$ □

Deuxième partie

Fractions rationnelles

15 Définitions et généralités

C'est un quotient de polynômes : $R(X) = \dfrac{A(X)}{B(X)}$. Mais il faut définir cette notion (car il n'y a pas de division dans $\mathbb{K}$)

Définition (informelle). Si $A, B, C, D \in \mathbb{K}$ avec $B \neq 0, D \neq 0$, on dit que les objets $\dfrac{A(X)}{B(X)}$ et $\dfrac{C(X)}{D(X)}$ sont égaux si et seulement si on a :$A(X)D(X) - B(X)C(X) = 0$
Cela définit ces objets qu'on appelle **fractions rationnelles**.

Définition (formelle). Les fractions sont les classes d'équivalences dans $\mathbb{K}[X].\mathbb{K}[X]^*$ pour la relation d'équivalence $(A, B) \sim (C, D) \Leftrightarrow AD - CB = 0$. On note $\dfrac{A}{B}$ la classe d'équivalence de A, B

On note $\mathbb{K}[X]$ l'ensemble des fractions rationnelles sur $\mathbb{K}$. On identifie le polynômes $A \in \mathbb{K}$ avec la fraction $\dfrac{A}{1}$. (On va avoir que les opérations dans $\mathbb{K}[X]$ sur les A compatibles avec les opérations à définir dans $\mathbb{K}[X]$ sur les $\dfrac{A}{1}$)
Donc $\mathbb{K}[X] \subset \mathbb{K}[X]$

Nota Bene. $\dfrac{A}{1} = \dfrac{B}{1} \Leftrightarrow A1 - B1 = 0 \Leftrightarrow A = B$ donc $A \to \dfrac{A}{1}$ est injective.

Définition : Additions dans $\mathbb{K}[X]$.

$$\frac{A}{B} + \frac{C}{D} \overset{def}{=} \frac{AD + BC}{BD}$$

Démonstration. Si $\dfrac{A}{B} = \dfrac{A'}{B'}$ et $\dfrac{C}{D} = \dfrac{C'}{D'}$, a t'on $\dfrac{A'D' + B'C'}{B'D'} = \dfrac{AD + BC}{BD}$?
Autrement dit , a-t-on : $\dfrac{A}{B} + \dfrac{C}{D} = \dfrac{A'}{B'} + \dfrac{C'}{D'}$?
Autrement dit : la somme des fonction est elle bien indépendante du terme $\dfrac{A}{B}$ ou $\dfrac{A'}{B'}$,$\dfrac{C}{D}$ ou $\dfrac{C'}{D'}$ La réponse est oui car :
$\dfrac{A}{B} = \dfrac{A'}{B'} \Leftrightarrow AB' = A'B$
$\dfrac{C}{D} = \dfrac{C'}{D'} \Leftrightarrow CD' = C'D$
Et alors $\dfrac{A'}{B'} + \dfrac{C'}{D'} = \dfrac{A}{B} + \dfrac{C}{D} \Leftrightarrow \dfrac{A'D' + B'C'}{B'D'} = \dfrac{AD + BC}{BD}$
$\Leftrightarrow (A'D' + B'C')BD = (AD + BC)B'D' \Leftrightarrow A'D'BD + B'C'BD = ADB'D' + BCB'D'$
$\Leftrightarrow AB'D'D + CD'BB' = AB'DD' + CD'BB'$ □

Définition : Produit dans $\mathbb{K}[X]$.

$$\frac{A}{B}\frac{C}{D} \overset{def}{=} \frac{AC}{BD} \text{Avec} C \neq 0$$

Démonstration. Si $\frac{A}{B}=\frac{A'}{B'}$ et $\frac{C}{D}=\frac{C'}{D'}$, a-t-on $\frac{AC}{BD}=\frac{A'B'}{B'D'}$?
Oui car : $\frac{AC}{BD}=\frac{A'C'}{B'D'}\Leftrightarrow ACB'D'=A'C'BD$ or $\frac{A}{B}=\frac{A'}{B'}\Leftrightarrow AB'=BA'$
$\frac{C}{D}=\frac{C'}{D'}\Leftrightarrow CD'=C'D$
Donc $\frac{AC}{BD}=\frac{A'C'}{B'D'}\Leftrightarrow AB'C'D=AB'C'D$ □

Remarques : Compatibilité avec l'identification $A=\frac{A}{1}$. $\frac{A}{1}+\frac{B}{1}=\frac{A1+B1}{1}=\frac{A+B}{1}$
et $\frac{A}{1}\frac{B}{1}=\frac{AB}{1}=AB$

Définition (division ou quotient dans $\mathbb{K}[X]$).

$$\frac{\frac{A}{B}}{\frac{C}{D}}\overset{def}{=}\frac{AD}{BC}$$

Démonstration. Si $\frac{A}{B}=\frac{A'}{B'}$ et $\frac{C}{D}=\frac{C'}{D'}$ autrement dit si $AB'=A'B$ et $CD'=C'D$
alors $\frac{\frac{A'}{B'}}{\frac{C'}{D'}}=\frac{\frac{A}{B}}{\frac{C}{D}}\Leftrightarrow\frac{A'B'}{B'C'}=\frac{AD}{BC}\Leftrightarrow A'D'BC=ADB'C'\Leftrightarrow A'BDC'=A'BDC'$ □

Remarque : Compatibilité avec l'identification $A=\frac{A}{1}$. $\frac{\frac{A}{1}}{\frac{C}{1}}=\frac{A.1}{C.1}=\frac{A}{C}$

Proposition. $(\mathbb{K}(X),+,X)$ est un anneau unitaire, intègre et commutatif (comme $(\mathbb{K}[X],+,X)$). Et ainsi $(\mathbb{K}(X),+,X)$ est un **corps commutatif**.
Ainsi $\mathbb{K}(X)$ est le corps des quotients de $\mathbb{K}[X]$

Définition. Degré d'une fraction rationnelle : soient $A,B\in\mathbb{K}[X],B\neq 0$. On a $deg(\frac{A}{B})=deg(A)-deg(B)$

Corollaire. Si $\frac{A}{B}=\frac{A'}{B'}$, alors$AB'=A'B$ donc $deg(AB')=deg(A'B)$ donc $deg(A)+deg(B')=deg(A')+deg(B)$, donc $deg(A')-deg(B')=deg(A)-deg(B)$ et donc $deg(\frac{A'}{B'})=deg(\frac{A}{B})$

Proposition. Soient $F,F'\in\mathbb{K}(X)$

1. $deg(FF')=deg(F)+deg(F')$
2. $deg(F+F')\leq max\{deg(F),deg(F')\}$

Démonstration. 1. $F=\frac{A}{B},F'=\frac{A'}{B'}$: $deg(FF')=deg(\frac{AA'}{BB'})=deg(AA')-deg(BB')=deg(A)+deg(A')-deg(B')-deg(B)=deg(A)-deg(B)+deg(A')-deg(B')=deg(F)+deg(F')$

2. De même $deg(F+F') = deg(\frac{A}{B}+\frac{A'}{B'}) = deg(\frac{AB'+A'B}{BB'})$
$= deg(AB'+A'B) - deg(BB') \leq max\{deg(AB'), deg(A'B)\} - deg(B) - deg(B') \leq max\{deg(F), deg(F')\}$

□

16 Théorème de décomposition des fonctions rationnelles en éléments simples

Maintenant on peut se diriger vers le théorème de décomposition des fonctions rationnelles en éléments simples.

Lemme 1. Soit $F \in \mathbb{K}(X)$. Il existe un **unique** polynôme $E \in \mathbb{K}[X]$(appelé partie entière de F) et une **unique** fonction $R \in \mathbb{K}(X)$ tel que$F = E + R$ et $deg(R) < 0$

Démonstration. Posons $F = \frac{A}{B}$ où $A, B \in \mathbb{K}[X], B \neq 0$ □

Existence. Division euclidienne de A par B : $A = QB + S, deg(S) < deg(B)$
Donc $F = \frac{A}{B} = Q + \frac{S}{B}$ où $deg(\frac{S}{B}) = deg(S) - deg(B) < 0$ Donc on peut prendre $E = Q$ et $R = \frac{S}{B}$
Unicité. Si $F = E + R = E' + R'$ où $E, E' \in \mathbb{K}[X], deg(R) < 0, deg(R') < 0$
alors $E - E' = R' - R$ d'où$deg(E - E') = deg(R' - R) \leq max(deg(R'), deg(-R)) < 0$

Lemme 2. Soit $F = \frac{A}{B_1 B_2} \in \mathbb{K}(X)$ avec $deg(F) < 0 (A, B_1, B_2 \in \mathbb{K}(X))$
Il existe une **unique** décomposition tel que $F = \frac{A_1}{B_1} + \frac{A_2}{B_2}$ avec $deg(\frac{A_1}{B_1}) < 0$et $deg(\frac{A_2}{B_2} < 0$ avec $(A_1, A_2 \in \mathbb{K}[X])$.

Démonstration. **Existence.** Bézout $\Rightarrow \exists U_1, U_2 \in \mathbb{K}[X]$ tel que $U_1 B_1 + U_2 B_2 = 1$
Alors $\frac{A}{B_1 B_2} = \frac{A(U_1 B_1 + U_2 B_2)}{B_1 B_2} = \frac{AU_2}{B1} + \frac{AU_1}{B_2}$
Rien ne garantit que $deg(\frac{AU_2}{B_1}) < 0$ (i.e. que $deg(AU_2) < deg(B_1)$)
Faisons la division euclidienne :
$AU_2 = QB_1 + R_1, deg(R_1) < deg(B_1)$. Alors : $\frac{A}{B_1 B_2} = \frac{AU_2}{B_1} + \frac{AU_1}{B_2} = \frac{R_1}{B_1} + Q + \frac{AU_1}{B_2} = \frac{R_1}{B_1} + \frac{R_2}{B_2}$ où $R_2 = AU_1 + Q.R_2$
et $deg(\frac{R_1}{B_1}) < 0$ et $deg(\frac{R_2}{B_2} = deg(F - \frac{R_1}{B_1}) \leq max(deg(F), deg(\frac{-R_1}{B_1})) < 0$.
On peut donc prendre $A_1 = R_1, A_2 = R_2$.

Unicité. Supposons que $F = \frac{A_1}{B_1} + \frac{A_2}{B_2} = \frac{A'_1}{B_1} + \frac{A'_2}{B_2}$ avec $\begin{cases} deg(A_i) < deg(B_i) \\ deg(A'_i) < deg(B'_i) \end{cases}$
$\frac{A_1 - A'_1}{B_1} = \frac{A'_2 - A_2}{B_2} \Rightarrow (A_1 - A'_1)B_2 = (A'_2 - a_2)B_1$ (égalité dans $\mathbb{K}[X]$) Mais B_1, B_2 sont premier entre eux donc (Gauss) $B_1 | A_1 - A'_1$ et donc :$A_1 - A'_1 = QB_1$ d'où $deg(A_1 - A'_1) = deg(Q) + deg(B_1)$
Or par hypothèse : $deg(A_1 - A'_1) \leq max\{deg(A), deg(A'_1)\} < deg(B_1)$
On a donc $deg(A_1 - A'_1) = deg(Q) + deg(B_1) < deg(B_1)$ donc $deg(Q) < 0$, donc $Q = 0$ et donc $A_1 - A'_1 = 0$.
Et donc $\frac{A'_2 - A_2}{B_2} = \frac{A_1 - A'_1}{B_1} = 0$ d'où l'unité $(A'_1 = A_1, A'_2 = A_2)$

□

.

Lemme 3. Soit $F = \frac{A}{B^n}(A, B \in \mathbb{K}[X], n \in \mathbb{N}^*)$,avec $deg(F) < 0$. Il **existe** une décomposition **unique** de la forme :
$F = \sum_{j=1}^{n} \frac{A_j}{B^j}$ où $A_j \in \mathbb{K}[X], deg(A_j) < deg(B)$

Preuve par récurrence sur n.

Initialisation. Si n=1 : $F = \frac{A}{B}$ avec $deg(F) < 0$ donc $deg(A) < deg(B)$: on a $A_1 = a$ et il y a évidemment unicité :
$\frac{A'_1}{B} = F \Rightarrow \frac{A'_1}{B} = \frac{A}{B} \Rightarrow A'_1 = A = A_1$

Hérédité. Supposons le résultat (existence et unicité) acquis pour n. Montrons qu'il subsiste pour n+1.
Soit donc $F = \frac{A}{B^{n+1}}, deg(F) < 0$. Faisons la division euclidienne $A = BQ + R, deg(R) < deg(B)$ donc $F = \frac{R}{B^{n+1}} + \frac{Q}{B^n}$ où $deg(R) < deg(B)$.
Et cette décomposition est unique car $F = \frac{R'}{B^{n+1}} + \frac{Q'}{B^n} = \frac{R' + Q'B}{B^{n+1}} \Rightarrow R' + Q'B = A$ et la condition $deg(R') < deg(B)$ implique R' est la reste de la division euclidienne de A par B et Q' le quotient (unicité de la division euclidienne). On a donc, d'une façon unique : $F = \frac{R}{B^{n+1}} + \frac{Q}{B^n}$ avec $deg(R) < deg(B)$.
Noter que $deg(\frac{Q}{B^n}) = deg(F - \frac{R}{B^{n+1}}) < 0$.
Or l'hypothèse de récurrence garantit l'existence et l'unicité de la décomposition $\frac{Q}{B^n} = \sum_{j=1}^{n} \frac{Q_j}{B^j}$ où $Q_j \in \mathbb{K}[X, deg(Q_j) < deg(B)$.
On a donc bien la décomposition unique : $F = \sum_{j=1}^{n+1} \frac{A_j}{B^j}$ avec $A_j = Q_j (1 \leq j \leq n)$ et $A_{n+1} = R$

Théorème de décomposition en éléments simples dans $\mathbb{K}(X)$. Soit $F \in \mathbb{K}(X)$: $F = \frac{A}{B}$ où $A, B \in \mathbb{K}[X], B \neq 0$

Il **existe** une **unique** décomposition :
$F = E + \sum_{i=1}^{n} \sum_{j=1}^{n_i} \frac{A_{ij}}{P_i^j}$ où $B = cd(B) \prod_{i=1}^{n} P_i^{n_i}$ est la décomposition de B en facteurs irréductible unitaire.
Et $A_j \in \mathbb{K}[X], deg(A_{ij}) < deg(P_i), (1 \leq j \leq n_i)$ et $E \in \mathbb{K}[X]$ (partie entière de F).

Démonstration. On applique les lemme 1,2,3 :

Le lemme 1 donc E (quotient de la division euclidienne de A par B). Le lemme donne ensuite une décomposition de F-E sous la forme $\sum_{i=1}^{n} \frac{A'_i}{P_i^{n_i}}$ et le lemme 3 décompose chacune de ces fonctions comme dans le théorème. □

Corollaire dans $\mathbb{C}$. Soit $F = \frac{A}{B} \in \mathbb{C}(X), B = cd(B) \prod_{i=1}^{n} (X - a_i)^{n_i}$ (Décomposition de B en facteurs irréductible unitaire cf le théorème de d'Alembert).
Alors il existe une unique décomposition : $F = \sum_{i=1}^{n} \sum_{j=1}^{n_i} \frac{\lambda_j}{(X-a)^j}$ où $\lambda j \in \mathbb{C}$

Démonstration. En effet, a priori (théorème ci dessus) $\lambda_{ij} \in \mathbb{C}[X]$, mais $deg(\lambda_{ij}) < deg(X - a_i)$ donc au fait les λ_{ij} sont des constantes. □

Corollaire dans $\mathbb{R}$. Soit $F = \dfrac{A}{B} \in \mathbb{R}(X), B = cd(B) \prod_{i=1}^{n}(X-a_i)^{n_i} \prod_{k=1}^{m}(X^2+b_kX+c_k)^{m_k}$
La décomposition de B est en fait irréductible unitaire dans $\mathbb{R}[X]$. Alors il existe une unique décomposition : $F = \sum_{i=1}^{n}\sum_{j=1}^{n_i} \dfrac{\lambda_{ij}}{(X-a)^j}$

17 Partie polaire

Définition de la partie polaire. Soit $F = \dfrac{A}{B} \in \mathbb{K}[X], a \in \mathbb{K}$ est une racine de B (qui ne soit pas racine de A), d'ordre m dit que a est un **pôle** de F d'ordre m. Alors la décomposition en éléments plus simples de F s'écrit :
$F(x) = \sum_{j=1}^{m} \dfrac{a_j}{(X-a)^j} + R(X)$ où $R(X) \in \mathbb{K}[X]$ est une fraction dont a n'est pas un pôle, la somme $\sum_{j=1}^{m} \dfrac{a_j}{(X-a)^j}$ est la partie polaire relative au pôle a de la décomposition de F en éléments simples.

Exemple. $F(X) = \dfrac{1}{X(X+1)} = \dfrac{1}{X} - \dfrac{1}{X+1}$. On $\dfrac{1}{X}$ partie polaire relative au pôle 0 et $\dfrac{1}{X+1}$ la partie polaire relative au pôle -1.

Proposition. Soient $F \in \mathbb{K}(X), a \in \mathbb{K}$ un pôle de F d'ordre m :
$F(X) = \sum_{j=1}^{m} \dfrac{a_j}{(X-a)^j} + R(X)$ Alors : $a_j = \dfrac{1}{(m-j)!}\dfrac{d^{m-j}}{dX^{m-j}}((X-a)^m F(X))$

Démonstration. $(X-a)^m F(X) = \sum_{j=1}^{m} a_j(X-a)^{m-j} + (X-a)^m R(X)$.

Dérivons $m-j$ fois $(X-a)^m R(X)$ (Leibniz) :

$\dfrac{d^{m-j}}{dX^{m-j}}((X-a)^m R(X)) = \sum_{p=0}^{m-j} \binom{m-j}{v}((X-a)^m)^{(p)} R^{(m-j-p)}(X) = \sum_{p=0}^{m-j} \dfrac{m!}{(m-p)!}(X-a)^{m-p}$.

Or $1 \le m-j \le m-1 \Rightarrow m-p \ge 1$,donc $\dfrac{d^{m-j}}{dX^{m-j}}((X-a)^m R(X))|_{X=a} = 0$.

Et donc $\dfrac{1}{(m-j)!}(\dfrac{d}{dX})^{m-j}((X-a)^m F(X))|_{X=a} = \dfrac{1}{(m-j)!}(\dfrac{d}{dX})^{m-j}(\sum_{k=1}^{m} a_k(X-a)^{m-k})|_{X=a} = a_j$(Taylor).

□

Exemple. $F(X) = \dfrac{1}{X^2(X-1)^3} = \dfrac{a}{X^2} + \dfrac{b}{X} + \dfrac{c}{(X-1)^3} + \dfrac{d}{(X-1)^2} + \dfrac{e}{X-1}$
$a = X^2F(X)|_{X=0} = \dfrac{1}{(X-1)^3}|_{X=0} = -1$
$b = \dfrac{1}{1!}\dfrac{d}{dX}(X^2F(X))|_{X=0} = (\dfrac{1}{(X-1)^3})'|_{X=0} = -\dfrac{3}{(X-1)^4}|_{X=0} = -3$
$c = (X-1)^3F(X)|_{X=1} = \dfrac{1}{X^2}|_{X=1} = 1$
$d = \dfrac{d}{dX}((X-1)^3F(X))|_{X=1} = \dfrac{-2}{X^3}|_{X=1} = -2$
$e = \dfrac{1}{2}\dfrac{d^2}{dX^2}((X-1)^3F(X))|_{X=1} = \dfrac{1}{2}(-\dfrac{2}{X^3})'|_{X=1} = \dfrac{3}{X^4}|_{X=1} = 3$
Ainsi $F(X) = \dfrac{1}{X^2(X-1)^3} = \dfrac{-1}{X^2} - \dfrac{3}{X} + \dfrac{1}{(X-1)^3} - \dfrac{2}{(X-1)^2} + \dfrac{3}{X-1}$

Remarque. Avant de se lancer das la décomposition en élément simples d'une fonction rationnelles $F(X) = \frac{A(X)}{B(X)}$, on a intérêt à simplifier la fraction (s'il y a lien), c'est à dire à supprimer les facteurs communs à A et B.

S'il y a des facteurs irréductibles du second degré dans $B(X)(\in \mathbb{R}[X])$ il n'y a pas de formule simple analogue à celles d'une partie polaire pour la partie correspondante de la décomposition en éléments simples [1].

1. Voir TD

Troisième partie

Espaces vectoriels

En gros, un espace vectoriel, c'est un ensemble d'objets ("vecteurs") qu'on peut ajouter entre eux et multiplier par les éléments d'un corps $\mathbb{K}$ ("scalaire").

18 Définitions et généralités

Définition. Un espace vectoriel en un corps $\mathbb{K}$ (ou $\mathbb{K}$-ev) est un ensemble E **non vide** muni de deux opérations :

— Une "addition" $E \times E \to E : (x, y) \Rightarrow x + y$

— Un "produit par les scalaires" : $\mathbb{K} \times E \to E, (\lambda, x) \to \lambda x$

Avec les propriétés suivantes.

1. $(E, +, \times)$ est un groupe **commutatif**, i.e :
   — Associativité $(x + y) + z = x + (y + z)$
   — Il existe un élément de E, noté 0 ou 0_e ("vecteur nul") tel que $x + 0 = 0 + x = x$
   — Tout $x \in E$ admet un (unique) **opposé** $-x : (-x) + x = x + (-x) = 0$
   — Commutativité $x + y = y + x$
2. Distributivité des scalaires : $\forall \lambda, \mu \in \mathbb{K}, x \in E. (\lambda + \mu).x = \lambda x + \mu x$
3. Distributivité des vecteurs : $\lambda(x + y) = \lambda x + \lambda y$
4. $\forall \lambda\mu \in \mathbb{K}, \forall x \in E : (\lambda\mu)x = \lambda(\mu x)$
5. $1x = x$

Nota Bene. Les éléments de E sont appelés **vecteurs** et ceux de $\mathbb{K}$ sont appelés **scalaires**.

Quelques propriétés immédiates.

— $0x = 0$ en effet $(\lambda + 0)x = \lambda x + 0x \Rightarrow 0x = 0$

— De même $\lambda 0 = 0_E$ en effet $\lambda(x + 0_E) = \lambda x + \lambda 0_E \Rightarrow \lambda 0_E = 0_E$

— $\lambda(-x) = -\lambda x$: car $\lambda(-x) + \lambda x = \lambda(-x + x) = \lambda 0_E = 0_E$

— $\lambda x = 0 \Rightarrow \lambda = 0_{\mathbb{K}}$ ou $x = 0_E$: en effet, si $\lambda x = 0_e$ et $\lambda \neq 0_{\mathbb{K}}, x = 1x = (\lambda^{-1}\lambda)x = \lambda^{-1}(\lambda x) = 0_E$.

Exemples d'espaces vectoriels. $(\mathbb{K}^n, +, -)$ où $(x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 + y_1, ..., x_n + y_n)$ et $\lambda x = \lambda(x_1, ..., x_n) = (\lambda x_1, ..., \lambda x_n) \in \mathbb{K}^n$ et $\mathbb{K} - ev$

$\mathbb{K}[X], \mathbb{K}(X)$ sont des $\mathbb{K} - ev$

L'ensemble des fonctions d'une partie A de $\mathbb{R}$ dans $\mathbb{R}$. $\tilde{f}(A, \mathbb{R})$ est un $\mathbb{R} - ev$: $(f + g) : (f + g)(a) = f(a) + g(a)$, $(\lambda f)(a) = \lambda f(a)$.

En particulier $C^0(I, \mathbb{R})$ fonctions continues pour un intervalle I de $\mathbb{R}$

$C^1(I, \mathbb{R})$ fonctions continuellement dérivables I de $\mathbb{R}$.

L'ensemble des solutions d'une équation différentielle linéaires (sans second membre) est un $\mathbb{R}-ev$: par exemple l'espace des solutions de $y''+a(x)y'+b(x)=0$

$\mathbb{K}[X]$ est un $\mathbb{K}-ev$ mais l'ensemble des polynômes de degré égaux n n'en n'est pas un ! En effet, $X^n+(-X^n)=0$ n'est pas de degrés n !

19 Sous espace vectoriel.

Définition. Si E est un $\mathbb{K}-ev$, un sous espace vectoriel F de E est un sous ensemble non vide de E qui est un $\mathbb{K}-ev$ (pour les mêmes, $+,\times$)

Proposition. Soit F tel que $\emptyset \neq F \subset E$. F est un $\mathbb{K}-ev$ si et seulement si il est stable par combinaison linéaires, i.e $\forall x,y,\in E, \forall \mu,\lambda \in \mathbb{K}, (x,y\in F) \Rightarrow \lambda x+\mu y \in F$

Démonstration. La stabilité par combinaison linéaire signifie que $+,\times : ExE \to E$ envoie $F\times F$ dans F ($x,y\in F \Rightarrow x+y\in F$ prendre $\lambda=\mu=1$). Et que $\mathbb{K}\times E\to E$ envoie $\mathbb{K}xF$ dans $F(x\in F,\lambda\in\mathbb{K}\Rightarrow \lambda x\in F)$ et touts les propriétés (1) à (5) dans la définition d'un $\mathbb{K}-ev$ sont satisfait pour tous les vecteurs de E, donc a fortiori pour les états de F (puisque $F\subset E$) Donc $(F,+,\times)$ (où ,$+,\times$ sont les restituons des opérations $E\times E\to E, \mathbb{K}\times E\to E$ à $F\times F\to F, \mathbb{K}\times F\to F$ respectivement) est un $\mathbb{K}-ev$. □

Remarques. Un sous espace vectoriel contient nécessairement le vecteur nul de E (qui n'est pas celui de F). En effet $F\neq\emptyset$ par définition, donc soit $x\in F$, F est stable par combinaison linéaire donc $x-x\in F$ et donc $0_E\in F$ (et donc $0_E=0_F$). Donc si $F\neq 0_E$,F n'est peut pas être un sous espace vectoriel de E !

Exemple. L'ensemble des solutions de $y''(x)+y(x)=1$ ne continent pas 0 (fonction nulle), donc ce n'est pas un sous espace vectoriel de $C^2(\mathbb{R},\mathbb{R})$.

Définition de la famille. Soit E un $\mathbb{K}-ev$. Soit A une partie de E. Soit $(x_i)_{i\in I}$ une famille de vecteurs de E indexée par un ensemble I quelconque (Par exemple, si $I=\{1,...,n\}$), une famille $(x_i)_{i\in I}$ est un n-uplet $(x_1,...x_n)$ de vecteurs de E : $(x_1\in E,...,x_n\in E)$.

On appelle sous espace vectoriel de E engendré par A et on note $VectA$ l'ensemble des combinaisons linéaires d'éléments de A, c'est à dire l'ensemble des $\lambda_1 a_1+...+\lambda_n a_n$ où $n\in\mathbb{N}^*$ (quelconque), $\lambda_i\in\mathbb{K}(1\leq i\leq n), a_i\in A(1\leq i\leq n)$.

Il est clair que $Vect(A)$ est non vide si $A\neq\emptyset$ et stable par combinaisons linéaires, donc il est bien un sous espace vectoriel de E si $A\neq\emptyset$. Si $A\neq\emptyset$ on convient que $Vect(\emptyset)=\{0\}$.
On appelle sous espace vectoriel de E engendré par $(x_i)_{i\in I}$ et on note $Vect(x_i)_{i\in E}$ l'ensemble des combinaisons linéaires formée avec les x_i , c'est à dire les sous espace vectoriel engendré par les éléments de la famille.

Proposition. $Vect(A)$ et le plus petit (au sens de l'inclussions) de sous espace vectoriel de E contenant A.

Démonstration. Tout sous espace vectoriel de E contenant A contient les combinaisons linéaires d'éléments de A (car il est stable par combinaison linéaire), ie il contient $vect(A)$. □

Remarque. Soient F,G deux sous espace vectoriel d'un $\mathbb{K}-ev$ E. En général , $F \cup G$ n'est pas un sous espace vectoriel de E.
Mais on remarque $F+G = \{(x,0)+(y,0).x \in \mathbb{R}, y \in \mathbb{R}\} = \{(x,y) : x \in \mathbb{R}, y \in \mathbb{R}\} = \mathbb{R}^2$ est le sous espace vectoriel de $E = \mathbb{R}^2$ égal à E lui même. C'est un fait général.

Proposition. Si F,G sont deux sous espace vectoriel d'un $\mathbb{K}-evE, F+G = \{x+y : x \in F, y \in G\}$ est un sous espace vectoriel de E. Plus généralement , si $(F_i)_{i\in I}$ est une famille de sous espace vectoriel de E, et si on note $\sum\limits_{i\in I} F_i$ l'ensemble des sommes finies $\sum\limits_{i\in I} x_i$ où $x_i \in F_i$. I.e tous les $x = 0$ sauf peut être un nombre fini d'entre eux.
Alors $\sum\limits_{i\in I} F_i$ est un sous espace vectoriel de E (Le cas de $F+G$ correspond à $I = \{1,i\}, F_1 = F, F_2 = G$).

Démonstration. Il est clair que $\sum\limits_{i\in I} F_i$ est non vide (il contient $0 = \sum\limits_{i\in I} 0$) et qu'il est stable par combinaison linéaire : $\lambda \sum\limits_{i\in I} x_i + \mu \sum\limits_{i\in I} x'_i = \sum\limits_{i\in I} (\lambda x_i + \mu x'_i)$. □

Exemple. Dans $\mathbb{K}[X]$, l'ensemble des polynômes pairs ($P(X) = P(-X)$) est $\sum\limits_{i\in\mathbb{N}} \mathbb{K}X^{2i}$ qui est un sous espace vectoriel de $\mathbb{K}[X]$ (où $\mathbb{K}X^{2i}, \lambda \in \mathbb{K}$) et les polynômes pairs sont les $\sum\limits_{i\in\mathbb{N}} a_{2i}X^{2i}$ qui sont bien les éléments de $\sum\limits_{i\in\mathbb{N}} \mathbb{K}X^{2i}$

Proposition. L'intersection de deux sous espace vectoriel F,G de E est un sous espace vectoriel de E. Plus généralement, si $(F_i)_{i\in I}$ est une famille de sous espace vectoriel de E, $\bigcap\limits_{i\in I} F_i$ est un sous espace vectoriel de E.

Démonstration. $x, y \in \bigcap\limits_{i\in I} F_i \Rightarrow \forall i \in I : x, y \in F_i$, donc $\forall i \in I, \forall \lambda, \mu \in \mathbb{K} : \lambda x + \mu y \in F_i$ et donc $\bigcap F_i$ est stable par combinaison linéaire (et évidement $\neq \emptyset$ donc c'est un sous espace vectoriel de E. □

20 Famille

Définition famille libre. On dit qu'une famille $(v_i)_{i\in I}$ de vecteurs d'un $\mathbb{K}-ev, E$ (resp qu'une partie B de E) est **libre** si :
$\sum\limits_{i\in I} \lambda_i v_i = 0 \Rightarrow \forall i \in I, \lambda_i = 0$. (resp $\sum\limits_{v\in L} \lambda_v v = 0 \Rightarrow \forall V \in L, \lambda_V = 0$)
Où il est sous entendu que les sommes sont finies, i.e. $\{i : \lambda_i \neq 0\}$**fini** (resp, $\{v : \lambda_v \neq 0\}$ **fini**).

Définition famille liée. On dit que $(v_i)_{i\in I}$ (resp une partie de A) est **liée** si elle n'est **pas libre** ie il existe une relation linéaire non triviale (ie les λ_i ne sont pas tous nuls) $\sum\limits_{i\in I} \lambda_i v_i = 0$ (resp $\sum\limits_{v\in A} \lambda_v v = 0$ avec λ_v non tous nuls).

Définition génératrice. On dit que $(v_i)_{i\in I}$ (resp une partie G de E) est **génératrice** si $Vect(v_i)_{i\in I} = E$ (resp $Vect(G) = E$) ie si tout vecteur w de E s'écrit $w = \sum_i \lambda_i v_i$ (resp $w = \sum_{v\in G} \lambda_v v$)

21 Bases.

Définition base. On dit que $(V_i)_{i\in I}$ est une **base** (resp qu'une partie B de E est basique, ou est une base) si elle est **libre et génératrice**.

Remarque.

— Une partie contenue dans une partie libre est libre.

— Une partie contenant une partie liée est liée.

— Un partie contenant une partie génératrice est génératrice.

Proposition (Caractérisation d'une base).

1. $(V_i)_{i\in I}$ (resp $B \subset E$) est une base si et seulement si tout vecteur $u \in E$ s'écrit de façon unique : $u = \sum_{i\in I} x_i v_i$ ou $x_i \in \mathbb{K}$ (resp $u = \sum_{v\in B} x_v v$ où $x_v \in \mathbb{K}$)
2. Soit G une partie génératrice de E. Une partie $L \subset G$ est une base si et seulement si c'est une **partie maximale** dans G (ie elle est libre et $\forall g \in G \setminus \{L\}, L \cup \{g\}$ non libre).
3. Une partie B de E est une base si et seulement si elle est **génératrice minimale** (ie elle est génératrice et $\forall v \in B, B \setminus \{v\}$

Démonstration. 1. $(V_i)_{i\in I}$ est une base

$\Leftrightarrow (V_i)_{i\in I}$ libre et génératrice (def).

$\Leftrightarrow$ tout $u \in E$ s'écrit $u = \sum_{i\in I} x_i v_i$ cet $\sum_{i\in I} x_i v_i = 0 \Rightarrow \forall i \in I, x_i = 0$

$\Rightarrow$ tout $u \in E$ s'écrit $u = \sum_i x_i v_i$ et de façon unique car $\sum_i x_i v_i = \sum_i x'_i v_i \Rightarrow \sum_i (x'_i - x_i) v_i = 0 \Rightarrow$ $\forall i, x'_i - x_i = 0$

$\Leftarrow$ tout $u \in E$ s'écrit $u = \sum_i x_i v_i$ et de façon unique (en particulier $\sum_i x_i v_i = 0 \Rightarrow \forall i, x_i = 0$)

2. L libre maximale dans G

$\Leftrightarrow$ L libre et $\forall g \in G \setminus L, L \cup \{g\}$ non libre.

$\Leftrightarrow$ L libre et $\forall g \in G \setminus L$, il existe une relation non triviale $\sum_{v\in L} \cup \{g\} \lambda_v v = 0$ ie $\sum_{v\in L} \lambda_v v + \lambda_g g = 0$

(avec $\lambda_g \neq 0$)sinon on avait $\sum_{v\in L} \lambda_v v = 0$ non triviale $\Rightarrow \lambda_v v = 0$ non triviale $\begin{cases} \Rightarrow \lambda_v \text{ non tous nul} \\ \Rightarrow \text{ L non libre} \end{cases}$

$\Leftrightarrow$ L libre et $\forall g \in G \setminus L, \exists \lambda_g \neq 0$ et des λ_v tel que $g = -\frac{1}{\lambda_g} \sum_{v\in L} \lambda_v v \in Vect(L)$

$\Leftrightarrow$ L libre et $G \setminus L \subset Vect(L)$

$\Leftrightarrow$ L libre et $G \subset Vect(L)(\text{car} G = LU(G \setminus L))$

$\Leftrightarrow$ L est **libre et génératrice** (car $G \subset Vect(L)) \Rightarrow E = Vect(G) \subset Vect(Vect(L)) = Vect(L) \Rightarrow Vect(L) = E$

L base.

3. B génératrice minimale. Si B n'était pas libre, on aurait une relation **non triviale** $\sum_{x \in B} \lambda_z z = 0$, avec disons $z_0 \in B$ tel que $\lambda_{z_0} \neq 0$ et donc $\sum_{z \in B} \setminus \{z_0\} \lambda_z z + \lambda_{z_0} z_0 = 0$ avec $\lambda_{z_0} \neq 0$ d'où $z_0 = -\frac{1}{\lambda_{z_0}} \sum_{z \in B} \setminus \{z_0\} \lambda_z z$. Et donc $z_0 \in Vect(B \setminus \{z_0\})$ Prenons $v = z_0$, alors $v \in Vect(B \setminus \{v\})$ donc toute combinaison linéaire de vecteurs de $B = (B \setminus \{v\}) \cup \{v\}$ se récrit comme une combinaison linéaire de vecteurs de $B \setminus \{v\}$ (en remplaçant v par $-\frac{1}{\lambda_v} \sum_{z \in B \setminus \{v\}} \lambda_z z$) donc $B \setminus \{v\}$
Donc B non libre $\Rightarrow$ B non minimal (comme partie génératrice) et par contraposéé, B génératrice minimale $\Rightarrow$ B génératrice et libre $\Rightarrow$ B est une base.
Réciproquement, si B est une base, elle est génératrice minimale car sinon il existerait $v \in B$ tel que $B \setminus \{v\}$ génératrice, donc $v \in Vect(B \setminus \{v\})$, ie $v - \sum_{w \in B \setminus \{v\}} \lambda_w w = 0$, et donc B ne serait pas libre !

□

Exemples de bases. Dans $\mathbb{K}^n = \{(x_1, ..., x_n) : x_1 \in \mathbb{K}, ..., x_n \in \mathbb{K}\}$.

Soient $\begin{cases} e_1 = (1, 0, ..., 0) \\ e_2 = (0, 1, 0, ..., 0) \\ ... \\ e_i = (0, ..., 0, 1, 0, ..., 0) \\ ... \\ e_n = (0, 0, 0, ..., 0, 1) \end{cases}$

La famille $(e_i)_{i \in \{1,...,n\}} = (e_1, e_2, ..., e_n)$ est une base de $\mathbb{K}^n$ (appelée la base canonique de $\mathbb{K}^n$) .En effet , tout $v \in \mathbb{K}^n$ s'écrit de manière unique $v = x_1.e_1 + ...x_n e_n = (x_1, 0, ..., 0) + ... + (x_1, ..., x_n)$
Pour $n = 2 : (x_1, x_2) = x_1(1, 0) + x_2(0, 1) = x_1 e_1 + x_2 e_2$
$((1, 0), (0, 1))$ est la base canonique de $\mathbb{R}^2$ (ou $\mathbb{K}^2$).

- Tout polynôme de $\mathbb{K}[X]$ s'écrit de manière unique $\sum_{i \geq 0} a_i X^i$, donc $(X^0, X^1, ...) = (X^i)_{i \in \mathbb{N}}$ est une base de $\mathbb{K}[X]$.
- Toute fraction rationnelle de $\mathbb{K}(X)$ a une unique décomposition en éléments simples, donc on a une base de $\mathbb{K}(X)$, formée des $(X^i)_{i \in \mathbb{N}}$ est des $\frac{X^j}{P^k}$ où $j < deg(P), P$ irréductible dans $\mathbb{K}[X], k \in \mathbb{N}^*$.
- $\mathbb{C}$ comme $\mathbb{R} - ev$: une base est $\{1, i\}$ (car tout $z \in \mathbb{C}$ s'écrit de manière unique $z = x + i_y$ avec $x, y \in \mathbb{R}$). Une autre base est $\{1, z\}$ par exemple.
- $\mathbb{C}$ comme $\mathbb{C} - ev$ a pour base 1, car tout $z \in \mathbb{C}$ s'écrit de façon unique $z = z.1, z \in \mathbb{C}$ et n'importe quel $w \in \mathbb{C}^*$ forme une base de $\mathbb{C}$ car $\forall z \in \mathbb{C}, z = (\frac{z}{w}).w$.

Définition. On dit qu'un $\mathbb{K}-evE$ est de **dimension finie** s'il admet une partie génératrice finie.

Exemple. $\mathbb{K}^n$, car il est engendré par sa base canonique. $(e_1,...,e_n)$ où $e_j=(0,...,0,1,0,...,0)\in\mathbb{K}^n$

Contre-exemple. $\mathbb{K}[X]$ n'est pas de dimension finie, car si $\{P_1,...,P_k\}$ est une partie **finie** de $\mathbb{K}[X]$, toute combinaison linéaire, $\lambda_1P_1+...+\lambda_kP_k$ est de degré $\leq max\{deg(P_1),...,deg(P_k)\}=m$ et donc $X^{m+1}\notin Vect\{P_1,...,P_k\}$ n'engendre pas $\mathbb{K}[X]$.

Lemme (extraction d'une partie génératrice finie). Soit E un $\mathbb{K}-ev$ de dimension finie. Soit G une partie génératrice de E. Alors G contient une partie génératrice finie G_0.

Démonstration. E est de dimension finie. Donc il contient une partie génératrice finie $F=\{f_1,...,f_k\}$. G est génératrice, donc f_1 est combinaison linéaire d'un nombre fini d'éléments de G : $f_1\in Vect(F_1)$ où $F_1\subset G, F_1$ finie.
De même : $f_2\in Vect(F_2),...,f_k\in Vect(F_k)$ où $F_2,...,F_k$ sont des parties finies de G. Donc $f_1,...,f_k\in Vect\{F_1\cup...\cup F_k\}$.
Or tout vecteur de E est une combinaison linéaire de $f_1,...,f_k$ donc il est combinaison linéaire des éléments de $F_1\cup...\cup F_k$.
Donc $G_0=F_1\cup...\cup F_k$ répond à la question (c'est une partie génératrice finie de G). □

Théorème de la base incomplète. Soit E un $\mathbb{K}-ev$ de dimension finie, non réduit à $\{0\}$. Soient L une partie libre de E et G une partie génératrice. Il existe une base B de E tel que $L\subset B\subset L\cup G$.
Autrement dit toute partie libre peut être complétée en une base en y adjoignant éventuellement des vecteurs pris dans une partie génératrice donnée.

Démonstration. Soit $G_0\subset G$ une partie génératrice finie (cf le lemme). Considérons une partie S de G_0 maximale telle que $L\cup S$ soit libre. Il existe des $S\subset G_0$ tel que $L\cup S$ soit libre ; $L\cup\emptyset$ est libre : Puisque G_0 est finie, donc n'a qu'un nombre fini de parties, toutes finies, il en existe au mois une qui a le plus grand nombre d'éléments. Alors $L\cup S$ est libre maximale dans la partie génératrice $L\cup G_0$. Donc c'est une base (d'après la proposition de caractérisation des bases.) □

Lemme. Il y a $n+1$ vecteurs dans un espace engendré par n vecteurs sont liés.

Preuve (récurrence).

Initialisation

$\underline{n=1:}$

$u_1,u_2\in Vect(v)$ Donc $u_1=\lambda_1v, u_2=\lambda_2v$.

Si $\lambda_1\lambda_2$ sont nuls, alors $u_1=u_2=0$ et on a la relation linéaire non triviale $u_1-u_2=0$.

Si λ_1, λ_2 ne sont pas tous les deux nuls, on a la relation linéaire non triviale $\lambda_2 u_1 - \lambda_1 u_2 = 0$ (car $\lambda_2\lambda_1 v - \lambda_1\lambda_2 v = 0$). Donc pour $n = 1$, l'énoncé du lemme est vrai.

Hérédité On suppose l'énoncé vrai pour $n-1$, montrons qu'il est vrai pour n. $\begin{cases} u_1 = a_{11}v_1 + a_{12}v_2 + ... + a_{1n}v_n \\ u_2 = a_{21}v_1 + a_{22}v_2 + ... + a_{2n}v_n \\ \vdots \\ u_{n+1} = a_{n+1,1}v_1 + a_{n+2,2}v_2 + ... + a_{n+1,n}v_n \end{cases}$

Si tous les a_{in} sont nuls $(1 \leq i \leq n+1)$ alors $u_1, ..., u_n, u_{n+1}$ sont des $Vect\{v_1, ..., v_{n-1}\}$ donc $\{u_1, ..., u_n\}$ est liée (hypothèses de récurrences) et a fortiori $\{u_1, ..., u_n, u_{n+1}\}$ aussi.

S'il existe au moins sur $i \in \{1, ..., n+1\}$ tel que a_{in} (quitte à renuméroter).

Alors $u_2 - \frac{a_{2n}}{a_{1n}}u_1 \in Vect\{v_1, ..., v_{n-1}\}$ car dans $u_2 - \frac{a_{2n}}{a_{1n}}u_1$ le coefficient de V_n est : $a_{2n} - \frac{a_{2n}}{a_{1n}}a_{1n} = 0$.
De même : $u_3 - \frac{a_{3n}}{a_{1n}}u_1, ..., u_{n+1} - \frac{a_{n+1,n}}{a_{1n}}u_1 \in vect(v_1, ...v_{n-1})$.
L'hypothèse de récence montre que $u_2 - \frac{a_{2n}}{a_{1n}}u_1, u_3 - \frac{a_{3n}}{a_{1n}}u_1, ..., u_{n+1} - \frac{a_{n+1,n}}{a_{1n}}u_1$ sont liés. Il existe $\lambda_2, ..., \lambda_{n+1}$ non nuls tel que $\lambda_2(u_2 - \frac{a_{2n}}{a_{1n}}u_1 + ... + \lambda_{n+1}(u_{n+1} - \frac{a_{n+1,n}}{a_{1n}}u_1) = 0$.
$\Leftrightarrow \lambda_2 u_2 + ... + \lambda_{n+1}u_{n+1} - (\sum_{i=2}^{n+1} \lambda_i \frac{a_{in}}{a_{1n}})u_1 = 0$ qui est une relation linéaire non triviale (car $\lambda_2, ..., \lambda_{n+1}$ non tous nuls) entre $u_2, ..., u_{n+1}, u_1$.

Théorème de la dimension. Soit E un $\mathbb{K} - ev$ de dimension finie non réduit à $\{0\}$. Toutes ses bases sont finies et ont le même ombre d'éléments qu'on note $dim(E)$ et qu'on appelle la dimension de E.

Démonstration. D'après le théorème de la base incomplète avec $L = \{u_1\}, u_1 \neq 0$, il existe une base B tel que $L \subset B \subset L \cup S$ avec S finie, donc B est finie. Soit n le nombre d'éléments de B. Soit B' une autre base de E. Si B' contenait plus de n éléments, elle serait liée (d'après le lemme précédent) et donc B' ne serait plus une base. Donc $card(B') \leq card(B)$. Le même argument en échangeant B' (dont on sait maintenant qu'elle est finie) et B montre que $card(B) \leq card(B')$. Donc :

$$card(B') = card(B)$$

□

Corollaire. Soit E un $\mathbb{K} - ev$ de dimension n.

1. Toute partie libre a au plus n éléments.
2. Toute partie génératrice a au moins n éléments.
3. Une partie à n éléments est une base si et seulement si elle est est libre.

4. Une partie à n éléments est une base si et seulement si elle est génératrice.
5. Tout sev F de E est de dimension finie : $dim(F) \leq n$. De plus : $dim(F) = n \Leftrightarrow F = E$

Démonstration. 1. D'après le théorème de la base incomplète, on peut compléter toute partie libre L en une base (à n éléments), donc $card(L) \leq n$.

2. L'argument dans le théorème de la base incomplète est valable même si $L = \emptyset$. donc $\forall G$ génératrice, il existe une base $B \subset G$ Et $card(B) = n$, donc $card(G) \geq n$.
3. Soit L libre à n éléments. On peut la compléter en une base B, à n éléments donc $L = B$, donc L est une base.
4. Soit G génératrice à n éléments. Elle contient une base B, à n éléments, donc $G = B$, et donc G est une base.
5. Si $F = Vect\{u_1\}, u_1 \neq 0 : \{u_1\}$ est libre et génératrice et c'est une base : $dim(F) = 1$. Si $F \supset Vect\{u_1\}$ strictement, il existe $u_2 \neq 0$ dans F tel que $u_2 \notin \{u_1\}$ strictement, il existe $u_2 \neq 0$ dans F tel que $u_2 \notin Vect\{u_1\}$, donc $F \supset Vect\{u_1, u_2\}$ et $\{u_1, u_2\}$ est libre. Si $\{u_1, u_2\}$ engendre F, c'est une base et $dim(F) = 2 \leq dim(E)$ (puisque $u_1, u_2 \in E$).
   On arrive à $F \supset Vect\{u_1, ..., u_p\}$ et $u_{p+1} \in F$ tel que $u_{p+1} \notin Vect\{u_1, ..., u_p\}$ donc $\{u_1, ..., u_p, u_{p+1}\}$ libre, donc $p+1 \leq n$. Donc le processus finit par s'arrêter, i.e. il existe $p \leq n$ tel que $\{u_1, ...u_p\}$ engendre F et donc $dim(F) = p$ est finie (et $dim(F) \leq dime(E)$ puisque $\{u_1, ..., u_p\} \subset E$).
   Enfin si $dim(F) = n$, soit $(f_1, ..., f_n)$ une base de F : c'est une partie libre de e à un élément donc c'est une base de E et donc $\begin{cases} F = Vect\{f_1, ..., k_n\} \\ E = Vect\{f_1, ..., f_n\} \end{cases}$. D'où $F = E$.

□

22 Dimension

Convention.

$$dim\{0\} = 0$$

Noter que $\{0\}$ n'a pas de base car son unique vecteur 0 est lié ($1.0 = 0$: relation linéaire non triviale)

Maintenant, voyons deux propriétés essentielles de la dimension :

Proposition. Soient E, F deux $\mathbb{K}-ev$ de dimensions finies. Le produit (cartésien) $E \times F = \{(x, y) : x \in E, y \in F\}$ est un $\mathbb{K} - ev$ de dimension finie : $dim(E \times F) = dim(E) + dim(F)$.

Démonstration. Le fait que $E \times F$ soit un $\mathbb{K} - ev$ est asinitrottant.

Soient $(e_1, ..., e_n)$ une base de E $(dim(E) = n)$ et $(f_1, ...f_k)$ une base de F $(dim(F) = k)$

Tout $(x, y) \in E \times F$ s'écrit de manière unique :

$(x, y) = (\sum_{i=1}^{n} x_i e_i, \sum_{j=1}^{k} y_j f_j) = (\sum_{i=1}^{n} x_i e_i, 0) + (0, \sum_{j=1}^{k} y_j f_j) = \sum_{i=1}^{n} x_i (e_1, 0) + \sum_{j=1}^{k} y_j (0, f_j)$

Donc $((e_1, 0), ..., (e_n, 0), (0, f_1), ..., (0, f_k))$ est une base de $E \times F$ (car génératrice et écriture **unique** pour chaque $(x, y) \in E \times F$). □

Exemples. $dim(\mathbb{R}^2) = dim(\mathbb{R} \times \mathbb{R}) = 2dim(\mathbb{R}) = 2$
$dim(\mathbb{R}^2) = dim(\mathbb{R} \times \mathbb{R} \times \mathbb{R}) = 3dim(\mathbb{R}) = 3$

Nota benne. $dim(E_1 \times ... \times E_m) = dim(E_1) + ... + dim(E_m)$ si $E_1, ..., E_m$ sont des $\mathbb{K} - ev$ de dimension finies.

Proposition (Théorème ou relation de Grassmann). Soient V, W deux sev de dimensions finies d'un $\mathbb{K} - ev$ E (de dimension finie ou non). Alors $V + W$ est de dimension finie et

$$dim(V + W) = dim(V) + dim(W) - dim(V \cap W)$$

Démonstration. $V \cap W$ est de dimension finie (cart c'est un sev de V). Soit $(e_1, ..., e_k)$ est une base de $V \cap W$. On la complète en une base de V, disons $(e_1, ..., e_k, e_{k+1}, ..., e_n)$ où $n = dim(V)$. Par ailleurs, complétons là aussi en une base de W, disons $(e_1, ..., e_k, e'_{k+1}, ...e'_m)$ où $m = dim(W)$.
$V + W = \{x + y : x \in V, y \in W\}$
$= \left\{\lambda_1 e_1 + ... + \lambda_k e_k + \lambda_{k+1} e_{k+1} + ... + \lambda_n e_n + \mu_1 e_1 + ... + \mu_k e_k + \mu_{k+1} e'_{k+1} + ... + \mu_m e'_m : \lambda_1, ..., \lambda, \mu_1, ..., \mu_n \in \mathbb{K}\right\}$
$= \left\{(\lambda_1 + \mu_1)e_1 + ... + (\lambda_k + \mu_k)e_k + \lambda_{k+1} e_{k+1} + ... + \lambda_n e_n + \mu_{k+1} e'_{k+1} + ... + \mu_m e'_m\right\}$
$\{: \lambda_1, ..., \lambda_k, \mu_1, ...\mu_k, \lambda_{k+1}, ..., \lambda_n, \mu_{k+1}, ..., \mu_m \in \mathbb{K}\}$
$= \left\{\alpha_1 e_1 + ... + \lambda_k e_k + \lambda_{k+1} e_{k+1} + ... + \lambda_n e_n + \mu_{k+1} e'_{k+1} + ... + \mu_m e'_m : \alpha_1, ..., \alpha_k, \lambda_{k+1}, ..., \lambda_n, \mu_{k+1}, ..., \mu_m \in \mathbb{K}\right\}$
$= Vect\left\{e_1, ..., e_k, e_{k+1}, ..., e_n, e'_{k+1}, ..., e'_m\right\}$.

Plus directement (ce qu'il faut savoir) :
$V + W = Vect\left\{e_1, ..., e_k, e_{k+1}, ..., e_n\right\} + Vect\left\{e_1, ..., e_k, e'_{k+1}, ..., e'_n\right\}$
$= Vect\left\{e_1, ..., e_k, e_{k+1}, ..., e_n, e_1, ..., e_k, e'_{k+1}, ..., e'_n\right\}$.

Donc $\left\{e_1, ..., e_k, e_{k+1}, ..., e_n, e'_{k+1}, ..., e'_m\right\}$ est une partie génératrice de $V + W$.
Vérifions qu'elle est libre :
$\underbrace{\lambda_1 e_1 + ... + \lambda_k e_k + \lambda_{k+1} e_{k+1} + ... + \lambda_n e_n}_{\in V} = \underbrace{-(\lambda'_{k+1} e'_{k+1} + ... + \lambda'_m e'_m) \in V \cap W}_{\in W}(*)$.
$\Rightarrow \lambda_{k+1} = ... = \lambda_n = 0$ et $\lambda'_{k+1} = ... = \lambda'_m = 0$
$\Rightarrow \lambda_1 e_1 + ... + \lambda_k e_k = 0$ (ce qu'il reste de (*))
$\lambda_1 = ... = \lambda_k = 0$ (car $(e_1, ..., e_k)$ est libre).
Donc $\left\{e_1, ..., e_k, e_{k+1}, ..., e_n, e'_{k+1}, ..., e'_n\right\}$ est libre, et donc c'est une base de $V+W$ (partie **génératrice** et **libre**).
Donc : $dim(V+W) = card\left\{e_1, ..., e_k, e_{k+1}, ..., e, e'_{k+1}, ..., e'_m\right\} = n+m-k = dim(V)+dim(W)-dim(V \cap W)$. □

Définition. Soient V, W deux sev d'un $\mathbb{K} - evE$.

1. On dit que la somme $V + W$ est **directe** si $V \cap W = \{0\}$. Dans ce cas, on la note $V \oplus W$.
2. On dit que V et W sont **supplémentaires** (dans E) si $E = V \oplus W$; i.e. si $\begin{cases} V \cap W = \{0\} \\ V + W = E \end{cases}$.

Exemple. Dans $\mathbb{R}^2$, prenons $\begin{cases} V = \mathbb{R}(1,0) \\ W = \mathbb{R}(0,1) \end{cases}$.

$V \cap W = \{(0,0)\}$ le seul vecteur de $\mathbb{R}^2$ qui soit à la fois de la forme $(x,0)$ (donc $y=0$) et de la forme $(0,y)$ (donc $x=0$).

Et $V+W = \{(x,0) : x \in \mathbb{R}\}+\{(0,y) : y \in \mathbb{R}\} = \{(x,y) : x \in \mathbb{R}, y \in \mathbb{R}\} = \mathbb{R}^2$. Donc V et W sont supplémentaires (dans $\mathbb{R}^2$)

Mise en garde. Dans l'exemple ci dessus, W est **un** supplémentaire de V, **mais ce n'est pas le seul**. Soit $W' = \mathbb{R}(a,b)$ où $b \neq 0$. (a quelconque) : alors on a aussi $V \cap W' = \{(0,0)\}$ (car $(x,0) = (au, bu) \Rightarrow bu = 0 \Rightarrow u = 0 \Rightarrow (au, bu) = (0,0)$

et $V + W' = Vect\{(0,1),(a,b)\} = \mathbb{R}^2$ donc $\mathbb{R}^2 = V \oplus W'$.

C'est un fait général : il n'y a pas unicité du supplémentaire, il y a toujours une infinité de supplémentaires d'un sev V sauf si $V = 0$ où le seul supplémentaire est E. Ou si $V = E$ le seul supplémentaire est 0.

En particulier, ne pas cofonder **supplémentaire** (notion **algébrique**, **non unique**) et **complémentaire** (notion **ensemblistes**, **unique**).

Proposition. Soit E un $\mathbb{K} - ev$ de dimension finie. Soient V, W deux sev de E. Alors la somme $V + W$ est directe si et seulement si $dim(V + W) = dim(V) + dim(W)$

Démonstration. $dim(V + W) = dim(V) + dim(W) \Leftrightarrow dim(V \cap W) = 0 \Leftrightarrow V \cap W = \{0\}$ □

Quatrième partie

Applications linéaires

23 Définitions et généralités

Définition Soient E, F des $\mathbb{K}-ev$. Une application $\Phi : E \to F$ est dites **linéaire** si :

$$\forall x, y \in E, \forall \lambda, \mu \in \mathbb{K} : \Phi(\lambda x + \mu y) = \lambda\Phi(x) + \mu\Phi(x)$$

Nota Bene. Si ϕ est linéaire, alors (par récurrence) :
$\forall x_1, ..., x_k \ inE, \forall \lambda_1, ..., \lambda_k \in \mathbb{K} : \Phi(\sum_{i=1}^{k} \lambda_i x_i) = \sum_{i=1}^{k} \lambda_i \Phi(x_i)$.

Exemples.

1. $\Phi : \mathbb{R} \to \mathbb{R}$ est linéaire si et seulement si elle est de la forme $\Phi(x) = ax$ où $a = cte$. En effet : Φ linéaire $\Rightarrow \forall x \in \mathbb{R}, \Phi(x) = \Phi(1.x) = x\Phi(1)$.
2. $\Phi : \mathbb{R}^2 \to \mathbb{R}$ est linéaire si et seulement si $\Phi(x, y) = ax + by$ où a, b sont des constantes. En effet : Φ linéaire $\Leftrightarrow \Phi(x, y) = \Phi(x(1, 0) + y(0, 1)) = x\Phi(1, 0) + y\Phi(0, 1)$.
3. $\Phi : \begin{cases} \mathbb{K}[X] \to \mathbb{K}[X] \\ P(X) \to X.P(X) \end{cases}$. Et $\Psi : \begin{cases} \mathcal{F}(\mathbb{R}, \mathbb{R}) \to \mathcal{F}(\mathbb{R}, \mathbb{R}) \\ x \to x.f(x) \end{cases}$ sont linéaires.
4. $\Phi : \begin{cases} \mathbb{K}[X] \to \mathbb{K}[X] \\ P(X) \to P'(X) \end{cases}$. Et $\Psi : \begin{cases} C^\infty(\mathbb{R}, \mathbb{R}) \to C^\infty(\mathbb{R}, \mathbb{R}) \\ f \to f' \end{cases}$ sont linéaires.

Proposition et notation. On note $\mathcal{L}(E, F)$ l'ensemble des applications linéaires de E dans F.
$\mathcal{L}(E, F)$ est un $\mathbb{K}-ev$. [Pour les opérations évidentes : $(\Phi+\Psi)(x) = \Phi(x)+\Psi(x) \forall x \in E$, $(\lambda\Phi)(x) = \lambda\Phi(x) \quad (\lambda \in \mathbb{K}, x \in E)$].
Si $\begin{cases} dim(E) < \infty \\ dim(F) < \infty \end{cases}$ alors $dim(\mathcal{L}(E, F)) < \infty$ et $dim(\mathcal{L}(E, F)) = dim(E) \times dim(F)$.

Démonstration. $\mathcal{L}(E, F)$ est un $\mathbb{K} - ev$: Si $dim(E) < \infty, dim(F) < \infty$, soient $(e_1, ..., e_n)$ une base de E, $(f_1, ..., f_m)$ une base de F.

Soit $\Phi : E \to F$.

Φ linéaire $\Rightarrow \forall x = x_1e_1 + ... + x_ne_n \in E, \Phi(x) = \Phi(\sum_{i=1}^{n} x_i e_i) = \sum_{i=1}^{n} x_i \Phi(e_i)$.
Posons $\Phi(e_i) = \sum_{j=1}^{m} a_{ij} b_j$. Alors $\Phi(x) = \sum_{i=1}^{n} \sum_{j=1}^{m} x_i a_{ij} f(e)$.
On voit que Φ est entièrement caractérisé par les a_{ij}.

Montrons que les applications linéaires Φ_{ij} définies par $\Phi_{ij}(e_i) = f_j$ et $\Phi_{ij}(e_k) = 0$ si $k \neq i$ forment une base de $\mathcal{L}(E,F)$. Soit $\Phi \in \mathcal{L}(E,F) : \Phi(x) = \sum_{i=1}^{n} e_1 \sum_{j=1}^{m} a_{ij} b_j$.

$$\Phi(e_i) = \sum_{j=1}^{m} a_{ij} b_j = \sum_{j=1}^{m} a_{ij} \Phi_{ij}(e_i) = \sum_{k=1}^{n} \sum_{j=1}^{m} a_{kj} \Phi_{kj}(e_i) \text{ car } \Phi_{kj}(e_i) = \begin{cases} 0 \text{ si } k \neq i \\ \\ \phi_{ij}(e_i) \text{ si } k = i \end{cases}.$$

Comme Φ est caractérisée par l'image des e_i (puisque $\Phi(x) = \sum_{i=1}^{n} x_i \Phi(e_i)$). On a donc :
$\Phi = \sum_{k=1}^{n} \sum_{j=1}^{m} a_{k_j} \Phi_{k_j} = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} \Phi_{ij}$ et donc la famille $(\Phi_{ij})_{\substack{n \leq i \leq m \\ 1 \leq j \leq m}}$ est génératrice de $\mathcal{L}(E,F)$.

Et elle est libre car : $\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} \Phi_{ij} = 0 \Rightarrow \forall k \in \{1, ..., n\}, \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} \Phi_{ij}(e_k) = 0$
$\Rightarrow \sum_{j=1}^{m} a_{k_j} f_k = 0$
$\Rightarrow \forall k ß \{1, ..., n\}, \forall j \in \{1, ..., m\}, a_k j = 0.$

Donc $(\Phi_{ij})_{\substack{n \leq i \leq m \\ 1 \leq j \leq m}}$ est une base de $\mathcal{L}(E,F)$ et donc $dim(\mathcal{L}(E,F)) = n \times m$.

□

Proposition. Soient $\Phi, \Psi \in \mathcal{L}(E,F)$ (on note simplement : $\mathcal{L}(E)$). Alors $\Psi o \Phi \in \mathcal{L}(E)$. Plus généralement : si $\Phi \in \mathcal{L}(E,F)$ et $\Psi \in \mathcal{L}(E,F)$ alors $\Psi o \Phi \in \mathcal{L}(E,G)$ (où E, F, G sont trois $\mathbb{K} - ev$).

Démonstration. $\Psi o \Phi(\lambda x + \mu y) = \Psi(\Phi(\lambda x + \mu y)) = \Psi(\lambda \Phi(x) + \mu \Phi(x)) = \lambda \Psi(\Phi(x)) + \mu \Psi(\Phi(x)) = \lambda \Psi o \Phi(x) + \mu \Psi o \Phi(y)$ □

Proposition. Soit E un $\mathbb{K} - ev$: $(\mathcal{L}(E), +, \times, 0)$ est un $\mathbb{K} -$ algèbre , i.e :

1. $(\mathcal{L}(E), +, \times)$ est un $\mathbb{K} - ev$.
2. Distributivité à droite $(\Phi + \Psi) + \Theta = \Phi o \Theta + \Psi o \Theta$
   Distributivité à gauche : $\Theta o (\Phi + \Psi) = \Theta o \Phi + \Theta o \Phi$.
3. Jeu entre $\times$ et o : $(\lambda \Phi) o \Psi = \Phi o (\lambda \Psi) = \lambda \Phi o \Psi$

Démonstration.

1. Déjà vu
2. à droite : $(\Phi + \Psi) o \Theta(x) = (\Phi + \Psi)(\Theta(x)) = \Phi(\Theta(x)) + \Psi(\Theta(x))$ (définition de $+$ dans $\mathcal{L}(E)$) $= \Phi o \Theta(x) + \Psi o \Theta(x)$ (cela n'utilise pas la linéarité des applications).
   à gauche : $\Theta o (\Phi + \Psi)(x) = \Theta(\Phi(x) + \Psi(x)) = \Theta(\Phi(x)) + \Theta(\Psi(x)) = \Theta o \Phi(x) + \Theta o \Psi(x)$.
3. $(\lambda \Phi) o \Psi(x) = \lambda \Phi(\Psi(x)) = \Phi(\lambda \Psi(x)) = (\Phi o (\lambda \Psi))(x)$

□

Proposition. Si $\Phi \in \mathcal{L}(E)$ est bijective, alors la réciproque Φ^{-1} est aussi dans $\mathcal{L}(E)$ (i.e elle est linéaire).

Démonstration. $\Phi^{-1}(\lambda x + \mu y) = \lambda\Phi^{-1}(x) + \mu\Phi^{-1}(y)$
$\Leftrightarrow \Phi(\Phi^{-1}(\lambda x + \mu y)) = \Phi(\lambda\Phi^{-1}(x) + \mu\Phi^{-1}(y))$
$\Leftrightarrow \lambda x + \mu y = \lambda\Phi(\Phi^{-1}(x)) + \mu\Phi(\Phi^{-1}(y))$
$\Leftrightarrow \lambda x + \mu y = \lambda x + \mu y$ Vrai ! □

Terminologie.

— Une application linéaire est appelée aussi un homomorphisme (d'espaces vectoriels), ou simplement morphisme (d'espaces vectoriels).
— Un morphisme bijectif est appelé **isomorphisme**
— Un morphisme $E \to E$ est appelé **endomorphisme**
— Un isomorphisme $E \to E$ est appelé **automorphisme**

24 Notion de Ker et Im

Définition et proposition.

— Soit $\Phi \in \mathcal{L}(E, F)$, on note $Ker(\Phi) = \{x \in E : \Phi(x) = 0\}$. C'est un *sev* de E : on l'appelle le noyau de Φ
— On note $Im(\Phi) = \{y \in F : \exists x \in E, y = \Phi(x)\}$. C'est un *sev* de F : on l'appelle l'image de Φ.

Preuve (que ce sont des sev).

— $o \in Ker(\Phi)$ car $\Phi(0) = 0$ pour toute application linéaire : en effet , $\Phi(2x) = 2\Phi(x) \Rightarrow \Phi(0) = 2\Phi(0) \Rightarrow \Phi(0) = 0$. On a donc $Ker(\Phi)$ est stable par combinaison linéaire :
$$\left.\begin{array}{l}\Phi(x) = 0\\ \Phi(y) = 0\\ \lambda, \mu \in \mathbb{K}\end{array}\right\} \Rightarrow \Phi(\lambda x + \mu y) = \lambda\Phi(x) + \mu\Phi(y) = 0 \Rightarrow \lambda x + \mu y \in Ker(\Phi).$$
— $0 = \Phi(0) \Rightarrow 0 \in Im(\Phi)$. $Im(\Phi)$ stable par combinaison linéaire car si $x' = \Phi(x), y' = \Phi(y)$ alors $\forall \lambda, \mu \in \mathbb{K}$,

Proposition. $\phi \in \mathcal{L}(E, F)$ est injective si et seulement si $Ker(\phi) = \{0\}$ et surjective si et seulement si $Im(\phi) = F$.

Démonstration. ϕ injective si et seulement si :

— $\phi(x) = \phi(y) \Rightarrow x = y, x, y \in E$ (définition d'injective)
— $\phi(x - y) = 0 \Rightarrow = 0 \Rightarrow x - y = 0, x, y \in E(\phi$ linéaire)
— $\phi(z) = 0 \Rightarrow z = 0, z \in E$
— $Ker(\phi) = \{0\}$

□

— ϕ surjective $\Leftrightarrow Im(\phi) = F$ (définition de "surjective")

Définition.

— Le rang d'une famille de vecteurs $(x_i)_{i\in I}$ d'un $\mathbb{K}-ev$ E est : $dim(Vect\{x_i : i\in I\})) = rg(x_i)_{i\in I}$ (la dimension finie ou infinie du sev engendré par les x_i).

— Le rang d'une application linéaire $\phi : E \to F$ est le rang de la famille $(\phi(x))_{x\in E}$

I.e c'est $dim(Vect\{\phi(x) : x\in E\}) = dim(\phi(E))$

I.e $rg(\phi) = dim(Im(\phi))$ (finie ou infinie)

25 Notion de rang

Théorème du rang. Soit $\phi \in \mathcal{L}(E,F)$ avec E de dimension finie. Alors $Ker(\phi)$ et $Im(\phi)$ sont de dimension finie.

$$dim(Ker(\phi)) + dim(Im(\phi)) = dim(E)$$

Démonstration. Soit $(e_1,...,e_n)$ une base de E. Alors $Im(\phi)$ est engendrée par $\{\phi(e_1),...,\phi(e_n)\}$. Donc $Im(\phi)$ est de dimension finie. De cette partie génératrice de $Im(\phi)$, extrayons une base de $Im(\phi)$, disons $(\phi(e_1),...,\phi(e_r))$ (quitte à renuméroter les e_i), où $r = dim(Im(\phi)) = rg(\phi)$.

Alors : Soit $x\in E$: $\underbrace{\phi(x)}\in Im(\phi) = \sum_{j=1}^{r}\lambda_j\phi(e_j)$ donc $\phi(x - \sum_{j=1}^{r}\lambda_j e_j) = 0$ et donc $x - \sum_{j=1}^{r}\lambda_j e_j \in Ker(\phi)$. Mais $Ker(\phi)$ est une sev de E et E est de dimension finie, donc $Ker(\phi)$ est de dimension finie.

Soit $(e'_1,...,e'_k)$ une base de $Ker(\phi)$: on a alors $x - \sum_{j=1}^{r}\lambda_j e_j = \sum_{i=1}^{k}\lambda'_i e'_i$.

i.e $x = \sum_{j=1}^{r}\lambda_j e_j + \sum_{i=1}^{k}\lambda_j e_j + \sum_{i=1}^{k}\lambda'_i e'_i$. Donc $\{e_1,...,e_r,e'_1,...,e'_k\}$ est génératrice de E.

Justifions qu'elle est libre : $\sum_{j=1}^{r}\lambda_j e_j + \sum_{i=1}^{k}\lambda'_i e'_i = 0 \to \sum_{j=1}^{r}\lambda_j\phi(e_j) + \sum_{i=1}^{k}\lambda'_i\phi(e'_i) = 0$

$\Rightarrow \sum_{j=1}^{r}\lambda_j\phi(e_j) = 0 \Rightarrow (e_j) = 0 \Rightarrow \lambda_1 = ... = \lambda_r = 0$ (car $(\phi(e_1),...,\phi(e_r))$ est libre : base de $Im(\phi)$.

Ainsi $\sum_{j=1}^{r}\lambda_j\phi(e_j) = 0$ devient $\sum_{i=1}^{k}\lambda'_i e'_1 = 0$, d'où $\lambda'_1 = ... = \lambda'_k = 0$

Donc $(e_1,...,e_r,e'_1,...,e'_k)$ est une famille génératrice de E est libre, donc c'est une base de E. Et donc $dim(E) = r + k = dim(Im(\phi)) + dim(Ker(\phi))$.

□

Proposition. Soit $\phi\in\mathcal{L}(E,F)$, avec E,F de dimension finies.

— Si ϕ envoie une base de E sur une base de F, alors ϕ est un isomorphisme.

— Si ϕ est un isomorphisme, alors ϕ envoie toute base de E sur une base de F (et $dim(F) = dim(E)$)

Démonstration.

— Soit $(b_1,...,b_n)$ une base de E tel que $(\phi(b_1),...,\phi(b_n))$ soit une base de F. Alors : $Im(\phi) = Vect(\{\phi(b_1),...,\phi(b_n)\})$ soit une base de F. Alors : $Im(\phi) = Vect\{\phi(b_1),...,\phi(b_n)\} = F$ donc $Im(\phi) = F$ et donc ϕ est surjective

(et $dim(F) = n = dim(E)$). Par le théorème du rang : $dim(Ker(\phi)) = dim(E) - dim(Im(\phi)) = 0$ donc $Ker(\phi) = \{0\}$ et donc ϕ est injective. Et donc ϕ est un isomorphisme.

— Soit $\phi : E \to F$ un isomorphisme. Soit $(b_1, ..., b_n)$ une base de E. ϕ est surjective, donc $F = Im(\phi) = Vect\{\phi(b_1), ..., \phi(b_n)\}$ donc $\{\phi(b_1), ..., \phi(b_n)\}$ engendre F et cette partie de F est libre car :$\lambda_1\phi(b_1) + ... + \lambda_n\phi(b_n) = 0 \to \phi(\lambda_1 b_1 + ... + \lambda_n b_n) = 0$

$\Rightarrow \lambda_1 b_1 + ... + \lambda_n b_n = 0 \Rightarrow \lambda_1 = ... = \lambda_n = 0$ (car $(b_1, ...b_n)$ libre). Et donc $(\phi(b_1), ..., \phi(b_n))$ est une base de F (et $dim(F) = n = dim(E)$)

□

Corollaire. Deux $\mathbb{K}-ev$, E et F de dimensions finies sont isomorphes (ie : il existe un isomorphisme $\phi : E \to F$, et donc un isomorphisme $\phi^{-1} : F \to E$) si et seulement si $dim(E) = dim(F)$. (En particulier , un $\mathbb{K} - ev$ est isomorphisme à $\mathbb{K}^n$ si et seulement si il est de dimension n.)

Démonstration. D'après la proposition précédente, si E et F sont isomorphes alors $dim(E) = dim(F)$. Réciproquement si $dim(E) = dim(F) = n$, soient $(e_1, ..., e_n)$ une base de $E, (f_1, ..., f_n)$ une base de F, on définit $\phi \in \mathcal{L}(E, F)$ par $\phi(e_i) = f_i$, c'est à dire $\forall x = \sum_{i=1}^{n} x_i f_i$, ϕ envoie la base $(e_1, ..., e_n)$ de E sur la base $(f_1, ..., f_n)$ de F, donc c'est un isomorphisme. □

Nota Bene. Autrement dit, si E, F sont de dimensions finies , un isomorphisme est une application linéaire qui transforme les bases de E en bases de F, et cela suppose $dim(F) = dim(E)$

Proposition- Caractérisation des isomorphismes en dimension finie. Soient E et F deux $\mathbb{K} - ev$ de même dimension finie. Soit $\phi \in \mathcal{L}(E, F)$. Les assertions suivantes sont équivalentes :

1. ϕ est un isomorphisme
2. ϕ est injective
3. ϕ est surjective
4. ϕ envoie une base de E sur une base de F

Démonstration. Il suffit de vérifier (2) $\Leftrightarrow$ (3) (car leur conjonction $\Rightarrow$ (1)). On a (2) (ϕ est injective) $\Leftrightarrow$ $Ker(\phi) = \{0\} \Leftrightarrow dim(Ker(\phi)) = 0$

$\Leftrightarrow dim(Im(\phi)) = dim(E)$(théorème du rang)

$\Leftrightarrow dim(Im(\phi)) = dim(F)$ (puisque $dim(F) = dim(E)$) $\Leftrightarrow$ (3)(ϕ est injective). □

Remarque. C'est faux si E, F sont de dimension infinie. Contre exemple classiques :

$$\phi : \begin{cases} \mathbb{K}[X] \to \mathbb{K}[X] \\ P(X) \to XP(X) \end{cases}$$

1. ϕ est linéaire, injective car $XP(X) = XQ(X) \Rightarrow P(X) = Q(X)$ mais pas surjective car $1 \notin Im(\phi)$:il n'existe pas $P(X) \in \mathbb{K}[X]$. Tel que $XP(X) = 1$ puisqu'on aurait $P(X) = \frac{1}{X} \notin \mathbb{K}[X]$.

2. $\Psi : \begin{cases} \mathbb{K}[X] \to \mathbb{K}[X] \\ P \to P' \end{cases}$. Ψ est linéaire, surjective car tout polynôme $\sum_{i\geq 0} a_i X^i$ est la dérivée d'un polynôme : $\sum_{i\geq 0} a_i X^i = (\sum_{i\geq 0} \frac{a_i}{i+1} X^{i+1})' = \Psi(\sum_{i\geq 0} \frac{a_i}{i+1} X^{i+1})$. Mais Ψ n'est pas injective : $\Psi(1) = 0 \Rightarrow 1 \in Ker(\Psi)$!

26 Deux exemples important d'applications linéaires.

1. **Homothétie** $h(x) = \lambda x, \lambda \in \mathbb{K}$ (bijective si et seulement si $\lambda \neq 0$). Si $\lambda = 0, h = 0, Ker(h) = E, Im(h) = \{0\}$. Si $\lambda \neq 0$, h est automorphe, $h^{-1}(y) = \lambda^{-1} y$. avec $Ker(h) = \{0\}, Im(h) = E$
2. $E = V \oplus W$ Tout $x \in E$ s'écrit de manière unique $x = v + w, v \in V, w \in W$ car $V \cap W = \{0\}$: $v + w = v' + w' \Rightarrow v(v') = w' - w \Rightarrow v - v' = 0$ et $w - w' = 0$. On note $v = p(x)$: p linéaire, le projecteur (ou la projection) sur V parallèlement à W.

27 Projecteurs et symétries.

Nota Bene. Projecteurs et symétries sont des applications **linéaires**.

Proposition. Soient $E = V \oplus W$, p le projecteur sur V parallèlemet à W, S la symétrie par rapport à V parallèlement à W. On a : $pop = p$ et $sos = id_E$

Démonstration. $x = v + w$

— $p(x) = v = v + 0 \Rightarrow pop(x) = p(p(x)) = p(v) = v = p(x)$ donc $pop = p$

— $S(x) = v - w \Rightarrow S(S(x)) = v - (-w) = v + w = x$ donc $sos = id_E$

□

Proposition (Caractérisation des projecteurs). Soient E un $\mathbb{K} - ev$ et $p \in \mathcal{L}(E))$ tel que $pop = p$. Alors $E = Im(p) \oplus Ker(p)$ et p est la projecteur sur $Im(p)$ parallèlement à $Ker(p)$.

Démonstration. Pour tout $x \in E$: $x = p(x) + (x - p(x))$ où $p(X) \in Im(p)$ et $x - p(x) \in Ker(p)$ car $p(x - p(x)) = p(x) - pop(x) = 0$ puisque $pop = p$. Cela prouve déjà que $E = Im(p) + Ker(p)$. Montrons que $Im(p) \cap Ker(p) = \{0\}$. soit $x \in Im(p) \cap Ker(p)$: $x \in Im(p) \Rightarrow \exists y / x = p(y) \Rightarrow p(x) = pop(y) = p(y) = x$. Donc $x = 0$.

On e conclut que $E = Im(p) \oplus Ker(p)$ Donc la décomposition $x = v + w$ avec $v \in Im(p), w \in Ker(p)$ est unique (pour chaque $x \in E$) : nécessairement $v = p(x), w = x - p(x)$.

Le projecteur sur $Im(p)$ parallèlement à $Ker(p)$ envoie x sur $v = p(x)$ (pour tout x) donc c'est p. □

Proposition (Caractérisation des symétries). Soit E un $\mathbb{K} - ev$ et $S \in \mathcal{L}(E) \setminus sos = id_E$. Alors $E = Ker(id_E - S) \oplus Ker(id_E + S)$ et S est la symétrie par rapport à $Ker(id_E - S)$ parallèle à $Ker(id_E + S)$.

Démonstration. Pour $x \in E$: $x = \frac{x + S(x)}{2} + \frac{x - S(x)}{2}$ où $\frac{x + S(x)}{2} \in Ker(id_E - S)$ car $(id_E - S)(\frac{x + S(x)}{2}) = \frac{x + S(x)}{2} - S(\frac{x + S(x)}{2}) = \frac{x + S(x)}{2} - \frac{S(x) + sos(x)}{2} = \frac{x + S(x)}{2} - \frac{S(x) + x}{2} = 0$

Et de même $\frac{x-S(x)}{2} \in Ker(id_e+S)$. Donc $E = Ker(id_E - S) + Ker(id_E + S)$. Montrons que $Ker(id_E - S) \cap Ker(id_E + S) = \{0\}$.

Soit $x \in Ker(id_E - S) \cap Ker(id_E + S)$: alors $\begin{cases} (id_E - S)(x) = 0 \\ (id_E + S)(x) = 0 \end{cases}$ donc $\begin{cases} S(x) = x \\ S(x) = -x \end{cases}$ d'où $x = -x$ et donc $x = 0$.

Ainsi : $E = Ker(id_E - S) \oplus Ker(id_E + S)$. Pour tout $x \in E$, la décomposition $x = v + w$ où $v \in Ker(id_E - S)$ et $w \in Ker(id_E + S)$ est unique. Nécessitant : $v = \frac{x+S(x)}{2}, w = \frac{x-S(x)}{2}$ la symétrie par rapport à $Ker(id_E - S)$ parallèlement à $Ker(id_E + S)$ envoie x sur $v - w = \frac{x+S(x)}{2} - \frac{x-S(x)}{2} = S(x)$: donc c'est S. □

28 Hyperplan.

Définition. Soit E un $\mathbb{K} - ev$. On dit qu'un *sev* H de E est un **hyperplan** de E s'il est le noyau d'une application linéaie $\phi : E \to \mathbb{R}$ non nulle (ie ϕ n'est pas l'application nulle).

Nota Bene. Une application linéaire $E \to \mathbb{R}$ est applée une **forme linéaire**.

Proposition. Soit E un $\mathbb{K} - ev$ de dimension finie : $dim(E) = n$. Un *sev* H de E est un hyperplan si et seulemet si $dim(H) = n - 1$

Remarque. Pour $n = 3$, un hyperplan est un plan : $dim(H) = 2$. D'où le nom.

Démonstration.

— Soit H un hyperplan : $H = Ker(\phi), \phi \neq 0$. $\phi \neq 0$ donc il existe $v \in E / \phi(v) = \lambda \neq 0$. Alors $\phi(\lambda^{-1}v) = \lambda^{-1}\phi(v) = 1$ et $\forall t \in \mathbb{R}, \phi(t\lambda^{-1}v) = t\phi(\lambda^{-1}v)$ donc $Im(\phi) = \mathbb{R}$ (L'image d'une forme linéaire non nulle est $\mathbb{R}$)

Et donc : $dim(H) = dim(Ker(\phi)) = n - dim(Im(\phi)) = n - 1$

— (Réciproque). Soit H un *sev* de E de dimension $n-1$. Soit $v \in H$: $\forall \lambda \neq 0, \lambda v \notin H$ (car $\lambda v \in H \Rightarrow \lambda^{-1}(\lambda v) \in H$). Donc $\mathbb{K}v \cap H = \{0\}$.

Grassmann $\Rightarrow dim(\mathbb{K}v + H) = dim(\mathbb{K}v) + dim(H) - dim(\mathbb{K}v \cap H)$

$\Rightarrow dim(\mathbb{K}v + H) = n = dim(E)$ et donc $\mathbb{K}v + H = E$. On obtient donc $E = H \oplus \mathbb{K}v$. Soit p le projecteur sur $\mathbb{K}v$ parallèlement à H : $\forall x \in E : x = h + p(x)$ où $h \in H, p(x) = \phi(x)v$, ϕ est ue forme linéaire, non nulle car $\phi(v) = 1 (p(v) = v)$. Et il est clair que $x \in H \Leftrightarrow \phi(x) = 0$ donc $H = Ker(\phi)$.

□

Définition. L'espace $\mathcal{L}(E, \mathbb{R})$ des formes linéaires sur E (ie définies sur E) est appelé l'espace dual de E : on le note $E*$

Proposition. Si E est de dimension finie, soit $(e_1, ..., e_n)$ une base de E. Alors $E*$ est de dimension finie à $n = dim(E)$ et il existe une unique base $(e*_1, ..., e*_n)$ de $E*$ vérifiant : $e *_i (e_j) = \begin{cases} 1 \text{ si } j = i \\ 0 \text{ sinon} \end{cases}$ $(1 \leq i, j \leq n)$

on l'appelle la base double de $(e_1, ..., e_n)$. Et pour tout $\phi \in E*$, on a la décomposition :

$$\phi = \sum_{i=1}^{n} \phi(e_i) e*_i$$

Démonstration. On définit $e *_i (1 \leq i \leq n)$ par

$$e *_i (e_j) = \begin{cases} i \text{ si } j = 1 \\ 0 \text{ sinon} \end{cases}$$

Cela définit bien un $e*_i \in E*$ pour tout $i \in \{1, ..., n\}$. Montrons que $(e*_1, ..., e*_n)$ est libre : $\sum_{i=1}^{n} \lambda_i e*_i = 0 \Rightarrow \forall j, \sum_{i=1}^{n} \lambda_i e *_i (e_j) = 0 \Rightarrow \forall j, \lambda_j = 0$. Donc $(e*_1, ..., e*_n)$ est libre. Pour justifier que c'est une famille génératrice (donc une base) de $E*$, il suffit de justifier la formule : $\forall \phi \in E*, \phi = \sum_{i=1}^{n} \phi(e_i) e *_i$. Or, $\forall j \in \{1, ..., n\}$. Donc $\phi(e_j) = \sum_{i=1}^{n} \phi(e_i) e *_i (e_j)$ □

Cinquième partie

Matrices

29 Introduction et généralités

Définition Une matrice sur $\mathbb{K}$ à n lignes et m colonnes est un tableau d'élements de $\mathbb{K}$:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix} = (a_{ij})$$

($i = n^\circ$ de la ligne , $j = n^\circ$ de la colonne)

On note $\mathcal{M}_{n,m}(\mathbb{K})$ l'ensemble de ces matrices. Si $n = m$ on le note simplement $\mathcal{M}_n(\mathbb{K})$

Définition (Opérations sur les matrices).

— Addition dans $\mathcal{M}_{n,m}(\mathbb{K})$: $(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$
Exemple ($n = m = 2$) : $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}$

— Multiplication par un scalaire : $\lambda(a_{ij}) = (\lambda a_{ij})$ Exemple ($n = m = 2$) : $\lambda \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}$

— Produit d'une matrice de $\mathcal{M}_{n,m}(\mathbb{K})$ et d'une matrice $\mathcal{M}_{m,l}(\mathbb{K})$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} . \begin{pmatrix} e & f & g \\ h & i & j \end{pmatrix} = \begin{pmatrix} ae+bh & af+bi & ag+bj \\ ce+dh & cf+di & cg+dj \end{pmatrix}$$

Le produit se fait en multipliant terme à terme chaque ligne de A par chaque colone de B. En général on a $AB \neq BA$ et $A \neq 0$, $B \neq 0$.

Proposition.

1. Soit $(\mathcal{M}_{n,m}(\mathbb{K}), +, \times)$ un $\mathbb{K} - ev$ de dimension nm. Une base est (E_{ij}) où E_{ij} est la matrice ayant 1 à l'intersection de la ligne i et de la colonne j, et des 0 partout ailleurs. (E_{ij}) est appelée la base canonique de $\mathcal{M}_{n,m}(\mathbb{K})$.
2. $\mathcal{M}_n(\mathbb{K}) = \mathcal{M}_{n,m}(\mathbb{K})$ muni de $+, ., \times$ est une $\mathbb{K} - algebre$, unitaire (l'élément neutre pour $\times$ est $I_m = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$: 1 sur la diagonale, 0 partout ailleurs : on l'appelle la matrice unité), non commutative ($AB \neq BA$ en général), non intègre ($A \neq 0$ et $B \neq 0$ n'impliquent pas $AB \neq 0$).

Démonstration. 1. On va justifier que (E_{ij}) est une base pour le cas où $n = m = 2$ (le cas général n'est pas plus difficile). (Le fait que $\mathcal{M}_{n,m}(\mathbb{K})$ est un $\mathbb{K} - ev$ est assuré par le trot de l'âne...)

Pour $n = m = 2$: $\mathcal{M}_2(\mathbb{K}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{K} \right\}$. Or $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + b \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + c \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + d \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ donc $(E_{11}, E_{12}, E_{21}, E_{22})$ est génératrice de $\mathcal{M}_2(\mathbb{K})$. Et elle est libre car :

$$aE_{11} + bE_{12} + cE_{21} + dE_{22} = 0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Leftrightarrow \begin{cases} a = 0 \\ b = 0 \\ c = 0 \\ d = 0 \end{cases}$$

Donc c'est une base pour n, m quelconques. Donc $dim\mathcal{M}_{n/m}(\mathbb{K}) = n \times m$

2. Âne qui trotte et exemple déjà vu pour $AB \neq BA, AB = 0$ avec $A \neq 0, B \neq 0$

□

Définition. On dit qu'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est carrée (même nombre de lignes et de colonnes), $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est une matrice carée.

Définition et proposition. Une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est dite **inversible** s'il existe une matrice $B \in \mathcal{M}_n(\mathbb{K})$ tel que $AB = BA = I_n$. Cette matrice B est alors unique (et il suffit d'avoir $AB = I_n$ ou $BA = I_n$ pour qu'on ait $AB = BA = I_n$. On la note : $B = A^{-1}$.

Preuve (unicité). Si $AB = BA = I_n$ alors : $BAB' = (BA)B' = I_nB' = B'$ et $BAB' = B(AB') = BI_n = B$. Ainsi $B' = B$.

Définition. L'ensemble des matrices inversibles de $\mathcal{M}_n(\mathbb{K})$ est un groupe (pour la multiplication des matrices), qu'on note $\mathcal{GL}_n(\mathbb{K})$ (car il s'identifie au groupe linéaire $\mathcal{GL}_n(\mathbb{K})$ formé des automorphismes de $\mathbb{K}^n$ on va voir cela...).

Définition (Matrice d'une application linéaire). Soient E un $\mathbb{K} - ev$ de dimension m, F un $\mathbb{K} - ev$ de dimension n, $B_E = (e_1, ..., e_m)$ une base de E, $B_F = (f_1, ..., f_n)$ une base de F, $\phi \in \mathcal{L}(E, F)$. Ecrivons $\phi(e_j) = \sum_{i=1}^{n} a_{ij} f_i$. On appelle matrice de ϕ par rapport aux bases B_E, B_F la matrice $A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}$

Nota Bene. La j^{me} colonne de $Mat_{B_E,B_F}(\phi)$ donne (de haut en bas) les coordonées de $\phi(e_j)$ dans la base B_F.

Proposition. Sous les hypothèses et notations de la définition, si on note $X = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$ la colonne des coordonnées d'un vecteur x de E dans la base $B_E (x = \sum_{j=1}^{m} x_j e_j)$ et $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$. La colone des coordonées d'un vecteur y de F dans la base $B_F (y = \sum_{i=1}^{n} y_i f_i)$, alors :

$$y = \phi(x) \Leftrightarrow Y = AX \text{ où } A = Mat_{B_E, B_F}(\phi)$$

Démonstration. $y = \sum_{i=1}^{n} y_i f_i$ et $x = \sum_{j=1}^{m} x_j e_j \Rightarrow \phi(x) = \sum_{j=1}^{m} x_j \phi(e_j) = \sum_{j=1}^{m} x_j \sum_{i=1}^{n} a_{ij} f_i = \sum_{i=1}^{n} (\sum_{j=1}^{m} a_{ij} x_j) f_i$

Donc $y = \phi(x) \Leftrightarrow \forall i \in \{1, ..., n\}, y_1 = \sum_{j=1}^{m} a_{ij} x_j$

$$\Leftrightarrow \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1m}x_m \\ a_{21}x_1 + a_{22}x_2 + ... + a_{2m}x_m \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nm}x_m \end{pmatrix}$$ □

Proposition (Correspondance entre matrices et applications linéaires : suite). Soient E, F des $\mathbb{K}-ev$ de dimension finie, B_E une base de E, B_F une base de F. $\Phi, \Psi \in \mathcal{L}(E, F)$. Alors :

1. $Mat_{B_E, B_F}(\Phi + \Psi) = Math_{B_E, B_F}(\Phi) + Mat_{B_E, B_F}(\Psi)$
2. $\forall \lambda \in \mathbb{K}, Mat_{B_E, B_F}(\lambda\Phi) = \lambda Mat_{B_E, B_F}(\Phi)$.
3. Si G est un 3ème $\mathbb{K} - ev$ de $dim < \infty$, et $\Phi \in \mathcal{L}(E, F), \Psi \in \mathcal{L}(F, G)$, et B_G une base de G alors : $Mat_{B_E, B_G}(\Psi o \Phi) = Mat_{B_F, B_G}(\Psi) \times Mat_{B_E, B_F}(\Phi)$.

Démonstration. (du (3))

$y = \sum_{i=1}^{n} y_i f_i$ et $x = \sum_{j=1}^{m} x_j e_j \Rightarrow \phi(x) = \sum_{j=1}^{m} x_j \phi(e_j) = \sum_{i=1}^{n} (\sum_{j=1}^{m} a_{ij} x_j) f_i$ et $z = \Psi(y) = \Psi o \Phi(x) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} x_j \Psi(f_i)$

Donc : $\Psi o \Phi(x) = \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{k=1}^{l} a_{ij} b_{ki} x_j g_k = \sum_{k=1}^{l} (\sum_{j=1}^{m} (\sum_{i=1}^{n} b_{ki} a_{ij}) x_f) g_k) = \sum_{k=1}^{l} (\sum_{j=1}^{m} c_{kj} x_j) g_k$

Donc les coordonnées dans B_G de $\Psi o \Phi(x)$ sont les $(\sum_{j=1}^{m} c_{kj} x_j)$, i.e $Mat_{B_E, B_G}(\Psi o \Phi) = C = BA$ □

Corollaire. Soient E, F dans $\mathbb{K} - ev$ de $dim < \infty, B_E, B_F$ des bases $\Psi \in \mathcal{L}(E, F), A = Mat_{B_E, B_F}(\Phi)$. Alors Φ est bijective $\Leftrightarrow A$ est inversible. Et alors $Mat_{B_F, B_E}(\Phi^{-1}) = (Mat_{B_E, B_F}\Phi)^{-1}$

Démonstration. pour $F = E$, $B_F = B_E$.

Si Φ est bijective : $\Phi o \Phi_{-1} = id_E \Rightarrow Mat(\Phi).Mat(\Phi^{-1}) = Mat(id_E) = I_n$ (où $n = dim(E)$). Et réciproquement, si $Mat(\Phi)$ est inversible, soit $\Psi \in \mathcal{L}(E)$ tel que $Mat_{B_E}\Psi = Mat_{B_E}\Phi^{-1}$: alors $Mat(\Phi o \Psi) = Mat_{B_E} id_E \Rightarrow \Phi o \Psi = id_E \Rightarrow \Psi = \Phi^{-1}$ □

Définition (Matrice de passage). Soient E un $\mathbb{K}-w$ de $dim(n)<\infty$, B, B' deux bases de E : $B=(e_1,...,e_n), B'=(e'_1,...,e'_n)$

On appelle **matrice de passage** P de B à B' la matrice de id_E où E est muni de la base B' au départ et de la base B à l'arrivée.

$$\begin{cases}(E,B')\to(E,B)\\ P=Mat_{B',B}(id_E)\end{cases}$$

Nota Bene. Les colonnes de P sont les colonnes de coordonnées des e'_j dans la base $(e_1,...,e_n)=B$

Exemple. $E=\mathbb{R}^2, B=((1,0),(0,1)), B'=((1,1),(1,-1)) : \begin{cases}e'_1=e_1+e_2\\ e'_2=e'_1-e_1\end{cases} \Rightarrow P=\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$

Proposition. Soit E un $\mathbb{K}-ev$ de $dim(n)<\infty$. Soient B, B' deux bases de E. Soient $x\in E$, X la colonne de ses coordonnées dans la base B et X' la colonne de ses coordonnées dans la base B'.
P est la matrice de passage de B à B'. Alors : $X=PX'$ (autrement dit : $X'=P^{-1}X$. Noter que P^{-1} est la matrice de passage de B' à B : $(E,B')\to(E,B)$ par p et $(E,B)\to(E,B')$ par $p-1$.

Démonstration. On a vu que $y=f(x)\Leftrightarrow Y=AX$ où A est la matrice de f. Ici on a X' (et non X) au départ, X à l'arrivée donc $x=id_E(x)\Leftrightarrow X=PX'$ □

Théorème de changement de base. Soient E, F deux $\mathbb{K}-ev$ de dimension finies B_1 , B'_1 deux bases de E, B_2, B'_2 deux bases de F. P la matrice de passage de B_1 à B'_1 et Q la matrice de passage de B_2 à B'_2.
Ainsi $f\in\mathcal{L}(E,F), A=Mat_{(B_1,B_2)}(f), A'=Mat_{B'_1,B'_2}(f)$ Alors

$$A'=Q^{-1}AP$$

En particulier. Si $F=E$ et $B_2=B_1$ et $B'_2=B'_1$, alors $Q=P$ et

$$A'=P^{-1}AP$$

Démonstration. $(E,B'_1)\overset{id_E}{\to}(E,B_1)\overset{f}{\to}(F,B_2)\overset{id_F}{\to}(F,B'_2)$. On compose : $id_F o f o id_E$ et les matrices : $A'=Mat_{B_2,B'_2}(id_F)Mat_{B_1,B_2}(f)Mat_{B'_1,B_1}(id_E)=Q^{-1}AP$. □

Définition.

- Deux matrices A, B de $\mathcal{M}_{n,m}(\mathbb{K})$ sont dites équivalentes s'il existe $P\in\mathcal{M}_m(\mathbb{K})$ inversible et $Q\in\mathcal{M}_n(\mathbb{K})$ inversible tel que $B=Q^{-1}AP$. Cela revient à dire qu'il existe une application linéaire de $\mathbb{K}^m$ dans $\mathbb{K}^n$ dont A et B sont les matrices relativement à certaines bases.
- Deux matrices $A, B\in\mathcal{M}_n(\mathbb{K})$ sont dites semblables s'il existe $P\in\mathcal{M}_n(\mathbb{K})$ inversible tel que $B=P^{-1}AP$. Cela revient à dire que A et B sont les matrices d'un endomorphisme de $\mathbb{K}^n$ relativement à deux bases B_A (au départ et à l'arrivée) et B_B (au départ et à l'arrivée) respectivement.

30 Matrice Transposée et Symétrique

Définition. Soit $A \in \mathcal{M}_{n,m}(\mathbb{K})$. On appelle transposée de A, et on note ${}^tA$, la matrice de $\mathcal{M}_{m,n}(\mathbb{K})$ obtenue en mettant les colonnes de A en lignes. (ou les lignes de A et colonnes : ça revient au même).

Exemple. ${}^t\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$.

Définition. Une matrice carrée $A \in \mathcal{M}_n(\mathbb{K})$ est dite symétrique si et seulement si ${}^tA = A$, antisymétrique si ${}^tA = -A$.

Exemples. Les matrices symétriques sont : pour $n = 2$: $\begin{pmatrix} a & b \\ b & d \end{pmatrix} = a\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

En effet : ${}^t\begin{pmatrix} a & b \\ c & d \end{pmatrix} \Leftrightarrow c = b$.

Noter que transposition est une symétrie par rapport à la diagonale : .${}^t\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$

Pour n quelconque : l'ensemble des matrices symétriques de $\mathcal{M}_n(\mathbb{K})$ est le *sev* $Sym_n(\mathbb{K})$ de $\mathcal{M}_n(\mathbb{K}$ engendré par les E_{ii} $(1 \leq i \leq n)$ et les $E_{ij} + E_{ji}$ $(1 \leq i < j \leq n)$. Clairement : $dim(Sym_n(\mathbb{K})) = n + \dfrac{n^2 - n}{2} = \dfrac{n(n+1)}{2}$

${}^t(a_{ij}) = (a_{ji})$ la transposition échange les indices donc (a_{ij}) est symétrique $\Leftrightarrow a_{ij} = a_{ji} \forall i$ et $\forall j$.

Pour $n = 3$: $\begin{pmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{pmatrix} = a(E_{12} - E_{21}) + b(E_{13} - E_{31}) + c(E_{23} - E_{32})$

Pour n général : L'ensemble $Ant_n(\mathbb{K})$ des matrices antisymétriques de $\mathcal{M}_n(\mathbb{K})$ est le sev engendré par les $E_{ij} - E_{ji}$ $(1 \leq i \leq j \leq n)$: donc

$$dim(Ant_n(\mathbb{K})) = \frac{n^2 - n}{2} = \frac{n(n-1)}{2}$$

31 Trace

Définition. On appelle **trace** d'une matrice carée $A = (a_{ij}) \in \mathcal{M}_n(\mathbb{K})$ le scalaire : $tr(A) = \sum_{i=1}^{n} a_{ii}$ (la somme des éléments diagonaux).

Proposition.

1. $tr({}^tA) = tr(A) \forall A \in \mathcal{M}_n(\mathbb{K})$
2. $tr(AB) = tr(BA) \forall A, B \in \mathcal{M}_n(\mathbb{K})$
3. Deux matrices semblables ont la même trace. Et donc deux matrices A, A' d'un même endomorphisme (relation à des bases identiques au départ et à l'arrivée) ont même trace.

Démonstration. 1. $tr({}^tA) = tr(A)$ car les éléments de la diagonales de ${}^tA$ sont les mêmes que ceux de la diagonale de A

$$\begin{pmatrix} a_{11} & & a_{ij} \\ & \ddots & \\ a_{ji} & & a_{nm} \end{pmatrix}$$

2. $A = (a_{ij}), B = (b_{ij}) \Rightarrow AB = (c_{ij})$ où $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$

   Donc $tr(AB) = \sum_{i=1}^{n} c_{ii} = \sum_{i=1}^{n}\sum_{k=1}^{n} a_{ik}b_{ki}$

   De même en échangeant les a et les b : $tr(BA) = \sum_{i=1}^{n}\sum_{k=1}^{n} b_{ik}a_{ki} = \sum_{i=1}^{n}\sum_{k=1}^{n} a_{ki}b_{ik} = tr(AB)$

3. $tr(P^{-1}AP) = tr(APP^{-1}) = tr(A)$

□

Nota Bene. La trace est un invariant : étant donné un endomorphisme f de E ($dim(E) < \infty$), quand je change de base dans E, la matrice de f change mais sa trace ne change pas.

Sixième partie

Déterminants

Proposition et définition. Il existe une fonction $det(\mathcal{M}_n(\mathbb{K})) \to \mathbb{K}$ (appelée déterminant), unique, tel que :

1. *det* est linéaire par rapport à chaque colonne : c'est à dire que si $c_1, ..., c_n$ désignent les colonnes de la matrice $A \in \mathcal{M}_n(\mathbb{K})$, alors $\forall j \in \{1, ..., n\}$, l'application $c_j \to det(c_1, ..., c_{j-1}, c_j, c_{j+1}, ..., c_n)$ est linéaire.
2. Si on échange deux colonnes de A, $det(A)$ change de signe (on dit que *det* est antisymétrique ou alterné).

$$det(C_1, ..., C_j, ..., C_k, ..., C_n) = -det(C_1, ..., C_j, ..., C_n)$$

3. $det(I_n) = 1$ (où I_n est la matrice unité)

$det(A)$ est appelé determinant de A. La fonction *det* vérifie en outre la propriété : $det({}^tA) = det(A)$ pour toute $A \in \mathcal{M}_n(\mathbb{K})$, où $det({}^tA)$ est la transposée de A. D'où il découle que $det(A)$ est aussi une fonction linéaire de chaque ligne de A et une fonction antisymétrique des lignes de A (puisque les lignes de A sont les colonnes de $det({}^tA)$).

Proposition. Pour toute $A \in \mathcal{M}_n(\mathbb{K})$ et tout $\lambda \in \mathbb{K}$: $det(\lambda A) = \lambda^n det(A)$.

Démonstration. Comme le déterminant est linéaire par rapport à chaque colonne, on a pour tous $\lambda_1, ..., \lambda_n \in \mathbb{K}$: $det(\lambda_1 C_1, ..., \lambda_n C_n) = \lambda_1 ... \lambda_n det(C_1, ..., C_n)$. Prenant $\lambda_1, ..., \lambda_n$ égaux à λ on obtient $det(\lambda A) = \lambda^n det(A)$. □

Proposition.

1. Si deux colones de A sont égales, alors $det(A) = 0$.
2. Si on ajoute à une colonne une combinaison linéaire des autres, le déterminant ne change pas.
3. Les deux propriétés ci-dessus sont vraies aussi pour les lignes.

Démonstration.

1. Si $C_j = C_k (j < k)$, on a $det(C_1, ..., C_j, ..., C_k, ..., C_n) = -det(C_1, ..., C_k, ..., C_j, ..., C_n)$ (antisymétrie) et $det(C_1, ..., C_j, ..., C_k, ..., C_n) = det(C_1, ..., C_k, ..., C_j, ..., C_n)$ (puisque $C_j = C_k$) donc $det(C_1, ..., C_j, ..., C_k, ..., C_n) = 0$
2. Par linéarité :

$$det(C_1, ..., C_j + \sum_{k \neq j} \lambda_k C_k, ..., C_n)$$

$$= det(C_1, ..., C_j, ..., C_n) + \sum_{k \neq j} \lambda_k det(C_1, ..., C_k, ..., C_n)$$

mais $det(C_1, ..., C_k, .., C_n)$ est nul (pour $k \neq j$), vu la propriété précédente, puisque la même colonne C_k se trouve aussi à la place k.

3. Vu que $det(A) = det({}^tA)$, les propriétés ci-dessus sot vraies pour les lignes de A (qui sont les colonnes de $det({}^tA)$)

□

Proposition.

$$\text{Si } det(A) \neq 0, \text{ alors } A \text{ est inversible}$$

Démonstration. Si A n'est pas inversible, c'est que ses colonnes ne sont pas linéairemet indépendantes (confère la caractérisation des isomorphismes, appliquée à l'endomorphisme de $\mathbb{K}^n$ dont la matrice dans la base canonique est A) : disons $C_j = \sum_{k \neq j} \lambda_k C_k$ pour un certain j. Vu la proposition précédente,

$$det(A) = det(C_1, ..., \sum_{k \neq j} \lambda_k C_k, ..., C_n) = det(C_1, ..., 0, ..., C_n)$$

Or, $det(C_1, ..., 0, ..., C_n) = 0$ (car c'est une fonction linéaire de la colonne j, ici nulle), donc $det(A) = 0$. Par contraposition, si $det(A) \neq 0$, alors A est inversible. □

Remarque 1. Si $A \neq 0$, c'est qu'aucune des colonnes n'est combinaison linéaire des autres (puisqu'on vient de voir que si une colonne est combinaison linéaire des autres), le déterminant est le même que si on remplace cette colonne par $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ et par linéarité le déterminant est nul, et donc les colonnes de A sont indépendantes.
Mais ces colonnes sont les colonnes de coordonnées de $f(e_1), ..., f(e_n)$ où $(e_1, ..., e_n)$ est la base canonique de $\mathbb{K}^n$ et f l'endomorphisme de $\mathbb{K}^n$ dont A est la matrice (relativement à la base canonique). Donc dire les connes de A sont linairement indépendantes, c'est à dire que $(f(e_1), ..., f(e_n))$ est libre, c'est à dire que c'est une base de $\mathbb{K}^n$, donc que f est un automorphisme , c'est à dire que A est inversible.

Lemme. Soient $A \in \mathcal{M}_n(\mathbb{K})$ tel que $det(A) \neq 0$ et $X_1, ..., X_n \in \mathcal{M}_{n,l}(\mathbb{K})$ des colonnes quelconques. Alors :

$$\frac{det(AX_1, ..., AX_n)}{det(A)} = det(X_1, ..., X_n)$$

Démonstration. Il est clair que le premier membre de (1) est une fonction linéaire de chaque X_j, qu'il est antisymétrique comme fonction de $(X_1, ..., X_n)$, et qu'il vaut 1 quand $(X_1, ..., X_n) = I_n$ (car alors $AX_1, ..., AX_n = AI_n = A$) : ce sont les propriétés caractéristiques du second membre. □

Théorème. Soient $A, B \in \mathcal{M}_n(\mathbb{K})$. Alors :

$$det(AB) = det(A)det(B)$$

Démonstration. Prouvons-le d'abord pour le cas où $det(A) \neq 0$. O prend $(X_1, ..., X_n) = B$ dans (1) (donc $(AX_1, ..., AX_n) = AB$) : alors $\frac{det(AB)}{det(A)} = det(B)$ d'où $det(AB) = det(A)det(B)$.
Si $det(A) = 0$, considérons $det(A + xI_n)$: vu que det est linéaire par rapport à chaque colonne et que la colonne j de $A + xI_n$ contient le terme $a_{jj} + x$ à la $j - ime$ place, $det(A + xI_n)$ est une fonction polynomiale de x ; elle a donc

un ombre fini de racines (dont 0, par hypothèse). Soit $\epsilon > 0$ tel que $0 < x < \epsilon \Rightarrow det(A+xI_n) \neq 0$. Pour $0 < x < \epsilon$ on a $det((A+xI_n)B) = det(A+xI_n)det(B)$ d'où par continuité, en faisant $x \to 0$: $det(AB) = det(A)det(B)$. □

Corollaire. Si A est inversible, alors $det(A) \neq 0$ et $det(A^{-1}) = \dfrac{1}{det(A)}$, alors $det(A) \neq 0$ et $det(A^{-1}) = \dfrac{1}{det(A)}$

Démonstration. $AA^{-1} = I_n \Rightarrow det(AA{-}1) = det(I_n) = 1 \Rightarrow det(A)det(A^{-1}) = 1$ □

Corollaire. Soient E un $\mathbb{K} - ev$ de dimension n, $\phi : E \to E$ un endomorphisme, A la matrice de ϕ dans une base B, A' sa matrice dans une base B' : alors $det(A') = det(A)$. Autrement dit, le déterminant de la matrice de ϕ est indépendant de la base et on peut donc le notre simplement $det(\phi)$. Et pour tous endomorphismes ϕ, ψ de E, $det(\phi o \psi) = det(\psi)det(\phi)$

Démonstration. On a $A' = P^{-1}AP$ (où P est la matrice de passage de B à B') donc

$$det(A') = det(P^{-1})det(A)det(P) = \frac{1}{det(P)}det(A)det(P) = det(A)$$

La formule $det(\psi o \phi) = det(\psi)det(\phi)$ n'est qu'une réécriture de $det(BA) = det(B)det(A)$ où A et B sont les matrices de ϕ et ψ dans une base quelconque. □

Définition. Soient E un $\mathbb{K} - ev$ de dimension $n, B = (e_1, ..., e_n)$ une base de $E, x_1, ..., x_n$ des vecteurs de $E, X_j (1 \leq j \leq n)$ la colonne des coordonnées de x_j dans la base B (écritues de haut en bas). On définit le déterminant de la famille $(x_1, ..., x_n)$ dans la base B comme étant le déterminant de la matrice dont les colonnes sont $X_1, ..., X_n$: $det_B(x_1, ..., x_n) = det(X_1, ..., X_n)$.

Remarque (interprétation géométrique).

1. Soient u, v deux vecteurs du plan $\mathbb{R}^{\not 2}$, rapporté à sa base canonique B : l'aire du parallélogramme construit sur les côtés u, v est $|det(u, v)|$.
2. Soient u, v, w trois vecteurs de l'espace $\mathbb{R}^3$, rapporté à sa base canonique B : le volume du parallélépipède construit sur les côtes u, v, w est $|det(u, v, w)|$.

Corollaire. Dans la situation de la définition ci-dessus, si B' est une autre base de E et P la matrice de passage de B à B', on a :

$$det_B(x_1, ..., x_n) = det(P)det_{B'}(x_1, ..., x_n)$$

Preuve Soit X'_j la colonne des coordonnées de x_j dans la base B' : on sait que $X_j = PX'_j$, donc $(X_1, ..., X_n) = P(X'_1, ..., X'_n)$, d'où $det(X_1, ..., X_n) = det(P)det(X'_1, ..., X'_n)$.

Proposition (critère d'inversibilité et caractérisation des bases par les déterminants).

1. Une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est inversible si et seulement si $det(A) \neq 0$.
2. Un endomorphisme ϕ d'un $\mathbb{K} - ev$ de dimension n est un isomorphisme si et seulement si $det(\phi) \neq 0$.

3. Soient n vecteurs $x_1, ..., x_n$ dans un $\mathbb{K} - ev$, E de dimension n et B une base quelconque de E. alors $(x_1, ..., x_n)$ est une base si et seulement si $det_B(x_1, ..., x_n) \neq 0$.

Démonstration.

1. L'implication "$det(A) \neq 0 \Rightarrow A$ est inversible" a fait l'objet d'une proposition, et le premier corollaire donne la réciproque.
2. $det(\phi) = det(A)$ où A est la matrice de ϕ dans une base quelconque et ϕ est bijective si et seulement si A est inversible : ce qui nous ramène à l'assertion précédente.
3. $det_B(x_1, ..., x_n) \neq 0$ signifie $det(X_1, ..., X_n) \neq 0$ (où X_j est la colonne des coordonnées de x_j dans la base B) : cela équivaut à dire que la matrice $(X_1, ..., X_n)$ est inversile et donc que $(x_1, ..., x_n)$ est une base.

□

Théorème. Soit $A = (a_{ij})_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{K})$. Pour tous $i, j \in \{1, ..., n\}$, soit $A_{ij} \in \mathcal{M}_{n-1}(\mathbb{K})$ la matrice obtenue en supprimant dans A la ligne i et la colonne j. On a :

$$det(A) = \sum_{j=1}^{n} a_{ij}(-1)^{i+j} det(A_{ij})$$

$$= \sum_{i=1}^{n} a_{ij}(-1)^{i+j} det(A_{ij})$$

Exemples.

1. $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Alors $A_11 = (d) = dI_1$ et $A_{12} = (c) = cI_1$, donc $det(A_11) = d$ et $det(A_{12}) = c$. Le développement selon la première ligne donne $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$
2. $\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = aei + dhc + gbf - gec - dbi - ahf$

Définition. Pour $A \in \mathcal{M}_n(\mathbb{K})$, on appelle comatrice de A la matrice $Com(A) \in \mathcal{M}_n(\mathbb{K})$ dont l'élément à la ligne i et à la colonne j est $(-1)^{i+j} det(A_{ij})$.

Corollaire. Pour toute $A \in \mathcal{M}_n(\mathbb{K})$,

$$A {}^t Com(A) = det(A) I_n$$

En particulier, on retrouve le fait que si $det(A) \neq 0$ alors A est inversbile ; et en plus on a cette formule d'inversion :

$$A^{-1} = \frac{1}{det(A)} {}^t Com(A)$$

Démonstration. L'élément de la ligne i et de la colonne j de $A{}^tCom(A)$ est $\sum_{k=1}^{n} a_{ik}(-1)^{j+k}det(A_{jk})$. Si $j = i$, c'est $det(A)$ (le développement selon la ligne i). Si $j \neq i$, c'est le déterminant de la matrice déduite de A en y remplaçant la ligne j par la ligne i : mais dans la matrice ainsi obtenue il y donc deux fois la ligne i et ce déterminant est nul. □

Définition. On dit qu'une matrice $A = (a_{ij})_{1\leq i,j\leq n} \in \mathcal{M}(\mathbb{K})$ est triangulaire inférieure si $ji \Rightarrow a_{ij} = 0$ (ie s'il n'y a que des 0 au dessus de la diagonale) : donc une matrice de la forme

$$\begin{pmatrix} a_{11} & 0 & 0 & \dots & 0 \\ a_{21} & a_{22} & 0 & \dots & 0 \\ a_{31} & a_{32} & a_{33} & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nm} \end{pmatrix}$$

On dit qu'une matrice $A = (a_{ij_{1\leq i,j\leq n}} \in \mathcal{M}_n(\mathbb{K})$ est triangulaire supérieure si $j < i \rightarrow a_{ij} = 0$ (ie s'il n'y a que des 0 au dessous de la diagonale) : c'est donc une matrice de la forme

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & a_{22} & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & a_{nm} \end{pmatrix}$$

On dit qu'une matrice $A = (a_{ij_{1\leq i,j\leq n}}) \in \mathcal{M}_n(\mathbb{K})$ est une diagonale si elle est triangulaire inférieure et supérieure, c'est donc une matrice de la forme :

$$\begin{pmatrix} a_{11} & 0 & 0 & \dots & 0 \\ 0 & a_{22} & 0 & \dots & 0 \\ 0 & 0 & a_{33} & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & a_{nm} \end{pmatrix}$$

Corollaire. Le déterminant d'une matrice diagonale, ou plus généralement triangulaire (inférieure ou supérieure), est le produit des éléments diagonaux : $det(A) = \prod_{i=1}^{n} a_{ii}$

Démonstration. Il suffit de le montrer pour une matrice triangulaire inférieure (le cas d'une trangulaire supérieure s'en déduit immédiatement car c'est la transposée d'une triangulaire inférieure : elle a donc même déterminant et mêmes éléments diagonaux). On raisonne par récurrence : si $n = 1$ c'est trivial ($det(a_{11}) = a_{11}$) ; et c'est vrai pour les matrices trianguaires inférieures de $\mathcal{M}_{n-1}(\mathbb{K})$ alors c'est vrai aussi pour celle de $\mathcal{M}_n(\mathbb{K})$

car en développant selon la première ligne on a

$$\begin{vmatrix} a_{11} & 0 & 0 & \dots & 0 \\ a_{21} & a_{22} & 0 & \dots & 0 \\ a_{31} & a_{32} & a_{33} & \dots & \\ \vdots & \vdots & \vdots & \dots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{vmatrix} = a_1 1 \begin{vmatrix} a_{22} & 0 & \dots & 0 \\ a_{32} & a_{33} & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ a_{n2} & a_{n3} & \dots & a_{nn} \end{vmatrix}$$

□

Septième partie

Système linéaire

Introduction(système linéaire). On considère un système linéaire de n équations à m inconnues :

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1m}x_m = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2m}x_m = b_2 \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nm}x_m = b_n \end{cases}$$

où les coefficients $a_{ij} \in \mathbb{K}$ et les seconds membres $b_i \in \mathbb{K}$ sont données, les inconnues sont les $x_j \in \mathbb{K}$.
On peut l'écrire sous la forme matricielle : $AX = B$, où $A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$ est la matrice du système et $B = {}^t(b_1, ..., b_n)$ la colonne des seconds membres.
On peut aussi l'écrire sous la forme d'une équation vectorielle : $f(x) = b$, où $x = (x_1, ..., x_m) \in \mathbb{K}^m$, $b = (b_1, ..., b_n) \in \mathbb{K}^n$ et $f \in \mathcal{L}(\mathbb{K}^m, \mathbb{K}^n)$ est l'application linéaire dont la matrice (relativement aux bases canoniques) est A.

Proposition et définition. Le système admet des solutions si et seulement si $b \in Im(f)$ (par définition de $Im(f)$). Si $x^\circ = (x^\circ{}_1, ..., x^\circ{}_m)$ est une solution, l'ensemble des solutions est $\{x^\circ + z : z \in Ker(f)\} = x^\circ + Ker(f)$: géométriquemet, c'est ce qu'on appelle un sous-espace affine de $\mathbb{K}^m$, c'est-à-dire l'image d'un sev (ici $Ker(f)$) par une translation (ici la translation de vecteur x°). On dit que $x^\circ + Ker(f)$ est le sous-espace affine de $\mathbb{K}^m$ de direction $Ker(f)$ et apssant par x°. La dimension de $x^\circ + Ker(f)$, c'est-à-dire de $Ker(f)$, est $m - r$ où m est le nombre d'inconnues et r le rang de f (qu'on appelle aussi le rang du système).

Démonstration. $f(x) = b \Leftrightarrow f(x) = f(x^\circ) \Leftrightarrow f(x - x^\circ) = 0 \Leftrightarrow x - x^\circ \in Ker(f)$. Le théorème du rang donne : $dim(Ker(f)) = m - r$ □

Détermination pratique du rang. Le rag du système, ou $rg(A)$, est la dimension du sev de $\mathcal{M}_{n,1}(\mathbb{K})$ engendré par les colonnes de A, c'est à dire le nombre maximum de colonnes linéairement du système.

Définition. On dit que le système initial est de Cramer si $m = n$ et que son rang est n.

Proposition. Pour un système de Cramer

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{1n}x_n = b_2 \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n = b_n \end{cases}$$

il existe une solution unique. Elle est donnée par les formules de Cramer :

$$x_1 = \frac{\begin{vmatrix} b_1 & a_{12} & \dots & a_{1n} \\ b_2 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ b_n & a_{n2} & \dots & a_{nn} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}}, x_2 = \frac{\begin{vmatrix} a_{11} & b_1 & \dots & a_{1n} \\ a_{21} & b_2 & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & b_n & \dots & a_{nn} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}}, ..., x_n = \frac{\begin{vmatrix} a_{11} & a_{12} & \dots & b_1 \\ a_{21} & a_{22} & \dots & b_2 \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & b_n \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}}$$

Nota Bene. Dans le numérateur donnant x_j la colonne numéro j de A est remplacée par la colonne B des seconds membres).

Démonstration. A est inversible (car de rang n, ie ses colonnes sont linéairement indépendantes) et

$$AX = B \Leftrightarrow X = A^{-1}B = \frac{1}{det(A)}{}^tCom(A)B \Leftrightarrow x_j = \frac{1}{det(A)}\sum_{i=1}^{n}(-1)^{i+j}det(A_{ij})b_i$$

Or, $det(A) = \sum_{i=1}^{n}(-1)^{i+j}det(A_{ij})a_{ij}$ (développement selon la colonne j). Donc $\sum_{i=1}^{n}(-1)^{i+j}det(A_ij)b_i$ est le déterminant obtenu en remplaçant la colonne j par B. □

Méthode du pivot. C'est une méthode de résolution qui fonctionne pour tous les systèmes (de Cramer ou non). On écrit un double tableau :

$$\begin{array}{cccc|cc} a_{11} & a_{12} & \dots & a_{1m} & b_1 & L_1 \\ a_{21} & a_{22} & \dots & a_{2m} & b_2 & L_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} & b_n & L_n \end{array}$$

A gauche le tableau des coefficients a_{ij} du système initial, à droite la colonne des seconds membres b_i ; les lignes sont numérotées : $L_1, ..., L_n$. Puis on fait des combinaisons linéaires des lignes (et pas des colonnes !), toujours réversibles (on raisonne par équivalences), jusqu'à obtenir à gauche une matrice unité I_r de rang r maximum (r est alors nécessairement égal à $rg(A)$).

Exemple.

$$\begin{cases} x - y + z = a \\ 5x + 2y - z = b \\ -3x - 4y + 3z = c \end{cases}$$

On écrit le double tableau

$$\begin{array}{ccc|cc} 1 & -1 & 1 & a & L_1 \\ 5 & 2 & -1 & b & L_2 \\ -3 & -4 & 3 & c & L_3 \end{array}$$

On commence par annihiler les coefficients de la première colone sur les lignes 2 et 3.

$$\begin{array}{ccc|cc} 1 & -1 & 1 & a & L_1 \\ 0 & 7 & -6 & b-5a & L_2 - 5L_1 = L_2' \\ 0 & -7 & 6 & c+3a & L_3 + 3L_1 = L_3' \end{array}$$

— Si $c+3a \neq -(b-5a)$ (c'est à dire si $c \neq 2a-b$), les lignes L_2', L_3' exprimet des conditions incompatibles : le système n'a pas de solution.

— Si $c = 2a - b$, la troisième ligne est redondante et le système se réduit à :

$$\begin{array}{ccc|cc} 1 & -1 & 1 & a & L_1 \\ 0 & 7 & -6 & b-5a & L_2' \end{array}$$

C'est un système de rang 2 (deux lignes linéairement indépendantes). On peut encore introduire un 0 dans la partie gauche de la première ligne :

$$\begin{array}{ccc|cc} 7 & 0 & 1 & 2a+b & 7L_1 + L_2' = L_1' \\ 0 & 7 & -6 & b-5a & L_2' \end{array}$$

On divise tout par 7 :

$$\begin{array}{cc|c} 1 & 0 & \frac{1}{7} & \frac{2a+b}{7} \\ 0 & 1 & -\frac{6}{7} & \frac{6-5a}{7} \end{array}$$

et on a obtenu une matrice unité maximale $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Ce qui corresponnd au système :

$$\begin{cases} x + \frac{1}{7}z = \frac{1}{7}(2a+b) \\ y - \frac{6}{7}z = \frac{1}{7}(b-5a) \end{cases}$$

dont la solution générale est

$$\begin{cases} x = \frac{1}{7}(2a+b) - \frac{1}{7}z \\ y = \frac{1}{7}(b-5a) + \frac{6}{7}z \end{cases}$$

avec $z \in \mathbb{R}$ quelconque. L'ensemble des solutions est donc l'ensemble des triplets :

$$(x,y,z) = (\frac{2a+b}{7} - \frac{1}{7}z, \frac{b-5a}{7} + \frac{6}{7}z, z) = (\frac{2a+b}{7}, \frac{b-5a}{7}, 0) + z(-\frac{1}{7}, \frac{6}{7}, 1)$$

autrement dit c'est l'ensemble

$$(\frac{2a+b}{7}, \frac{b-5a}{7}, 0) + \mathbb{R}(-\frac{1}{7}, \frac{6}{7}, 1) = (\frac{2a+b}{7}, \frac{b-5a}{7}, 0) + \mathbb{R}(1, -6, -7)$$

C'est donc la doite affine dirigée par le vecteur $(1, -6, -7)$ et passant par le point de coordonnées $(\frac{2a+b}{7}, \frac{b-5a}{7}, 0)$. On note que la dimension de l'espace des solutions (qui est 1) est bien la différence entre le nombre d'inconnues (qui est 3) et le rang du système (qui est 2).

Inversion d'une matrice par la méthode du pivot. Dans la partie gauche du double tableau on met encore la matrice A ; dans la partie droite, au lieu d'une colonne de seconds membres on écrit la matrice unité I_n. Puis on fait des combinaisons linéaires de lignes, jusqu'à obtenir la matrice I_n à gauche : la matrice de droite est alors A^{-1} (NB : Si à gauche on obtient une ligne de 0, c'est que la matrice n'est pas inversible)

Exemple.

$$\begin{array}{ccc|ccc|c} 1 & 5 & 3 & 1 & 0 & 0 & L_1 \\ 2 & 3 & 1 & 0 & 1 & 0 & L_2 \\ 3 & 4 & 1 & 0 & 0 & 1 & L_3 \end{array}$$

On commence par annihiler les coefficients de la première colonne sur les lignes 2 et 3 :

$$\begin{array}{ccc|ccc|c} 1 & 5 & 3 & 1 & 0 & 0 & L_1 \\ 0 & -7 & -5 & -2 & 1 & 0 & L'_2 = L_2 - 2L_1 \\ 0 & -11 & -8 & -3 & 0 & 1 & L'_3 = L_3 - 3L_1 \end{array}$$

Puis on annihile le deuxième coefficient de la ligne 3 (en conservant les deux 0 sur la première colonne) :

$$\begin{array}{ccc|ccc|c} 1 & 5 & 3 & 1 & 0 & 0 & L_1 \\ 0 & -7 & -5 & -2 & 1 & 0 & L'_2 = L_2 - 2L_1 \\ 0 & 0 & 1 & -1 & 11 & -7 & L''_3 = -7L'_3 + 11L'_2 \end{array}$$

Avec L''_3 on annihile les coefficients de la troisième colonne au-dessus du 1 :

$$\begin{array}{ccc|ccc|c} 1 & 5 & 0 & 4 & -33 & 21 & L'_1 = L_1 - 3L''_3 \\ 0 & -7 & 0 & -7 & 56 & -35 & L'_2 = 5L''_3 \\ 0 & 0 & 1 & -1 & 11 & -7 & L''_3 \end{array}$$

Avec L''_2 on annihile le deuxième coefficient de la première ligne (après simplification par 7) :

$$\begin{array}{ccc|ccc|c} 1 & 0 & 0 & 4 & -33 & 21 & L'_1 \\ 0 & 1 & 0 & 1 & -8 & 5 & L''_2 \\ 0 & 0 & 1 & -1 & 11 & -7 & L''_3 \end{array}$$

Autre méthode : par la comatrice. On note A_{ij} la matrice obtenue en supprimant dans A la ligne et la colonne j, $|A_{ij}|$ son déterminant.

$$|A_{11}| = \begin{vmatrix} 3 & 1 \\ 4 & 1 \end{vmatrix} = -1$$

$$|A_{12}| = \begin{vmatrix} 2 & 1 \\ 3 & 1 \end{vmatrix} = -1$$

$$|A_{13}| = \begin{vmatrix} 2 & 3 \\ 3 & 4 \end{vmatrix} = -1$$

$$|A_{21}| = \begin{vmatrix} 5 & 3 \\ 4 & 1 \end{vmatrix} = -7$$

$$|A_{22}| = \begin{vmatrix} 1 & 3 \\ 3 & 1 \end{vmatrix} = -8$$

$$|A_{23}| = \begin{vmatrix} 1 & 5 \\ 3 & 4 \end{vmatrix} = -11$$

$$|A_{31}| = \begin{vmatrix} 5 & 3 \\ 3 & 1 \end{vmatrix} = -4$$

$$|A_{32}| = \begin{vmatrix} 1 & 3 \\ 2 & 1 \end{vmatrix} = -5$$

$$|A_{33}| = \begin{vmatrix} 1 & 5 \\ 2 & 3 \end{vmatrix} = -7$$

la comatrice de A a pour coefficients $(-1)^{i+j}|A_{ij}|$

$$Com(A) = \begin{pmatrix} -1 & 1 & -1 \\ 7 & -8 & 11 \\ -4 & 5 & -7 \end{pmatrix}$$

donc ${}^tCom(A) = \begin{pmatrix} -1 & 7 & -4 \\ 1 & -8 & 5 \\ -1 & 11 & -7 \end{pmatrix}$