Semaine 19

lundi 3 mars 2025
> samedi 8 mars 2025

Chapitre 12 Arithmétique

■ Rudiments d'arithmétique :

► **Définition :** On appelle ensemble des entiers naturels et on note $\mathbb{N}$ un ensemble ordonné *non vide* vérifiant les trois propriétés suivantes :
- **N1** • toute partie non vide admet un plus petit élément.
- **N2** • toute partie non vide et majorée admet un plus grand élément.
- **N3** • $\mathbb{N}$ n'a pas de plus grand élément.

On admet qu'un tel ensemble existe et est unique à bijection croissante près.

► **Définition :** Multiples et diviseurs d'un entier.

►

Propriété (division euclidienne dans $\mathbb{N}$) :
$$\forall (a,\, b) \in \mathbb{N} \times \mathbb{N}^*,\quad \exists !(q,\, r) \in \mathbb{N} \times [\![0,\, b-1]\!],\quad a = bq + r$$

► **Vocabulaire :** On dit que a est le *dividende*, b le *diviseur*, q le *quotient*, r le *reste* de la division euclidienne de a par b.

► **Définition :** PGCD et PPCM de deux entiers naturels non nuls.
Si a et b sont deux entiers non nuls, on note $a \wedge b$ le pgcd de a et b, et $a \vee b$ le ppcm de a et b.

► **Algorithme :** Algorithme d'Euclide pour le calcul du *pgcd*.

►

Propriété (propriété de Bézout) : Si $(a,\, b) \in (\mathbb{N}^*)^2$, il existe $(u,\, v) \in \mathbb{Z}^2$ tels que $au + bv = a \wedge b$.

► **Propriété (de Gauss) :** Si a et b sont deux entiers premiers entre eux $(a \wedge b = 1)$ et si $a \mid bc$, alors $a \mid c$.

► **Propriété :** Si a et b sont deux entiers non nuls, $ab = (a \wedge b)(a \vee b)$.

► **Définition :** Un entier positif est dit *premier* s'il admet exactement 2 diviseurs distincts dans $\mathbb{N}^*$.

► **Théorème :** Tout entier $n \in \mathbb{N} \setminus \{0, 1\}$ est divisible par un entier premier.

► **Théorème :** Il existe une infinité d'entiers premiers.

► **Théorème :** Tout entier $n \geqslant 2$ se décompose en produit de nombres premiers ; on *admet* que cette décomposition est unique à l'ordre près des facteurs.

Chapitre 13 Systèmes linéaires, calcul matriciel

■ Calcul matriciel :

► **Définition :** Ensemble des matrices à n lignes et p colonnes (ou de type $(n,\, p)$) à coefficients dans $\mathbb{K}$, noté $\mathscr{M}_{n,p}(\mathbb{K})$.

► **Définition :** Addition de matrices de type $(n,\, p)$; multiplication d'une matrice par une constante ; produit d'une matrice de type $(n,\, p)$ par une matrice de type $(p,\, q)$.

► **Propriétés (admises) :** Le produit matriciel est pseudo-associatif, pseudo-distributif à droite et à gauche ; compatible avec la multiplication par un scalaire ; pour résumer :
$$\forall A \in \mathscr{M}_{n,\,p},\ \forall B \in \mathscr{M}_{p,\,q},\ \forall C \in \mathscr{M}_{q,\,r},\quad (AB)C = A(BC)$$
$$\forall A \in \mathscr{M}_{n,\,p},\ \forall (B,\, C) \in \mathscr{M}^2_{p,\,q},\quad A(B+C) = AB + AC$$
$$\forall (A,\, B) \in \mathscr{M}^2_{n,\,p},\ \forall C \in \mathscr{M}^2_{p,\,q},\quad (A+B)C = AC + BC$$
$$\forall \lambda \in \mathbb{K},\ \forall A \in \mathscr{M}_{n,\,p},\ \forall B \in \mathscr{M}_{p,\,q},\quad (\lambda A)B = \lambda(AB) = A(\lambda B)$$

► **Exemples -- Vocabulaire :**
- matrices carrées d'ordre n ;
- matrices diagonales (notation $\mathrm{diag}(\alpha_1,\, \ldots,\, \alpha_n)$) ;
- matrice identité (notation I_n) ;
- matrices triangulaires supérieures et inférieures.
- matrices élémentaires $E_{i,\,j}$ en taille $(n,\, p)$

► **Propriété :** Le produit matriciel est associatif. Le produit de matrices carrées d'ordre n est non commutatif si $n > 1$.

► **Notation :** Symbole de Kronecker : $\delta_{\alpha,\beta} = \begin{cases} 1 & \text{si } \alpha = \beta \\ 0 & \text{sinon} \end{cases}$.

►

Exercice : Cas particulier du produit des matrices élémentaires (pour des matrices de tailles compatibles) : $E_{i,\,j} \times E_{k,\,\ell} = \delta_{j,\,k} E_{i,\,\ell}$.

► **Définition :** *Matrices d'opérations élémentaires :* matrices de transvection, de transposition et de dilatation.
Traduction des opérations élémentaires en produits matriciels.
Si $i \neq j$ et $\lambda \in \mathbb{K}$, on définit les matrices carrées d'ordre n :
- $S^n_{i,j} = I_n + E_{i,j} + E_{j,i} - E_{i,i} - E_{j,j}$.
- $T^n_{i,j}(\lambda) = I_n + \lambda E_{i,j}$.
- Si $\lambda \neq 0$, on pose $H_i(\lambda) = I_n + (\lambda - 1)E_{i,i}$.
  - $L_i \longleftrightarrow L_j$ $\qquad M \longleftrightarrow S^n_{i,j} M$
  - $L_i \longleftarrow L_i + \lambda L_j$ $\qquad M \longleftrightarrow T^n_{i,j}(\lambda) M$
  - $L_i \longleftarrow \lambda L_i$ $\qquad M \longleftrightarrow R_i(\lambda) M$

► **Propriété :** Effet de la multiplication à gauche (ou à droite - énoncé mais pas prouvé) par une matrice élémentaire.
Conséquence pour les matrices d'opérations élémentaires

■ Généralités sur les systèmes linéaires :

► **Définitions :** Équation linéaire à p inconnues ; système linéaire de n équations à p inconnues.
Matrice associée à un système linéaire.
Si $n \in \mathbb{N}^*$ et $p \in \mathbb{N}^*$, on considère $\left(a_{i,\,j}\right)_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}} \in \mathcal{M}_{n,\,p}(\mathbb{K})$, $\left(b_i\right)_{1 \leqslant i \leqslant n} \in \mathbb{K}^n$, et le système :
$$(S)\ :\ \begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,p}x_p = b_1 \\ \qquad\qquad \vdots \\ a_{n,1}x_1 + a_{n,2}x_2 + \cdots + a_{n,p}x_p = b_n \end{cases}$$
La matrice augmentée associée à ce système linéaire est la matrice $(A \mid B) \in \mathcal{M}_{n,\,p+1}(\mathbb{K})$ obtenue en plaçant à la droite de la matrice du système, la colonne des seconds membres.

► **Définition (opérations élémentaires) :** Opérations élémentaires sur les lignes d'un système ou d'une matrice :
- échange des lignes L_{i_1} et L_{i_2} : $L_{i_1} \leftrightarrow L_{i_2}$
- ajout de λL_{i_2} à L_{i_1} pour $i_1 \neq i_2$: $L_{i_1} \leftarrow L_{i_1} + \lambda L_{i_2}$
- multiplication de L_i par $\mu \neq 0$: $L_i \leftarrow \mu L_i$

► **Propriété :** Deux systèmes équivalents ont le même ensemble de solutions.

► **Propriété :** Si l'on passe d'un système S à un autre système S' par une suite finie d'opérations élémentaires sur les lignes, la matrice augmentée de S' s'obtient en effectuant la même suite d'opérations élémentaires sur la matrice augmentée de S.

► **Définitions :** Lorsqu'on ramène la matrice augmentée d'un système linéaire à sa matrice échelonnée réduite par lignes équivalente, on dit que
- Le système est *compatible* si la dernière colonne n'est pas une colonne contenant un pivot : dans ce cas le système admet au moins une solution.
- Le système est *incompatible* si la dernière colonne contient un pivot : dans ce cas le système n'admet aucune solution.

Lorsque le système est compatible, les inconnues correspondant aux colonnes des pivots sont appelées *inconnues principales*, les autres sont les *inconnues secondaires* ou les paramètres.

► **Remarque :** Le nombre de paramètres est égal à la différence du nombre d'inconnues et du rang.

► **Propriété :** Pour un système linéaire, **si** on dispose d'une solution particulière s_0, alors l'ensemble des solutions est $\left\{s_0 + h,\ h \in \mathcal{S}_H\right\}$, où $\mathcal{S}_H$ est l'ensemble des solutions du système homogène associé (c'est-à-dire celui ayant même matrice que le système initial, mais des seconds membres nuls).

■ Matrices inversibles :

► **Définition :** Matrices inversibles, inverse.
Propriétés des matrices inversibles (structure de groupe - sans définir l'axiomatique d'un groupe).

► **Propriété :** Inverse d'un produit de matrices inversibles.

► **Propriété :** Les matrices d'opérations élémentaires sont inversibles et leurs inverses sont encore des matrices d'opérations élémentaires.

► **Exercice :** Définition de l'ensemble des matrices diagonales, triangulaires. Stabilité de ces ensembles par les opérations matricielles.

►

Propriété : Pour une matrice $A \in \mathcal{M}_n(\mathbb{K})$, les propriétés suivantes sont équivalentes :
- A est inversible
- Pour tout B, le système $AX = B$ admet une unique solution ;

Remarque : le théorème complet démontré en cours est : Pour une matrice $A \in \mathcal{M}_n(\mathbb{K})$, les propriétés suivantes sont équivalentes :
- A est inversible
- Pour tout B, le système $AX = B$ admet une unique solution ;
- A peut se ramener à la matrice I_n en effectuant un nombre fini d'opérations élémentaires sur les lignes ;
- Pour tout B, le système $AX = B$ admet au moins une solution ;
- L'unique solution du système $AX = 0$ est la solution nulle.

► **Propriété :** Caractérisation des matrices inversibles parmi les matrices triangulaires supérieures (ou inférieures).

Chapitre 14 Polynômes

■ Définitions, Construction :

► **Définition :** Dans toute cette partie, $\mathbb{K}$ désigne un corps ; en pratique, il s'agit de $\mathbb{R}$ ou $\mathbb{C}$. On appelle *support* de la suite $(a_n) \in \mathbb{K}^{\mathbb{N}}$ l'ensemble $\{n \in \mathbb{N},\quad a_n \neq 0\}$.
Un polynôme à une indéterminée à coefficients dans $\mathbb{K}$ est un suite de $\mathbb{K}^{\mathbb{N}}$ à *support fini* (on parle également de suite *presque nulle*) ; on note $\mathbb{K}[X]$ l'ensemble des polynômes.

► **Exemples et vocabulaire :**
◊ La suite nulle est appelée polynôme nul et noté 0
◊ L'ensemble des polynômes constants est : $\left\{(a_n) \in \mathbb{K}^{\mathbb{N}},\ \forall n \geqslant 1,\ a_n = 0\right\}$.
◊ On dit qu'un polynôme est un monôme si un seul des coefficients est non nul.

- **Remarque :** $\mathbb{K}[X] \neq \mathbb{K}^{\mathbb{N}}$.
- **Définitions :** Soit $P \in \mathbb{K}[X] \setminus \{0\}$
  - ◊ On appelle *degré de P* et on note $\deg(P)$ l'entier $\max\{n \in \mathbb{N}, a_n \neq 0\}$.
  - ◊ $a_{\deg(P)}$ est le *coefficient dominant* de P.
  - ◊ On dit que P est *unitaire* si son coefficient dominant vaut 1.
  - ◊ Par convention $\deg(0) = -\infty$.
- **Proposition -- Définition :** On définit l'addition de $P = (a_n) \in \mathbb{K}[X]$ et $Q = (b_n) \in \mathbb{K}[X]$ par $P + Q = (a_n + b_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$.
  On a $\forall (P, Q) \in \mathbb{K}[X]^2$:
  - $\deg(P+Q) \leqslant \max\big(\deg(P), \deg(Q)\big)$ et si $\deg(P) \neq \deg(Q)$, il y a égalité.
- **Proposition - Définition :** On définit la multiplication de 2 polynômes $P = (a_n) \in \mathbb{K}[X]$ et $Q = (b_n) \in \mathbb{K}[X]$ par $P \times Q = PQ = (c_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$ où :
$$\forall n \in \mathbb{N}, \quad c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{i+j=n} a_i b_j$$
  On a $\forall (P, Q) \in \mathbb{K}[X]^2$, $\deg(PQ) = \deg(P) + \deg(Q)$.
- **Proposition :** Les éléments inversibles (pour la loi $\times$) de cet anneau sont les polynômes constants non nuls.
- **Proposition - Définition :** On définit un produit externe sur $\mathbb{K} \times \mathbb{K}[X]$: pour $\lambda \in \mathbb{K}$ et $P = (a_n) \in \mathbb{K}[X]$, on note $\lambda \cdot P = \lambda P = (\lambda a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$.
- **Proposition - Définition :** On dit que $\big(\mathbb{K}[X], +, \cdot\big)$ admet une structure d'*espace vectoriel sur* $\mathbb{K}$ (ou de $\mathbb{K}$–espace vectoriel, ou en abrégé $\mathbb{K}$-e.v.) ; cela signifie :
  - $(\mathbb{K}[X], +)$ groupe abélien.
  - $\cdot$ est une loi externe de $\mathbb{K} \times \mathbb{K}[X]$ dans $\mathbb{K}[X]$ telle que :
$$\forall (\alpha, \beta) \in \mathbb{K}^2, \forall (P, Q) \in \mathbb{K}[X]^2 : \begin{cases} (\alpha+\beta)\cdot P = \alpha\cdot P + \beta\cdot P \\ \alpha\cdot(P+Q) = \alpha\cdot P + \alpha\cdot Q \\ \alpha\cdot(\beta\cdot P) = (\alpha\beta)\cdot P \\ 1_{\mathbb{K}}\cdot P = P \end{cases}.$$
- **Proposition - Définition :** Pour résumer le fait que $\big(\mathbb{K}[X], +, \times\big)$ est un anneau et $\big(\mathbb{K}[X], +, \cdot\big)$ est un $\mathbb{K}$-e.v. ainsi que la relation de compatibilité :
  $\forall \lambda \in \mathbb{K}, \forall (P, Q) \in \mathbb{K}[X]^2, \quad (\lambda \cdot P) \times Q = \lambda \cdot (P \times Q) = P \times (\lambda \cdot Q)$
  on dit que $\mathbb{K}[X]$ est une *algèbre sur* $\mathbb{K}$ (ou encore $\mathbb{K}$-algèbre).

■ Arithmétique sur $\mathbb{K}[X]$:

- **Définition :** Si $(A, B) \in \mathbb{K}[x]^2$, on dit que A est un multiple de B ou que B divise A si et seulement s'il existe $C \in \mathbb{K}[X]$ tel que $A = BC$, et on note $B \mid A$.
- **Définition :** Deux polynômes $(A, B) \in (\mathbb{K}[x] \setminus \{0\})^2$, sont *associés* ssi il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda Q$ (cela équivaut à $P \mid Q$ et $Q \mid P$).

Théorème : Soit $(A, B) \in \mathbb{K}[X]^2$, $B \neq 0$, alors $\exists!(Q, R) \in \mathbb{K}[X]^2$ tels que $A = BQ + R$ et $\deg(R) < \deg(B)$.
On dit que Q est le *quotient* et R le *reste* de la division euclidienne de A par B.

- **Algorithme :** Mise en œuvre de l'*algorithme de division euclidienne* pour les polynômes.

■ Fonctions polynomiales, racines d'un polynôme :

- **Définition :** À tout polynôme formel $P = \sum_{k\geqslant 0} a_k X^k$ de $\mathbb{K}[X]$, on associe la fonction $\widetilde{P}$ de $\mathbb{K}^{\mathbb{K}}$ définie par $x \mapsto \sum_{k\geqslant 0} a_k x^k$.
- **Algorithme (Hörner) :** Mise en œuvre de l'*algorithme de Hörner*.
- **Propriétés :** L'application $P \mapsto \widetilde{P}$ est « compatible » avec les opérations algébriques, la composition, (la dérivation lorsque $\mathbb{K} = \mathbb{R}$)...

Théorème (Formules de Taylor pour les polynômes) :
$$\forall P \in \mathbb{K}[X], \ \forall \alpha \in \mathbb{K}, \quad P = \sum_{k\geqslant 0} \Big(D^k(P)\Big)(\alpha)\frac{(X-\alpha)^k}{k!} ;$$
autre formulation : $P(X+\alpha) = \sum_{k\geqslant 0} \Big(D^k(P)\Big)(\alpha)\frac{X^k}{k!}$.

- **Corollaire (Formule de Mac-Laurin) :**
$$\forall P \in \mathbb{K}[X], \quad P = \sum_{k\geqslant 0} \Big(D^k(P)\Big)(0)\frac{X^k}{k!}$$
- **Corollaire :** $\forall a \in \mathbb{K}$, tout polynôme $P \in \mathbb{K}_n[X]$ peut s'écrire de façon unique comme combinaison linéaire des $\big\{(X-a)^j, \ j \in 0, n\big\}$.
- **Définition :** Si $P \in \mathbb{K}[X]$ et si $\alpha \in \mathbb{K}$, on dit que α est un *zéro* ou une *racine* de P ssi $\widetilde{P}(\alpha) = 0$.
- **Propriété :** α est un zéro de P ssi $(X - \alpha) \mid P$.
- **Corollaire :** $P \in \mathbb{K}[X]$ admet deux zéros distincts α, β ssi $\big(X-\alpha\big)\big(X-\beta\big) \mid P$.

Corollaire : Un polynôme de degré $n \in \mathbb{N}$ admet au plus n racines deux à deux distinctes.
Autre formulation : un polynôme de degré inférieur ou égal à n qui admet au moins $n+1$ racines est le polynôme nul.

- **Notation :** X désigne le polynôme $(0, 1, 0, \ldots) \in \mathbb{K}[X]$, on convient de noter $X^0 = 1$, $X^1 = X$ et $\forall k \in \mathbb{N}^*$, $\quad X^k = (\underbrace{0, \ldots, 0}_{k \text{ termes}}, 1, 0, \ldots)$.
  Par construction, tout polynôme s'écrit comme combinaison linéaire finie à coefficients dans $\mathbb{K}$ de polynômes de $\{X^j, \ j \in \mathbb{N}\}$. Pour tout $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n.
- **Définition :** Si $P = \sum_{n=0}^{N} a_n X^n \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$; on définit le *polynôme composé*, noté $P \circ Q$ ou $P(Q)$, par $P \circ Q = \sum_{n=0}^{N} a_n Q^n$.
- **Proposition :** $\forall (P, Q) \in \mathbb{K}[X]^2$ avec Q polynôme non constant, on a : $\deg(P \circ Q) = \deg(P)\deg(Q)$.
- **Propriétés :** $\forall (P, Q, R) \in \mathbb{K}[X]^3$, $\forall \alpha \in \mathbb{K}$:
  - ◊ $(P + \alpha Q) \circ R = P \circ R + \alpha Q \circ R$;
  - ◊ $(PQ) \circ R = (P \circ R)\,(Q \circ R)$;
  - ◊ $(P \circ Q) \circ R = P \circ (Q \circ R)$;
  - ◊ $X \circ P = P \circ X = P$.
- **Définition :** Pour tout $P = \sum_{n=0}^{N} a_n X^n \in \mathbb{K}[X]$, on note P' ou $D(P)$ le *polynôme dérivé de P* par $P' = \sum_{n=1}^{N} n a_n X^{n-1} = \sum_{n=0}^{N-1} (n+1) a_{n+1} X^n$.
  On a en particulier $\forall P \in \mathbb{K}[X]$, $\deg(P) \geqslant 1$, $\quad \deg(P') = \deg(P) - 1$ et $\deg(P') = -\infty$ si $\deg(P) \leqslant 0$.
  On définit par récurrence la dérivée n-ième d'un polynôme.

Cas particulier important :
$$\forall (k, n) \in \mathbb{N}^2, \quad D^k(X^n) = \begin{cases} \dfrac{n!}{(n-k)!} X^{n-k} & \text{si } k \leqslant n \\ 0 & \text{si } k > n \end{cases}$$

- **Propriétés :** $\forall (P, Q) \in \mathbb{K}[X]^2$, $\forall \alpha \in \mathbb{K}$: $(P + \alpha Q)' = P' + \alpha Q'$, $(PQ)' = P'Q + PQ'$ et $\forall n \in \mathbb{N}$, $\quad (PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$.

- **Corollaire :** On en déduit en particulier que l'application $P \mapsto \widetilde{P}$ est injective lorsque $\mathbb{K}$ est infini.
  Il existe donc une bijection entre polynômes et fonctions polynomiales pour $\mathbb{K} = \mathbb{R}$ et $\mathbb{K} = \mathbb{C}$.
- **Définition (Ordre de multiplicité d'une racine) :** $\alpha \in \mathbb{K}$ est une racine de $P \in \mathbb{K}[X]$ de multiplicité $k \in \mathbb{N}^*$ si $(X-\alpha)^k$ divise P et $(X-\alpha)^{k+1}$ ne divise pas P.
- **Propriété :** α est une racine de P d'ordre k ssi $\exists Q \in \mathbb{K}[X]$ tel que $P = (X-\alpha)^k Q$ et $Q(\alpha) \neq 0$.

Propriété (Caractérisation avec les dérivées n-ièmes) :
$\alpha \in \mathbb{K}$ est une racine de $P \in \mathbb{K}[X]$ d'ordre $k \in \mathbb{N}^*$ ssi :
◊ $\forall j \in 0, k-1, \quad D^j(P)(\alpha) = 0$;
◊ $D^k(P)(\alpha) \neq 0$.

- **Corollaire :** Si $\alpha \in \mathbb{K}$ est une racine de multiplicité $m \geqslant 1$ de P, c'est une racine de multiplicité $m-1$ de P'.
- **Définition :** On dit qu'un polynôme $P \in \mathbb{K}[X]$ est scindé sur $\mathbb{K}$ ssi :
$$\exists r \in \mathbb{N}, \ \exists a \in \mathbb{K}^*, \ \exists(\alpha_1, \ldots, \alpha_r) \in \mathbb{K}^r, \quad P = a\prod_{j=1}^{r}(X - \alpha_j)$$