Chap 19 : Polynômes

$\mathbb{K}$ est un corps commutatif

I. Algèbre $\mathbb{K}[X]$

Un polynôme à coefficients dans $\mathbb{K}$ est une suite presque nulle (nulle à partir d'un certain rang) $(a_k)_{k\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$

$\mathbb{K}[X] = \{$polynômes à coefficients dans $\mathbb{K}\}$

$(\mathbb{K}[X],+,\cdot)$ est un sous-espace vectoriel de $(\mathbb{K}^{\mathbb{N}},+,\cdot)$

Multiplication sur $\mathbb{K}[X]$: $(a_k)_{k\in\mathbb{N}} \times (b_k)_{k\in\mathbb{N}} = \left(\sum_{k=0}^{n} a_k b_{n-k}\right)_{n\in\mathbb{N}}$

$(\mathbb{K}[X],+,\times)$ est un anneau d'élément neutre $1_{\mathbb{K}[X]} = (\delta_{0,n})_{n\in\mathbb{N}} = (1,0,0,\ldots)$

$\mathbb{K}$ corps commutatif $\Rightarrow \mathbb{K}[X]$ anneau commutatif

$\mathcal{I}\begin{cases}\mathbb{K} \to \mathbb{K}[X] \\ \alpha \mapsto \alpha \times 1_{\mathbb{K}} = (\alpha,0,0,\ldots)\end{cases}$ est un morphisme d'algèbre injectif $\quad \alpha\cdot(a_n)_{n\in\mathbb{N}} = (\alpha\cdot 1_{\mathbb{K}[X]})\times(a_n)_{n\in\mathbb{N}}$

$X = (\delta_{1,n})_{n\in\mathbb{N}} = (0,1,0,0,\ldots)$

$X^k = (\delta_{k,n})_{n\in\mathbb{N}} = (0,\ldots,0,1,0,0,\ldots)$ (le 1 est en $k-ième$ position) $\quad X^k \times X^l = X^{k+l}$

$(X^n)_{n\in\mathbb{N}}$ est une base de $\mathbb{K}[X]$ $\quad P = (a_n)_{n\in\mathbb{N}} = \sum_{k\in\mathbb{N}} a_k X^k$

Degré du polynôme : $\deg P = -\infty$ si $P = 0_{\mathbb{K}[X]}$ $\quad \deg P = \max\{k\in\mathbb{N}, a_k \neq 0\}$ sinon

Valuation d'un polynôme non nul $val(P) = \min\{k\in\mathbb{N}, a_k \neq 0\}$

$\deg P \leq n \Leftrightarrow \forall k > n, a_k = 0$ $\quad \deg P = n \Leftrightarrow \forall k > n, a_k = 0$ et $a_n \neq 0$

$\deg P \in \mathbb{N} \Leftrightarrow P \neq 0_{\mathbb{K}[X]}$ $\quad \deg(P\times Q) = \deg P + \deg Q$

$\deg(P+Q) \leq \max(\deg P, \deg Q)$ avec égalité si $\deg P \neq \deg Q$

Le coefficient dominant de $P = \sum_{k=0}^{n} a_k X^k$ de degré n est a_n $\quad P$ est unitaire si $a_n = 1$

a_p coefficient dominant de P, b_q celui de $Q \Rightarrow a_p \times b_q$ est celui de $P\times Q$

$\mathbb{K}_n[X] = \{P\in\mathbb{K}[X], \deg P \leq n\}$ sev de $\mathbb{K}[X]$

$(X^k)_{k\in[\![0,n]\!]}$ base de $\mathbb{K}_n[X]$ $\quad \Rightarrow \quad \dim_{\mathbb{K}}(\mathbb{K}_n[X]) = n+1$

$(P_k)_{k\in[\![0,n]\!]}$ avec pour tout $k : \deg P_k = k$, est une base de $\mathbb{K}_n[X]$

/!\ seul $\mathbb{K}_0[X]$ est un sous-anneau

$P\in\mathbb{K}[X]$ est inversible *ssi* $\deg P = 0$

$\mathbb{K}[X]$ est intègre

II. Arithmétique sur $\mathbb{K}[X]$

Division euclidienne : $(A,B)\in\mathbb{K}[X]\times(\mathbb{K}[X]\setminus\{0_{\mathbb{K}[X]}\})$ $\quad \exists!(Q,R)\in\mathbb{K}[X]^2\ tq$

$$\begin{cases} A = BQ + R \\ \deg R < \deg B \end{cases}$$

Preuve : Unicité : regrouper chacun d'un côté, utiliser les degrés pour montrer l'égalité

Existence : Récurrence forte sur deg A. A = $a_{n+1}X^{n+1} + A_0$, p = deg B, $A_1 = A - \left(\frac{a_{n+1}}{b_p}X^{n+1-p}\right)B$

$\deg A_1 \leq n \Rightarrow hyp.rec.\quad A_1 = Q_1B + R_1 \quad A = \left(\frac{a_{n+1}}{b_p}X^{n+1-p} + Q_1\right)B + R_1$

$\mathbb{K}[X]$ est un anneau principal : pour tout I idéal de $\mathbb{K}[X]$, il existe $P\in\mathbb{K}[X]$ tq $I = P\cdot\mathbb{K}[X] = \{PQ, Q\in\mathbb{K}[X]\}$
Si $I \neq \{0_{\mathbb{K}[X]}\}$, on a unicité du P unitaire

Preuve : on prend l'ensemble des degrés des polynômes de l'idéal I, on le minore, on prend un polynôme A_0 de I qui corresponde à ce degré minimum, un prend P dans I, on en fait la division euclidienne par A_0, le reste est dans I (car R=P-A_0Q), il a donc un degré plus petit que A, ce qui est impossible si deg R $\geqslant 0$ → A_0 | P

On dit que B divise $A\in\mathbb{K}[X]$ s'il existe $Q\in\mathbb{K}[X]$ tel que $A = QB$

$B|A \Leftrightarrow$ le reste de la DE de A par B est nul $\Leftrightarrow A\in B\mathbb{K}[X] \Leftrightarrow A\mathbb{K}[X]\subset B\mathbb{K}[X]$

P et Q sont associés si $\begin{cases} P|Q \\ Q|P \end{cases} \Leftrightarrow \exists\lambda\in\mathbb{K}^*$ tq $P = \lambda Q$

Il existe un unique $D\in\mathbb{K}[X]$ tel que $A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X] : D = PGCD(A,B) = A\wedge B$

$D = A\wedge B \Rightarrow \exists(U,V)\in\mathbb{K}[X]^2,\ D = AU + BV \qquad D = A\wedge B\ ssi \begin{cases} D|A \quad D|B \\ D = AU + BV \qquad (U,V)\in\mathbb{K}[X]^2 \end{cases}$

A et B sont premiers entre eux $ssi\ A\wedge B = 1\ ssi\ \exists(U,V)\exists\mathbb{K}[X]^2, AU + BV = 1$

Lemme de Gauss : $(A,B,C)\in\mathbb{K}[X]^3, \begin{cases} A|BC \\ A\wedge B = 1 \end{cases} \Rightarrow A|C$

$$\begin{cases} P\wedge Q_1 = 1 \\ P\wedge Q_2 = 1 \end{cases} \Rightarrow P\wedge(Q_1Q_2) = 1$$

$(P,Q_1,\ldots,Q_n)\in\mathbb{K}^{n+1} \quad \forall j\in[\![1,n]\!], P\wedge Q_j = 1 \Leftrightarrow P\wedge\prod_{j=1}^{n}Q_j = 1$

$(P,Q_1,\ldots,Q_n)\in\mathbb{K}^{n+1} \quad \forall(j,k)\in[\![1,n]\!], j\neq k, Q_k\wedge Q_j = 1 \qquad \forall k\in[\![1,n]\!], Q_j | P \qquad \Rightarrow \prod_{j=1}^{n}Q_j | P$

$A\wedge(B\wedge C) = (A\wedge B)\wedge C = A\wedge B\wedge C$

/!\ Premiers entre eux dans leur ensemble : $P_1\wedge P_2\wedge\ldots\wedge P_n = 1$

$\neq$ Premiers entre eux deux à deux : $\forall(j,k)\in[\![1,n]\!]^2, j\neq k, P_j\wedge P_k = 1$

$A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\,\mathbb{K}[X]$ $\quad M = PPCM(A,B) = A \vee B$

$(A,B) \in (\mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\})^2 \quad \begin{cases} D = A \wedge B \\ M = A \vee B \end{cases} \Rightarrow \exists \lambda \in \mathbb{K}^*, AB = \lambda MD$

Preuve : $A = DA_1, B = DB_1, \{mult.comm. A \,\&\, B\} = \{D \times P, P \; mult.comm. A_1 \,\&\, B_1\} \Rightarrow A \vee B = D(A_1 \vee B_1)$

$A_1 \wedge B_1 = 1 \Rightarrow A_1 \vee B_1 = \mu A_1 B_1 \qquad DM = D \times D(\mu A_1 B_1) = \mu AB$

P est irréductible si ses seuls diviseurs sont les polynômes inversibles $(\lambda, \lambda \in \mathbb{K}^*)$
les polynômes associés à P $(\mu P, \mu \in \mathbb{K}^*)$

P irréductible $\Leftrightarrow \forall (Q,R) \in \mathbb{K}[X] \quad P = QR \Rightarrow Q = \lambda \in \mathbb{K}^*$ ou $R = \lambda \in \mathbb{K}^*$

$\Leftrightarrow \forall Q \in \mathbb{K}[X] \qquad P \wedge Q = \begin{cases} \dfrac{P}{\lambda} \text{ si } P \mid Q \\ 1 \text{ sinon} \end{cases}$

$K \subset \mathbb{K}$ Si P est irréductible dans $\mathbb{K}[X]$, alors il est irréductible dans $K[X]$

Algorithme d'Euclide $\Rightarrow (P,Q) \in K[X]^2 \qquad PGCD_{\mathbb{K}[X]}(P,Q) = PGCD_{K[X]}(P,Q) \in K[X]$

$\Rightarrow \wedge \quad P \quad Q = \quad 1 \Rightarrow \wedge$ dans $K[X] \quad P = Q \quad 1$ dans $\mathbb{K}[X]$

Un polynôme de degré 1 est toujours irréductible

P et Q irréductibles $\Rightarrow$ Ils sont soit premiers entre eux, soit associés

P irréductible, $P \mid \prod_{k=1}^{n} Q_k \Rightarrow \exists j \in [\![1,n]\!], P \mid Q_j$

Tout polynôme $P \in \mathbb{K}[X]$ de degré ≥ 1 admet un diviseur irréductible

$\Rightarrow$ Décomposition en polynômes irréductibles : $\forall P \in \mathbb{K}[X]$, $\deg P \geq 1$,

$\exists \lambda \in \mathbb{K}^*, \qquad (P_1, \ldots, P_n)$ polynômes irréductibles unitaires premiers 2 à 2

$(\alpha_1, \ldots, \alpha_n) \in (\mathbb{N}^*)^n \qquad P = \prod_{k=1}^{n} P_k^{\alpha_k}$, et cette décomposition est unique à l'ordre près des facteurs

III. Polynômes et fonctions polynômiales associées

$P = \sum_{k=0}^{n} a_k X^k \quad P \circ Q = \sum_{k=0}^{n} a_k Q^k \in \mathbb{K}[X]$ car $\mathbb{K}[X]$ anneau

$\varphi \begin{cases} \mathbb{K}[X] & \to \mathbb{K}[X] \\ P & \mapsto P \circ Q \end{cases}$ est un morphisme d'algèbre (app. lin. + morphisme d'anneau)

$P(X) = P \circ X = P \qquad X$ N'EST PAS UNE VARIABLE (on n'écrit pas "posons $X = 3$")

$\deg P \geq 1$ et $\deg Q \geq 1 \Rightarrow \deg(P \circ Q) = \deg P \times \deg Q$

$\deg P = 0 \Rightarrow P \circ Q = P,\ \deg(P \circ Q) = 0 \qquad \deg Q = 0 \Rightarrow \deg(P \circ Q) \leq 0$

$P \in \mathbb{K}[X], P = \sum_{k=0}^{n} a_k X^k$ sa fonction polynômiale associée est : $\widetilde{P} \begin{cases} \mathbb{K} \to \mathbb{K} \\ x \mapsto \widetilde{P}(x) = \sum_{k=0}^{n} a_k x^k \end{cases}$

$\theta \begin{cases} \mathbb{K}[X] & \to \mathfrak{F}(\mathbb{K},\mathbb{K}) \\ P & \mapsto \tilde{P} \end{cases}$ est un morphisme d'algèbre

Si $\mathbb{K}$ est fini, θ n'est pas injective (dans $\mathbb{Z}/p\mathbb{Z} : x \to x^p - x$ fonction nulle (Fermat), mais $X^p - X$ non nul)

Une racine (ou zéro) de P dans $\mathbb{K}$ est un $a \in \mathbb{K}$ tel que $\tilde{P}(a) = 0_{\mathbb{K}}$

$P \in \mathbb{K}, a \in \mathbb{K},$ le reste de la div. euclidienne de P par $(X-a)$ est $\tilde{P}(a)$

Preuve : $P = (X-a)Q + R \qquad \tilde{P}(a) = (a-a)Q + R$

$P \in \mathbb{K}[X], a \in \mathbb{K}$ est racine de P *ssi* $(X-a) | P$

$P \in \mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\}$ $\quad P$ a un nombre fini de racines différentes (nbre $\leq \deg P$)

Soit $\mathbb{K}$ corps infini. $\theta \begin{cases} \mathbb{K}[X] & \to \mathfrak{F}(\mathbb{K},\mathbb{K}) \\ P & \mapsto \tilde{P} \end{cases}$ est injective. (car fct nulle $\Rightarrow \infty$ racines)

a racine de P, son ordre de multiplicité est $ord_P(a) = \max\{ j \in \mathbb{N}^*, (X-a)^j | P\}$

$(X-a)^k | P \Leftrightarrow ord_p(a) \geq k \qquad \begin{cases} (X-a)^k | P \\ (X-a)^{k+1} \nmid P \end{cases} \Leftrightarrow ord_p(a) = k$

Le nombre de racines de P (non nul) comptées avec leur multiplicité est inférieur au degré de P

P est scindé sur $\mathbb{K}$ s'il a autant de racines comptées avec leur multiplicité que son degré

$\Leftrightarrow \exists (a_1,\dots,a_n) \in \mathbb{K}^n$ 2 à 2 $\neq$, $(\alpha_1,\dots,\alpha_n) \in (\mathbb{N}^*)^n, \lambda \in \mathbb{K}^*, \qquad P = \lambda \prod_{k=0}^{n} (X-a_k)^{\alpha_k}$

La fonction polynômiale associée à $P = \sum_{k=0}^{n} a_k X^k$ est paire *ssi* pour tout k impair, $a_k = 0$

IV. Polynôme dérivé

$P = \sum_{k=0}^{n} a_k X^k$ Son polynôme dérivé $DP = \sum_{k=1}^{n} k a_k X^{k-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k$

$D \begin{cases} \mathbb{K}[X] & \to \mathbb{K}[X] \\ P & \mapsto DP \end{cases}$ est une application linéaire

$D(PQ) = D(P) \times Q + P \times D(Q) \qquad Leibniz : D^n(PQ) = \sum_{k=0}^{n} \binom{n}{k} (D^k P)(D^{n-k} Q)$

Dans $\mathbb{R}$ ou $\mathbb{C}$: $\widetilde{DP} = (\tilde{P})'$

Pour la suite, on prend $car(\mathbb{K}) = 0$ (par exemple $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$)

Si $\deg P \geq 1, \ \deg DP = \deg P - 1 \qquad$ Si $\deg P \leq 0, \deg DP = -\infty \qquad \Rightarrow \ker D = \mathbb{K}$

$Taylor : n \geq \mathrm{d} \;\; \mathrm{g} P, \; \mathrm{e} P(X) = \sum_{k=0}^{n} \frac{D^k P(a)}{k!} (X-a)^k = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} (X-a)^k$

Preuve : $Mq, \forall b \in \mathbb{K}, \tilde{P}(b) - \sum_{k=0}^{n} \frac{\widetilde{D^k P(a)}}{k!}(b-a)^k = 0 \qquad Q_b = \tilde{P}(b) - \sum_{k=0}^{n} \frac{D^k P(X)}{k!}(b-X)^k \qquad DQ_b = 0$

a racine d'ordre de multiplicité k de P $\Leftrightarrow \begin{cases} \forall j \in [\![0, k-1]\!] \quad P^{(j)}(a) = 0 \\ P^{(k)}(a) \neq 0 \end{cases}$ (Preuve: div.euclid. $P/(X-a)^p$)

V. Dans $\mathbb{R}$ ou dans $\mathbb{C}$

$\mathbb{K}$ est algébriquement clos $\Leftrightarrow$ Tout polynôme $P \in \mathbb{K}[X]$, $\deg P \geq 1$ a au moins une racine dans $\mathbb{K}$

$\Leftrightarrow$ Tout polynôme $P \in \mathbb{K}[X]$, $\deg P \geq 1$ est scindé sur $\mathbb{K}$

$\Leftrightarrow$ Les seuls polynômes irréductibles sont de degré 1

Théorème fondamental de l'algèbre (de d'Alembert-Gauss) : $\mathbb{C}$ est algébriquement clos

Tout polynôme $P \in \mathbb{C}[X]$ s'écrit $P = \lambda \prod_{j=0}^{n} (X - a_j)^{\alpha_j}$

$P = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X] \Rightarrow \overline{P} = \sum_{k=0}^{n} \overline{a_k} X^k$

$\varphi \begin{cases} \mathbb{C}[X] & \to \mathbb{C}[X] \\ P & \mapsto \overline{P} \end{cases}$ est un isomorphisme d'algèbre

$\alpha \in \mathbb{C}$ est racine de P *ssi* $\overline{\alpha}$ est racine de $\overline{P}$, $ord_P(a) = ord_{\overline{P}}(\overline{a})$

Les seuls polynômes irréductibles dans $\mathbb{R}$ sont :

– les polynômes de degré 1

– les polynômes de degré 2 sans racine réelle

Soit $P \in \mathbb{K}[X]$ scindé sur $\mathbb{K}$, $n = \deg P$, $(\alpha_1 ... \alpha_n)$ les racines de P (avec multiplicité), $P = \sum_{k=0}^{n} a_k X^k$

Pour tout $j \in [\![1, n]\!], \sigma_j = \sum_{\{i_1 ... i_n\} \in P_n(\mathbb{N}_n)} \prod_{k=1}^{j} \alpha_{i_k} = \sum_{1 \leq i_1 < ... < i_n \leq n} \prod_{k=1}^{j} \alpha_{i_k}$. On a $\forall j \in [\![1, n]\!] \qquad \frac{a_{n-j}}{a_n} = (-1)^j \sigma_j$

VI. Familles essentielles de polynômes

Polynômes d'interpolation de Lagrange : $(a_1 ... a_n) \in \mathbb{K}^n$ 2 à 2 distincts; $(\alpha_1 ... \alpha_n) \in \mathbb{K}^n$

Il existe un unique $P \in \mathbb{K}_{n-1}[X]$ tel que pour tout $j \in [\![1, n]\!]$, $P(a_j) = \alpha_j$:

$P = \sum_{k=1}^{n} \alpha_k L_k$ avec $\forall k \in [\![1, n]\!], L_k = \prod_{j \neq k} \frac{(X - a_j)}{(a_k - a_j)}$

Polynômes de Tchebychev : $\forall n \in \mathbb{N}, \exists! T_n \in \mathbb{R}[X]$ tq $\forall x \in \mathbb{R}, T_n(\cos x) = \cos(nx)$ $\qquad (preuve : \mathrm{Re}(e^{inx}))$

$\begin{cases} T_0 = 1 \qquad T_1 = X \\ \forall n \in \mathbb{N}, T_{n+1} = 2XT_n - T_{n-1} \end{cases} \qquad (preuve : \cos((n+1)x) + \cos((n-1)x) = 2\cos x \cos(nx))$

T_n est scindé sur $\mathbb{R}[X]$ et admet n racines distinctes