Les polynômes et l'algèbre $K[X]$

K corps.

1. Définition de l'algèbre $K[X]$

1.1. Suites presque nulles.

déf On appelle polynôme à coefficient dans un corps K toute suite (p_n) d'éléments de K, nulle à partir d'un certain rang, i.e.

$$\exists N \in \mathbb{N} : \quad \forall n > N, \quad p_n = 0.$$

déf Soient $P = (p_n)$ et $Q = (q_n)$ deux poly à coeff dans K, $\lambda \in K$.
On définit :

- la somme $P + Q = (p_n + q_n)$
- le produit de P par λ. $\lambda . P = (\lambda p_n)$
- le produit des polynômes : $P \times Q = (r_n)$ où r_n est défini par :

$$r_n = \sum_{k=0}^{n} p_k q_{n-k} = \sum_{i+j=n} p_i q_j$$

prop L'ensemble des polynômes à coeff dans K est muni :

- d'une structure d'ev avec les opérations $+$ et $.$
- d'une structure d'anneau avec les opérations $+$ et $\times$.
- d'une structure d'algèbre avec les op $+, ., \times$.

notation On notera : $(1, 0, \ldots, 0, \ldots) = 1$

$(0, 1, 0, \ldots) = X$

On a alors $X^2 = (0, 0, 1, 0, \ldots)$, et plus généralement

$$X^n = (0, \ldots, \underset{\substack{\uparrow \\ n+1}}{1}, 0, \ldots)$$

Ainsi, si $P = (p_0, p_1, \ldots, p_n, 0, \ldots, 0)$, on notera :

$$P = p_0 (1, 0, \ldots) + p_1 (0, 1, 0, \ldots) + \ldots + p_n (0, \ldots, 1, 0, \ldots)^n$$

$$= p_0 + p_1 X + \ldots + p_n X^n.$$

L'ensemble des polynômes à coeff dans K se note $K[X]$.

exple $A = (1, 2, 3, 4, 0, \ldots)$ $\quad B = (3, -1, -2, 0, \ldots)$. $\quad A(X) = \ldots \quad B(X) = \ldots$

$A + B$, $A \times B$

Rem $\times$ $(K[X], +, \cdot)$ sev de $(K^{\mathbb{N}}, +, \cdot)$: il n'est pas de dim finie, sa base canonique est $(1, X, X^2, \dots, X^n, \dots)$

$\times$ $(K[X], +, \times)$ n'est pas un sous-ann de $(K^{\mathbb{N}}, +, \times)$: le produit est $\neq$!

1.2. Degré d'un polynôme

déf On appelle degré d'un polynôme P non-nul le plus grand entier n tq $p_n \neq 0$. On dit alors que p_n est le coeff dominant de P, et que P est unitaire (ou normalisé) si $p_n = 1$.
Par convention, on notera $-\infty$ le degré du poly nul.
On notera $\deg(P)$ le degré du polynôme P.

déf On appelle polynôme constant les poly de deg ≤ 0. L'ens des poly constants s'identifie à K.

prop Si $A, B \in K[X]$, on a :
(i) $\deg(A+B) \leq \max(\deg A, \deg B)$
(ii) $\forall \alpha \in K^*$, $\deg(\alpha P) = \deg(P)$
(iii) $\deg(A \times B) = \deg(A) + \deg(B)$.

COR L'anneau $K[X]$ est intègre. (ie $P \times Q = 0 \Leftrightarrow P = 0$ ou $Q = 0$).
COR Le groupe des inversible $K[X]^*$ est l'ens des poly constants $\neq 0$, $(K[X])^* \simeq K^*$
prop Une famille de polynômes non-nuls étagée en degré est libre, ie si $A_1, \dots, A_n \in K[X]$ tq $\deg(A_1) < \dots < \deg(A_n)$, alors $(A_1, \dots, A_n)$ libre

Notation $K_n[X]$: ens des poly de deg $\leq n$.

prop $(K_n[X], +, \cdot)$ est un sesp vectoriel de $K[X]$ de dimension $n+1$.
De plus, $(1, X, \dots, X^n)$ est une base de $K_n[X]$, appelée base canonique

2. Arithmétique dans l'anneau $K[X]$

2.1. Division euclidienne dans $K[X]$

Thm Etant donné deux polynômes A, B avec $B \neq 0$, il existe un unique couple (Q, R) de poly tq.

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

expl div eucl de :
- $X^2 + 3X + 3$ par $X + 1$
- $X^3 + 2X^2 + X + 1$ par $X^2 + 1$
- $X^5 + 3X^4 + 1$ par $X^3 + X + 1$.

Exercice Écrire un algo de div eucl.

Thm L'anneau $(K[X], +, \times)$ est principal, ie c'est un anneau commutatif intègre tel que tout idéal est principal.

rem La principalité de $K[X]$, tout comme celle de $\mathbb{Z}$ dans le chapitre 2, va nous permettre de faire de l'arithmétique dans cet anneau. En particulier, il sera intéressant de mettre en parallèle les résultat obtenu pour $\mathbb{Z}$ avec ceux de cette section.

2.2. Diviseurs et multiples d'un polynôme

déf On dit que A divise B, ou que B est multiple de A, si
$$\exists Q \in K[X] \text{ tq } B = AQ$$
On écrit $A | B$.

rem $A | B \iff B.K[X] \subseteq A.K[X]$.

expl $(X-1) | (X^n - 1)$ et $(X+1) | (X^{2n+1} + 1)$.

déf Deux polynômes A et B sont dits associés s'ils vérifient l'une des 3 cond équiv suivantes :

(i) $A | B$ et $B | A$

(ii) $\exists \lambda \in K^*$, $A = \lambda B$

(iii) $B K[X] = A K[X]$

rem "être associé à" est une relation d'équivalence.

2.3. Diviseurs communs - PGCD

On note $\mathcal{D}(A)$ l'ens des diviseurs d'un polynôme A

<u>lemme</u> . Si A et B sont deux poly avec $B \neq 0$, et si R est le reste de la div eucl de A par B, alors $\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(B) \cap \mathcal{D}(R)$.

× $\mathcal{D}(A) \cap \mathcal{D}(0) = \mathcal{D}(A)$.

<u>Algo d'Euclide</u> $R_0 = A$, $R_1 = B$.

× Si $R_1 = 0$ on arrête.

× sinon div eucl de R_0 par R_1 $\rightsquigarrow R_2$.

$$\mathcal{D}(R_0) \cap \mathcal{D}(R_1) = \mathcal{D}(R_1) \cap \mathcal{D}(R_2).$$

. On construit ainsi une suite (R_k) de poly tq

$$\deg(R_{k+1}) < \deg(R_k).$$

$\Rightarrow \exists N$ tq $R_N \neq 0$ et $R_{N+1} = 0$ et on arrête.

On a alors $\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(R_N)$.

<u>prop</u> A et B deux polynômes. Il existe un unique polynôme unitaire (ou nul) $A \wedge B$ appelé PGCD de A et B tel que

. $A \wedge B$ divise A et B.

. tout diviseur de A et B divise $A \wedge B$.

Ce PGCD est le dernier reste non-nul de l'algo d'Euclide (après division de celui-ci par son coeff dominant).

<u>exple</u> $(X^4 - 3X^2 - 4) \wedge (X^3 + 2X^2 - X - 2)$, $(X^3 - X^2 + X - 1) \wedge (X^2 + 1)$.

<u>prop</u> A et B deux polynômes. On a :

$$A\,K[X] + B\,K[X] = (A \wedge B)\,K[X].$$

<u>prop</u> (Égalité de Bezout) Pour tout couple (A, B) de polynômes, il existe un couple (non unique !) de polynômes (U, V) tel que :

$$AU + BV = A \wedge B.$$

<u>exple</u> Couple de Bezout pour $\left((X^4 - 3X^2 - 4), (X^3 + 2X^2 - X - 2)\right)$.

③

2.4. Polynômes premiers entre eux

déf On dit que A et B sont 1$^{\text{er}}$ entre eux si : $A \wedge B = 1$.

expl . $\forall a, b \in K$, $a \neq b$, $(X-a) \wedge (X-b) = 1$.

- $\forall A \in K[X]$, $\forall a \in K^*$, $A \wedge a = 1$.

prop $A \wedge B = 1 \iff \exists U, V \in K[X] : AU + BV = 1$.

rem On montre alors que pour tout couple $(A,B) \neq (0,0)$,

$$\left(\frac{A}{A \wedge B}\right) \wedge \left(\frac{B}{A \wedge B}\right) = 1.$$

COR (Thm de Gauss) $\left.\begin{array}{l} A \mid BC \\ A \wedge B = 1 \end{array}\right\} \Rightarrow A \mid C$.

COR $\left.\begin{array}{l} A \mid C \\ B \mid C \\ A \wedge B = 1 \end{array}\right\} \Rightarrow AB \mid C$.

COR $\left.\begin{array}{l} A \wedge C = 1 \\ B \wedge C = 1 \end{array}\right\} \Rightarrow AB \wedge C = 1$.

expl $(X-a)^p \wedge (X-b)^q = 1$ $\forall p, q \in \mathbb{N}$

2.5. PPCM de deux polynômes

prop Pour tout couple (A,B) de polynômes, $\exists!$ polynôme unitaire (ou nul) $A \vee B$ appelé PPCM de A et B, tel que :

. $A \vee B$ est multiple de A et B.

. Tout multiple de A et B est multiple de $A \vee B$.

De plus on a :

$$(A \vee B) \times (A \wedge B) = \frac{A \times B}{a_p b_q}$$ (où a_p, b_q coeff dom de A et de B resp)

2.5. Généralisation aux PGCD et PPCM de plusieurs polynômes

Soient $A_1, \dots, A_n \in K[X]$ $(n \geq 2)$.

- $A_1 K[X] + \dots + A_n K[X]$ idéal de $K[X]$ $\Rightarrow$ $\exists!$ polynôme unitaire D tq
$$D K[X] = A_1 K[X] + \dots + A_n K[X].$$

- $A_1 K[X] \cap \dots \cap A_n K[X]$ idéal de $K[X]$ $\Rightarrow$ $\exists!$ polynome unitaire M tq
$$M K[X] = \bigcap_k A_k K[X].$$

<u>déf</u> . D est appelé le PGCD de $A_1, \dots, A_n$, noté $A_1 \wedge \dots \wedge A_k$.

. M est appelé le PPCM de $A_1, \dots, A_n$, noté $A_1 \vee \dots \vee A_n$.

<u>prop</u> (i) Caract du PGCD : $D \in K[X]$.

$$D = A_1 \wedge \dots \wedge A_n \Leftrightarrow \begin{cases} D \text{ divise } A_1, \dots, A_n. \\ \text{Tout diviseur de } A_1, \dots, A_n \text{ divise } D \end{cases}$$

(ii) Caract du PPCM : $M \in K[X]$.

$$M = A_1 \vee \dots \vee A_n \Leftrightarrow \begin{cases} A_1, \dots, A_n \text{ divisent } M. \\ \text{Tout multiple de } A_1, \dots, A_n \text{ est un multiple de } M. \end{cases}$$

<u>prop</u> (i) Commutativité : $\forall \sigma \in S_n$

$$A_{\sigma(1)} \wedge \dots \wedge A_{\sigma(n)} = A_1 \wedge \dots \wedge A_n.$$
$$A_{\sigma(1)} \vee \dots \vee A_{\sigma(n)} = A_1 \vee \dots \vee A_n.$$

(ii) Homogénéité : $\forall P \in K[X]$ unitaire,

$$(PA_1) \wedge \dots \wedge (PA_n) = P(A_1 \wedge \dots \wedge A_n)$$
$$(PA_1) \vee \dots \vee (PA_n) = P(A_1 \vee \dots \vee A_n).$$

(iii) Associativité : $[\![1, n]\!] = \bigcup_{j=1}^{k} I_j$ tq $I_j \cap I_i \neq \emptyset$ $\forall i \neq j$.

$$A_1 \wedge \dots \wedge A_n = \text{pgcd}(\text{pgcd}\{A_j, j \in I_1\}, \dots, \text{pgcd}\{A_j, j \in I_k\})$$
$$A_1 \vee \dots \vee A_n = \text{ppcm}(\text{ppcm}\{A_j, j \in I_1\}, \dots, \text{ppcm}\{A_j, j \in I_k\})$$

<u>prop</u> (Bezout) $A_1, \dots, A_n \in K[X]$. $\exists (U_1, \dots, U_n)$ tq

$$A_1 U_1 + \dots + A_n U_n = A_1 \wedge \dots \wedge A_n.$$

④

2.6. Polynômes irréductibles dans $K[X]$

<u>déf</u> Un polynôme $P \in K[X]$ est irréductible dans $K[X]$ si ses seuls diviseurs sont les polynômes constants non nuls et ses associés :

$$P = A \cdot B \Rightarrow A \in K^* \text{ ou } B \in K^*$$

<u>exple</u> × Tout polynôme de degré 1 est irréductible.

× X^2+X+1 est irréductible dans $\mathbb{R}[X]$.

× $X^2+X+1 = (X-j)(X-\bar{j})$ n'est pas irréductible dans $\mathbb{C}[X]$. En particulier, il sera essentiel de prendre en compte le corps K sur lequel on travaille.

<u>Thm</u> Pour tout polynôme A ($\deg(A) \geq 1$), il existe un entier $m \geq 1$, m poly irréductibles $P_1, \ldots, P_m$ et des entiers $r_1, \ldots, r_m \in \mathbb{N}^*$ tq :

$$A = \lambda P_1^{r_1} \cdots P_m^{r_m} \qquad (\lambda \in K^*).$$

On l'appelle la factorisation de A en produit de poly irréductibles.

Elle est unique (à l'ordre près des facteurs).

<u>rem</u> λ est le coeff dominant de A.

<u>rem</u> Comme dans $\mathbb{Z}$, les PGCD et PPCM de polynômes peuvent être obtenus à partir de leurs factorisations en prod de poly irréductibles.

3. Fonctions polynômes - Racines

3.1. Fonctions polynômes à coeff dans K

<u>Rappel</u> Polynômes : suite presque nulle d'éléments de K.

X = suite $(0,1,0,\ldots)$.

On aimerait substituer à X des éléments de K, et ainsi évaluer un polynôme en un scalaire $a \in K$. Pour cela on introduit la notion suivante

déf On appelle fonction polynomial associée à $P(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0$.
la fonction : $\tilde{P} : K \to K$
$x \mapsto \tilde{P}(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$.

prop L'application :
$\theta : P \in K[X] \longmapsto \tilde{P} \in \mathcal{P}_K = \{$fonctions polynomiales sur $K\}$.
est un morphisme d'algèbres surjectif.

Rem Nous verrons plus tard que θ est en fait un isomorphisme d'algèbres dans le cas où K est infini
ce qui nous permettra d'identifier polynômes et fonctions polynomiales.

Algorithme de Hörner : $\tilde{P}(x) = (\dots(a_n x + a_{n-1})x + a_{n-2})x \dots)x + a_0$ n mult et n additions.
$\to$ évaluer $5X^4 - 4X^3 + 3X^2 - 2X + 1$ en 3.

3.2. Racine d'un polynôme

déf $a \in K$ est une racine de $P \in K[X]$ si $\tilde{P}(a) = 0$.

exple . Tout poly de degré 1 a une racine : la racine de $aX+b$ est $-b/a$
. Pour un poly de deg 2, l'existence de racines dépend du corps K.
$\to$ $X^2 - 2$ n'a pas de racine dans $\mathbb{Q}$, il a les racines $\pm\sqrt{2}$ dans $\mathbb{R}$.
$\to$ $X^2 + 1$ n'a pas de racine dans $\mathbb{R}$, il a les racines $\pm i$ si $K = \mathbb{C}$.
. Si z est racine de $P \in \mathbb{R}[X]$, alors $\bar{z}$ est aussi racine de P.

prop a est racine de $P \iff (X-a) \mid P$.

exple -2 racine de $X^3 - X + 6$. avec l'algorithme de Hörner.

prop Soit P polynôme et $a_1, \dots, a_n$ n scalaires distincts
$a_1, \dots, a_n$ racines de $P \iff (X-a_1)\dots(X-a_n)$ divise P

COR . Un polynôme de degré n a au plus n racines distinctes
. Le seul polynôme qui possède une infinité de racines est nul

Supposons K infini
COR $\theta : P \in K[X] \to \tilde{P} \in \mathcal{P}_K$ est un isomorphisme d'algèbres.

À présent, on identifiera le polynôme P et la fonction polynomiale associée $\tilde{P}$.

5

<u>expl</u> Factorisation de X^5-1 dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$.

3.3. Ordre de multiplicité des racines d'un polynôme

<u>déf</u> On appelle dérivée d'un polynôme $P(X)=\sum_{k=0}^{n} a_k X^k$ le polynôme noté P', tq

$$P'(X) = \sum_{k=1}^{n} k a_k X^{k-1}.$$

On définit de même $P''=(P')'$, $P^{(k)}=(P^{(k-1)})'$.

<u>prop</u>
- $P'=0 \Leftrightarrow P$ constant
- si $\deg P \geq 1$, $\deg P' = \deg(P)-1$.
- $(\lambda P+\mu Q)' = \lambda P' + \mu Q'$.
- $(PQ)' = P'Q + Q'P$.

<u>prop</u> Formule de Leibniz : $\forall P, Q \in K[X]$, $\forall n \in \mathbb{N}$,

$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

<u>prop</u> Formule de Taylor : Si P poly de deg n, $\forall a \in K$

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

<u>prop</u> Si $P\in K[X]$, $a\in K$, $r\in \mathbb{N}^*$, on a équivalence entre :
- $(X-a)^r$ divise P
- $P(a)=P'(a)=\dots=P^{(r-1)}(a)=0$.

<u>rem</u> On dit que a est racine de P de multiplicité au moins r.

<u>prop</u> On a équivalence entre :
(i) $\exists Q\in K[X]$ tq $P=(X-a)^r Q$ et $Q(a)\neq 0$.
(ii) $(X-a)^r$ divise P et $(X-a)^{r+1} \nmid P$.
(iii) $P(a)=P'(a)=\dots=P^{(r-1)}(a)=0$ et $P^{(r)}(a)\neq 0$.

<u>déf</u> On dit alors que a est racine de multiplicité r exactement de P.

exple $P(X) = X^5 - 7X^4 + 19X^3 - 25X^2 + 16X - 4$.

On mq $P(1) = P'(1) = P''(1) = 0$ et $P'''(1) = 6$.

On factorise avec l'algo d'Hörner.

prop $P \in K[X]$, $a_1, \dots, a_n \in K$ des scalaires distincts, $r_1, \dots, r_n \in \mathbb{N}^*$.

a_i racine de P de mult r_i, $i = 1, \dots, n \iff (X-a_1)^{r_1} \dots (X-a_n)^{r_n}$ divise P.

COR Un poly de deg n a au plus n racines comptées avec leur ordre de multiplicité.

4. Polynômes scindés

4.1. Définition

déf On dit que $P \in K[X]$ est scindé (dans K) s'il peut s'écrire

$$P = \lambda (X - a_1) \dots (X - a_n)$$

où $\lambda \in K^*$, $a_i \in K$.

rem λ : coeff dominant, a_i : racines.

4.2. Thm de d'Alembert-Gauss. csqus

Thm (D'Alembert-Gauss) Tout polynôme $P \in \mathbb{C}[X]$ est scindé.

COR Les seuls polynômes irréductibles non constants de $\mathbb{C}[X]$ sont les polynômes de degré 1.

COR Les polynômes non-constants, irréductibles de $\mathbb{R}[X]$ sont :

(1) les polynômes de deg 1

(2) les polynômes de deg 2 à $\Delta < 0$.

rem Dans $\mathbb{Q}[X]$, $X^3 - 2$ est irréductible. On peut trouver des poly irréductibles de tout degré ≥ 1.

exple Factoriser dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$ le polynôme $X^{2n} - 1$.

⑥ 4.3. Relations coefficients-racines

P un poly scindé de deg ≥ 2

- deg P = 2 : $P = aX^2+bX+c = a(X-x_1)(X-x_2) = a(X^2-(x_1+x_2)X+x_1x_2)$.

$s = x_1+x_2 \quad p = x_1x_2 \Rightarrow s = -\frac{b}{a} \quad p = \frac{c}{a}$.

- deg P = 3 : $\sigma_1 = x_1+x_2+x_3 = \frac{-b}{a}$

$\sigma_2 = x_1x_2+x_2x_3+x_1x_3 = \frac{c}{a}$

$\sigma_3 = x_1x_2x_3 = \frac{-d}{a}$.

Fonctions symétriques élémentaires : $\sigma_1 = x_1+\dots+x_n$

$\sigma_2 = \sum_{1\leq i<j\leq n} x_ix_j$

$\sigma_k = \sum_{1\leq i_1<\dots<i_k\leq n} x_{i_1}\dots x_{i_k}$

$\sigma_n = x_1x_2\dots x_n$.

$P(X) = a_nX^n+\dots+a_0 = a_n(X-x_1)\dots(X-x_n)$.

$\sigma_1 = -\frac{a_{n-1}}{a_n} \quad \sigma_2 = \frac{a_{n-2}}{a_n}, \dots, \sigma_k = (-1)^k\frac{a_{n-k}}{a_n}, \dots, \sigma_n = (-1)^n\frac{a_0}{a_n}$

5. Thèmes d'étude.

→ Recherche de solutions d'équations polynomiales. On connait les relations entre coefficients et racines. On pose à présent la question des relations entre racines et coeff, ie à partir des coeff d'un polynôme, exprimer les racines par +, × et radicaux.

→ deg 2. ok

→ deg 3. formules de Cardan (1545)

→ deg 4 : formules de FERRARI (élève de Cardan)

$\Big\}$ très compliquées ...

→ deg 5. pas de résultat pendant 200 ans.

1826 ⇝ Abel : impossible de donner des formules explicites similaires à celles obtenues pour les deg <.

1830 : Galois (sans connaître les résultats d'Abel) crée la notion de gpes pour l'étude de ce pb. Il donne un critère de résolubilité par radicaux de toutes les équations polynomiales. Il meurt à 20 ans dans un duel (1932) "provoqué par deux patriotes" (...) "victime d'une infâme coquette" (une certaine Stéphanie D.).

La veille, il écrit une lettre à Chevalier où il dresse le bilan de ses recherches. et il lui demande de les faire publier.

→ <u>Solutions approchées</u> Pour la résolution d'une équation polynomiale de deg ≥ 3, on cherchera en pratique des solutions approchées, par les méthodes classiques : (méthode de Newton)

→ <u>Approximation polynomiale</u>

. Les fonctions les plus faciles à évaluer numériquement sont les fonctions polynômiales. Il est donc important de savoir approx une fonction arbitraire par des polynômes.

× Thm de Weierstrass ⇒ C'est théoriquement possible.

× Interpolation de Lagrange : $\exists p_n \in \mathbb{R}_n[X] : p_n(x_i) = f(x_i)$
$(x_0 < x_1 < \dots < x_n)$

⇝ si les x_i sont bien choisit, $p_n \to f$ uniformément sur le segment $[a,b]$