Compléments polynômes

Déf : Les diviseurs triviaux d'1 polynôme P de degré d ($\neq 0$, $\neq$ nul) sont les inversibles et ses associés.

Un polynôme P est dit *irréductible* si tous ses diviseurs sont triviaux et réductible dans le cas contraire.

Th : Tout polynôme non constant est produit de polynômes irréductibles

Corollaire : Il y a une infinité de polynômes irréductibles unitaires (2 à 2 non associés)

Preuve : Si le corps $\mathbb{K}$ est infini, il suffit de considérer les $X-a$, $a \in \mathbb{K}$

Dans le cas contraire, supposons qu'il y ait un nombre fini de polynômes irréductibles, notés $P_1, \dots P_k$ avec $k \neq 0$

Soit $P = P_1 \dots P_k + 1$ est de degré sup ou égal à k, donc divisible par un polynôme irréductible Q (unitaire).

Si Q est l'un des P_i alors $Q \mid P_1 \dots P_k$ donc $Q \mid P - P_1 \dots P_k = 1$

impossible.

Th L'anneau $\mathbb{K}[X]$ est principal.

Th de Bézout : Soient F et G deux polynômes non tous deux nuls. Ils admettent un pgcd $\Delta = F \wedge G$. C'est le générateur de l'idéal $\langle F, G \rangle$ engendré par F et G et il existe donc $A, B \in \mathbb{K}[X]$ tq

$\Delta = AF + BG$.

(premiers entre eux $\Leftrightarrow$ pas de diviseur commun non inversible)

On obtient alors les théorèmes suivants :

Th Lemme de Gauss

Soient F et G premiers entre eux et $H \in \mathbb{K}[X]$ tq $F \mid GH$

alors $F \mid H$.

Th Lemme d'Euclide.

Tout élément F irréductible est premier c.a.d tq

$$F \mid GH \Rightarrow F \mid G \text{ ou } F \mid H.$$

Th fondamental. Tout polynôme P non nul admet une factorisation

$$P = C P_1 \dots P_r \quad \text{avec } C \in \mathbb{K}^* \text{ et } P_1, \dots P_r \text{ irréductibles unitaires}$$

Cette décomp est unique à l'ordre près.

Fonctions polynomiales et racines d'un polynôme.

Déf: Soit $P = \sum_{n \geq 0} a_n X^n \in \mathbb{K}[X]$ sur le corps commutatif $\mathbb{K}$.

L'application $x \mapsto P(x) = \sum_{n \geq 0} a_n x^n$ de $\mathbb{K} \to \mathbb{K}$ est appelée application polynomiale associée à P.

Th Soit $P \in \mathbb{K}[X]$ non nul et $a \in \mathbb{K}$

1) On dit que a est une racine de P si $P(a) = 0$. Pour que a soit une racine de P ⇔ $X - a \mid P$

2) On suppose que a est 1 racine de P, $\exists ! \, m \in \mathbb{N}^*$ tel que $(X-a)^m \mid P$ et $(X-a)^{m+1} \nmid P$.

$m \in [\![1, \deg(P)]\!]$. m est l'ordre de multiplicité de a.

Polynôme d'interpolation de Lagrange.

Soient $(a_0 \dots a_n)$ éléments distincts 2 à 2 de $\mathbb{K}$.

$$\forall i \in [\![0, n]\!] \quad L_i = \prod_{\substack{j=0 \\ j \neq i}}^{n} \frac{X - a_j}{a_i - a_j}$$

Ces polynômes sont de degré n et $L_i(a_j) = \delta_{ij}$

Th Pour tout $(b_0, \dots b_n) \in \mathbb{K}^{n+1}$, il existe un unique polynôme $P \in \mathbb{K}_n[X]$ tq $P(a_0) = b_0, \dots P(a_n) = b_n$.

Il s'agit de $P = \sum_{i=0}^{n} b_i L_i$

Def un polynôme P est scindé s'il est produit de polynômes du premier degré. Il est dit **scindé à racines simples** si toutes ses racines sont simples.

Th et déf : Le corps commutatif $\mathbb{K}$ est dit **algébriquement clos** si les conditions équivalentes suivantes sont vérifiées :

i) tout polynôme non constant sur $\mathbb{K}$ admet une racine au moins

ii) tout polynôme non constant sur $\mathbb{K}$ est scindé

iii) les polynômes irréductibles de $\mathbb{K}[X]$ sont de degré 1.

Déf : Soient $x_1, \dots x_n$ des éléments de $\mathbb{K}$.

Les **fonctions symétriques élémentaires** des x_i sont les expressions.

$$\forall k \in [\![1, n]\!] \quad \sigma_k(x_1, \dots x_n) = \sum_{1 \le i_1 < \dots < i_k \le n} x_{i_1} \dots x_{i_k}.$$

Ex $\sigma_1(x_1, \dots x_n) = x_1 + x_2 + \dots + x_n$

$$\sigma_2(x_1, \dots x_n) = \sum_{1 \le i < j \le n} x_i x_j = x_1 x_2 + \dots + x_{n-1} x_n$$

$$\vdots$$

$$\sigma_n(x_1, \dots x_n) = \prod_{i=1}^{n} x_i$$

Ainsi : chaque $\sigma_k(x_1, \dots x_n)$ est la somme de $\binom{n}{k}$ monômes.

Th **Relations entre coeff et racines**

Soit $P = a_0 + a_1 X + \dots + a_n X^n = a_n (X - x_1) \dots (X - x_n)$ polynôme scindé de degré n.

$$\forall k \in [\![1, n]\!] \quad \sigma_k(x_1, \dots, x_n) = (-1)^k \frac{a_{n-k}}{a_n}$$

Application aux corps finis

Soit $\mathbb{K}$ corps fini de q éléments commutatif.

LC

Th : Le polynôme $X^q - X \in \mathbb{K}[X]$ est scindé et égal à

$$X^q - X = \prod_{a \in \mathbb{K}} (X - a)$$

Preuve - Le groupe multiplicatif $\mathbb{K}^*$ a $q-1$ éléments par Lagrange

$\forall x \in \mathbb{K}^*$ vérifie $x^{q-1} = 1$ donc $x^q = x$

c'est aussi vrai pour $x = 0$, donc tous les éléments de $\mathbb{K}$ sont racines de $X^q - X$, d'où $\prod_{a \in \mathbb{K}} (X - a)$ le divise.

Th = Le groupe $\mathbb{K}^*$ multiplicatif est cyclique.

Polynômes sur $\mathbb{R}$ ou $\mathbb{C}$

Th Inégalité des accroissements finis.

Soit $P \in \mathbb{C}[X]$ et $a, b \in \mathbb{C}$, on suppose que $|P'| \leq R$ sur le segment $[a, b]$ où $R \in \mathbb{R}_+$. Alors

$$|P(b) - P(a)| \leq R|b - a|$$

Applications du th de Gauss - D'Alembert.

Th Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos : tout polynôme non nul de $\mathbb{C}[X]$ est scindé. En particulier, un polynôme de $\mathbb{R}[X]$ est scindé ssi toutes ses racines dans $\mathbb{C}$ sont réelles

Corollaire : Soit $P \in \mathbb{R}[X]$ unitaire tq $\forall x \in \mathbb{R}\ P(x) > 0$

Alors il existe $A, B \in \mathbb{R}[X]$ tq $P = A^2 + B^2$

Cyclotomie

On note $\mu_n = \{ e^{2ik\pi/n} \mid k \in [\![0, n-1]\!] \}$ racines $n^{ième}$ de l'unité.

Th : Soit $n \geq 1$, le polynôme $X^n - 1 \in \mathbb{C}[X]$ est scindé et séparable.

Il admet la factorisation suivante :

$$X^n - 1 = \prod_{j \in \mu_n} (X - j) = \prod_{k=0}^{n-1} \left(X - e^{2ik\pi/n}\right)$$

Ex Soit $P(X) = X^n - 1$ alors $P'(1) = n$

mais $P'(1) = \prod_{j \in \mu_n \setminus \{1\}} (1 - j) = \prod_{k=1}^{n-1} \left(1 - e^{2ik\pi/n}\right)$

$$\prod_{k=1}^{n-1} e^{ik\pi/n} \prod_{k=1}^{n-1} \left(e^{-ik\pi/n} - e^{+ik\pi/n}\right) = e^{(n-1)i\pi/2} \prod_{k=1}^{n-1} \left(-2i \sin \frac{k\pi}{n}\right)$$

Soit $\prod_{k=1}^{n} \sin \frac{k\pi}{n} = \frac{n}{2^{n-1}}$

Corollaire : la décomposition en facteurs irréductibles de $X^n - 1$ sur $\mathbb{R}$ est donnée par la formule suivante :

- si $n = 2p$ $\quad X^n - 1 = (X-1)(X+1) \prod_{k=1}^{p-1} \left(X^2 - 2X \cos \frac{2k\pi}{n} + 1\right)$
- si $n = 2p+1$ $\quad X^n - 1 = (X-1) \prod_{k=1}^{p} \left(X^2 - 2X \cos \frac{2k\pi}{n} + 1\right)$

Polynômes cyclotomiques

Avec la décomposition de $X^n - 1$ dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$, on étudie la décomposition dans $\mathbb{Q}[X]$

Soit $E_n = \{k \in [\![0, n-1]\!] \mid k \wedge n = 1\}$

alors $\mu_n^* = \{e^{2ik\pi/n} \mid k \in E_n\}$ est l'ensemble des racines primitives $n^{\text{ème}}$ de l'unité

Def : le $n^{\text{ème}}$ polynôme cyclotomique est le polynôme unitaire Φ_n dont les racines sont les racines primitives $n^{\text{ième}}$ de l'unité

$$\Phi_n = \prod_{j \in \mu_n^*} (X - j) = \prod_{k \in E_n} \left(X - e^{2ik\pi/n}\right)$$

Rem le polynôme Φ_n est de degré $\operatorname{card} \mu_n^* = \operatorname{card} E_n = \varphi(n)$

On a $\Phi_1 = X-1$. Soit p premier, tous les entiers $[\![1, p-1]\!]$ sont premiers avec p et l'on a

$$\Phi_p = \frac{X^p - 1}{X-1} = X^{p-1} + \dots + X + 1$$

Prop - Soit $n \geq 1$ alors $X^n - 1 = \prod_{d \mid n} \Phi_d$

Démo - Soit j racine $n^{ième}$ de l'unité et soit d son ordre en tant qu'élément du groupe μ_n : c'est l'unique diviseur de n tel que j est racine primitive $d^{ième}$. Le groupe μ_n est l'union disjointe des μ_d^* pour $d \mid n$. On a

$$X^n - 1 = \prod_{j \in \mu_n} (X-j) = \prod_{d \mid n} \left(\prod_{j \in \mu_d^*} (X-j) \right) = \prod_{d \mid n} \Phi_d$$

Soient par exemple p premier et $k \geq 1$ alors

$$\Phi_{p^k} = \frac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = \sum_{i=0}^{p-1} X^{i p^{k-1}}$$

Lemme - Soit $A, B \in \mathbb{Q}[X]$, des polynômes à coeff rationnels et $C = AB$ on suppose A unitaire et que A et C sont à coeff entiers. ($A, C \in \mathbb{Z}[X]$) Alors $B \in \mathbb{Z}[X]$

Th Les polynômes cyclotomiques sont à coeff entiers $\Phi_n \in \mathbb{Z}[X]$