Hommage à Samuel Paty et Dominique Bernard

Cet après-midi 13h55 : MPI math.

Bonne : 130.1

Compléments sur les polynômes

Je me souviens

1. Que sont les polynômes ?
2. Quelles sont les opérations sur les polynômes ?

déf : polynôme = suite d'éléments de $\mathbb{K}$ à support fini

$$P = (a_0, a_1, a_2, \dots, a_n, \dots, a_p, 0, 0, \dots)$$

Structure : lois.

$+ \rightarrow$ addition coeff à coeff.

$\cdot \rightarrow$ loi externe = mult de chq coeff par λ

$\times \rightarrow$ pour $P = (a_0, a_1, \dots, a_n, \dots, a_p, 0 \dots)$

$$Q = (b_0, b_1, \dots b_n \dots b_q, 0 \dots)$$

on définit $PQ = (c_0, c_1, \dots, c_n, \dots, 0, \dots)$

où $c_n = \sum_{k=0}^{n} a_k b_{n-k}$

On peut munir $(\mathbb{K}[X], +, \times, \cdot)$ algèbre

Notation : $(0, 0\ldots 0\ldots)$ — 0

$(1, 0, \ldots 0\ldots)$ est noté 1

$(0, 1, 0, \ldots 0\ldots)$ est noté X

"indéterminée formelle".

Alors $P = (a_0, a_1, \ldots, a_n, \ldots, a_p, 0\ldots)$

$= a_0 1 + a_1 X + \ldots + a_n X^n + \ldots + a_p X^p$

$= \sum_{n=0}^{p} a_n X^n$

$= \sum_{n=0}^{+\infty} a_n X^n$ ← pas une somme infinie (CL)

Autres opérations : $P \circ Q$ ...

3. Que désigne $\mathbb{K}_n[X]$?

4. Énoncer le théorème de la division euclidienne dans $\mathbb{K}[X]$.

9. Quels sont les idéaux de $\mathbb{K}[X]$?

$\mathbb{K}_n[X] = \text{Vect}(1, X, \dots, X^n)$

$= \{\text{les pol de degré} \leq n\}$

↑ inclus 0.

Divisionclidienne de A par B :

$\exists ! (Q, R)$ tq $\begin{cases} A = BQ + R \\ R = 0 \text{ ou } \deg R < \deg B \end{cases}$

Idéaux de $\mathbb{K}[X]$: ce sont les $P\mathbb{K}[X]$

Analogie avec $\mathbb{Z}$.

5. Qu'est-ce que la fonction polynomiale associée à P ?

Soit $P \in \mathbb{K}[X]$ $\quad P = \sum_{k=0}^{n} a_k X^k$

On définit $\tilde{P} : \mathbb{K} \longrightarrow \mathbb{K}$ fonction polynomiale

$t \longmapsto \sum_{k=0}^{n} a_k t^k$

On peut noter $\tilde{P}$ cette fct.

On peut identifier P et $\tilde{P}$ (si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$)

C'est la même chose

$P = 0 \iff \forall k,\ a_k = 0$

$\tilde{P} = 0 \iff \forall t \in \mathbb{K},\ \tilde{P}(t) = 0$

6. Parlons de racines d'un polynôme.

α racine de P $\Leftrightarrow$ $\tilde{P}(\alpha) = 0$ (analytique)

$\Leftrightarrow$ $(X-\alpha) \mid P$ (algébrique/arithmétique)

$P = X^2 + 1$ n'a pas de racine réelle

- $P \in \mathbb{R}[X]$

  $\tilde{P} : \mathbb{R} \longrightarrow \mathbb{R}$

  $t \longmapsto t^2 + 1 > 0$

- $P \in \mathbb{C}[X]$

  $\tilde{P} : \mathbb{C} \longrightarrow \mathbb{C}$

  $z \longmapsto z^2 + 1$

  $= (z-i)(z+i)$

Dans $\mathbb{C}$, tout polynôme est scindé

ie $\forall P \in \mathbb{C}[X]$, $\exists \alpha_1 \dots \alpha_n$ tq

$P = \lambda (X-\alpha_1) \cdots (X-\alpha_n)$

$\Leftrightarrow$ Tout pol de $\mathbb{C}[X]$ non constant admet une racine dans $\mathbb{C}$.

α racine d'ordre $\geq k$ de P

$\Leftrightarrow (X-\alpha)^k \mid P$

$\Leftrightarrow P(\alpha) = 0 = P'(\alpha) = \dots = P^{(k-1)}(\alpha) = 0$

α racine d'ordre exactement k de P

$$\Leftrightarrow (X-\alpha)^k \mid P \text{ et } (X-\alpha)^{k+1} \nmid P$$

$$\Leftrightarrow \begin{cases} P(\alpha)=0 \\ \vdots \\ P^{(k-1)}(\alpha)=0 \\ P^{(k)}(\alpha)\neq 0 \end{cases}$$

7. Qu'est-ce qu'un polynôme scindé ?

8. Relations coefficients-racines.

Le programme se limite au cas où le corps de base $\mathbb{K}$ est un sous-corps de $\mathbb{C}$. Typiquement $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{Q}$.

1 PGCD de deux polynômes

1.1 Définition du PGCD par les idéaux

Lemme. Soit $A, B \in \mathbb{K}[X]$. Alors :

$$(A) + (B) = A\mathbb{K}[X] + B\mathbb{K}[X] = \{AU + BV,\ U, V \in \mathbb{K}[X]\}$$

est un idéal de $\mathbb{K}[X]$.

Définition. Soit $A, B \in \mathbb{K}[X]$ non tous les deux nuls. Alors il existe un unique polynôme unitaire D, appelé **PGCD de A et B**, tel que :

$$(A) + (B) = (D) \text{ i.e. } A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$$

Notation.

- On note $A \wedge B$ le PGCD de A et B.
- La relation $AU + BV = A \wedge B$ s'appelle **relation de Bézout**.

Proposition. Soit A, B deux polynômes non nuls. Les diviseurs communs à A et B sont les diviseurs de $A \wedge B$.

Remarque. *On retrouve la définition de première année : $A \wedge B$ est le polynôme unitaire, de plus grand degré, qui divise à la fois A et B.*

Lemme : sous-groupe de $\mathbb{K}[X]$

$(A)+(B)$ est absorbant pour $\times$.

Définition : $A, B \in \mathbb{K}[X]$

$A\mathbb{K}[X] + B\mathbb{K}[X]$ idéal de $\mathbb{K}[X]$

donc de la forme $D\mathbb{K}[X]$

unicité : Si $D_1\mathbb{K}[X] = D_2\mathbb{K}[X]$

alors $D_1 \mid D_2$ et $D_2 \mid D_1$

donc $\exists \lambda \in \mathbb{K}^*$ tq $D_1 = \lambda D_2$

or D_1, D_2 unitaires donc $D_1 = D_2$

$D = A \wedge B$

$D \in A\mathbb{K}[X] + B\mathbb{K}[X]$ donc $\exists U, V \in \mathbb{K}[X]$ tq $D = AU + BV$

1.2 Algorithme d'Euclide

Proposition. Soit $A, B \in \mathbb{K}[X]$, supposés non nuls. En notant R le reste de la division euclidienne de A par B, on a :

$$A \wedge B = B \wedge R$$

Corollaire. En itérant l'utilisationde cette propriété, le degré du second polynôme est strictement décroissant, donc les itérations se terminent avec un reste nul. Le PGCD de A et B est alors le dernier reste non nul obtenu.

Corollaire. L'analyse de l'algorithme d'Euclide permet de construire un couple (U, V) de polynômes satisfaisant la relation de Bézout.

Preuve: les diviseurs communs de A et B

sont les diviseurs communs de B et R

Longue $A = BQ + R$

$R_0 = B$

$R_1 = R$ où $A = BQ + R$

⋮

$A\,\mathbb{K}[X]+B\mathbb{K}[X]=1.\,\mathbb{K}[X]$

1.3 Polynômes premiers entre eux

Définition. On dit que A et B sont premiers entre eux lorsque $A \wedge B = 1$.

Remarque. *Deux polynômes sont premiers entre eux lorsque les seuls diviseurs communs sont les polynômes constants.*

Théorème de Bézout.

Deux polynômes A et B sont premiers entre eux si et seulement s'il existe des polynômes U et V tels que :

$$AU + BV = 1$$

Proposition. Soit A, B deux polynômes non nuls, D un polynôme unitaire.

$$D = A \wedge B \iff \exists A_1, B_1 \in \mathbb{K}[X],\ \begin{cases} A = A_1 D \text{ et } B = B_1 D \\ A_1 \text{ et } B_1 \text{ sont premiers entre eux} \end{cases}$$

2 Un peu d'arithmétique des polynômes

Lemme de Gauss.

Soit $A, B, C \in \mathbb{K}[X]$. Si $A \mid BC$ et $A \wedge B = 1$, alors $A \mid C$.

Corollaire. Si $A \mid C$, $B \mid C$ et $A \wedge B = 1$, alors $AB \mid C$.

Corollaire. Si $A \wedge C = 1$ et $B \wedge C = 1$, alors $AB \wedge C = 1$.

Lemme de Gauss:

On suppose que $A \mid BC$ et $A \wedge B = 1$

ie $\exists U, V$ tq $AU + BV = 1$ et $\exists Q$ tq $BC = AQ$

On a donc:

$$C = C \times 1$$
$$= C(AU + BV)$$
$$= ACU + BC.V \quad \text{où } BC = AQ$$
$$= A(CU + QV)$$
$$\in A\mathbb{K}[X]$$

Corollaire:

On suppose $A \mid C$ et $B \mid C$ et $A \wedge B = 1$

ie $\exists Q, R$ tq $C = AQ$ et $C = BR$

donc $AQ = BR$

donc $A \mid BR$

or $A \wedge B = 1$

donc $A \mid R$ par le lemme de Gauss

ie $\exists P \quad R = AP$

et alors $C = B(AP) \in AB\,\mathbb{K}[X]$

ie $AB \mid C$

Remarque. il est intéressant de "relire" ces 3 propriétés avec la notion de décomposition en irréductibles.

3 Polynômes irréductibles, décomposition en facteurs irréductibles

3.1 Définition

Définition. Un polynôme P est dit **irréductible** s'il est non constant, et que ses seuls diviseurs sont les polynômes constants et les polynômes associés à P, i.e. les λP où $\lambda \neq 0$.

Analogie. *Les polynômes irréductibles sont aux polynômes ce que les nombre premiers sont aux entiers.*

3.2 Propriétés

Proposition. Un polynôme P est irréductible si et seulement s'il n'existe pas de factorisation $P = AB$ où $0 < \deg(A) < \deg(P)$.

Proposition. Soit P irréductible, et Q quelconque. Alors soit $P \wedge Q = 1$, soit $P \mid Q$.

3.3 Exemples

Remarque. *L'étude générale des polynômes irréductibles n'est pas au probramme. Seuls la description des irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$ est à connaître.*
La description des irréductibles de $\mathbb{Q}[X]$ est, par exemple, très délicate.

Proposition.

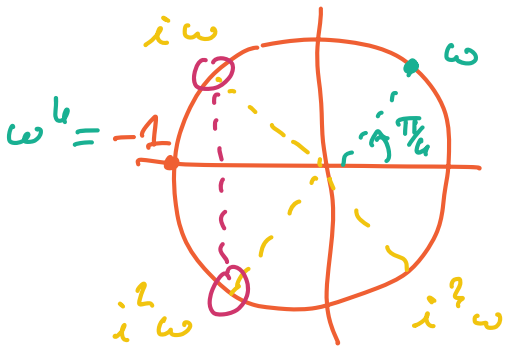
- Dans $\mathbb{C}[X]$, les polynômes irréductibles sont les polynômes de degré 1. $(X-\alpha)$
- Dans $\mathbb{R}[X]$, les polynômes irréductibles sont les polynômes de degré 1, et ceux de degré 2 à discriminant < 0.

Remarque. *$X^4 + 1$ n'a pas de racine réelle, mais ce n'est pas un irréductible de $\mathbb{R}[X]$.*

$(X-\alpha)$ $\quad (X^2+pX+q)$ où $p^2-4q<0$

$P : X^4+1$ $\quad \tilde{P} : \mathbb{R} \longrightarrow \mathbb{R}$, $t \longmapsto t^4+1$ n'a pas de racine

mais n'est pas irréductible.



$P = X^4+1$

$= \ldots$ dans $\mathbb{C}[X]$

$(X-\omega)(X-i\omega)(X-i^2\omega)(X-i^3\omega)$

où $\omega = e^{i\pi/4}$

$$= (X - e^{i\pi/4})\left(X - e^{i\frac{\pi}{4}+\frac{3\pi}{2}}\right)\left(X - e^{i\frac{\pi}{4}+\frac{\pi}{2}}\right)\left(X - e^{i\frac{\pi}{4}+\pi}\right)$$

$$= (X - e^{i\pi/4})(X - e^{-i\pi/4})\left(X - e^{i\frac{3\pi}{4}}\right)\left(X - e^{-i\frac{3\pi}{4}}\right)$$

$X^2 - 2\mathrm{Re}(\ )X + |\ |^2$

$$= (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$$

Sans racines réelles, donc ce sont

2 irréductibles de $\mathbb{R}[X]$.

Rmq: $X^4 + 1 = (X^2+1)^2 - 2X^2$

$a^2 \quad - b^2$

3.4 Décomposition en facteurs irréductibles

Théorème.

Tout polynôme P non constant se décompose de façon unique (à l'ordre des facteurs près) sous la forme :

$$P = \lambda \prod_{i=1}^{k} P_i^{m_i}$$

où les P_i sont irréductibles unitaires, les m_i dans $\mathbb{N}^*$ et λ le coefficient dominant de P.

Remarque. *Cette décomposition s'écrit :*

- *sur* $\mathbb{C}[X]$: $P = \lambda \prod_{i=1}^{k} (X - a_i)^{m_i}$
- *sur* $\mathbb{R}[X]$: $P = \lambda \prod_{i=1}^{k} (X - a_i)^{m_i} \prod_{j=1}^{\ell} (X^2 + b_j X + c_j)^{n_j}$ *où* $b_j^2 - 4c_j < 0$.

Rmq : déc. en éléments simples des fractions rationnelles à venir

(connaître la forme a priori de la déc.)

3.5 Utilisation de la décomposition en facteurs irréductibles pour le calcul du PGCD

Proposition. Soit P, Q deux polynômes non nuls, que l'on décompose en facteurs irréductibles :

$$P = \lambda \prod_{i=1}^{k} P_i^{m_i} \text{ et } Q = \mu \prod_{i=1}^{k} P_i^{n_i}$$

Les P_i sont supposés irréductibles, unitaires, deux à deux distincts et les m_i, n_i sont des entiers éventuellement nuls. Alors :

$$\text{pgcd}(P, Q) = \prod_{i=1}^{k} P_i^{\text{Min}(m_i, n_i)}$$

Proposition. Soit P, Q deux polynômes non nuls, que l'on décompose en facteurs irréductibles. Alors P et Q sont premiers entre eux si et seulement s'il n'ont aucun facteur irréductible commun.

4.6 Rel coeff racines.

130.2

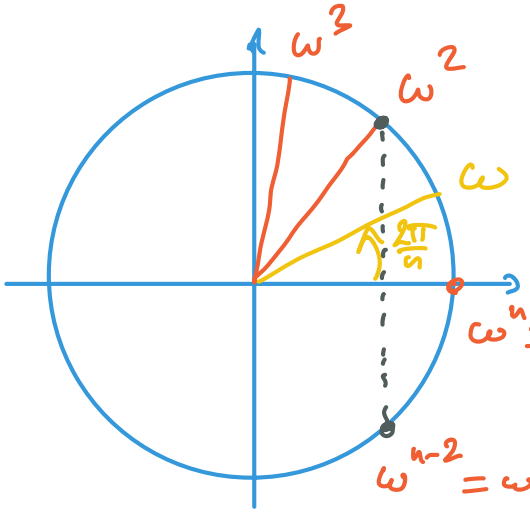
(a) $X^n - 1 = \prod_{\alpha \in \mathbb{U}_n} (X - \alpha)$

$= \prod_{k=0}^{n-1} \left(X - e^{i \frac{2k\pi}{n}} \right)$

$= \prod_{k=0}^{n-1} (X - \omega^k)$

où $\omega = e^{i \frac{2\pi}{n}}$

car $(\mathbb{U}_n, \times)$ groupe et c'est $\langle \omega \rangle$



car $\omega\bar{\omega} = 1$

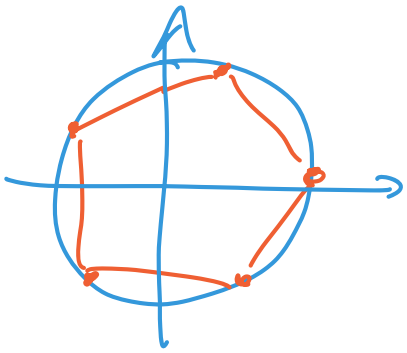
(b) Dem $\mathbb{R}[X]$

z racine de $X^n - 1 \iff z^n = 1$

$\iff \bar{z}^n = 1$

$\iff \bar{z}$ racine de $X^n - 1$

1er cas : $n = 2p+1$



$$X^{2p+1} - 1 = \prod_{k=0}^{2p} X - \omega^k \qquad \text{où } \omega = e^{i\frac{2\pi}{2p+1}}$$

$$= (X-1) \prod_{k=1}^{p} (X-\omega^k) \prod_{k=p+1}^{2p} (X-\omega^k)$$

$k = 0$

$k' = 2p+1-k$

k' de 1 à p

$$= (X-1) \prod_{k=1}^{p} (X-\omega^k)(X-\omega^{2p+1-k})$$

$$= (X-1) \prod_{k=1}^{p} (X-\omega^k)(X-\omega^{-k})$$

car $\omega^{2p+1} = 1$

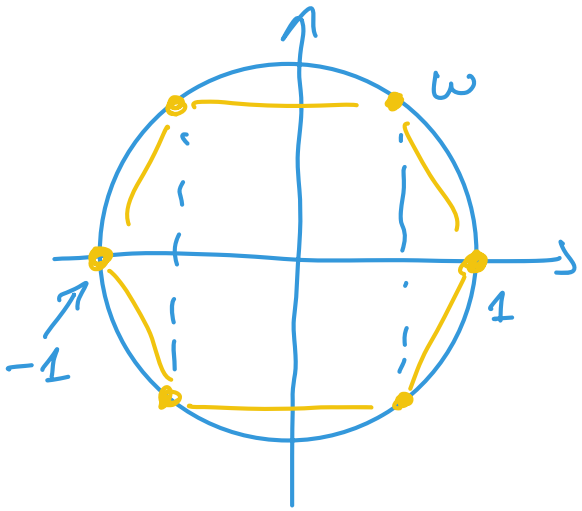
$$= (X-1) \prod_{k=1}^{p} (X-\omega^k)(X-\overline{\omega^k})$$

car $|\omega| = 1$

$$= (X-1) \prod_{k=1}^{p} (X^2 - 2\mathrm{Re}\,\omega^k + 1)$$

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

Cas où $n = 2p$



$$X^{2p} - 1 = \prod_{k=0}^{2p-1} (X-\omega^k) \qquad \omega = e^{i\frac{2\pi}{2p}} = e^{i\frac{\pi}{p}}$$

$$= (X-1)(X+1) \prod_{k=1}^{p-1} (X-\omega^k) \prod_{k=p+1}^{2p-1} (X-\omega^k)$$

↑ racine $k=0$ ↑ racine $k=p$

on pose $k' = 2p - k$ dans le second produit

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

130.6