Résumé de CM11

Conséquences de division euclidienne $\mathbb{K}$: un corps commutatif, e.g., $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ etc.

Définition On dit que un polynôme non nul B **divise** A, noté $B|A$, si le reste de la division euclidienne de A par B est nul, i.e., il existe un polynôme Q tel que $A = BQ$. □

Soit $(A, B) \in \mathbb{K}[X]^2 \backslash \{(0, 0\}$.
L'ensemble des multiples communs à A et B a un unique élément unitaire de degré minimal appelé le **plus petit commun multiple** (PPCM en bref) de A et B, noté $\text{ppcm}(A, B)$.
L'ensemble des diviseur commun de A et B a un unique élément unitaire de degré maximal appelé le **plus grand diviseur commun** (PGCD en bref) de A et B, noté $\text{pgcd}(A, B)$.

Théorème (PPCM) Soit $(A, B) \in \mathbb{K}[X]^2 \backslash \{(0, 0)\}$ et soit $M \in K[X]$ non nul tel que $A|M$ et $B|M$. Alors, $\text{ppcm}(A, B)$ divise M. □

Théorème (PGCD) Soit $(A, B) \in \mathbb{K}[X]^2 \backslash \{(0, 0)\}$ et soit $D \in \mathbb{K}[X]$ non nul tel que $D|A$ et $D|B$. Alors, D divise $\text{pgcd}(A, B)$. □

Théorème Soient $A, B \in \mathbb{K}[X]$ deux polynômes non nuls.
Alors, il existe un constant $\lambda \in \mathbb{K}^*$ tel que $AB = \lambda \cdot \text{ppcm}(A, B) \cdot \text{pgcd}(A, B)$. □

Comme pour les entiers, des divisions euclidiennes successives, nous permet de montrer

Théorème (Bézout) Soient A et B deux polynômes non nuls. Alors, A et B sont **premiers entre eux**, i.e., $\text{pgcd}(A, B) = 1$ si et seulement si il existe un pair $(U, V) \in \mathbb{K}[X]^2$ tel que $AU + BV = 1$ (**identité de Bézout**). □

Une application importante est le théorème suivant:

Théorème (**Lemme de Gauss**) Soient $A, B \in \mathbb{K}[X]$ deux polynômes qui sont premiers entre eux. Soit $C \in \mathbb{K}[X]$ non nul tel que A divise BC. Alors, A divise C. □

Définition Un polynôme $P \in \mathbb{K}[X]$ est dit **irréductible dans** $\mathbb{K}[X]$ s'il est non nul et ne peut pas s'écrire comme le produit de deux polynômes de degrés strictement inférieurs. □

Le lemme de Gauss est un clé pour montrer le théorème suivant:

Théorème Soit $P \in \mathbb{K}[X]$ non nul. Il existe une écriture de P sous la forme

$$P = \lambda \cdot P_1^{m_1} \cdot P_2^{m_2} \cdots P_s^{m_s}$$

où

1. $\lambda \in \mathbb{K}$ est une constante,
2. les polynômes P_i sont irréductibles dans $\mathbb{K}[X]$,
3. les polynômes P_i sont unitaires et non constants,
4. les exposants m_i sont des entiers naturels non nuls.

De plus, cette écriture est unique à la numérotation des P_i près. □

Un simple corollaire de ce théorème est suivant:

Théorème Soient $(A, B) \in \mathbb{K}[X]^2 \backslash \{(0,0)\}$. Soit $\lambda, \mu \in \mathbb{K}^*$ et soient $P_1, P_2, \cdots, P_s \in \mathbb{K}[X]$ irréductibles et unitaires 2 à 2 distincts tels qu'ils existent $m_1, m_2, \cdots, m_s$ et $n_1, n_2, \cdots, n_s \in \mathbb{N}$ tels que

$$A = \lambda P_1^{m_1} P_2^{m_2} \cdots P_s^{m_s}, \qquad B = \mu P_1^{n_1} P_2^{n_2} \cdots P_s^{n_s}.$$

Alors,

1. $\mathrm{ppcm}(A, B) = P_1^{\max(m_1,n_1)} P_2^{\max(m_2,n_2)} \cdots P_s^{\max(m_s,n_s)}$,
2. $\mathrm{pgcd}(A, B) = P_1^{\min(m_1,n_1)} P_2^{\min(m_2,n_2)} \cdots P_s^{\min(m_s,n_s)}$. □

Définition Soit $P \in \mathbb{K}[X]$ non nul et soient $A, B \in \mathbb{K}[X]$.
On dit que A et B sont **congrus modulo** P, noté $A \equiv B\,[P]$, si P divise $A - B$. □

Comme pour les entiers, cette relation «≡» est une **relation d'équivalence**.

Théorème Soit $P \in \mathbb{K}[X]$ non nul et soient $A, B, C, D \in \mathbb{K}[X]$ tels que $A \equiv B\,[P]$ et $C \equiv D\,[P]$. Alors,

1. $A + C \equiv B + D\,[P]$,
2. $AC \equiv BD\,[P]$. □

Théorème (**Théorème de reste chinois**) Soient $P_1, P_2 \in \mathbb{K}[X]$ deux polynômes qui sont premiers entre eux et soient $A_1, A_2 \in \mathbb{K}[X]$. Notons l'ensemble des solutions de l'équation sur S

$$S \equiv A_i\,[P_i] \quad (i = 1, 2)$$

par $\mathcal{S}$. Alors, il existe un unique $S_0 \in \mathbb{N}$ vérifiant

1. $\mathcal{S} = S_0 + P_1 P_2 \mathbb{K}[X]$,
2. $\deg(S_0) < \deg(P_1) + \deg(P_2)$. □.

On pourra montrer ces énoncés comme des énoncés analogues pour $\mathbb{Z}$. Celui qui joue le rôle de $|\cdot|$ pour $\mathbb{Z}$ est le degré $\deg(\cdot)$ pour $\mathbb{K}[X]$.

Racines d'un polynôme $\mathbb{K}$: un corps commutatif, e.g., $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ etc.

Théorème Soit $P \in \mathbb{K}[X]$ non nul et $\alpha \in \mathbb{K}$. Alors, les deux conditions suivantes sont équivalentes:

1. $P(\alpha) = 0$,
2. $X - \alpha$ divise P.

On dit alors que α est une **racine** de P. □

Preuve D'après la division euclidienne de P par $X - \alpha$, il existe un polynôme $Q \in \mathbb{K}[X]$ et un constant $R \in \mathbb{K}$ tels que

$$P(X) = (X - \alpha)Q(X) + R.$$

Évaluons X en α dans cette identité, on obtient $R = P(\alpha)$. □

Appliquant ce théorème plusieurs fois, on peut montrer le corollaire suivant:

Corollaire Soit $P \in \mathbb{K}[X]$ un polynôme non nul de degré d. Alors, P a au plus d racines. □

N.B. Si $\mathbb{K}$ n'est pas $\mathbb{C}$, une racine d'un polynôme P n'existe pas forcément dans $\mathbb{K}$.
Cependant, dans $\mathbb{C}$, d'après le théorème de D'Alembert-Gauss, il en existe toujours. □

La proposition suivante est une conséquence simple du théorème de D'Alembert-Gauss:

Proposition

1. Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
2. Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif. □

Pour le deuxième énoncé, notons que si un polynôme réel $P \in \mathbb{R}[X]$ admet une racine complexe α, alors son conjugé est aussi une racine de P, puisque $0 = \overline{P(\alpha)} = \overline{P}(\overline{\alpha}) = P(\overline{\alpha})$.

Définition Soit P un polynôme dans $\mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$.
On dit que α est une racine d'**ordre** (ou de la **multiplicité**) m si $(X - \alpha)^m | P$ et $(X - \alpha)^{m+1} \nmid P$. □

On note la dérivée k-ième de P par $P^{(k)}$. L'ordre d'une racine peut -être caractérisée en terme des polynômes dérivés:

Théorème Soit $P \in \mathbb{K}[X]$ un polynôme non constant et soit $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$.
Alors, les deux conditions suivantes sont équivalentes:

1. $(X - \alpha)^m$ divise P,
2. $P(\alpha) = P'(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0$. □

Ce théorème est montré essentiellement par la formule de Leibniz:

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

Remarque. Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n \in \mathbb{N}^*$. Alors, pour $\alpha \in \mathbb{K}$, on a

$$P(X) = P(\alpha) + \sum_{k=1}^{n} \frac{1}{k!} P^{(k)}(\alpha)(X-\alpha)^k \qquad \text{(Formule de Taylor)}.$$

C'est le « **développement limité** » du polynôme P. □

Interpolation de Lagrange* Fixons $n \in \mathbb{N}^*$, on considère un problème suivant:

Étant donné $(\alpha_0, \lambda_0), (\alpha_1, \lambda_1), \cdots, (\alpha_n, \lambda_n) \in \mathbb{K}^2$ avec les α_i's tous distincts, trouver un polynôme $P \in \mathbb{K}[X]$ de degré (au plus) n vérifiant $P(\alpha_i) = \lambda_i$ pour tout $0 \leqslant i \leqslant n$.

En terme de graphe d'une fonction polynomiale, c'est la même question de trouver une fonction polynomiale $f : \mathbb{K} \to \mathbb{K}$ dont le graphe Γ_f (une courbe de degré n) passe les points (α_i, λ_i) $(0 \leqslant i \leqslant n)$.

Pour cette question, on pose

$$Q(X) := \prod_{0 \leqslant i \leqslant n} (X - \alpha_i) \qquad \widetilde{Q}_i(X) := \frac{Q(X)}{X - \alpha_i} = (X-\alpha_0)\cdots(X-\alpha_{i-1})(X-\alpha_{i+1})\cdots(X-\alpha_n)$$

pour $0 \leqslant i \leqslant n$. Il est claire que, pour $0 \leqslant j \neq i \leqslant n$, on a $\widetilde{Q}_i(\alpha_j) = 0$, et

$$\widetilde{Q}_i(\alpha_i) = \prod_{0 \leqslant j \neq i \leqslant n} (\alpha_i - \alpha_j) = (\alpha_i - \alpha_0)\cdots(\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \cdot (\alpha_i - \alpha_n) \neq 0.$$

Donc, posons $Q_i(X) = \dfrac{\widetilde{Q}_i(X)}{\widetilde{Q}_i(\alpha_i)}$, on obtient

$$Q_i(\alpha_j) = \delta_{i,j} := \begin{cases} 1 & i = j, \\ 0 & i \neq j. \end{cases}.$$

Ce $\delta_{i,j}$ s'appelle le **delta de Kronecker**. À l'aide des polynôme $Q_i(X)$ $(0 \leqslant i \leqslant n)$, appelés les **polynômes interpolateurs de Lagrange**, on peut exprimer le polynôme P comme suit:

$$P(X) = \sum_{i=0}^{n} \lambda_i Q_i(X).$$

Alors, ce polynôme P, appelé le polynôme d'**interpolation de Lagrange**, vérifie

$$P(\alpha_i) = \lambda_i \qquad 0 \leqslant \forall\, i \ \leqslant n.$$