Résumé de CM10

Vocabulaires et Opérations sur Polynômes $\mathbb{K}$: un corps commutatif, e.g., $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ etc.

1. Vocabulaires:
   - Pour $a_i \in \mathbb{K}$ $(0 \leqslant i \leqslant n)$, une formule (ou expression)
   $$P(X) = a_0 + a_1 X + \cdots + a_n X^n$$
   où X est un indéterminée, est appelée un **polynôme**.
   - Pour un $\alpha \in \mathbb{K}$, on peut substituer X par α; on obtient un nombre $P(\alpha)$. L'application associée $\mathbb{K} \to \mathbb{K}; \alpha \longmapsto P(\alpha)$ sera notée P.
   - Le **degré** de P est le plus grand d tel que $a_d \neq 0$, noté $\deg(P)$. Pour le **polynôme nul** 0, le degré est $-\infty$, par convention.
   - Pour un polynôme P de degré d, le coefficient a_d de X^d est appelé le **coefficient dominant**.
   - Un polynôme est dit **unitaire** si son coefficient dominant vaut 1.
   - L'ensemble des polynômes à coefficients dans $\mathbb{K}$ sera noté $\mathbb{K}[X]$.
2. Opérations: $P(X) = a_0 + a_1 X + \cdots + a_p X^p, \quad a_k := 0 \text{ pour } k > p,$
   $Q(X) = b_0 + b_1 X + \cdots + b_q X^q, \quad b_k := 0 \text{ pour } k > q.$
   - La **somme** $P + Q$: le polynôme $c_0 + c_1 X + \cdots + c_{\max(p,q)} X^{\max(p,q)}$ où $c_k := a_k + b_k \quad \forall\, k \geqslant 0.$
   - Le **produit** PQ: le polynôme $c_0 + c_1 X + \cdots + c_{p+q} X^{p+q}$ où $c_k := \sum_{i+j=k} a_i b_j \quad \forall\, k \geqslant 0.$
   - Le **polynôme dérivé** P': le polynôme $a_1 + 2a_2 X + \cdots + p a_p X^{p-1}$.
   - Le **polynôme composé** $P \circ Q$: le polynôme
   $$(P \circ Q)(X) := P(Q(X)) = a_0 + a_1 Q(X) + \cdots + a_p Q(X)^p.$$
   - Le **conjugé** $\overline{P}$ (pour $P \in \mathbb{C}[X]$): le polynôme $\overline{P}(X) = \overline{a_0} + \overline{a_1} X + \cdots + \overline{a_p} X^p$. Pour un $\alpha \in \mathbb{C}$; $\overline{P(\alpha)} = \overline{P}(\overline{\alpha})$.

Lemme Pour $P, Q \in \mathbb{K}[X]$,

1. $\deg(PQ) = \deg(P) + \deg(Q)$,
2. $\deg(P + Q) \leqslant \max(\deg(P), \deg(Q))$,
3. $\deg(P') = \deg(P) - 1$,
4. $\deg(P \circ Q) = (\deg P)(\deg Q)$. □

Arithmétique sur $\mathbb{K}[X]$ $\mathbb{K}$: un corps commutatif, e.g., $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ etc.

L'ensemble $\mathbb{K}[X]$ muni de l'addition $+$ et la multiplication $\cdot$ vérifie les prorpriétés suivantes:

1. $(\mathbb{K}[X], +)$: groupe abélien, i.e.,
   i) $(P + Q) + R = P + (Q + R)$,
   ii) $P + 0 = 0 + P = P$ où $0 \in \mathbb{K}[X]$ est le polynôme nul,
   iii) pour $P \in \mathbb{K}[X]$, posons $-P = (-1) \cdot P$. Alors, $P + (-P) = (-P) + P = 0$.
   iv) $P + Q = Q + P$.
2. $(\mathbb{K}[X], \cdot)$: monoïde commutatif, i.e.,
   i) $(P \cdot Q) \cdot R = P \cdot (Q \cdot R)$,
   ii) $1 \cdot P = P \cdot 1 = P$,
   iii) $P \cdot Q = Q \cdot P$.
3. Distributivité: $P, Q, R \in \mathbb{K}[X]$,

$$(P + Q) \cdot R = P \cdot R + Q \cdot R, \qquad P \cdot (Q + R) = P \cdot R + Q \cdot R.$$

On dit que $(\mathbb{K}[X], +, \cdot)$ est un **anneau commutatif**. De plus, grâce aux résultat suivant, les propriétés suivantes sont montrés par une méthode très similaire comme pour $\mathbb{Z}$:

Théorème (Division Euclidienne).
Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]\backslash\{0\}$. Il existe un unique couple de polynômes $(Q, R) \in \mathbb{K}[X]^2$ tels que

1. $A = BQ + R$,
2. $R = 0$ ou $\deg(R) < \deg(B)$. □

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 uintaire 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 $AB = \lambda \text{ppcm}(A, B) \cdot \text{pgcd}(A, B)$. □

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

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. $\deg(S_0) < \deg(P_1) + \deg(P_2)$. $\square$.

Les structures en commun entre l'anneau des entiers $\mathbb{Z}$ et l'anneau des polynômes $\mathbb{K}[X]$ est appelé **anneau euclidienne**, ou plus généralement **anneau principal**. Les théorèmes mentionnés jusqu'ici pour $\mathbb{Z}$ et $\mathbb{K}[X]$ peuvent être montrés de façon complètement parallèle.