Compléments de CM

Arithmétique sur $\mathbb{Z}$

Définition Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^* := \mathbb{Z}\backslash\{0\}$. Lorsque il existe un entier $q \in \mathbb{Z}$ tel que $a = bq$, on dit que a est un **multiple** de b et que b est un **diviseur** de a. On la note par $b|a$. □

Un des théorèmes principal est

Théorème (Division Euclidienne).
Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Alors, il existe un unique paire $(q, r) \in \mathbb{Z}^2$ tel que

1. $a = bq + r$,
2. $0 \leqslant r < |b|$. □

Ce théorème est un clé pour montrer plusieurs propriétés qui l'on décrit ici.

Soit $(a, b) \in \mathbb{Z}^2\backslash\{(0, 0)\}$.
Alors, l'ensemble $\mathcal{M} := \{m \in \mathbb{N} \,|\, a|m \text{ et } b|m\}$ est non-vide car $ab \in \mathcal{M}$. Le plus petit élément de $\mathcal{M} \cap \mathbb{N}^*$ est appelé le **plus petit commun multiple** (PPCM en bref), noté $\text{ppcm}(a, b)$.
Pareillement, l'ensemble $\mathcal{D} := \{d \in \mathbb{N}^* \,|\, d|a \text{ et } d|b\}$ est non-vide car $1 \in \mathcal{D}$ et fini. Le plus grand élément de $\mathcal{D}$ est appelé le **plus grand diviseur commun** (PGCD en bref), noté $\text{pgcd}(a, b)$.

Théorème (PPCM) Soit $(a, b) \in \mathbb{Z}^2\backslash\{(0, 0)\}$ et soit $m \in \mathbb{Z}$ tel que $a|m$ et $b|m$.
Alors, $\text{ppcm}(a, b)$ divise m. □

Théorème (PGCD) Soit $(a, b) \in \mathbb{Z}^2\backslash\{(0, 0)\}$ et soit $d \in \mathbb{Z}$ tel que $d|a$ et $d|b$.
Alors, d divise $\text{pgcd}(a, b)$. □

Théorème Soient $a, b \in \mathbb{N}^*$. Alors, $ab = \text{ppcm}(a, b) \cdot \text{pgcd}(a, b)$. □

L'**algorithme d'Euclide**, i.e., des divisions euclidiennes successives, nous permet de montrer

Théorème (Bézout) Soit $a, b \in \mathbb{Z}^*$ deux entiers. Alors, a et b sont **premiers entre eux**, i.e., $\text{pgcd}(a, b) = 1$ si et seulement si il existe un pair $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$ (**identité de Bézout**). □

Corollaire Soient $a, b \in \mathbb{Z}^*$ et $d \in \mathbb{Z}^*$. Alors, l'équation $ax = by = d$ (**équation diophantienne**) admet une solution $(x, y) \in \mathbb{Z}^2$ si et seulement si $\text{pgcd}(a, b)$ divise d. □

Une application importante du Théorème de Bézout est le théorème suivant:

Théorème (**Lemme de Gauss**) Soient $a, b \in \mathbb{Z}^*$ deux entiers qui sont premiers entre eux. Soit $c \in \mathbb{Z}$ non nul tel que a divise bc. Alors, a divise c. □

Définition Un entier $p \in \mathbb{N}^*$ est dit un nombre **premier** si les seuls diviseurs positifs sont 1 et p. □

N.B. 1 n'est pas un nombre premier. □

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

Théorème (**Décomposition en facteurs premiers**) Soit $n \in \mathbb{N}$ supérieur à 2. Alors, il existe une unique écriture de n sous la forme $n = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$ où

1. les entiers $p_1, p_2, \cdots, p_s$ sont premiers,
2. les exposants $m_i \in \mathbb{N}^*$,
3. $p_1 < p_2 < \cdots < p_s$. □

Un simple corollaire de ce théorème est suivant:

Théorème Soient $a, b \in \mathbb{Z}^*$. Soient $p_1, p_2, \cdots, p_s$ nombres premiers 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 $a = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$, $b = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$. 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 $n \in \mathbb{N}^*$ et soient $a, b \in \mathbb{Z}$. On dit que a et b sont **congrus modulo** n, noté $a \equiv b\,[n]$, si n divise $a - b$. □

Cette relation «≡» vérifie les trois axiomes suivants:

1. (Réflexivité) $a \equiv a\,[n]$,
2. (Symétrie) $a \equiv b\,[n] \iff b \equiv a\,[n]$,
3. (Transitivité) $a \equiv b\,[n]$ et $b \equiv c\,[n]$ entraîne $a \equiv c\,[n]$.

On dit que cette relation «≡» est une **relation d'équivalence**.

Théorème Soit $n \in \mathbb{N}^*$ et soient $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b\,[n]$ et $c \equiv d\,[n]$. Alors,

1. $a + c \equiv b + d\,[n]$,
2. $ac \equiv bd\,[n]$. □

Théorème (**Théorème de reste chinois**) Soient $n_1, n_2 \in \mathbb{N}^*$ deux entiers qui sont premiers entre eux et soient $a_1, a_2 \in \mathbb{Z}$. Notons l'ensemble des solutions de l'équation sur $x \in \mathbb{Z}$

$$x \equiv a_i\ [n_i] \quad (i = 1, 2)$$

par $\mathcal{S}$. Alors, il existe un unique $k_0 \in \mathbb{N}$ vérifiant

1. $\mathcal{S} = k_0 + n_1 n_2 \mathbb{Z}$,
2. $0 \leqslant k_0 < n_1 n_2$. □.

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: $P(X) = a_0 + a_1 X + \cdots + a_p X^p, \quad a_k := 0$ pour $k > p$,
   $Q(X) = b_0 + b_1 X + \cdots + b_q X^q, \quad b_k := 0$ 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.

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

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.

D'ici, nous allons traiter les racines d'un polynôme.

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 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:

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