• **Objectif.** L'existence d'une division euclidienne dans $\mathbb{K}[X]$ permet d'y faire de l'arithmétique comme dans $\mathbb{Z}$. L'objectif de ce complément est de recenser rapidement les résultats d'arithmétique dans $\mathbb{K}[X]$.

1 PGCD et algorithme d'Euclide

Dans cette partie, A et B sont deux polynômes fixés de $\mathbb{K}[X]$ non tous deux nuls.

Définition 1

On appelle *un* PCGD de A et B tout diviseur commun à A et B *de degré maximal*.

• **Remarque.** La définition est légitime car A et B possèdent des diviseurs de degré maximal. En effet, l'ensemble des degrés des polynômes non nuls divisant A et B est une partie de $\mathbb{N}$ non vide (elle possède 0 car les polynômes constants non nuls divisent A et B) et majorée (par $\deg A$ si $A \neq 0$, $\deg B$ si $B \neq 0$). Cette partie possède ainsi un plus grand élément r et il existe donc des polynômes de degré r divisant A et B.

• **Remarque.** A et B possèdent une infinité de PGCD. En effet, si P est un PGCD de A et B, alors tous ses associés *i.e.* tous les λP avec $\lambda \in \mathbb{K}^*$ sont des PGCD de A et B. En revanche un seul PGCD est unitaire.

Algorithme d'Euclide

On définit une suite finie de polynômes (R_k) par récurrence :
- On définit R_{-1} et R_0 par : $R_{-1} = A$ et $R_0 = B$.
- Pour tout $k \in \mathbb{N}$, *tant que* $R_k \neq 0$, on définit R_{k+1} comme le reste de la division euclidienne de R_{k-1} par R_k.

• **« Pourquoi ça marche ? ».** L'algorithme d'Euclide fournit un PGCD de A et B, et ce pour les deux mêmes raisons que dans $\mathbb{Z}$:
  i) L'algorithme se termine : Si à l'étape k, $R_k \neq 0$, alors $\deg R_{k+1} < \deg R_k$. Ainsi il existe $n \in \mathbb{N}$ tel que $R_n \neq 0$ et $R_{n+1} = 0$.
  ii) L'algorithme fournit un PGCD : A l'étape n, R_n est un PGCD de A et B ceci pour la même raison que dans $\mathbb{Z}$: les diviseurs communs sont conservés à chaque étape. $A = R_{-1}$ et $B = R_0$ ont les mêmes diviseurs communs que R_0 et R_1, puis que R_1 et R_2, …, et enfin que R_n et $R_{n+1} = 0$ (et les diviseurs communs de R_n et 0 sont les diviseurs de R_n). R_n est donc un diviseur commun de A et B de degré maximal *i.e.* un PGCD de A et B.

• **Conséquences de l'algorithme d'Euclide.**
1. Tous les PGCD de A et B sont associés à R_n. En effet, si D est un PGCD de A et B, c'est un diviseur commun à A et B donc un diviseur de R_n : R_n s'écrit $R_n = QD$ pour un certain polynôme Q. De plus D et R_n sont de même degré (le degré maximal des diviseurs communs), donc $\deg Q = 0$ *i.e.* $Q \in \mathbb{K}^*$.
2. Puisque tous les PGCD sont associés, un seul est unitaire.

Théorème 1

- Il existe un unique PGCD unitaire de A et B, il est noté $A \wedge B$.
- *Relation de Bézout* : il existe U et $V \in \mathbb{K}[X]$ tels que $AU + BV = A \wedge B$.
- *PGCD et diviseurs communs :* les diviseurs communs à A et B sont les diviseurs de $A \wedge B$
- *Factorisation :* Pour tout $K \in \mathbb{K}[X]$: $(AK) \wedge (BK)$ et $K(A \wedge B)$ sont associés.

En pratique : PGCD et relation de Bézout avec l'algorithme d'Euclide

Exemple 1 — 1. Calculer $A \wedge B$ où $A = 6X^4 + 8X^3 - 7X^2 - 5X - 2$ et $B = 6X^3 - 4X^2 - X - 1$.
2. Trouver une relation de Bézout entre A et B.

2 Polynômes premiers entre eux

On considère deux polynômes $A, B \in \mathbb{K}[X]$.

Définition 2

On dit que A et B sont premiers entre eux si $A \wedge B = 1$, ou encore si leurs seuls diviseurs communs sont les polynômes constants non nuls.

Théorème 2 : Théorème de Bézout

Il y a équivalence entre : *i)* A et B sont premiers entre eux. *ii)* Il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$.

Théorème 3 : Lemme de Gauss

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

• **Conséquences.** Pour tous $A_1, \ldots, A_n, B_1, \ldots, B_n \in \mathbb{K}[X]$
- Si : $A \wedge B_1 = 1, \ldots, A \wedge B_n = 1$ alors : $A \wedge (B_1 \ldots B_n) = 1$
- Si $A_1, \ldots, A_n$ divisent C et sont premiers entre eux deux à deux alors leur produit $A_1 \ldots A_n$ divise C.

3 Extension du PGCD à un nombre fini de polynômes

Soient $A_1, A_2, \ldots A_n \in \mathbb{K}[X]$, non tous nuls.
- On définit comme dans $\mathbb{Z}$ par récurrence (à partir de l'associativité de $\wedge$) le polynôme $A_1 \wedge A_2 \wedge \cdots \wedge A_n$. Ce polynôme est appelé le PGCD de $A_1, A_2, \ldots A_n$ et ses diviseurs sont les diviseurs communs à $A_1, \ldots, A_n$.
- La *relation de Bézout* demeure valable : il existe $U_1, \ldots, u_n \in \mathbb{K}[X]$ tels que $\sum_{i=1}^{n} A_i U_i = A_1 \wedge A_2 \wedge \cdots \wedge A_n$.
- Lorsque $A_1 \wedge A_2 \wedge \cdots \wedge A_n = 1$, on dit que $A_1, A_2, \ldots, A_n$ sont premiers entre eux dans leur ensemble.

4 PPCM

Dans cette partie, A et B sont deux polynômes fixés de $\mathbb{K}[X]$ tous deux non nuls.

Définition 3

On appelle un PPCM de A et B tout multiple non nul commun à A et B de degré minimal.

• **Remarque.** La définition est légitime car A et B possèdent bien des multiples de degré minimal. En effet, l'ensemble des multiples communs à A et B possède des polynômes non nuls (AB par exemple). L'ensemble des degrés de ces multiples communs possède donc un plus petit élément q. Par suite il existe des polynômes de degré q multiples de A et B.

Théorème 4

1. Si M est un PPCM de A et B alors les multiples communs à A et B sont les multiples de M
2. *PPCM et multiples communs* Tous les PPCM de A et B sont associés, un seul est unitaire on le note $A \vee B$
3. *Factorisation :* Pour tout $K \in \mathbb{K}[X]$: $(AK) \vee (BK)$ et $K(A \vee B)$ sont associés.
4. *Lien PGCD-PPCM* Les polynômes $(A \wedge B) \times (A \vee B)$ et AB sont associés.

5 Polynômes irréductibles

Définition 4

Un polynôme P non constant est dit *irréductible dans* $\mathbb{K}[X]$ si ses seuls diviseurs sont 1 et P à une constante multiplicative non nulle près.

Exemple 2 — Tout polynôme de degré 1 est irréductible

En effet, soit $P \in \mathbb{K}[X]$, de degré 1 et A un diviseur de P. Montrons que A est constant ou associé à P.
Par hypothèse il existe $B \in \mathbb{K}[X]$ tel que : $P = AB$ donc : $1 = \deg P = \deg A + \deg B$.
Puisque A, B sont non nuls (car $P \neq 0$) on en déduit que A est de degé 0 ou 1 :
• Si $\deg A = 0$, alors A est une constante non nulle. • Si $\deg A = 1$, alors $\deg B = 0$ *i.e.* B est une constante non nulle λ et $A = \frac{1}{\lambda} P$.

Exemple 3 — Tout polynôme de $\mathbb{R}[X]$ de degré 2 à discriminant strictement négatif est irréductible dans $\mathbb{R}[X]$

En effet, soit $P \in \mathbb{R}[X]$ un tel polynôme. Supposons par l'absurde P réductible. Il posséderait alors un diviseur A de degré 1 *i.e.* de la forme $A = aX + b$ pour certains $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$. Dans ce cas $-\frac{b}{a}$ serait racine de A, donc de P ce qui est impossible car P n'a pas de racine réelle.

Théorème 5 : Lemme d'euclide

Soit $P \in \mathbb{K}[X]$ irréductible et soient $A, B \in \mathbb{K}[X]$. Si $P \mid AB$ alors : $P \mid A$ ou $P \mid B$.

Théorème 6

i) Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.
ii) Les polynômes irréductibles de $\mathbb{R}[X]$ sont :
• les polynômes de degré 1 • les polynômes de degré 2 à discriminant strictement négatif.

• **Demonstration du théorème.**

- *Irréductibles de* $\mathbb{C}[X]$. On sait déjà que tout polynôme de degré 1 est irréductible. Réciproquement, soit $P \in \mathbb{C}[X]$ irréductible. D'après le théorème de d'Alembert-Gauss, P possède une racine $\alpha \in \mathbb{C}$ donc $X - \alpha$ divise P. Puisque P est irréductible, P et $X - \alpha$ sont associés donc P est de degré 1.
- *Irréductibles de* $\mathbb{R}[X]$. On sait déjà que les polynômes mentionnés par le théorème sont irréductibles sur $\mathbb{R}[X]$.
  Réciproquement, soit $P \in \mathbb{R}[X]$ irréductible. D'après le théorème de d'Alembert-Gauss, P possède une racine $\alpha \in \mathbb{C}$:
  - Si $\alpha \in \mathbb{R}$ alors $X - \alpha \in \mathbb{R}[X]$ et divise P. Puisque P est irréductible, P et $X - \alpha$ sont associés donc P est de degré 1.
  - Si $\alpha \notin \mathbb{R}$ alors $\overline{\alpha}$ est aussi racine de P donc P est divisible par $A = (X - \alpha)(X - \overline{\alpha})$. Puisque P est irréductible, il existe $\lambda \in \mathbb{R}^*$ tel que $P = \lambda(X - \alpha)(X - \overline{\alpha})$ donc les racines de P sont α et $\overline{\alpha}$, non réelles : P est donc de degré 2 et à discriminant strictement négatif.

Théorème 7

Tout polynôme non nul de $\mathbb{K}[X]$ est le produit d'un élément de $\mathbb{K}^*$ et de polynômes unitaires irréductibles dans $\mathbb{K}[X]$; l'écriture est unique à l'ordre près des facteurs

• **Demonstration du théorème.**

- *Preuve dans* $\mathbb{C}[X]$. Soit $P \in \mathbb{C}[X]$ non constant. On sait déjà que tout polynôme non constant de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$. Puisque les polynômes de degré 1 sont irréductibles, ceci assure la partie existence de théorème. Concernant l'unicité, supposons que P est le produit d'un élément de $\mathbb{K}^*$ et de polynômes unitaires irréductibles dans $\mathbb{C}[X]$, d'après le théorème précédent cela signifie que : $P = \lambda(X - a_1)^{m_1} \dots (X - a_r)^{m_r}$ pour certains $a_1, \dots, a_r \in \mathbb{C}$ distincts et $m_1, \dots, m_r \in \mathbb{N}^*$. Par conséquent :
  - λ est nécessairement le coefficient dominant de P, donc il est déterminé de façon unique.
  - $a_1, \dots, a_r \in \mathbb{C}$ sont les racines de P et $m_1, \dots, m_r \in \mathbb{N}^*$ leurs ordres de multiplicités donc les facteurs $(X - a_1)^{m_1}, \dots (X - a_r)^{m_r}$ dont déterminés de façon unique (à l'ordre près).
- *Preuve dans* $\mathbb{R}[X]$. Soit $P \in \mathbb{R}[X]$ non constant. En écrivant la factorisation de P dans $\mathbb{C}[X]$ et en regroupant les racines non réelles de P par paires de conjugués on obtient une factorisation de P comme produit d'une constante non nulle et de facteurs de la forme $X - \lambda$ avec $\lambda \in \mathbb{R}$ ou $X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2$ avec $\alpha \in \mathbb{C} \setminus \mathbb{R}$; tous ces facteurs sont irréductibles (par théorème) et unitaires.
  Cette factorisation est en outre unique car, dans le cas contraire, on pourrait former plusieurs factorisations irréductibles de P dans $\mathbb{C}[X]$