Mathématiques

Chapitre B7
Polynômes

MPSI – Lycée Bellevue – Toulouse

Année 2024-2025

Chapitre B7. Polynômes

I. Définitions

Chapitre B7. Polynômes

Chapitre B7. Polynômes

Chapitre B7. Polynômes

Chapitre B7. Polynômes

$$\mathbb{K} = \mathbb{R} \quad \text{ou} \quad \mathbb{C}$$

Chapitre B7. Polynômes

Chapitre B7. Polynômes

Définition

X : indéterminée

Polynôme à coefficients dans $\mathbb{K}$:

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

$$= \sum_{k=0}^{n} a_k X^k$$

où $n \in \mathbb{N}$ et $a_0 \dots a_n \in \mathbb{K}$

Notation (parfois)

$$P = \sum_{k=0}^{+\infty} a_k X^k$$

À partir d'un certain rang les a_k sont tous nuls.

Notation (parfois)

$$P = \sum_{k=0}^{+\infty} a_k X^k = \sum_{k\in\mathbb{N}} a_k X^k$$

À partir d'un certain rang les a_k sont tous nuls.

Notation (parfois)

$$P = \sum_{k=0}^{+\infty} a_k X^k = \sum_{k\in\mathbb{N}} a_k X^k = \sum_k a_k X^k$$

À partir d'un certain rang les a_k sont tous nuls.

Proposition

Si $P = \sum_k a_k X^k$ et $Q = \sum_k b_k X^k$ alors :

$$P = Q \iff \forall k \in \mathbb{N} \quad a_k = b_k$$

Notation

$\mathbb{K}[X]$: ensemble des polynômes à coefficients dans $\mathbb{K}$

Définitions (Opérations usuelles)

Soit $P = \sum_k a_k X^k$ et $Q = \sum_k b_k X^k$

- Addition : $P + Q = \sum_k (a_k + b_k) X^k$

Définitions (Opérations usuelles)

Soit $P = \sum_k a_k X^k$ et $Q = \sum_k b_k X^k$

- Addition : $P + Q = \sum_k (a_k + b_k) X^k$
- Multiplication : $PQ =$

Définitions (Opérations usuelles)

Soit $P = \sum_k a_k X^k$ et $Q = \sum_k b_k X^k$

- Addition : $P + Q = \sum_k (a_k + b_k) X^k$
- Multiplication : $PQ = \sum_k c_k X^k$ avec

$$\forall k \in \mathbb{N} \qquad c_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i}$$

Définitions (Opérations usuelles)

Soit $P = \sum_k a_k X^k$ et $Q = \sum_k b_k X^k$

- Addition : $P + Q = \sum_k (a_k + b_k) X^k$
- Multiplication : $PQ = \sum_k c_k X^k$ avec

$$\forall k \in \mathbb{N} \qquad c_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i}$$

- Multiplication par un scalaire : $\lambda P = \sum_k (\lambda a_k) X^k$

Définitions (Opérations usuelles)

Soit $P = \sum_k a_k X^k$ et $Q = \sum_k b_k X^k$

- Addition : $P + Q = \sum_k (a_k + b_k) X^k$
- Multiplication : $PQ = \sum_k c_k X^k$ avec

$$\forall k \in \mathbb{N} \qquad c_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i}$$

- Multiplication par un scalaire : $\lambda P = \sum_k (\lambda a_k) X^k$
- Composition : $P \circ Q = P(Q(X))$

Définitions

- Polynôme constant :

$$P = a_0$$

Dans ce cas $P \in \mathbb{K}$. On en déduit :

$$\mathbb{K} \subseteq \mathbb{K}[X]$$

- Polynôme nul :

$$P = 0 = 0_{\mathbb{K}[X]}$$

Proposition

$(\mathbb{K}[X], +, \times)$ est un anneau.

Proposition

$(\mathbb{K}[X], +, \times)$ est un anneau.

L'élément nul est $0_{\mathbb{K}[X]}$.

Si $P = \sum_k a_k X^k$ alors $-P = \sum_k (-a_k) X^k$.

L'élément unité est 1.

Les éléments inversibles sont les polynôme constants non-nuls : $\mathbb{K}[X]^* = \mathbb{K}^*$.

I. Définitions

Définitions

$$P = \sum_k a_k X^k \neq 0$$

$$\deg P = \mathrm{Max}\left\{k \in \mathbb{N} \mid \ a_k \neq 0\right\}$$

Définitions

$$P = \sum_k a_k X^k \neq 0$$

$$\deg P = \mathrm{Max}\left\{k \in \mathbb{N} \mid \ a_k \neq 0\right\}$$

Si $n = \deg P$ alors $P = \sum_{k=0}^{n} a_k X^k$ avec $a_n \neq 0$

Définitions

$$P = \sum_k a_k X^k \neq 0$$

$$\deg P = \mathrm{Max}\left\{k \in \mathbb{N} \mid \ a_k \neq 0\right\}$$

Si $n = \deg P$ alors $P = \sum_{k=0}^{n} a_k X^k$ avec $a_n \neq 0$

a_n : coefficient dominant de P

Définitions

$$P = \sum_k a_k X^k \neq 0$$

$$\deg P = \mathrm{Max}\left\{k \in \mathbb{N} \mid \ a_k \neq 0\right\}$$

Si $n = \deg P$ alors $P = \sum_{k=0}^{n} a_k X^k$ avec $a_n \neq 0$

a_n : coefficient dominant de P

Si $a_n = 1$ alors P est unitaire.

Convention

$$\deg 0 = -\infty$$

Notation

$\mathbb{K}_n[X]$: ensemble des polynômes
à coefficients dans $\mathbb{K}$
de degré **inférieur ou égal** à n

$$\mathbb{K}_n[X] = \{ P \in \mathbb{K}[X] \mid \deg P \leqslant n \}$$

Exemples

(i) $\mathbb{K}_2[X] =$

Exemples

(i) $\mathbb{K}_2[X] = \{aX^2 + bX + c \mid (a, b, c) \in \mathbb{K}^3\}$

(ii) $\mathbb{K}_0[X] =$

Exemples

(i) $\mathbb{K}_2[X] = \{aX^2 + bX + c \mid (a, b, c) \in \mathbb{K}^3\}$

(ii) $\mathbb{K}_0[X] = \mathbb{K}$

(iii) Si $n \leqslant m$ alors

Exemples

(i) $\mathbb{K}_2[X] = \{aX^2 + bX + c \mid (a,b,c) \in \mathbb{K}^3\}$

(ii) $\mathbb{K}_0[X] = \mathbb{K}$

(iii) Si $n \leqslant m$ alors $\mathbb{K}_n[X] \subseteq \mathbb{K}_m[X]$

Proposition

Soit P et Q deux polynômes. Alors

$$\deg(P+Q)$$

$$\deg(PQ)$$

Proposition

Soit P et Q deux polynômes. Alors

$$\deg(P+Q) \leqslant \operatorname{Max}(\deg P, \deg Q)$$

$$\deg(PQ)$$

Proposition

Soit P et Q deux polynômes. Alors

$$\deg(P+Q) \leqslant \operatorname{Max}(\deg P, \deg Q)$$

$$\deg(PQ) = \deg P + \deg Q$$

Proposition

Soit P et Q deux polynômes. Alors

$$\deg(P+Q) \leqslant \operatorname{Max}(\deg P, \deg Q)$$

$$\deg(PQ) = \deg P + \deg Q$$

Remarque

Cette propriété est valable si l'un des polynômes est nul.

Démonstration.

Si $P = 0$ ou $Q = 0$ alors la propriété est valide :

$$\begin{aligned} & \deg(P+Q) \leqslant \operatorname{Max}(\deg P, \deg Q) \\ \iff & \deg Q \leqslant \deg Q \\ & \text{ou } \deg P \leqslant \deg P \end{aligned}$$

Démonstration.

Si $P = 0$ ou $Q = 0$ alors la propriété est valide :

$$\begin{aligned} & \deg(P+Q) \leqslant \operatorname{Max}(\deg P, \deg Q) \\ \iff & \deg Q \leqslant \deg Q \\ & \text{ou } \deg P \leqslant \deg P \end{aligned}$$

$$\begin{aligned} & \deg(PQ) = \deg P + \deg Q \\ \iff & -\infty = -\infty \end{aligned}$$

Suite de la démonstration.

On suppose que P et Q sont non-nuls.

Soit $n = \deg P$ et $m = \deg Q$ avec $n \geqslant m$.

$$P = \sum_{k=0}^{n} a_k X^k \qquad \text{et} \qquad Q = \sum_{k=0}^{n} b_k X^k$$

Si $m < n$ **alors** $b_{m+1} = b_{m+2} = \cdots = b_n = 0$

$$P + Q = \sum_{k=0}^{n} (a_k + b_k) X^k$$

Donc $\deg(P + Q) \leqslant n$.

Suite de la démonstration.

$$P+Q=\sum_{k=0}^{n}(a_k+b_k)X^k$$

De plus :

- Si $m<n$ alors $a_n+b_n=a_n\neq 0$ donc $\deg(P+Q)=n$.
- Si $m=n$ alors $\deg(P+Q)\leqslant n$.

Suite de la démonstration.

$$PQ = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k$$

Suite de la démonstration.

$$PQ = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k$$

$$a_i b_{k-i} \neq 0 \implies a_i \neq 0 \quad \text{et} \quad b_{k-i} \neq 0$$

$$\implies i \leqslant n \quad \text{et} \quad k - i \leqslant m$$

$$\implies k \leqslant m + n$$

Suite de la démonstration.

$$PQ = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k$$

$$a_i b_{k-i} \neq 0 \implies a_i \neq 0 \quad \text{et} \quad b_{k-i} \neq 0$$

$$\implies i \leqslant n \quad \text{et} \quad k - i \leqslant m$$

$$\implies k \leqslant m + n$$

Donc $\deg(PQ) \leqslant m + n$.

Suite de la démonstration.

$$PQ = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k$$

Si $k = m + n$ alors

$$\sum_{i=0}^{k} a_i b_{k-i} = a_n b_m \neq 0$$

Donc $\deg(PQ) = m + n = \deg P + \deg Q$. $\square$

Proposition

Pour tous polynômes P et Q :

$$PQ = 0 \quad \Longrightarrow \quad P = 0 \quad \text{ou} \quad Q = 0$$

Proposition

Pour tous polynômes P et Q :

$$PQ = 0 \quad \Longrightarrow \quad P = 0 \quad \text{ou} \quad Q = 0$$

Démonstration. Contraposée :

$$P \neq 0 \quad \text{et} \quad Q \neq 0 \quad \Longrightarrow \quad PQ \neq 0$$

Proposition

Pour tous polynômes P et Q :

$$PQ = 0 \quad \Longrightarrow \quad P = 0 \quad \text{ou} \quad Q = 0$$

Démonstration. Contraposée :

$$\begin{cases} P \neq 0 \\ Q \neq 0 \end{cases} \Longrightarrow \begin{cases} \deg P \geqslant 0 \\ \deg Q \geqslant 0 \end{cases}$$

$$\Longrightarrow \quad \deg(PQ) = \deg P + \deg Q \geqslant 0$$

$$\Longrightarrow \quad PQ \neq 0$$

□

Définition

$P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$

Si $P = \sum_{k=0}^{n} a_k X^k$ alors $P(\alpha) = \sum_{k=0}^{n} a_k \alpha^k$

$P(\alpha)$ est la spécialisation de P en α.

Remarque

$$P = P(X) \in \mathbb{K}[X]$$

$$P(\alpha) \in \mathbb{K}$$

Proposition

La spécialisation est compatible avec l'addition, la multiplication par un scalaire et la multiplication.

$$\forall (P,Q) \in \mathbb{K}[X]^2 \quad \forall \lambda \in \mathbb{K}$$

$$\begin{aligned} (P+Q)(\alpha) &= P(\alpha)+Q(\alpha) \\ (\lambda P)(\alpha) &= \lambda\, P(\alpha) \\ (PQ)(\alpha) &= P(\alpha)Q(\alpha) \end{aligned}$$

Définition

Polynôme : $P \in \mathbb{K}[X]$

Fonction polynomiale : $\mathbb{K} \longrightarrow \mathbb{K}$

$x \longmapsto P(x)$

Définition

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

Fonction polynomiale : $\mathbb{K} \longrightarrow \mathbb{K}$

$$x \longmapsto P(x) = \sum_{k=0}^{n} a_k x^k$$

Définition

B divise A ou A est un multiple de B s'il existe un polynôme C tel que $A = BC$.

Notation

B divise A : $B \mid A$

Exemple 1

(i) $X-4$ divise X^2-3X-4

Exemple 1

(i) $X-4$ divise X^2-3X-4

(ii) $\forall n \in \mathbb{N}$ $X-2$ divise X^n-2^n

Exemple 1

(i) $X-4$ divise X^2-3X-4

(ii) $\forall n \in \mathbb{N}$ $X-2$ divise X^n-2^n

(iii) X^2 divise $5X^6+7X^5-3X^3+2X^2$

Exemple 1

(i) $X-4$ divise X^2-3X-4

(ii) $\forall n \in \mathbb{N}$ $X-2$ divise X^n-2^n

(iii) X^2 divise $5X^6+7X^5-3X^3+2X^2$

(iv) $2X-3$ divise $X-\frac{3}{2}$

Exemple 1

(i) $X-4$ divise X^2-3X-4

(ii) $\forall n \in \mathbb{N}$ $X-2$ divise X^n-2^n

(iii) X^2 divise $5X^6+7X^5-3X^3+2X^2$

(iv) $2X-3$ divise $X-\frac{3}{2}$

(v) X^3-3X^2+6X+7 ne divise pas $2X^2-X+10$

Exemple 1

(i) $X-4$ divise X^2-3X-4

(ii) $\forall n \in \mathbb{N}$ $X-2$ divise X^n-2^n

(iii) X^2 divise $5X^6+7X^5-3X^3+2X^2$

(iv) $2X-3$ divise $X-\frac{3}{2}$

(v) X^3-3X^2+6X+7 ne divise pas $2X^2-X+10$

Remarque

Si B divise A et A est non-nul alors $\deg B \leqslant \deg A$.

Remarque

Si B divise A et A est non-nul alors $\deg B \leqslant \deg A$.

Démonstration.

Remarque

Si B divise A et A est non-nul alors $\deg B \leqslant \deg A$.

Démonstration.

□

Propositions

(i) Si B divise A et A' alors B divise $(A + A')$.

(ii) Si C divise B et B divise A alors C divise A.

(iii) Le polynôme nul est multiple de tous les polynômes

Le polynôme unité divise tous les polynômes.

Propositions

(i) $\forall (A, A', B) \in \mathbb{K}[X]^3$

$$B \mid A \quad \text{et} \quad B \mid A' \implies B \mid (A + A')$$

(ii) $\forall (A, B, C) \in \mathbb{K}[X]^3$

$$C \mid B \quad \text{et} \quad B \mid A \implies C \mid A$$

(iii) $\forall\ A \in \mathbb{K}[X]$ $\qquad A \mid 0 \quad \text{et} \quad 1 \mid A$

Remarques

(i) $P \in \mathbb{K}[X]$ $\lambda \in \mathbb{K}^*$:

$$P \mid \lambda P \quad \text{et} \quad \lambda P \mid P$$

Remarques

(i) $P \in \mathbb{K}[X] \qquad \lambda \in \mathbb{K}^* :$

$$P \mid \lambda P \qquad \text{et} \qquad \lambda P \mid P$$

(ii) La relation de divisibilité n'est pas une relation d'ordre sur $\mathbb{K}[X]$.

Remarques

(i) $P \in \mathbb{K}[X] \qquad \lambda \in \mathbb{K}^* :$

$$P \mid \lambda P \qquad \text{et} \qquad \lambda P \mid P$$

(ii) La relation de divisibilité n'est pas une relation d'ordre sur $\mathbb{K}[X]$.
Elle est réflexive, transitive, mais pas antisymétrique.

Remarques

(i) $P \in \mathbb{K}[X]$ $\quad$ $\lambda \in \mathbb{K}^*$:

$$P \mid \lambda P \quad \text{et} \quad \lambda P \mid P$$

(ii) La relation de divisibilité n'est pas une relation d'ordre sur $\mathbb{K}[X]$.
Elle est réflexive, transitive, mais pas antisymétrique.

$$X^2+3 \mid 2X^2+6 \quad \text{et} \quad 2X^2+6 \mid X^2+3$$

alors que $X^2+3 \neq 2X^2+6$

Définition

P et Q sont associés si :

$$P \mid Q \qquad \text{et} \qquad Q \mid P$$

Définition

P et Q sont associés si :

$$P \mid Q \qquad \text{et} \qquad Q \mid P$$

Proposition

P et Q sont associés si et seulement si :

$$\exists \lambda \in \mathbb{K}^* \qquad Q = \lambda P$$

Définition

P et Q sont associés si :

$$P \mid Q \qquad \text{et} \qquad Q \mid P$$

Proposition

P et Q sont associés si et seulement si :

$$\exists \lambda \in \mathbb{K}^* \qquad Q = \lambda P$$

Démonstration.

Définition

P et Q sont associés si :

$$P \mid Q \qquad \text{et} \qquad Q \mid P$$

Proposition

P et Q sont associés si et seulement si :

$$\exists \lambda \in \mathbb{K}^* \qquad Q = \lambda P$$

Démonstration.

□

Théorème - Division euclidienne dans $\mathbb{K}[X]$

A, B polynômes avec $B \neq 0$

Il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que

- $A = BQ + R$
- $\deg R < \deg B$.

Q : quotient de la division euclidienne de A par B

R : reste de la division euclidienne de A par B.

Démonstration de l'existence.

Soit $p = \deg B$. Alors $p \in \mathbb{N}$.

$\mathcal{P}_n$: Pour tout polynôme A de degré n il existe un couple (Q, R) de polynômes tels que $A = BQ + R$ et $\deg R < \deg B$.

On démontre par récurrence forte que $\mathcal{P}_n$ est vraie pour tout $n \in \{-\infty\} \cup \mathbb{N}$.

Suite de la démonstration de l'existence.

$\mathcal{P}_n$ **: Pour tout polynôme** A **de degré** n **il existe un couple** (Q, R) **de polynômes tels que** $A = BQ + R$ **et** $\deg R < \deg B$**.**

Initialisation. La propriété $\mathcal{P}_{-\infty}$ est vraie : Si $A = 0$ alors $A = B0 + 0$ et $\deg 0 < \deg B$.

Suite de la démonstration de l'existence.

$\mathcal{P}_n$: Pour tout polynôme A de degré n il existe un couple (Q, R) de polynômes tels que $A = BQ + R$ et $\deg R < \deg B$.

Hérédité. Supposons $\mathcal{P}_{-\infty}$, $\mathcal{P}_0$, $\mathcal{P}_1 \dots \mathcal{P}_{n-1}$ vraies.

$$A = \sum_{k=0}^{n} a_k X^k \qquad B = \sum_{k=0}^{p} b_k X^k$$

Si $n < p$: $A = B0 + A$ et $\deg A < \deg B$.

Suite de la démonstration de l'existence.

Si $n \geqslant p$ on pose $Q_1 = \frac{a_n}{b_p} X^{n-p}$. Alors :

$$\begin{aligned} Q_1 B &= a_n X^n + \frac{a_n}{b_p} b_{p-1} X^{n-1} + \cdots \\ A &= a_n X^n + a_{n-1} X^{n-1} + \cdots \end{aligned}$$

Suite de la démonstration de l'existence.

Si $n \geqslant p$ on pose $Q_1 = \frac{a_n}{b_p} X^{n-p}$. Alors :

$$\begin{aligned} Q_1 B &= a_n X^n + \frac{a_n}{b_p} b_{p-1} X^{n-1} + \cdots \\ A &= a_n X^n + a_{n-1} X^{n-1} + \cdots \end{aligned}$$

$\deg(A - Q_1 B) = m < n$ donc d'après $\mathcal{P}_m$:

$\exists (Q_2, R)$ tel que $A - Q_1 B = Q_2 B + R$

et $\deg R < \deg B$

Suite de la démonstration de l'existence.

Si $n \geqslant p$ on pose $Q_1 = \frac{a_n}{b_p} X^{n-p}$. Alors :

$$\begin{aligned} Q_1 B &= a_n X^n + \frac{a_n}{b_p} b_{p-1} X^{n-1} + \cdots \\ A &= a_n X^n + a_{n-1} X^{n-1} + \cdots \end{aligned}$$

$\deg(A - Q_1 B) = m < n$ donc d'après $\mathcal{P}_m$:

$\exists (Q_2, R)$ tel que $A - Q_1 B = Q_2 B + R$

et $\deg R < \deg B$

$$A = B(Q_1 + Q_2) + R \qquad \text{et} \qquad \deg R < \deg B$$

$\mathcal{P}_n$ est démontrée.

Suite de la démonstration de l'existence.

$\mathcal{P}_n$ **: Pour tout polynôme** A **de degré** n **il existe un couple** (Q, R) **de polynômes tels que** $A = BQ + R$ **et** $\deg R < \deg B$**.**

Conclusion. Par récurrence forte la propriété $\mathcal{P}_n$ est vraie pour tout $n \in \mathbb{N} \cup \{-\infty\}$.

Démonstration de l'unicité.

Démonstration de l'unicité.

□

Méthode

On pose la division comme pour les entiers.

Exemple 2

Calcul de la division euclidienne de A par B où :

(i) $A = X^5 - X^4 - X^3 + 8X^2 - 2$

$B = X^2 - X + 2$

(ii) $A = 2X^5 + 3X^4 - 4X^3 - X^2 + 4X + 1$

$B = X^3 + 2X^2 - 1$

▷ Exercice 1.

Calculer la division euclidienne de A par B avec :

a. $A = X^3 + 3X^2 + X - 3$ $\qquad$ $B = X + 5$

b. $A = 2X^4 + 4X^3 - 5X + 1$ $\qquad$ $B = 2X^2 + 1$

c. $A = 3X^2 + 6X + 5$ $\qquad$ $B = iX + 1 + i$

Représentation informatique

$$P = 3 + 4X - X^3$$

```
P = [3, 4, 0,-1]
```

Représentation informatique

$$P = 3 + 4X - X^3$$

```
P = [3, 4, 0,-1, 0, 0]
```

Indéterminée

$$P = X$$

```
P = [0, 1]
```

Multiplication par un scalaire

$$P = 3 + 4X - X^3$$

$$3P = 9 + 12X - 3X^3$$

```
P = [3, 4, 0,-1]
multS(3,P) = [9,12, 0,-3]
```

Addition

$$P = 3 + 4X - X^3$$

$$Q = 1 - 2X + 5X^2$$

$$P + Q =$$

```
P = [3, 4, 0,-1]
Q = [1,-2, 5]
somme(P,Q) =
```

Addition

$$P = 3 + 4X - X^3$$

$$Q = 1 - 2X + 5X^2$$

$$P + Q = 4 + 2X + 5X^2 - X^3$$

```
P = [3, 4, 0,-1]
Q = [1,-2, 5]
somme(P,Q) = [4, 2, 5,-1]
```

Multiplication

$$P = 3 + 4X - X^3$$

$$Q = 1 - 2X + 5X^2$$

$$PQ =$$

```
P = [3, 4, 0,-1]
```

```
produit(P,Q) =
```

Multiplication

$$P = 3 + 4X - X^3$$

$$Q = 1 - 2X + 5X^2$$

$$PQ =$$

```
P = [3, 4, 0,-1]
```

$$XP =$$ `[0, 3, 4, 0,-1]`

$$X^2P =$$ `[0, 0, 3, 4, 0,-1]`

`produit(P,Q) =`

Multiplication

$$P = 3 + 4X - X^3$$

$$Q = 1 - 2X + 5X^2$$

$$PQ =$$

```
P = [3, 4, 0,-1]
```

$$-2XP = [0,-6,-8, 0, 2]$$

$$5X^2P = [0, 0,15,20, 0,-5]$$

```
produit(P,Q) =
```

Multiplication

$$P = 3 + 4X - X^3$$

$$Q = 1 - 2X + 5X^2$$

$$PQ = 3 - 2X + 7X^2 + 19X^3 + 2X^4 - 5X^5$$

`P = [3, 4, 0,-1]`

`-2XP = [0,-6,-8, 0, 2]`

`5X^2P = [0, 0,15,20, 0,-5]`

`produit(P,Q) = [3,-2, 7,19, 2,-5]`

Fonctions à définir

- Degré
- Produit d'un polynôme par un scalaire
- Somme, produit de deux polynômes
- Spécialisation d'un polynôme en un scalaire
- Division euclidienne
- PGCD de deux polynômes
- etc.

Degré

```
def deg(P):
    """Calcul du degré de P.
       Renvoie -1 si P est nul."""
    n=len(P)-1
    while n>=0 and P[n]==0:
        n=n-1
    return n
```

Somme

```
def Somme(P,Q):
    """Renvoie la somme P+Q"""
    m,n=deg(P),deg(Q)
    S=[0]*max(m,n)
    for k in range(m):
        S[k]=S[k]+P[k]
    for k in range(n):
        S[k]=S[k]+Q[k]
    return S
```

Produit

```
def Produit(P,Q):
    """Renvoie le produit PQ"""
    m,n=deg(P),deg(Q)
    R=[0]*(m+n)
    for k in range(m+n):
        for i in range(m):
            if k-n<=i<=k:
                R[k]=R[k]+P[i]*Q[k-i]
    return R
```

Spécialisation

```
def Specialisation(P,a):
    """Calcule P(a)"""
    y=0
    for k in range(len(P)):
        y=y+P[k]*a**k
    return y
```

Spécialisation

Remarque

Algorithme de Hörner :

$$P(x) = (\cdots((a_n x + a_{n-1})x + a_{n-2})x + \cdots + a_0)$$

Spécialisation

Remarque

Algorithme de Hörner :

$$P(x) = (\cdots((a_n x + a_{n-1})x + a_{n-2})x + \cdots + a_0)$$

▷ Exercice 2.

a. Programmer l'algorithme de Hörner en Python.

b. Compter le nombre d'opérations nécessaires pour spécialiser un polynôme de degré n avec cet algorithme, puis avec l'algorithme naïf. Comparer ces deux méthodes.

Chapitre B7. Polynômes

II. **Dérivation**

A. Dérivée formelle

B. Dérivées k-èmes

Définition

$$P = \sum_{k=0}^{n} a_k X^k$$

Polynôme dérivé de P :

$$P' = \sum_{k=1}^{n} a_k k X^{k-1}$$

Définition

$$P = \sum_{k=0}^{n} a_k X^k$$

Polynôme dérivé de P :

$$P' = \sum_{j=0}^{n-1} a_{j+1}(j+1)X^j$$

Remarque

Si f est la fonction polynomiale de polynôme P alors

f' est la fonction polynomiale de polynôme P'.

En conséquence les propriétés calculatoires des dérivées sont toujours vraies.

Proposition

Pour tous polynômes P et Q et tout scalaire λ

- $(P+Q)' = P' + Q'$
- $(\lambda P)' = \lambda P'$
- $(PQ)' = P'Q + PQ'$
- $P' = Q' \iff \exists k \in \mathbb{K} \quad P = Q + k$

Proposition

Pour tous polynômes P et Q et tout scalaire λ

- $(P+Q)' = P' + Q'$
- $(\lambda P)' = \lambda P'$
- $(PQ)' = P'Q + PQ'$
- $P' = Q' \iff \exists k \in \mathbb{K} \quad P = Q + k$

Remarque

On peut démontrer directement ces propriétés.

Autre démonstration.

$$\begin{aligned}(P+Q)' &= \left(\sum_k (a_k + b_k)X^k\right)' \\ &= \sum_k (a_k + b_k)kX^{k-1} \\ &= \sum_k a_k k X^{k-1} + \sum_k b_k k X^{k-1} \\ &= P' + Q'\end{aligned}$$

Autre démonstration.

$$\begin{aligned}(\lambda P)' &= \left(\sum_k \lambda a_k X^k\right)' \\ &= \sum_k \lambda a_k k X^{k-1} \\ &= \lambda \sum_k a_k k X^{k-1} \\ &= \lambda P'\end{aligned}$$

Autre démonstration.

$$\begin{aligned}(X^m X^n)' &= (X^{m+n})' \\ &= (m+n)X^{m+n-1}\end{aligned}$$

$$\begin{aligned}(X^m)'X^n + X^m(X^n)' &= mX^{m-1}X^n + X^m nX^{n-1} \\ &= (m+n)X^{m+n-1}\end{aligned}$$

Par linéarité de la dérivation $(PQ)' = P'Q + PQ'$.

Autre démonstration.

$$P' = Q' \iff \sum_{k=1}^{+\infty} a_k k X^{k-1} = \sum_{k=1}^{+\infty} b_k k X^{k-1}$$

$$\iff \forall k \geqslant 1 \quad a_k = b_k$$

$$P = a_0 + \sum_{k=1}^{+\infty} a_k X^k \qquad Q = b_0 + \sum_{k=1}^{+\infty} a_k X^k$$

Proposition

Pour tout polynôme P non constant :

$$\deg(P') = \deg(P) - 1$$

II. **Dérivation**

A. Dérivée formelle

B. Dérivées k-èmes

Proposition

$P = X^n$

$\forall k \in \mathbb{N} \qquad P^{(k)} =$

Proposition

$$P = X^n$$

$$\forall k \in \mathbb{N} \qquad P^{(k)} = \begin{cases} \dfrac{n!}{(n-k)!} X^{n-k} & \text{si } 0 \leqslant k \leqslant n \\ 0 & \text{si } k > n \end{cases}$$

Proposition

$$P = X^n$$

$$\forall k \in \mathbb{N} \qquad P^{(k)} = \begin{cases} \dfrac{n!}{(n-k)!} X^{n-k} & \text{si } \ 0 \leqslant k \leqslant n \\ 0 & \text{si } \ k > n \end{cases}$$

Démonstration.

On commence par démontrer par récurrence finie sur k que cette propriété est vraie pour tout $k \in \{0, \ldots, n\}$.

Proposition

$P = X^n$

$$\forall k \in \mathbb{N} \qquad P^{(k)} = \begin{cases} \dfrac{n!}{(n-k)!} X^{n-k} & \text{si } \ 0 \leqslant k \leqslant n \\ 0 & \text{si } \ k > n \end{cases}$$

Démonstration.

$k = n$: $P^{(n)} = n!$

$k = n+1$: $P^{(n+1)} = 0$

$k > n$: $P^{(k)} = 0$ $\square$

Exemple

Dérivés successifs du produit AB

$$\begin{aligned} AB &= AB \\ (AB)' &= A'B + AB' \\ (AB)'' &= \\ (AB)''' &= \end{aligned}$$

Exemple

Dérivés successifs du produit AB

$$\begin{aligned}
AB &= AB \\
(AB)' &= A'B + AB' \\
(AB)'' &= A''B + 2A'B' + AB'' \\
(AB)''' &= A'''B + 3A''B' + 3A'B'' + AB'''
\end{aligned}$$

Exemple

Dérivés successifs du produit AB

$$(AB)^{(0)} = A^{(0)}B^{(0)}$$

$$(AB)^{(1)} = A^{(1)}B^{(0)} + A^{(0)}B^{(1)}$$

$$(AB)^{(2)} = A^{(2)}B^{(0)} + 2A^{(1)}B^{(1)} + A^{(0)}B^{(2)}$$

$$(AB)^{(3)} = A^{(3)}B^{(0)} + 3A^{(2)}B^{(1)} + 3A^{(1)}B^{(2)} + A^{(0)}B^{(3)}$$

Proposition - Formule de Leibniz

A, B polynômes

$$\forall n \in \mathbb{N} \qquad (AB)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} A^{(k)} B^{(n-k)}$$

Proposition - Formule de Leibniz

A, B polynômes

$$\forall n \in \mathbb{N} \qquad (AB)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} A^{(k)} B^{(n-k)}$$

Démonstration. Par récurrence sur n.

$$a^k b^{n-k}(a+b) = a^{k+1} b^{n-k} + a^k b^{n-k+1}$$

$$\left(A^{(k)} B^{(n-k)}\right)' = A^{(k+1)} B^{(n-k)} + A^{(k)} B^{(n-k+1)}$$

□

Proposition - Formule de Leibniz

A, B polynômes

$$\forall n \in \mathbb{N} \qquad (AB)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} A^{(k)} B^{(n-k)}$$

▷ Exercice 3.

Soit $P = X^7(X-3)^3$.

Calculer $P^{(9)}$ en utilisant la formule de Leibniz.

Exemple

Valeurs en 0 des dérivés successifs de $P = \sum_{k=0}^{n} a_k X^k$

Théorème - Formule de Taylor

P polynôme de degré n $\qquad$ $a \in \mathbb{K}$

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

Théorème - Formule de Taylor

P polynôme de degré n $\qquad$ $a \in \mathbb{K}$

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

Démonstration. Si $P = 0$ la formule est juste.

$\mathcal{P}_n$ **: la formule de Taylor est vraie pour tout polynôme de degré** n**.**

Initialisation. Si P est de degré nul alors P est constant, et $P = P^{(0)}(a)$.

Suite de la démonstration.

Hérédité. Soit P de degré n. On pose :

$$Q = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

Suite de la démonstration.

Hérédité. Soit P de degré n. On pose :

$$Q = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

Alors $$Q' = \sum_{k=1}^{n} \frac{P^{(k)}(a)}{(k-1)!}(X-a)^{k-1}$$

$$= \sum_{k=0}^{n-1} \frac{P^{(k+1)}(a)}{k!}(X-a)^k$$

Suite de la démonstration.

Hérédité. Soit P de degré n. On pose :

$$Q = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

Alors $$Q' = \sum_{k=1}^{n} \frac{P^{(k)}(a)}{(k-1)!}(X-a)^{k-1}$$

$$= \sum_{k=0}^{n-1} \frac{P^{(k+1)}(a)}{k!}(X-a)^k$$

Or $$P' = \sum_{k=0}^{n-1} \frac{P'^{(k)}(a)}{k!}(X-a)^k$$

Suite de la démonstration.

Hérédité. Soit P de degré n. On pose :

$$Q = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

Ainsi $Q' = P'$.

De plus $Q(a) = P(a)$ donc $P = Q$.

Conclusion. Par récurrence, la formule de Taylor est vraie pour tout polynôme. □

Théorème - Formule de Taylor

P polynôme de degré n $\quad a \in \mathbb{K}$

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

Remarque

Pour tout polynôme P : $\quad P^0 = 1$

Ceci montre que la spécialisation de $(X-a)^0$ en a est égale à 1.

Théorème - Formule de Taylor

P polynôme de degré n $\quad a \in \mathbb{K}$

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

Exemple 3

Application de la formule pour :

$$P = X^3 + 2X - 5 \qquad \text{et} \qquad a = 1$$

Théorème - Formule de Taylor

P polynôme de degré n $\quad a \in \mathbb{K}$

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

▷ Exercice 4.

Appliquer la formule pour :

a. $P = 2X^2 + 7X + 7$ en $a = -2$

b. $Q = X^3 - 9X^2 + 26X - 24$ en $a = 3$

Résoudre l'équation : $Q(X) = 0$

Chapitre B7. Polynômes

III. **Racines**

A. Définition

B. Ordre de multiplicité d'une racine

C. Relations entre coefficients et racines

Définition

$P \in \mathbb{K}[X]$

Une racine (ou un zéro) de P est un scalaire α tel que :

$$P(\alpha) = 0$$

Exemples

- Le polynôme $X + 3$ de $\mathbb{K}[X]$ a une racine.
- Le polynôme $X^2 + 1$ de $\mathbb{C}[X]$ a deux racines.
- Le polynôme $X^2 + 1$ de $\mathbb{R}[X]$ n'a pas de racine.
- Le polynôme 5 n'a pas de racine.
- Le polynôme nul a une infinité de racines.

Théorème

$P \in \mathbb{K}[X]$ $\alpha \in \mathbb{K}$

α est racine de P $\iff$ $(X - \alpha)$ divise P

Théorème

$P \in \mathbb{K}[X]$ $\alpha \in \mathbb{K}$

α est racine de P $\iff$ $(X - \alpha)$ divise P

Démonstration.

Théorème

$P \in \mathbb{K}[X]$ $\alpha \in \mathbb{K}$

α est racine de P $\iff$ $(X - \alpha)$ divise P

Démonstration.

□

Théorème

$P \in \mathbb{K}[X]$ $\alpha \in \mathbb{K}$

α est racine de P $\iff$ $(X - \alpha)$ divise P

Exemple 4

Résoudre :

$$3x^3 - 5x^2 + 2 = 0$$

Théorème

$P \in \mathbb{K}[X] \qquad \alpha \in \mathbb{K}$

α est racine de $P \iff (X - \alpha)$ divise P

▷ Exercice 5.

Résoudre :

$$x^5 - x^4 - 6x^3 + 14x^2 - 12x = 0$$

Corollaire

Soit P un polynôme et $k \in \mathbb{N}^*$.

Si $\alpha_1, \ldots, \alpha_k$ sont k racines distinctes de P alors :

$$\prod_{i=1}^{k}(X - \alpha_i) \quad \text{divise} \quad P$$

Corollaire

Si $\alpha_1, \ldots, \alpha_k$ sont k racines distinctes de P alors :

$$\prod_{i=1}^{k}(X - \alpha_i) \quad \text{divise} \quad P$$

Démonstration.

Initialisation. Le théorème précédent donne la propriété $\mathcal{P}_1$.

Corollaire

Si $\alpha_1, \ldots, \alpha_k$ sont k racines distinctes de P alors :

$$\prod_{i=1}^{k}(X-\alpha_i) \quad \text{divise} \quad P$$

Démonstration.

Hérédité. Soit $\alpha_1, \ldots, \alpha_k$ racines distinctes de P.

Comme $\mathcal{P}_{k-1}$ est supposée vraie :

$$P = (X-\alpha_1)\cdots(X-\alpha_{k-1})Q$$

Corollaire

Si $\alpha_1, \ldots, \alpha_k$ sont k racines distinctes de P alors :

$$\prod_{i=1}^{k}(X - \alpha_i) \quad \text{divise} \quad P$$

Démonstration.

Hérédité. Soit $\alpha_1, \ldots, \alpha_k$ racines distinctes de P.

Comme $\mathcal{P}_{k-1}$ est supposée vraie :

$$P = (X - \alpha_1) \cdots (X - \alpha_{k-1})Q$$

Spécialisation en α_k :

$$0 = (\alpha_k - \alpha_1) \cdots (\alpha_k - \alpha_{k-1})Q(\alpha_k)$$

Corollaire

Si $\alpha_1, \ldots, \alpha_k$ sont k racines distinctes de P alors :

$$\prod_{i=1}^{k}(X - \alpha_i) \quad \text{divise} \quad P$$

Démonstration.

Spécialisation en α_k :

$$0 = (\alpha_k - \alpha_1) \cdots (\alpha_k - \alpha_{k-1})Q(\alpha_k)$$

Les α_i sont distincts donc :

$$Q(\alpha_k) = 0$$

Corollaire

Si $\alpha_1, \ldots, \alpha_k$ sont k racines distinctes de P alors :

$$\prod_{i=1}^{k}(X - \alpha_i) \quad \text{divise} \quad P$$

Démonstration.

$$Q(\alpha_k) = 0$$

Il existe un polynôme Q_1 tel que :

$$Q = (X - \alpha_k)Q_1$$

Corollaire

Si $\alpha_1, \ldots, \alpha_k$ sont k racines distinctes de P alors :

$$\prod_{i=1}^{k}(X - \alpha_i) \quad \text{divise} \quad P$$

Démonstration.

$$Q(\alpha_k) = 0$$

Il existe un polynôme Q_1 tel que :

$$Q = (X - \alpha_k)Q_1$$

Ce qui donne :

$$P = (X - \alpha_1) \cdots (X - \alpha_{k-1})(X - \alpha_k)Q_1$$

Corollaire

Si $\alpha_1, \ldots, \alpha_k$ sont k racines distinctes de P alors :

$$\prod_{i=1}^{k}(X - \alpha_i) \quad \text{divise} \quad P$$

Démonstration.

Conclusion. Par récurrence, la propriété $\mathcal{P}_k$ est vraie pour tout entier non-nul k. □

Corollaire

Si $\alpha_1, \ldots, \alpha_k$ sont k racines distinctes de P alors :

$$\prod_{i=1}^{k}(X - \alpha_i) \quad \text{divise} \quad P$$

Corollaire

Un polynôme de degré n possède au plus n racines distinctes.

Corollaire

Un polynôme de degré n possède au plus n racines distinctes.

Démonstration. Si $\alpha_1 \dots \alpha_m$ sont m racines distinctes de P alors il existe Q tel que :

$$P = \left(\prod_{i=1}^{m} (X - \alpha_i) \right) Q$$

Corollaire

Un polynôme de degré n possède au plus n racines distinctes.

Démonstration.

$$P = \left(\prod_{i=1}^{m}(X-\alpha_i)\right)Q$$

Ceci donne :

$$\deg P = \deg\left(\prod_{i=1}^{m}(X-\alpha_i)\right) + \deg Q = m + \deg Q$$

Puis $n \geqslant m$. □

Corollaire

Un polynôme de degré n possède au plus n racines distinctes.

Corollaires

(i) P polynôme de degré inférieur ou égal à n.
Si P admet $n+1$ racines distinctes alors $P = 0$.

Corollaire

Un polynôme de degré n possède au plus n racines distinctes.

Corollaires

(i) P polynôme de degré inférieur ou égal à n.
Si P admet $n+1$ racines distinctes alors $P = 0$.

Démonstration. *(i)* est conséquence du corollaire précédent.

Corollaires

(i) P polynôme de degré inférieur ou égal à n.
Si P admet $n+1$ racines distinctes alors $P = 0$.

(ii) Soit P et Q de degrés inférieurs ou égaux à n.
Si les α_i sont $n+1$ scalaires distincts tels que :

$$\forall i = 0, \ldots, n \qquad P(\alpha_i) = Q(\alpha_i).$$

Alors $P = Q$.

Corollaires

(i) P polynôme de degré inférieur ou égal à n.
Si P admet $n+1$ racines distinctes alors $P = 0$.

(ii) Soit P et Q de degrés inférieurs ou égaux à n.
Si les α_i sont $n+1$ scalaires distincts tels que :

$$\forall i = 0, \ldots, n \qquad P(\alpha_i) = Q(\alpha_i).$$

Alors $P = Q$.

Démonstration. *(ii)* : $P - Q$ possède $\alpha_0, \ldots, \alpha_n$ pour racines.
donc $P - Q = 0$ d'après le *(i)*, puis $P = Q$.

Corollaires

(ii) Soit P et Q de degrés inférieurs ou égaux à n.
Si les α_i sont $n+1$ scalaires distincts tels que :

$$\forall i = 0, \ldots, n \qquad P(\alpha_i) = Q(\alpha_i).$$

Alors $P = Q$.

(iii) Soit $f, g : \mathbb{K} \to \mathbb{K}$ deux fonctions polynomiales de degrés inférieurs ou égaux à n.
Si f et g sont égales en au moins $n+1$ scalaires distincts alors f et g sont égales.

Corollaires

(ii) Soit P et Q de degrés inférieurs ou égaux à n.
Si les α_i sont $n+1$ scalaires distincts tels que :

$$\forall i = 0, \ldots, n \qquad P(\alpha_i) = Q(\alpha_i).$$

Alors $P = Q$.

(iii) Soit $f, g : \mathbb{K} \to \mathbb{K}$ deux fonctions polynomiales de degrés inférieurs ou égaux à n.
Si f et g sont égales en au moins $n+1$ scalaires distincts alors f et g sont égales.

Démonstration. *(iii)* est conséquence de *(ii)*. □

Corollaires

(iii) Soit $f, g : \mathbb{K} \to \mathbb{K}$ deux fonctions polynomiales de degrés inférieurs ou égaux à n.
Si f et g sont égales en au moins $n+1$ scalaires distincts alors f et g sont égales.

En d'autres termes une fonction polynomiale de degré au plus n est uniquement déterminée par $n+1$ de ses valeurs.

Corollaires

(iii) Soit $f, g : \mathbb{K} \to \mathbb{K}$ deux fonctions polynomiales de degrés inférieurs ou égaux à n.
Si f et g sont égales en au moins $n+1$ scalaires distincts alors f et g sont égales.

Remarque

L'application :

$$\begin{aligned} \mathbb{K}[X] &\longrightarrow \mathbb{K}[x] \\ P &\longmapsto \begin{pmatrix} \mathbb{K} \longrightarrow \mathbb{K} \\ x \longmapsto P(x) \end{pmatrix} \end{aligned}$$

est un isomorphisme d'anneau.

III. **Racines**

A. Définition

B. Ordre de multiplicité d'une racine

C. Relations entre coefficients et racines

Définition

Soit α une racine de P non-nul.

Ordre de multiplicité de α : le plus grand entier k tel que $(X-\alpha)^k$ divise P.

Définition

Soit α une racine de P non-nul.

Ordre de multiplicité de α : le plus grand entier k tel que $(X-\alpha)^k$ divise P.

De façon équivalente, c'est l'entier k tel que :

$$\begin{array}{ll} (X-\alpha)^k & \text{divise } P \\ (X-\alpha)^{k+1} & \text{ne divise pas } P \end{array}$$

Définition

Ordre de multiplicité de α : l'entier k tel que :

$$(X-\alpha)^k \quad \text{divise } P$$
$$(X-\alpha)^{k+1} \quad \text{ne divise pas } P$$

Remarque

Il existe alors un polynôme Q tel que

$$P = (X-\alpha)^k Q \qquad \text{et} \qquad Q(\alpha) \neq 0$$

Définition

Ordre de multiplicité de α : l'entier k tel que :

$$\begin{array}{ll} (X-\alpha)^k & \text{divise } P \\ (X-\alpha)^{k+1} & \text{ne divise pas } P \end{array}$$

Exemple 5

(i) $P = aX^2 + bX + c$

Définition

Ordre de multiplicité de α : l'entier k tel que :

$$(X-\alpha)^k \quad \text{divise } P$$
$$(X-\alpha)^{k+1} \quad \text{ne divise pas } P$$

Exemple 5

(i) $P = aX^2 + bX + c$

Si $\Delta \neq 0$: deux racines de multiplicités 1

Si $\Delta = 0$: une racine de multiplicité 2.

Définition

Ordre de multiplicité de α : l'entier k tel que :

$$\begin{array}{ll} (X-\alpha)^k & \text{divise } P \\ (X-\alpha)^{k+1} & \text{ne divise pas } P \end{array}$$

Exemple 5

(i) $P = aX^2 + bX + c$

Si $\Delta \neq 0$: deux racines de multiplicités 1

Si $\Delta = 0$: une racine de multiplicité 2.

(ii) Racines et multiplicités de : $X^3 - X^2 - X + 1$

Définition

Ordre de multiplicité de α : l'entier k tel que :

$$(X-\alpha)^k \quad \text{divise } P$$
$$(X-\alpha)^{k+1} \quad \text{ne divise pas } P$$

Exemple 5

(i) $P = aX^2 + bX + c$

Si $\Delta \neq 0$: deux racines de multiplicités 1

Si $\Delta = 0$: une racine de multiplicité 2.

(ii) Racines et multiplicités de : $X^3 - X^2 - X + 1$

(iii) Racines et multiplicités de : $4X^{28} - X^{26}$

Remarque - Suite de l'exemple *(ii)*

$$\begin{aligned} P &= X^3 - X^2 - X + 1 \\ P' &= 3X^2 - 2X - 1 \\ P'' &= 6X - 2 \end{aligned}$$

1 est racine de P et de P' mais pas de P''

-1 est racine de P mais pas de P'.

Remarque - Suite de l'exemple *(ii)*

$$\begin{aligned} P &= X^3 - X^2 - X + 1 &&= (X-1)^2(X+1) \\ P' &= 3X^2 - 2X - 1 &&= (X-1)(3X+1) \\ P'' &= 6X - 2 &&= 2(3X+1) \end{aligned}$$

1 est racine de P et de P' mais pas de P''

-1 est racine de P mais pas de P'.

Théorème

$P \in \mathbb{K}[X] \qquad \alpha \in \mathbb{K}$

α est racine de P de multiplicité k

est équivalent à

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

Théorème

$P \in \mathbb{K}[X] \qquad \alpha \in \mathbb{K}$

$$\alpha \text{ est racine de } P \text{ de multiplicité } k$$

est équivalent à

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

Remarque

Un scalaire α est racine d'un polynôme P de multiplicité 0 si et seulement si $P(\alpha) \neq 0$.

Exemple 6

Soit $P = X^4 + 2X^3 - 12X^2 - 40X - 32$.

Chercher une racine évidente de P, puis déterminer son ordre de multiplicité.

En déduire la factorisation de P.

Exemple 6

Soit $P = X^4 + 2X^3 - 12X^2 - 40X - 32$.

Chercher une racine évidente de P, puis déterminer son ordre de multiplicité.

En déduire la factorisation de P.

▷ Exercice 6.

Factoriser de même :

$$P = 2X^6 + 7X^5 + X^4 - 14X^3 - 8X^2 + 7X + 5$$

Théorème

$P \in \mathbb{K}[X] \qquad \alpha \in \mathbb{K}$

α est racine de P de multiplicité k

est équivalent à

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

Exemple 7

Démonstration du sens direct dans le cas où $k = 3$.

Sens direct. α est racine de P de multiplicité 3 :

$\exists Q \in \mathbb{K}[X]$ tel que :

$$P = (X-\alpha)^3 Q \qquad \text{et} \qquad Q(\alpha) \neq 0$$

Sens direct. α est racine de P de multiplicité 3 :

$$P = (X-\alpha)^3 Q \qquad \text{et} \qquad Q(\alpha) \neq 0$$

Dérivés successifs de P :

$$\begin{aligned} P &= (X-\alpha)^3 Q \\ P' &= 3(X-\alpha)^2 Q + (X-\alpha)^3 Q' \end{aligned}$$

Sens direct. α est racine de P de multiplicité 3 :

$$P = (X-\alpha)^3 Q \qquad \text{et} \qquad Q(\alpha) \neq 0$$

Dérivés successifs de P :

$$\begin{aligned} P &= (X-\alpha)^3 Q \\ P' &= 3(X-\alpha)^2 Q + (X-\alpha)^3 Q' \\ P'' &= 6(X-\alpha) Q + 6(X-\alpha)^2 Q' + (X-\alpha)^3 Q'' \end{aligned}$$

Sens direct. α est racine de P de multiplicité 3 :

$$P = (X-\alpha)^3 Q \qquad \text{et} \qquad Q(\alpha) \neq 0$$

Dérivés successifs de P :

$$\begin{aligned}
P &= (X-\alpha)^3 Q \\
P' &= 3(X-\alpha)^2 Q + (X-\alpha)^3 Q' \\
P'' &= 6(X-\alpha) Q + 6(X-\alpha)^2 Q' + (X-\alpha)^3 Q'' \\
P''' &= 6Q + 18(X-\alpha) Q' + 9(X-\alpha)^2 Q'' \\
&\qquad + (X-\alpha)^3 Q'''
\end{aligned}$$

Sens direct. α est racine de P de multiplicité 3 :

$$P = (X-\alpha)^3 Q \qquad \text{et} \qquad Q(\alpha) \neq 0$$

Dérivés successifs de P :

$$\begin{aligned}
P &= (X-\alpha)^3 Q \\
P' &= 3(X-\alpha)^2 Q + (X-\alpha)^3 Q' \\
P'' &= 6(X-\alpha) Q + 6(X-\alpha)^2 Q' + (X-\alpha)^3 Q'' \\
P''' &= 6Q + 18(X-\alpha) Q' + 9(X-\alpha)^2 Q'' \\
&\qquad + (X-\alpha)^3 Q'''
\end{aligned}$$

Donc α est racine de P, P' et P'' mais pas de P'''.

Sens indirect. Supposons :

$$P(\alpha) = P'(\alpha) = P''(\alpha) = 0 \quad \text{et} \quad P'''(\alpha) \neq 0.$$

Sens indirect. Supposons :

$$P(\alpha) = P'(\alpha) = P''(\alpha) = 0 \quad \text{et} \quad P'''(\alpha) \neq 0.$$

Formule de Taylor :

$$P = P(\alpha) + P'(\alpha)(X-\alpha) + \frac{P''(\alpha)}{2}(X-\alpha)^2 + \frac{P'''(\alpha)}{6}(X-\alpha)^3 + \frac{P^{(4)}(\alpha)}{24}(X-\alpha)^4 + \cdots$$

Sens indirect. Supposons :

$$P(\alpha) = P'(\alpha) = P''(\alpha) = 0 \quad \text{et} \quad P'''(\alpha) \neq 0.$$

Formule de Taylor :

$$\begin{aligned} P &= P(\alpha) + P'(\alpha)(X-\alpha) + \frac{P''(\alpha)}{2}(X-\alpha)^2 \\ &\quad + \frac{P'''(\alpha)}{6}(X-\alpha)^3 + \frac{P^{(4)}(\alpha)}{24}(X-\alpha)^4 + \cdots \\ &= (X-\alpha)^3\left[\frac{P'''(\alpha)}{6} + \frac{P^{(4)}(\alpha)}{24}(X-\alpha) + \cdots\right] \end{aligned}$$

Sens indirect. Supposons :

$$P(\alpha) = P'(\alpha) = P''(\alpha) = 0 \quad \text{et} \quad P'''(\alpha) \neq 0.$$

Formule de Taylor :

$$\begin{aligned} P &= P(\alpha) + P'(\alpha)(X-\alpha) + \frac{P''(\alpha)}{2}(X-\alpha)^2 \\ &\quad + \frac{P'''(\alpha)}{6}(X-\alpha)^3 + \frac{P^{(4)}(\alpha)}{24}(X-\alpha)^4 + \cdots \\ &= (X-\alpha)^3\left[\frac{P'''(\alpha)}{6} + \frac{P^{(4)}(\alpha)}{24}(X-\alpha) + \cdots\right] \end{aligned}$$

Donc $P = (X-\alpha)^3 Q$ avec $Q(\alpha) \neq 0$.

Démonstration du sens direct. Supposons que α est racine de P d'ordre de multiplicité k : Il existe un polynôme Q tel que

$$P = (X - \alpha)^k Q \qquad \text{et} \qquad Q(\alpha) \neq 0$$

Soit : $A = (X - \alpha)^k$

Démonstration du sens direct. Supposons que α est racine de P d'ordre de multiplicité k : Il existe un polynôme Q tel que

$$P = (X - \alpha)^k Q \qquad \text{et} \qquad Q(\alpha) \neq 0$$

Soit : $A = (X - \alpha)^k$

Formule de Leibniz :

$$\forall n \in \mathbb{N} \qquad P^{(n)} = \sum_{p=0}^{n} \binom{n}{p} A^{(p)} Q^{(n-p)}$$

Suite de la démonstration.

$$\forall n \in \mathbb{N} \qquad P^{(n)} = \sum_{p=0}^{n} \binom{n}{p} A^{(p)} Q^{(n-p)}$$

Comme

$$\forall p \in \mathbb{N} \quad A^{(p)} = \begin{cases} \frac{k!}{(k-p)!}(X-\alpha)^{k-p} & \text{si } 0 \leqslant p \leqslant k \\ 0 & \text{si } p > k \end{cases}$$

Alors

$$\forall p \in \mathbb{N} \qquad A^{(p)}(\alpha) = \begin{cases} k! & \text{si } p = k \\ 0 & \text{sinon} \end{cases}$$

Suite de la démonstration.

$$\forall n \in \mathbb{N} \qquad P^{(n)} = \sum_{p=0}^{n} \binom{n}{p} A^{(p)} Q^{(n-p)}$$

$$\forall p \in \mathbb{N} \qquad A^{(p)}(\alpha) = \begin{cases} k! & \text{si } p = k \\ 0 & \text{sinon} \end{cases}$$

Si $n \leqslant k-1$ alors $P^{(n)}(\alpha) = 0$

Si $n = k$ alors

$$P^{(k)}(\alpha) = A^{(k)}(\alpha) Q^{(k-k)}(\alpha) = k! Q(\alpha) \neq 0$$

Suite de la démonstration.

On a démontré le sens direct :

Si α est racine de P d'ordre de multiplicité k alors

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

Théorème

$P \in \mathbb{K}[X] \qquad \alpha \in \mathbb{K}$

α est racine de P de multiplicité k

est équivalent à

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

Démonstration du sens indirect.

Théorème

$P \in \mathbb{K}[X] \qquad \alpha \in \mathbb{K}$

α est racine de P de multiplicité k

est équivalent à

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

Démonstration du sens indirect.

□

III. **Racines**

A. Définition

B. Ordre de multiplicité d'une racine

C. Relations entre coefficients et racines

Remarque

$$P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

$$= a_n (X - \alpha_1) \cdots (X - \alpha_n)$$

Remarque

$$P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

$$= a_n (X - \alpha_1) \cdots (X - \alpha_n)$$

Exemple 8

(i) Pour $n = 2$

Remarque

$$P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

$$= a_n (X - \alpha_1) \cdots (X - \alpha_n)$$

Exemple 8

(i) Pour $n = 2$

(ii) Pour $n = 3$

Proposition : formules de Viète

Avec les notations ci-dessus :

$$\sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n} \qquad \text{et} \qquad \prod_{i=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}$$

Proposition : formules de Viète

Avec les notations ci-dessus :

$$\sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n} \qquad \text{et} \qquad \prod_{i=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}$$

Démonstration.

Il suffit de considérer l'égalité de la remarque.

$$\begin{aligned} P &= a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \\ &= a_n (X - \alpha_1) \cdots (X - \alpha_n) \end{aligned}$$

□

Proposition : formules de Viète

Avec les notations ci-dessus :

$$\sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n} \qquad \text{et} \qquad \prod_{i=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}$$

Exemple 9

Pour tout $n \geqslant 2$:

$$\sum_{\zeta \in \mathbb{U}_n} \zeta = 0 \qquad \prod_{\zeta \in \mathbb{U}_n} \zeta = (-1)^{n-1}$$

Proposition : formules de Viète

Avec les notations ci-dessus :

$$\sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n} \qquad \text{et} \qquad \prod_{i=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}$$

Exemple 10

Résoudre les systèmes :

(i) $\begin{cases} x + y = 7 \\ xy = 10 \end{cases}$ *(ii)* $\begin{cases} x + y = 2 \\ x^2 + y^2 = 10 \end{cases}$

Proposition : formules de Viète

Avec les notations ci-dessus :

$$\sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n} \qquad \text{et} \qquad \prod_{i=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}$$

▷ Exercice 7.

Résoudre le système :

$$\begin{cases} xy = 24 \\ x^2 + y^2 = 73 \end{cases}$$

Proposition : formules de Viète

Avec les notations ci-dessus :

$$\sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n} \qquad \text{et} \qquad \prod_{i=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}$$

▷ Exercice 8.

En considérant le polynôme unitaire dont x, y, z sont les racines, résoudre le système :

$$\begin{cases} x + y + z = 1 \\ xy + xz + yz = -16 \\ xyz = 20 \end{cases}$$

Proposition

Avec les notations précédentes :

$$\forall k = 1, \dots, n \qquad \frac{a_{n-k}}{a_n} = (-1)^k \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \alpha_{i_1} \dots \alpha_{i_k}$$

Proposition

Avec les notations précédentes :

$$\forall k = 0, \dots, n \qquad \frac{a_{n-k}}{a_n} = (-1)^k \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \prod_{j=1}^{k} \alpha_{i_j}$$

Proposition

Avec les notations précédentes :

$$\forall k = 1, \dots, n \qquad \frac{a_{n-k}}{a_n} = (-1)^k \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \alpha_{i_1} \dots \alpha_{i_k}$$

Démonstration. Ces formules proviennent du développement de l'égalité :

$$\begin{aligned} P &= a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \\ &= a_n (X - \alpha_1) \cdots (X - \alpha_n) \end{aligned}$$

□

Chapitre B7. Polynômes

IV. Factorisation d'un polynôme

Définition

Un polynôme P de $\mathbb{K}[X]$ est dit scindé s'il est produit de polynômes de $\mathbb{K}[X]$ du premier degré.

Définition

Un polynôme P de $\mathbb{K}[X]$ est dit scindé s'il est produit de polynômes de $\mathbb{K}[X]$ du premier degré.

Remarques

(i) Un polynôme est scindé ssi il peut s'écrire :

$$P = \lambda(X - \beta_1) \cdots (X - \beta_n)$$

avec $n = \deg P$

et $(\lambda, \beta_1, \ldots, \beta_n) \in \mathbb{K}^{n+1}$

Définition

Un polynôme P de $\mathbb{K}[X]$ est dit scindé s'il est produit de polynômes de $\mathbb{K}[X]$ du premier degré.

Remarques

(ii) Autre caractérisation :
Un polynôme de degré n est scindé ssi il admet n racines, comptées avec leurs multiplicités.

Définition

Un polynôme P de $\mathbb{K}[X]$ est dit scindé s'il est produit de polynômes de $\mathbb{K}[X]$ du premier degré.

Exemple 11

Dans $\mathbb{R}[X]$: X^2+1 n'est pas scindé

X^2-1 est scindé

Définition

Un polynôme P de $\mathbb{K}[X]$ est dit scindé s'il est produit de polynômes de $\mathbb{K}[X]$ du premier degré.

Exemple 11

Dans $\mathbb{R}[X]$:	X^2+1	n'est pas scindé
	X^2-1	est scindé
Dans $\mathbb{C}[X]$:	X^2+1	est scindé
	X^2-1	est scindé.

IV. Factorisation d'un polynôme

Théorème fondamental de l'algèbre
Théorème de d'Alembert-Gauss

Tout polynôme non constant de $\mathbb{C}[X]$ possède une racine.

Théorème fondamental de l'algèbre

Tout polynôme non constant de $\mathbb{C}[X]$ possède une racine.

Corollaire

Soit $P \in \mathbb{C}[X]$ de degré n. Alors il existe des complexes $\lambda, \beta_1, \ldots, \beta_n$ tels que :

$$P = \lambda(X - \beta_1) \cdots (X - \beta_n)$$

Théorème fondamental de l'algèbre

Tout polynôme non constant de $\mathbb{C}[X]$ possède une racine.

Corollaire

Soit $P \in \mathbb{C}[X]$ de degré n. Alors il existe des complexes $\lambda, \beta_1, \ldots, \beta_n$ tels que :

$$P = \lambda(X - \beta_1) \cdots (X - \beta_n)$$

Remarque

Ainsi tout polynôme de $\mathbb{C}[X]$ est scindé.

Théorème fondamental de l'algèbre

Tout polynôme non constant de $\mathbb{C}[X]$ possède une racine.

Démonstration. Admise. □

Théorème fondamental de l'algèbre

Tout polynôme non constant de $\mathbb{C}[X]$ possède une racine.

Remarque

On dit que $\mathbb{C}$ est algébriquement clos.

Théorème fondamental de l'algèbre

Tout polynôme non constant de $\mathbb{C}[X]$ possède une racine.

Remarque

On dit que $\mathbb{C}$ est algébriquement clos.

Ce n'est pas le cas de $\mathbb{R}$ ni de $\mathbb{Q}$.

Théorème fondamental de l'algèbre

Tout polynôme non constant de $\mathbb{C}[X]$ possède une racine.

Remarque

On dit que $\mathbb{C}$ est algébriquement clos.

Ce n'est pas le cas de $\mathbb{R}$ ni de $\mathbb{Q}$.

Par exemple :

- $X^2 + 1$ n'a pas de racine dans $\mathbb{Q}$ ni dans $\mathbb{R}$.

Théorème fondamental de l'algèbre

Tout polynôme non constant de $\mathbb{C}[X]$ possède une racine.

Remarque

On dit que $\mathbb{C}$ est algébriquement clos.

Ce n'est pas le cas de $\mathbb{R}$ ni de $\mathbb{Q}$.

Par exemple :

- X^2+1 n'a pas de racine dans $\mathbb{Q}$ ni dans $\mathbb{R}$.
- X^2-2 a des racines dans $\mathbb{R}$ mais pas dans $\mathbb{Q}$.

Théorème fondamental de l'algèbre

Tout polynôme non constant de $\mathbb{C}[X]$ possède une racine.

▷ Exercice 9.

Factoriser le polynôme :

$$P = X^3 - (1+6i)X - (6-2i)$$

Proposition

Soit P un polynôme de degré n.

Soit $\alpha_1, \ldots, \alpha_r$ ses racines,

et $m_1, \ldots, m_r$ leurs multiplicités.

Alors :

$$n = m_1 + \cdots + m_r$$

Proposition

Soit P un polynôme de degré n.

Soit $\alpha_1, \ldots, \alpha_r$ ses racines,

et $m_1, \ldots, m_r$ leurs multiplicités.

Alors :

$$n = m_1 + \cdots + m_r$$

Démonstration.

$$P = \lambda(X - \alpha_1)^{m_1} \cdots (X - \alpha_r)^{m_r}$$

□

IV. Factorisation d'un polynôme

Exemple 12

Le polynôme $X^4 + 1$ est-il scindé dans $\mathbb{R}[X]$?

Exemple 12

Le polynôme $X^4 + 1$ est-il scindé dans $\mathbb{R}[X]$?
Est-il possible de le factoriser dans $\mathbb{R}[X]$?

Exemple 12

Le polynôme $X^4 + 1$ est-il scindé dans $\mathbb{R}[X]$?
Est-il possible de le factoriser dans $\mathbb{R}[X]$?

Remarque

Tout polynôme non constant de $\mathbb{R}[X]$ admet une racine, éventuellement complexe.

$$P \in \mathbb{R}[X] \qquad \Longrightarrow \qquad P \in \mathbb{C}[X]$$

Proposition

Soit $P \in \mathbb{R}[X]$.

Soit α une racine de P, éventuellement complexe.

Alors $\bar{\alpha}$ est racine de P.

Proposition

Soit $P \in \mathbb{R}[X]$.
Soit α une racine de P, éventuellement complexe.
Alors $\bar{\alpha}$ est racine de P.

Démonstration.

Proposition

Soit $P \in \mathbb{R}[X]$.
Soit α une racine de P, éventuellement complexe.
Alors $\bar{\alpha}$ est racine de P.

Démonstration.

□

Proposition

Soit $P \in \mathbb{R}[X]$.
Soit α une racine de P, éventuellement complexe.
Alors $\bar{\alpha}$ est racine de P.

Proposition (suite)

Si α est de multiplicité k
alors $\bar{\alpha}$ est de multiplicité k.

Démonstration. Par théorème, si α est racine de P d'ordre de multiplicité k alors :

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

Les $P^{(n)}$ sont réels donc par conjugaison :

$$\begin{cases} P(\bar{\alpha}) = P'(\bar{\alpha}) = \cdots = P^{(k-1)}(\bar{\alpha}) = 0 \\ P^{(k)}(\bar{\alpha}) \neq 0 \end{cases}$$

$\bar{\alpha}$ est racine de P d'ordre de multiplicité k. □

Théorème

Tout polynôme de $\mathbb{R}[X]$ est produit de polynômes de degré 1 et de polynômes de degré 2 à discriminants strictement négatifs.

Démonstration. Soit $P \in \mathbb{R}[X]$, de racines dans $\mathbb{C}$:

$$\{\underbrace{\alpha_1, \ldots, \alpha_r, \bar{\alpha}_1, \ldots, \bar{\alpha}_r}_{\in \mathbb{C} \setminus \mathbb{R}}, \underbrace{\beta_1, \ldots, \beta_s}_{\in \mathbb{R}}\}$$

Démonstration. Soit $P \in \mathbb{R}[X]$, de racines dans $\mathbb{C}$:

$$\{\underbrace{\alpha_1, \ldots, \alpha_r, \bar{\alpha}_1, \ldots, \bar{\alpha}_r}_{\in \mathbb{C} \setminus \mathbb{R}}, \underbrace{\beta_1, \ldots, \beta_s}_{\in \mathbb{R}}\}$$

$$P = \lambda \prod_{i=1}^{r} (X - \alpha_i)^{k_i} \prod_{i=1}^{r} (X - \bar{\alpha}_i)^{k_i} \prod_{j=1}^{s} (X - \beta_j)^{\ell_j}$$

Démonstration. Soit $P \in \mathbb{R}[X]$, de racines dans $\mathbb{C}$:

$$\{\underbrace{\alpha_1, \dots, \alpha_r, \bar{\alpha}_1, \dots, \bar{\alpha}_r}_{\in \mathbb{C} \setminus \mathbb{R}}, \underbrace{\beta_1, \dots, \beta_s}_{\in \mathbb{R}}\}$$

$$P = \lambda \prod_{i=1}^{r} (X - \alpha_i)^{k_i} \prod_{i=1}^{r} (X - \bar{\alpha}_i)^{k_i} \prod_{j=1}^{s} (X - \beta_j)^{\ell_j}$$

$$= \lambda \prod_{i=1}^{r} [(X - \alpha_i)(X - \bar{\alpha}_i)]^{k_i} \prod_{j=1}^{s} (X - \beta_j)^{\ell_j}$$

Suite de la démonstration.

$$P = \lambda \prod_{i=1}^{r} \left[(X-\alpha_i)(X-\bar{\alpha}_i)\right]^{k_i} \prod_{j=1}^{s} (X-\beta_j)^{\ell_j}$$

$$= \lambda \left(\prod_{i=1}^{r} Q_i^{k_i} \right) \left(\prod_{j=1}^{s} (X-\beta_j)^{\ell_j} \right) \qquad (\star)$$

Avec

$$Q_i = (X-\alpha_i)(X-\bar{\alpha}_i) =$$

Suite de la démonstration.

$$P = \lambda \prod_{i=1}^{r} \left[(X-\alpha_i)(X-\bar{\alpha}_i)\right]^{k_i} \prod_{j=1}^{s} (X-\beta_j)^{\ell_j}$$

$$= \lambda \left(\prod_{i=1}^{r} Q_i^{k_i} \right) \left(\prod_{j=1}^{s} (X-\beta_j)^{\ell_j} \right) \qquad (\star)$$

Avec

$$Q_i = (X-\alpha_i)(X-\bar{\alpha}_i) = X^2 - 2\,\mathrm{Re}(\alpha_i)X + |\alpha_i|^2$$

Discriminant : $\Delta_i =$

Suite de la démonstration.

$$P = \lambda \prod_{i=1}^{r} \left[(X-\alpha_i)(X-\bar{\alpha}_i)\right]^{k_i} \prod_{j=1}^{s} (X-\beta_j)^{\ell_j}$$

$$= \lambda \left(\prod_{i=1}^{r} Q_i^{k_i} \right) \left(\prod_{j=1}^{s} (X-\beta_j)^{\ell_j} \right) \qquad (\star)$$

Avec

$$Q_i = (X-\alpha_i)(X-\bar{\alpha}_i) = X^2 - 2\,\mathrm{Re}(\alpha_i)X + |\alpha_i|^2$$

Discriminant : $\Delta_i = -4\,\mathrm{Im}(\alpha_i)^2 \quad < 0$ $\square$

Théorème

Tout polynôme de $\mathbb{R}[X]$ est produit de polynômes de degré 1 et de polynômes de degré 2 à discriminants strictement négatifs.

Corollaire

Tout polynôme de degré impair de $\mathbb{R}[X]$ possède une racine réelle.

Corollaire

Tout polynôme de degré impair de $\mathbb{R}[X]$ possède une racine réelle.

Démonstration. Si P n'a pas de racine réelle :

$$P = \prod_{i=1}^{r} Q_i^{k_i}$$

où les Q_i sont de degré 2.
Alors P est de degré pair, ce qui contredit l'hypothèse. □

Autre démonstration. Notons

$$P = a_n X^n + \cdots + a_0 \quad \text{avec} \quad a_n \neq 0$$

Quitte à remplacer P par $-P$ on suppose : $a_n > 0$

$$P(x) = x^n \left(a_n + a_{n-1} \frac{1}{x} + \cdots + a_1 \frac{1}{x^{n-1}} + a_0 \frac{1}{x^n} \right)$$

Donc

$$\lim_{x \to +\infty} P(x) = +\infty \qquad \text{et} \qquad \lim_{x \to -\infty} P(x) = -\infty$$

Suite de l'autre démonstration.

$$\lim_{x\to+\infty} P(x) = +\infty \qquad \text{et} \qquad \lim_{x\to-\infty} P(x) = -\infty$$

La fonction $x \mapsto P(x)$ est continue car elle est polynomiale.
D'après le TVI l'image de $\mathbb{R}$ par P est un intervalle.
Les limites montrent qu'il n'est ni majoré ni minoré.
Donc $P(\mathbb{R}) = \mathbb{R}$
Puis 0 admet un antécédent par P. □

Chapitre B7. Polynômes

V. Arithmétique des polynômes

A. PGCD

B. Relation de Bézout

C. PPCM

D. Extension à un nombre fini de polynômes

E. Polynômes irréductibles

Notation

Pour tout polynôme $A \in \mathbb{K}[X]$:

$$\mathcal{D}(A) = \{ D \in \mathbb{K}[X] \mid D \text{ divise } A \}$$

Remarque

$(A, B) \in (\mathbb{K}[X])^2 \setminus \{(0,0)\}$

- $\mathcal{D}(A) \cap \mathcal{D}(B)$ est non-vide.
- L'ensemble $R = \{\deg D \mid D \in \mathcal{D}(A) \cap \mathcal{D}(B)\}$ est une partie non-vide de $\mathbb{N}$
- R est majorée.

Donc

- R admet un plus grand élément r.
- $\mathcal{D}(A) \cap \mathcal{D}(B)$ admet un élément de degré maximal.

Remarque

$(A, B) \in (\mathbb{K}[X])^2 \setminus \{(0,0)\}$

- $\mathcal{D}(A) \cap \mathcal{D}(B)$ admet un élément de degré maximal.

Définition

Soit A et B deux polynômes non tous les deux nuls. Un PGCD de A et B est un polynôme de degré maximal divisant A et B.

Définition

Soit A et B deux polynômes non tous les deux nuls. Un PGCD de A et B est un polynôme de degré maximal divisant A et B.

Remarque

Si D est un PGCD de A et de B
alors pour tout $\lambda \in \mathbb{K}^*$
λD est un PGCD de A et de B
i.e., tout polynôme associé à D est un PGCD de A et B.

Lemme

Soit A, B, Q, R polynômes vérifiant $A = BQ + R$.
Alors :

$$\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(B) \cap \mathcal{D}(R)$$

Démonstration. Par double inclusion. □

Remarque

- $R_0 = A \quad R_1 = B$
- Si $R_{k+1} \neq 0$:

$$R_k = Q_{k+1}R_{k+1} + R_{k+2} \quad \deg R_{k+2} < \deg R_{k+1}$$

Remarque

- $R_0 = A \quad R_1 = B$
- Si $R_{k+1} \neq 0$:

$$R_k = Q_{k+1}R_{k+1} + R_{k+2} \quad \deg R_{k+2} < \deg R_{k+1}$$

La suite $(\deg R_k)_{1 \leqslant k}$ est finie.

- Soit n l'entier tel que $R_n \neq 0$ et $R_{n+1} = 0$.
  Alors :

Remarque

- $R_0 = A \quad R_1 = B$
- Si $R_{k+1} \neq 0$:

$$R_k = Q_{k+1}R_{k+1} + R_{k+2} \quad \deg R_{k+2} < \deg R_{k+1}$$

La suite $(\deg R_k)_{1 \leqslant k}$ est finie.

- Soit n l'entier tel que $R_n \neq 0$ et $R_{n+1} = 0$.
  Alors :

$$\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(R_0) \cap \mathcal{D}(R_1)$$

Remarque

- $R_0 = A \quad R_1 = B$
- Si $R_{k+1} \neq 0$:

$$R_k = Q_{k+1}R_{k+1} + R_{k+2} \quad \deg R_{k+2} < \deg R_{k+1}$$

La suite $(\deg R_k)_{1 \leqslant k}$ est finie.

- Soit n l'entier tel que $R_n \neq 0$ et $R_{n+1} = 0$.
  Alors :

$$\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(R_1) \cap \mathcal{D}(R_2)$$

Remarque

- $R_0 = A \quad R_1 = B$
- Si $R_{k+1} \neq 0$:

$$R_k = Q_{k+1}R_{k+1} + R_{k+2} \quad \deg R_{k+2} < \deg R_{k+1}$$

La suite $(\deg R_k)_{1 \leqslant k}$ est finie.

- Soit n l'entier tel que $R_n \neq 0$ et $R_{n+1} = 0$.
  Alors :

$$\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(R_2) \cap \mathcal{D}(R_3)$$

Remarque

- $R_0 = A \quad R_1 = B$
- Si $R_{k+1} \neq 0$:

$$R_k = Q_{k+1}R_{k+1} + R_{k+2} \quad \deg R_{k+2} < \deg R_{k+1}$$

La suite $(\deg R_k)_{1 \leqslant k}$ est finie.

- Soit n l'entier tel que $R_n \neq 0$ et $R_{n+1} = 0$.
  Alors :

$$\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(R_n) \cap \mathcal{D}(R_{n+1})$$

Remarque

- $R_0 = A \quad R_1 = B$
- Si $R_{k+1} \neq 0$:

$$R_k = Q_{k+1}R_{k+1} + R_{k+2} \quad \deg R_{k+2} < \deg R_{k+1}$$

La suite $(\deg R_k)_{1 \leqslant k}$ est finie.

- Soit n l'entier tel que $R_n \neq 0$ et $R_{n+1} = 0$.
  Alors :

$$\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(R_n) \cap \mathcal{D}(0)$$

Remarque

- $R_0 = A \quad R_1 = B$
- Si $R_{k+1} \neq 0$:

$$R_k = Q_{k+1}R_{k+1} + R_{k+2} \quad \deg R_{k+2} < \deg R_{k+1}$$

La suite $(\deg R_k)_{1 \leqslant k}$ est finie.

- Soit n l'entier tel que $R_n \neq 0$ et $R_{n+1} = 0$.
  Alors :

$$\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(R_n) \cap \mathcal{D}(0) = \mathcal{D}(R_n)$$

Donc R_n est un PGCD de A et B.

Proposition

Si D_1 et D_2 sont deux PGCD de A et de B alors ils sont associés.

Il existe donc un unique PGCD de A et de B unitaire.

Proposition

Si D_1 et D_2 sont deux PGCD de A et de B alors ils sont associés.
Il existe donc un unique PGCD de A et de B unitaire.

Démonstration.
D_1, D_2 sont deux diviseurs de degré maximal de R_n.
Donc ils sont associés à R_n, donc ils sont associés.

Proposition

Si D_1 et D_2 sont deux PGCD de A et de B alors ils sont associés.
Il existe donc un unique PGCD de A et de B unitaire.

Démonstration.
D_1, D_2 sont deux diviseurs de degré maximal de R_n.
Donc ils sont associés à R_n, donc ils sont associés.

Soit a le coefficient dominant de R_n.
Alors $D = \frac{1}{a} R_n$ est un PGCD unitaire de A et de B.
C'est le seul polynôme unitaire associé à R_n. $\square$

Proposition

Si D_1 et D_2 sont deux PGCD de A et de B alors ils sont associés.

Il existe donc un unique PGCD de A et de B unitaire.

Définition

Soit $(A, B) \in (\mathbb{K}[X])^2$ avec $(A, B) \neq (0, 0)$.

Le PGCD de A et B est le polynôme **unitaire** de degré maximal divisant A et B.

On le note $A \wedge B$.

Proposition

Si D_1 et D_2 sont deux PGCD de A et de B alors ils sont associés.

Il existe donc un unique PGCD de A et de B unitaire.

Définition

Soit $(A, B) \in (\mathbb{K}[X])^2$ avec $(A, B) \neq (0, 0)$.

Le PGCD de A et B est le polynôme **unitaire** de degré maximal divisant A et B.

On le note $A \wedge B$.

De plus on convient que $0 \wedge 0 = 0$.

Exemple 13

Déterminer :

$$\left(10X^3 + 10X^2\right) \wedge \left(2X^2 + 4X + 2\right)$$

Proposition

Le PGCD de A et B est le plus grand commun diviseur de A et B au sens de la relation de divisibilité.

$$\forall P \in \mathbb{K}[X]$$
$$(P \mid A \quad \text{et} \quad P \mid B) \iff (P \mid A \wedge B)$$

Proposition

Le PGCD de A et B est le plus grand commun diviseur de A et B au sens de la relation de divisibilité.

$$\forall P \in \mathbb{K}[X]$$
$$(P \mid A \quad \text{et} \quad P \mid B) \iff (P \mid A \wedge B)$$

Démonstration. Conséquence de :

$$\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(A \wedge B)$$ □

▷ Exercice 10.

Calculer le PGCD de A et B dans les cas suivants :

a. $A = X + 2$ et $B = 6X + 11$

b. $A = 2X^3 - X^2 - X - 3$ et $B = 4X^2 + 4X - 15$

c. $A = 4X^2 - 1$ et $B = 2X^2 + 5X - 3$

d. $A = X^n - \alpha^n$ et $B = (X - \alpha)^n$ avec $(\alpha, n) \in \mathbb{K} \times \mathbb{N}^*$.

V. Arithmétique des polynômes

Proposition

Soit $(A, B) \in (\mathbb{K}[X])^2$ avec $(A, B) \neq (0, 0)$. Alors :

$$\exists (U, V) \in (\mathbb{K}[X])^2 \qquad AU + BV = A \wedge B$$

U et V sont appelé coefficients de Bézout de (A, B).

Proposition

Soit $(A, B) \in (\mathbb{K}[X])^2$ avec $(A, B) \neq (0, 0)$. Alors :

$$\exists (U, V) \in (\mathbb{K}[X])^2 \qquad AU + BV = A \wedge B$$

U et V sont appelé coefficients de Bézout de (A, B).

Démonstration.

Conséquence de l'algorithme d'Euclide. □

Proposition

Soit $(A, B) \in (\mathbb{K}[X])^2$ avec $(A, B) \neq (0, 0)$. Alors :

$$\exists (U, V) \in (\mathbb{K}[X])^2 \qquad AU + BV = A \wedge B$$

U et V sont appelé coefficients de Bézout de (A, B).

▷ Exercice 11.

Déterminer des coefficients de Bézout pour :

$$A = (X - 4)(X - 1) \qquad \text{et} \qquad B = (X - 2)$$

Définition

A et B sont premiers entre eux si $A \wedge B = 1$.

Définition

A et B sont premiers entre eux si $A \wedge B = 1$.

Théorème de Bézout

A et B sont premiers entre eux ssi :

$$\exists (U, V) \in (\mathbb{K}[X])^2 \qquad AU + BV = 1$$

Définition

A et B sont premiers entre eux si $A \wedge B = 1$.

Théorème de Bézout

A et B sont premiers entre eux ssi :

$$\exists (U, V) \in (\mathbb{K}[X])^2 \qquad AU + BV = 1$$

Démonstration.

Sens direct : conséquence de la propriété précédente.

Définition

A et B sont premiers entre eux si $A \wedge B = 1$.

Théorème de Bézout

A et B sont premiers entre eux ssi :

$$\exists (U, V) \in (\mathbb{K}[X])^2 \qquad AU + BV = 1$$

Démonstration.

Sens direct : conséquence de la propriété précédente.

Sens indirect : si $AU + BV = 1$ alors tout diviseur de A et de B divise 1. □

Proposition (Lemme de Gauss)

A, B, C polynômes. Si A divise BC et A est premier avec B alors A divise C.

$$(A \mid BC \quad \text{et} \quad A \wedge B = 1) \quad \Longrightarrow \quad A \mid C$$

Proposition (Lemme de Gauss)

A, B, C polynômes. Si A divise BC et A est premier avec B alors A divise C.

$$(A \mid BC \quad \text{et} \quad A \wedge B = 1) \quad \Longrightarrow \quad A \mid C$$

Démonstration. Relation de Bézout :

$$AU + BV = 1 \qquad \text{donc} \quad C = ACU + BCV$$

Si $A \mid BC$ alors $A \mid ACU + BCV = C$. □

Proposition

Soit A et B deux polynômes et D leur PGCD. Alors il existe deux polynômes A_1 et B_1 tel que :

$$A = DA_1 \qquad B = DB_1 \qquad A_1 \wedge B_1 = 1$$

Démonstration. Laissée en exercice. □

V. Arithmétique des polynômes

Remarque

$(A, B) \in (\mathbb{K}[X] \setminus \{0\})^2$

- L'ensemble des multiples non-nuls de A et de B est non vide.
- L'ensemble des degrés de ses éléments est une partie de $\mathbb{N}$ non-vide.

Donc

- L'ensemble de degré admet un plus petit élément.
- L'ensemble des multiples non-nuls de A et B admet un élément de degré minimal.

Définition

Soit A et B deux polynômes non-nuls.
Un PPCM de A et B est un polynôme non-nul de degré minimal multiple de A et B.

Définition

Soit A et B deux polynômes non-nuls.
Un PPCM de A et B est un polynôme non-nul de degré minimal multiple de A et B.

Remarque

Si M est un PPCM de A et de B
alors pour tout $\lambda \in \mathbb{K}^*$
λM est un PPCM de A et de B
i.e., tout polynôme associé à M est un PPCM de A et B.

Proposition

Un PPCM de A et B est le plus petit commun multiple de A et B au sens de la divisibilité.

Si M est un PPCM de A et B alors :

$$\forall P \in \mathbb{K}[X]$$

$$(A \mid P \quad \text{et} \quad B \mid P) \quad \Longrightarrow \quad M \mid P$$

Proposition

Un PPCM de A et B est le plus petit commun multiple de A et B au sens de la divisibilité.

Si M est un PPCM de A et B alors :

$$\forall P \in \mathbb{K}[X]$$
$$(A \mid P \quad \text{et} \quad B \mid P) \implies M \mid P$$

Démonstration. Division euclidienne de P par M :

$$P = QM + R \qquad \deg R < \deg M$$

R est un multiple de A et B,

Proposition

Un PPCM de A et B est le plus petit commun multiple de A et B au sens de la divisibilité.

Si M est un PPCM de A et B alors :

$$\forall P \in \mathbb{K}[X]$$
$$(A \mid P \quad \text{et} \quad B \mid P) \implies M \mid P$$

Démonstration. Division euclidienne de P par M :

$$P = QM + R \qquad \deg R < \deg M$$

R est un multiple de A et B, donc $R = 0$. □

Proposition

Si M_1 et M_2 sont deux PPCM de A et de B alors ils sont associés.

Il existe donc un unique PPCM de A et de B unitaire.

Proposition

Si M_1 et M_2 sont deux PPCM de A et de B alors ils sont associés.
Il existe donc un unique PPCM de A et de B unitaire.

Démonstration. En effet, M_1 et M_2 sont deux PPCM de A et B donc ils sont multiples l'un de l'autre d'après la propriété précédente, et ils sont donc associés. □

Proposition

Si M_1 et M_2 sont deux PPCM de A et de B alors ils sont associés.

Il existe donc un unique PPCM de A et de B unitaire.

Définition

A, B polynômes non-nuls.

Le PPCM de A et B est le polynôme non-nul **unitaire** de degré minimal multiple de A et B.

On le note $A \vee B$.

Proposition

Si M_1 et M_2 sont deux PPCM de A et de B alors ils sont associés.

Il existe donc un unique PPCM de A et de B unitaire.

Définition

A, B polynômes non-nuls.

Le PPCM de A et B est le polynôme non-nul **unitaire** de degré minimal multiple de A et B.

On le note $A \vee B$.

De plus : $\forall A \in \mathbb{K}[X] \quad A \vee 0 = 0$

Remarques

(i) $\forall P \in \mathbb{K}[X]$

$$(A \mid P \quad \text{et} \quad B \mid P) \quad \Longrightarrow \quad (A \vee B \mid P)$$

Remarques

(i) $\forall P \in \mathbb{K}[X]$

$$(A \mid P \quad \text{et} \quad B \mid P) \iff (A \vee B \mid P)$$

Remarques

(i) $\forall P \in \mathbb{K}[X]$

$$(A \mid P \quad \text{et} \quad B \mid P) \iff (A \vee B \mid P)$$

(ii) De façon équivalente :

$$A\mathbb{K}[X] \cap B\mathbb{K}[X] = (A \vee B)\mathbb{K}[X]$$

Lemme

A, B, C polynômes non-nuls, C unitaire. Alors :

$$(AC) \vee (BC) = (A \vee B)C$$

Lemme

A, B, C polynômes non-nuls, C unitaire. Alors :

$$(AC) \vee (BC) = (A \vee B)C$$

▷ Exercice 12.

Démontrer ce lemme.

Proposition

Soit A et B deux polynômes non-nuls.

(i) Si A et B sont premiers entre eux alors : $A \vee B$ est associé à AB.

(ii) Dans tous les cas : $(A \wedge B)(A \vee B)$ est associé à AB.

Proposition

(i) Si A et B sont premiers entre eux alors : $A \vee B$ est associé à AB.

(ii) $(A \wedge B)(A \vee B)$ est associé à AB.

Démonstration.

(i) $A \mid M \qquad B \mid M \qquad \Longrightarrow \qquad AB \mid M \quad ?$

Proposition

(i) Si A et B sont premiers entre eux alors : $A \vee B$ est associé à AB.

(ii) $(A \wedge B)(A \vee B)$ est associé à AB.

Démonstration.

(i) $A \mid M \qquad B \mid M \qquad \Longrightarrow \qquad AB \mid M \quad ?$

$M = AQ$

Proposition

(i) Si A et B sont premiers entre eux alors : $A \vee B$ est associé à AB.

(ii) $(A \wedge B)(A \vee B)$ est associé à AB.

Démonstration.

(i) $A \mid M \quad B \mid M \quad \Longrightarrow \quad AB \mid M \quad ?$

$M = AQ \quad B \mid AQ$

Proposition

(i) Si A et B sont premiers entre eux alors : $A \vee B$ est associé à AB.

(ii) $(A \wedge B)(A \vee B)$ est associé à AB.

Démonstration.

(i) $A \mid M \quad B \mid M \quad \Longrightarrow \quad AB \mid M \quad ?$

$M = AQ \quad B \mid AQ$

$\Longrightarrow \quad Q = BR$

Proposition

(i) Si A et B sont premiers entre eux alors : $A \vee B$ est associé à AB.

(ii) $(A \wedge B)(A \vee B)$ est associé à AB.

Démonstration.

(i) $A \mid M \quad B \mid M \quad \Longrightarrow \quad AB \mid M \quad ?$

$M = AQ \quad B \mid AQ$

$\Longrightarrow \quad Q = BR \quad \Longrightarrow \quad M = ABR$

Proposition

(i) Si A et B sont premiers entre eux alors : $A \vee B$ est associé à AB.

(ii) $(A \wedge B)(A \vee B)$ est associé à AB.

Démonstration.

(i)
$$\begin{array}{lll} A \mid M & B \mid M & \\ M = AQ & B \mid AQ & \\ \Longrightarrow & Q = BR & \Longrightarrow \quad M = ABR \\ & & \Longrightarrow \quad AB \mid M \end{array}$$

Proposition

(i) Si A et B sont premiers entre eux alors : $A \vee B$ est associé à AB.

(ii) $(A \wedge B)(A \vee B)$ est associé à AB.

Démonstration.

(i)
$$\begin{array}{lll} A \mid M & & B \mid M \\ M = AQ & & B \mid AQ \\ \Longrightarrow & Q = BR & \Longrightarrow \quad M = ABR \\ & & \Longrightarrow \quad AB \mid M \end{array}$$

$A \vee B \mid AB$ et $AB \mid A \vee B$ donc $A \vee B = \lambda AB$

Proposition

(i) Si A et B sont premiers entre eux alors : $A \vee B$ est associé à AB.

(ii) $(A \wedge B)(A \vee B)$ est associé à AB.

Démonstration.

(ii) Soit $D = A \wedge B$. Alors :

$$A = DA_1 \qquad B = DB_1 \qquad A_1 \wedge A_2 = 1$$

Proposition

(i) Si A et B sont premiers entre eux alors : $A \vee B$ est associé à AB.

(ii) $(A \wedge B)(A \vee B)$ est associé à AB.

Démonstration.

(ii) Soit $D = A \wedge B$. Alors :

$$A = DA_1 \qquad B = DB_1 \qquad A_1 \wedge A_2 = 1$$

$$A \vee B = (A_1 D) \vee (B_1 D)$$

Proposition

(i) Si A et B sont premiers entre eux alors : $A \vee B$ est associé à AB.

(ii) $(A \wedge B)(A \vee B)$ est associé à AB.

Démonstration.

(ii) Soit $D = A \wedge B$. Alors :

$$A = DA_1 \qquad B = DB_1 \qquad A_1 \wedge A_2 = 1$$

Lemme précédent (D unitaire) :

$$A \vee B = (A_1 D) \vee (B_1 D) = (A_1 \vee B_1)D = \lambda A_1 B_1 D$$

Proposition

(i) Si A et B sont premiers entre eux alors : $A \vee B$ est associé à AB.

(ii) $(A \wedge B)(A \vee B)$ est associé à AB.

Démonstration.

(ii) Soit $D = A \wedge B$. Alors :

$$A = DA_1 \qquad B = DB_1 \qquad A_1 \wedge A_2 = 1$$

Lemme précédent (D unitaire) :

$$A \vee B = (A_1 D) \vee (B_1 D) = (A_1 \vee B_1)D = \lambda A_1 B_1 D$$

$$(A \vee B)(A \wedge B) = \lambda A_1 B_1 D^2 = \lambda AB \qquad \square$$

V. Arithmétique des polynômes

Proposition

$A_1, \ldots, A_n$ polynômes non tous nuls.

(i) Il existe un et un seul polynôme D unitaire de degré maximal divisant tous les A_i.

(ii) De plus il existe $U_1, \ldots, U_n$ tels que

$$A_1U_1 + \cdots + A_nU_n = D$$

(iii) Si P divise tous les A_i alors P divise D.

Proposition

$A_1, \ldots, A_n$ polynômes non tous nuls.

(i) Il existe un et un seul polynôme D unitaire de degré maximal divisant tous les A_i.

Définition

Le polynôme D est appelé PGCD de $A_1, \ldots, A_n$.

Il est noté :

$$D = A_1 \wedge \ldots \wedge A_n = \bigwedge_{i=1}^{n} A_i$$

Définition

Le polynôme D est appelé PGCD de $A_1, \ldots, A_n$.

Il est noté :

$$D = A_1 \wedge \ldots \wedge A_n = \bigwedge_{i=1}^{n} A_i$$

Remarque

$$\bigwedge_{i=1}^{1} A_i = A_1 \qquad \bigwedge_{i=1}^{0} A_i = 0$$

Définition

Les polynômes $A_1, \ldots, A_n$ sont :

(i) premiers entre eux dans leur ensemble si :

$$A_1 \wedge \ldots \wedge A_n = 1$$

(ii) premiers entre eux deux à deux si :

$$\forall (i,j) \in \{1, \ldots, n\}^2$$

$$i \neq j \quad \Longrightarrow \quad A_i \wedge A_j = 1$$

Remarque

Si :

$A_1, \ldots, A_n$ sont premiers entre eux deux à deux

alors :

$A_1, \ldots, A_n$ sont premiers entre eux dans leur ensemble.

La réciproque est fausse.

Remarque

Si :

$A_1, \ldots, A_n$ sont premiers entre eux deux à deux

alors :

$A_1, \ldots, A_n$ sont premiers entre eux dans leur ensemble.

La réciproque est fausse.

Exemple

$$A_1 = (X-2)(X-3)$$
$$A_2 = (X-1)(X-3)$$
$$A_3 = (X-1)(X-2)$$

V. Arithmétique des polynômes

Définition

Un polynôme P de $\mathbb{K}[X]$ est dit irréductible si :

(i) $\deg P \geqslant 1$

(ii) Les seuls diviseurs de P sont les scalaires non-nuls et les polynômes associés à P.

Définition

Un polynôme P de $\mathbb{K}[X]$ est dit irréductible si :

(i) $\deg P \geqslant 1$

(ii) Les seuls diviseurs de P sont les scalaires non-nuls et les polynômes associés à P.

$$\forall D \in \mathbb{K}[X]$$

$$D \mid P \quad \Longrightarrow \quad D = \lambda \quad \text{ou} \quad D = \lambda P$$

avec $\lambda \in \mathbb{K}^*$

Définition

Un polynôme P de $\mathbb{K}[X]$ est dit irréductible si :

(i) $\deg P \geqslant 1$

(ii) Les seuls diviseurs de P sont les scalaires non-nuls et les polynômes associés à P.

Remarque

Les polynômes irréductibles de $\mathbb{K}[X]$ jouent le rôle des nombres premiers dans $\mathbb{Z}$.

Définition

Un polynôme P de $\mathbb{K}[X]$ est dit irréductible si :

(i) $\deg P \geqslant 1$

(ii) Les seuls diviseurs de P sont les scalaires non-nuls et les polynômes associés à P.

Exemple 14

(i) $X - \alpha$ est irréductible.

Définition

Un polynôme P de $\mathbb{K}[X]$ est dit irréductible si :

(i) $\deg P \geqslant 1$

(ii) Les seuls diviseurs de P sont les scalaires non-nuls et les polynômes associés à P.

Exemple 14

(i) $X - \alpha$ est irréductible.

(ii) $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$.

Proposition

Les polynômes irréductible de $\mathbb{C}[X]$ sont :

$$\lambda(X-\alpha) \qquad \text{avec} \qquad (\alpha,\lambda)\in\mathbb{C}\times\mathbb{C}^*$$

Il s'agit des polynômes de degré 1.

Proposition

Les polynômes irréductible de $\mathbb{C}[X]$ sont :

$$\lambda(X-\alpha) \qquad \text{avec} \qquad (\alpha,\lambda)\in\mathbb{C}\times\mathbb{C}^*$$

Il s'agit des polynômes de degré 1.

Proposition

Les polynômes irréductibles de $\mathbb{R}[X]$ sont :

(i) $\lambda(X-\alpha) \qquad \text{avec} \qquad (\alpha,\lambda)\in\mathbb{R}\times\mathbb{R}^*$

(ii) Les polynômes de degré 2 à discriminant strictement négatif.

Rappel

Soit $P \in \mathbb{C}[X]$ de degré n. Alors il existe des complexes λ, $\beta_1, \ldots, \beta_n$ tels que :

$$P = \lambda(X - \beta_1) \cdots (X - \beta_n)$$

Soit $P \in \mathbb{R}[X]$. Alors il existe des réels $\lambda, \beta_1, \ldots, \beta_s$ et des polynômes $Q_1, \ldots, Q_r$ de degré 2 à discriminants strictement négatifs tels que :

$$P = \lambda \left(\prod_{i=1}^{r} Q_i^{k_i} \right) \left(\prod_{j=1}^{s} (X - \beta_j)^{\ell_j} \right)$$

Théorème

Tout polynôme de $\mathbb{K}[X]$ se décompose comme produit d'un élément de $\mathbb{K}^*$ et de facteurs irréductibles unitaires de $\mathbb{K}[X]$.
Cette décomposition est unique à permutation des facteurs près.

Théorème

Tout polynôme de $\mathbb{K}[X]$ se décompose comme produit d'un élément de $\mathbb{K}^*$ et de facteurs irréductibles unitaires de $\mathbb{K}[X]$.
Cette décomposition est unique à permutation des facteurs près.

Démonstration. Il reste à démontrer l'unicité.
Elle est vérifiée car l'ensemble des racines complexes et de leurs multiplicité est unique. □

Proposition

Soit A et B deux polynômes de $\mathbb{K}[X]$. Alors :

(i) A divise B si et seulement si les racines complexes de A sont racines de B avec une multiplicité inférieure ou égale.

Proposition

(i) A divise B si et seulement si les racines complexes de A sont racines de B avec une multiplicité inférieure ou égale.

Démonstration. *(i)*

$$B = \lambda(X - \alpha_1)^{m_1} \dots (X - \alpha_r)^{m_r}$$

Proposition

(i) A divise B si et seulement si les racines complexes de A sont racines de B avec une multiplicité inférieure ou égale.

Démonstration. *(i)*

$$B = \lambda(X-\alpha_1)^{m_1}\dots(X-\alpha_r)^{m_r}$$

$B = AQ$ donc

$$A = \mu(X-\alpha_1)^{k_1}\dots(X-\alpha_r)^{k_r}$$
$$Q = \nu(X-\alpha_1)^{\ell_1}\dots(X-\alpha_r)^{\ell_r}$$

Proposition

(i) A divise B si et seulement si les racines complexes de A sont racines de B avec une multiplicité inférieure ou égale.

Démonstration. *(i)*

$$B = \lambda(X-\alpha_1)^{m_1}\dots(X-\alpha_r)^{m_r}$$

$B = AQ$ donc

$$A = \mu(X-\alpha_1)^{k_1}\dots(X-\alpha_r)^{k_r}$$
$$Q = \nu(X-\alpha_1)^{\ell_1}\dots(X-\alpha_r)^{\ell_r}$$

$\forall i = 1,\dots,r \quad m_i = k_i + \ell_i \quad$ donc $\quad k_i \leqslant m_i.$

Proposition

(ii) A et B sont premiers entre eux si et seulement s'ils n'ont pas de racine commune dans $\mathbb{C}$.

Démonstration. *(ii)*

Proposition

(ii) A et B ne sont pas premiers entre eux si et seulement s'ils ont une racine commune.

Démonstration. *(ii)*

Proposition

(ii) A et B ne sont pas premiers entre eux si et seulement s'ils ont une racine commune.

Démonstration. *(ii)*

Soit $D = A \wedge B$. Alors :

$$\begin{aligned} & A \text{ et } B \text{ ne sont pas premiers entre eux} \\ \iff & \deg D \geqslant 1 \end{aligned}$$

Proposition

(ii) A et B ne sont pas premiers entre eux si et seulement s'ils ont une racine commune.

Démonstration. *(ii)*

Soit $D = A \wedge B$. Alors :

$$\begin{aligned} & A \text{ et } B \text{ ne sont pas premiers entre eux} \\ \iff & \deg D \geqslant 1 \\ \iff & \exists \alpha \in \mathbb{C} \qquad (X - \alpha) \mid D \end{aligned}$$

Proposition

(ii) A et B ne sont pas premiers entre eux si et seulement s'ils ont une racine commune.

Démonstration. *(ii)*

Soit $D = A \wedge B$. Alors :

$$\begin{aligned}
& A \text{ et } B \text{ ne sont pas premiers entre eux} \\
\iff \quad & \deg D \geqslant 1 \\
\iff \quad & \exists \alpha \in \mathbb{C} \qquad (X - \alpha) \mid D \\
\iff \quad & \exists \alpha \in \mathbb{C} \qquad \alpha \text{ est racine de } A \text{ et } B.
\end{aligned}$$

□

Prochain chapitre

Chapitre A9
Dérivation