

⇒ Division euclidienne entre polynômes

⇒ PGCD de polynômes

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

- 2.1. Multiples d'un polynôme
- 2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$
- 2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

- 3.1. Heuristique
- 3.2. Algo. d'Euclide (+Bézout)
- 3.3. PGCD

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algorithme d'Euclide et coefficients de Bézout

3.3. PGCD

⇒ Division euclidienne entre polynômes

⇒ PGCD de polynômes

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.1. Multiples d'un polynôme

2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.1. Heuristique

3.2. Algorithme d'Euclide et coefficients de Bézout

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Problème Arithmétique

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Problème Arithmétique

Problème Fonction arithmétique (multiplicative)

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Problème Arithmétique

Problème Fonction arithmétique (multiplicative)

Problème Théorème de FERMAT

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Problème Arithmétique

Problème Fonction arithmétique (multiplicative)

Problème Théorème de FERMAT

Problème Corps à p^k éléments

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ Division euclidienne entre polynômes

⇒ PGCD de polynômes

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.1. Multiples d'un polynôme

2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.1. Heuristique

3.2. Algorithme d'Euclide et coefficients de Bézout

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

3.3. PGCD

Définition - B divise A

Soit $(A, B) \in \mathbb{K}[X]^2$, $B \neq 0$. On dit que B *divise* A dans $\mathbb{K}[X]$ s'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$.

On dit aussi que A *est divisible* par B , que B est un diviseur de A , ou que A est un *multiple* de B . On note $B|A$.

$\Rightarrow$ D.E. entre
polynômes

$\Rightarrow$ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Définition - B divise A

Soit $(A, B) \in \mathbb{K}[X]^2$, $B \neq 0$. On dit que B *divise* A dans $\mathbb{K}[X]$ s'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$.

On dit aussi que A *est divisible* par B , que B est un diviseur de A , ou que A est un *multiple* de B . On note $B|A$.

Définition - Ensemble des multiples

Soit P un polynôme.

L'ensemble des multiples de P est noté $P\mathbb{K}[X]$ ou (P) .

C'est un idéal principal de l'anneau $\mathbb{K}[X]$.

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Théorème - Polynômes associés

Soient $P, Q \in \mathbb{K}[X]$ deux polynômes non nuls. On a

$$(P|Q \text{ et } Q|P) \Leftrightarrow (\exists \lambda \in \mathbb{K} \setminus \{0\}, Q = \lambda P).$$

On dit alors que P et Q sont des *polynômes associés*.

On a alors $P\mathbb{K}[X] = Q\mathbb{K}[X]$

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Théorème - Polynômes associés

Soient $P, Q \in \mathbb{K}[X]$ deux polynômes non nuls. On a

$$(P|Q \text{ et } Q|P) \Leftrightarrow (\exists \lambda \in \mathbb{K} \setminus \{0\}, Q = \lambda P).$$

On dit alors que P et Q sont des *polynômes associés*.

On a alors $P\mathbb{K}[X] = Q\mathbb{K}[X]$

Démonstration

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Théorème - Polynômes associés

Soient $P, Q \in \mathbb{K}[X]$ deux polynômes non nuls. On a

$$(P|Q \text{ et } Q|P) \Leftrightarrow (\exists \lambda \in \mathbb{K} \setminus \{0\}, Q = \lambda P).$$

On dit alors que P et Q sont des *polynômes associés*.

On a alors $P\mathbb{K}[X] = Q\mathbb{K}[X]$

Démonstration

Exercice

Montrer qu'il s'agit d'une relation d'équivalence.

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Théorème - Stabilité par combinaison linéaire

Soient $P, Q \in \mathbb{K}[X], A \in \mathbb{K}[X], A \neq 0$. Soient $\lambda, \mu \in \mathbb{K}, (\mu \neq 0)$.
Alors

$$(A|P \text{ et } A|Q) \Leftrightarrow (A|P \text{ et } A|\lambda P + \mu Q)$$

En terme de multiple : $P, Q \in A\mathbb{K}[X]$

$$\Leftrightarrow P \text{ et } (\lambda P + \mu Q) \in A\mathbb{K}[X]$$

Plus largement encore, pour $P, Q, R \in \mathbb{K}[X], A \in \mathbb{K}[X], \text{ non nul, } \mu \in \mathbb{K}^*,$

$$(A|P \text{ et } A|Q) \Leftrightarrow (A|P \text{ et } A|R \times P + \mu Q)$$

$\Rightarrow$ D.E. entre
polynômes

$\Rightarrow$ PGCD de
polynômes

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Théorème - Stabilité par combinaison linéaire

Soient $P, Q \in \mathbb{K}[X], A \in \mathbb{K}[X], A \neq 0$. Soient $\lambda, \mu \in \mathbb{K}, (\mu \neq 0)$.
Alors

$$(A|P \text{ et } A|Q) \Leftrightarrow (A|P \text{ et } A|\lambda P + \mu Q)$$

En terme de multiple : $P, Q \in A\mathbb{K}[X]$

$$\Leftrightarrow P \text{ et } (\lambda P + \mu Q) \in A\mathbb{K}[X]$$

Plus largement encore, pour $P, Q, R \in \mathbb{K}[X], A \in \mathbb{K}[X], \text{ non nul, } \mu \in \mathbb{K}^*,$

$$(A|P \text{ et } A|Q) \Leftrightarrow (A|P \text{ et } A|R \times P + \mu Q)$$

Démonstration

$\Rightarrow$ D.E. entre
polynômes

$\Rightarrow$ PGCD de
polynômes

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Exercice

Soient $A, B \in \mathbb{R}[X]$.

Montrer que B divise A dans $\mathbb{R}[X]$ si et seulement si B divise A dans $\mathbb{C}[X]$.

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Exercice

Soient $A, B \in \mathbb{R}[X]$.

Montrer que B divise A dans $\mathbb{R}[X]$ si et seulement si B divise A dans $\mathbb{C}[X]$.

Exercice

Soit $P \in \mathbb{K}[X]$. Montrer que $P(X) - X$ divise $P(P(X)) - X$.

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ Division euclidienne entre polynômes

⇒ PGCD de polynômes

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.1. Multiples d'un polynôme

2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.1. Heuristique

3.2. Algorithme d'Euclide et coefficients de Bézout

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Théorème - Existence et unicité de la division euclidienne

Soit $(A, B) \in \mathbb{K}[X]^2$, $B \neq 0$. Alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ vérifiant :

$$A = BQ + R$$

$$\deg R < \deg B \quad (\Leftrightarrow R = 0 \text{ ou } 0 \leq \deg R < \deg B)$$

On parle alors de division euclidienne (ou de division suivant les puissances décroissantes) de A par B .

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Théorème - Existence et unicité de la division euclidienne

Soit $(A, B) \in \mathbb{K}[X]^2$, $B \neq 0$. Alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ vérifiant :

$$A = BQ + R$$

$$\deg R < \deg B \quad (\Leftrightarrow R = 0 \text{ ou } 0 \leq \deg R < \deg B)$$

On parle alors de division euclidienne (ou de division suivant les puissances décroissantes) de A par B .

Démonstration

Remarque Nécessité d'un corps $\mathbb{K}$

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Savoir-faire. Algorithme de division euclidienne

La démonstration donne un algorithme pour obtenir Q puis R .

1. On divise le terme de plus haut degré de A par celui de B .
C'est possible car $\mathbb{K}$ est un corps, cela donne un facteur du type $\frac{a_{\deg(A)}}{b_{\deg(B)}} X^{\deg(A) - \deg(B)}$.

On peut, par habitude, noter ce nombre sous B .

2. Puis on soustrait à A , toute la multiplication de B par ce facteur.

On peut, par habitude, écrire cette multiplication sous A , ce qui permet de faire la soustraction aisément

3. On obtient un nouveau terme A_1
4. et on recommence la division, jusqu'à ce que $\deg A_n < \deg B$. On a alors $R = A_n$
Cela se termine bien car la suite $(\deg(A_k))$ est une suite entière strictement décroissante.

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Exercice

Effectuer la division euclidienne de $A = X^5 + 2X^4 + 3X^2 + X + 4$
par $B = X^2 + 2X + 2$.

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Exercice

Effectuer la division euclidienne de $A = X^5 + 2X^4 + 3X^2 + X + 4$ par $B = X^2 + 2X + 2$.

Proposition - Divisibilité et division euclidienne

On a l'équivalence :

$$B|A \iff R = 0$$

où R est le reste de la division euclidienne de A par B .

$\Rightarrow$ D.E. entre
polynômes

$\Rightarrow$ PGCD de
polynômes

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Exercice

Effectuer la division euclidienne de $A = X^5 + 2X^4 + 3X^2 + X + 4$
par $B = X^2 + 2X + 2$.

Proposition - Divisibilité et division euclidienne

On a l'équivalence :

$$B|A \iff R = 0$$

où R est le reste de la division euclidienne de A par B .

Démonstration

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ Division euclidienne entre polynômes

⇒ PGCD de polynômes

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.1. Multiples d'un polynôme

2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.1. Heuristique

3.2. Algorithme d'Euclide et coefficients de Bézout

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Proposition - Structure de $\mathbb{K}[X]$ (Anneau principal)

On suppose de $\mathbb{K}$ est un corps.

L'ensemble des multiples de P est un idéal principal de $\mathbb{K}[X]$.

Mieux : $\mathbb{K}[X]$ est donc un anneau euclidien, donc un anneau principal.

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Proposition - Structure de $\mathbb{K}[X]$ (Anneau principal)

On suppose de $\mathbb{K}$ est un corps.

L'ensemble des multiples de P est un idéal principal de $\mathbb{K}[X]$.

Mieux : $\mathbb{K}[X]$ est donc un anneau euclidien, donc un anneau principal.

Exercice A démontrer

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Définition - Congruence

Soient $P, Q, T \in \mathbb{K}[X]$.

On dit que P est congru à Q modulo T , noté $P \equiv Q[T]$,

si $P - Q$ est un multiple de T i.e. $P - Q \in T\mathbb{K}[X]$ ou encore
 $P = Q + KT$ avec $K \in \mathbb{K}[X]$.

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Définition - Congruence

Soient $P, Q, T \in \mathbb{K}[X]$.

On dit que P est congru à Q modulo T , noté $P \equiv Q[T]$,

si $P - Q$ est un multiple de T i.e. $P - Q \in T\mathbb{K}[X]$ ou encore
 $P = Q + KT$ avec $K \in \mathbb{K}[X]$.

Exercice

Montrer : $P \equiv Q[T] \iff P \% T = Q \% T$.

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ Division euclidienne entre polynômes

⇒ PGCD de polynômes

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.1. Multiples d'un polynôme

2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.1. Heuristique

3.2. Algorithme d'Euclide et coefficients de Bézout

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

3.3. PGCD

On note momentanément $\mathcal{D}(A)$ l'ensemble des diviseurs de $A \in \mathbb{K}[X]$.

Heuristique. PGCD

Soient A et B deux éléments de $\mathbb{K}[X]$ non nuls. $\mathcal{D}(A) \cap \mathcal{D}(B)$ est une partie non vide (contient 1) de $\mathbb{K}[X]$ dont les éléments sont de degré $\leq \max(\deg A, \deg B)$ donc

$\{\deg P; P \in \mathcal{D}(A) \cap \mathcal{D}(B)\} (\subset \mathbb{N})$ admet un plus grand élément d .

Tout élément de $\mathcal{D}(A) \cap \mathcal{D}(B)$ de degré d est appelé un *PGCD* (Plus Grand Commun Diviseur) de A et B .

On parlera parfois de « le » PGCD de A et de B , pour désigner le polynôme unitaire de $\mathcal{D}(A) \cap \mathcal{D}(B)$ de degré d . Les autres PGCD lui sont associés.

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

- 2.1. Multiples d'un polynôme
- 2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$
- 2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

- 3.1. Heuristique
- 3.2. Algo. d'Euclide (+Bézout)
- 3.3. PGCD

On note momentanément $\mathcal{D}(A)$ l'ensemble des diviseurs de $A \in \mathbb{K}[X]$.

Heuristique. PGCD

Soient A et B deux éléments de $\mathbb{K}[X]$ non nuls. $\mathcal{D}(A) \cap \mathcal{D}(B)$ est une partie non vide (contient 1) de $\mathbb{K}[X]$ dont les éléments sont de degré $\leq \max(\deg A, \deg B)$ donc

$\{\deg P; P \in \mathcal{D}(A) \cap \mathcal{D}(B)\} (\subset \mathbb{N})$ admet un plus grand élément d .

Tout élément de $\mathcal{D}(A) \cap \mathcal{D}(B)$ de degré d est appelé un *PGCD* (Plus Grand Commun Diviseur) de A et B .

On parlera parfois de « le » PGCD de A et de B , pour désigner le polynôme unitaire de $\mathcal{D}(A) \cap \mathcal{D}(B)$ de degré d . Les autres PGCD lui sont associés.

Ce n'est pas la définition que nous choisirons. Nous reprendrons la caractéristique, plus pratique, vue en arithmétique entière.

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

- 2.1. Multiples d'un polynôme
- 2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$
- 2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

- 3.1. Heuristique
- 3.2. Algo. d'Euclide (+Bézout)
- 3.3. PGCD

⇒ Division euclidienne entre polynômes

⇒ PGCD de polynômes

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.1. Multiples d'un polynôme

2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.1. Heuristique

3.2. Algorithme d'Euclide et coefficients de Bézout

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Lemme - Stabilité des diviseurs et algorithme d'Euclide

Soit $(A, B) \in \mathbb{K}[X]^2$. Si $A = BQ + R$, alors
 $\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(B) \cap \mathcal{D}(R)$.

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

- 2.1. Multiples d'un polynôme
- 2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$
- 2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

- 3.1. Heuristique
- 3.2. Algo. d'Euclide (+Bézout)
- 3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Lemme - Stabilité des diviseurs et algorithme d'Euclide

Soit $(A, B) \in \mathbb{K}[X]^2$. Si $A = BQ + R$, alors
 $\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(B) \cap \mathcal{D}(R)$.

Démonstration

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Définition - Algorithme d'Euclide

On pratique l'algorithme d'Euclide pour les polynômes A et B .

- ▶ On commence par poser $R_0 = A$ et $R_1 = B$;
- ▶ ensuite, k désignant un entier naturel non nul, tant que $R_{k+1} \neq 0$, on note R_{k+2} le reste de la division euclidienne de R_k par R_{k+1} (on a donc $\deg R_{k+2} < \deg R_{k+1}$).

Comme il n'existe qu'un nombre fini d'entiers naturels entre 0 et $\deg R_0$, il existe $N \in \mathbb{N}^*$ tel que $R_N = 0$.

$$\mathcal{D}(R_{N-1}) = \mathcal{D}(A) \cap \mathcal{D}(B).$$

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

- 2.1. Multiples d'un polynôme
- 2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$
- 2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

- 3.1. Heuristique
- 3.2. Algo. d'Euclide (+Bézout)
- 3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Définition - Algorithme d'Euclide

On pratique l'algorithme d'Euclide pour les polynômes A et B .

- ▶ On commence par poser $R_0 = A$ et $R_1 = B$;
- ▶ ensuite, k désignant un entier naturel non nul, tant que $R_{k+1} \neq 0$, on note R_{k+2} le reste de la division euclidienne de R_k par R_{k+1} (on a donc $\deg R_{k+2} < \deg R_{k+1}$).

Comme il n'existe qu'un nombre fini d'entiers naturels entre 0 et $\deg R_0$, il existe $N \in \mathbb{N}^*$ tel que $R_N = 0$.

$$\mathcal{D}(R_{N-1}) = \mathcal{D}(A) \cap \mathcal{D}(B).$$

Démonstration

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

- 2.1. Multiples d'un polynôme
- 2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$
- 2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

- 3.1. Heuristique
- 3.2. Algo. d'Euclide (+Bézout)
- 3.3. PGCD

Analyse Suites (U_n) et (V_n)

$$\forall n \in \mathbb{N}, \quad U_{n+2} = U_n - Q_{n+1}U_{n+1}, V_{n+2} = V_n - Q_{n+1}V_{n+1}$$

avec pour conditions initiales : $U_0 = 1, U_1 = 0$ et $V_0 = 0, V_1 = 1$.

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Couple de Bézout

Analyse Suites (U_n) et (V_n)

$$\forall n \in \mathbb{N}, \quad U_{n+2} = U_n - Q_{n+1}U_{n+1}, V_{n+2} = V_n - Q_{n+1}V_{n+1}$$

avec pour conditions initiales : $U_0 = 1, U_1 = 0$ et $V_0 = 0, V_1 = 1$.

Par récurrence :

Théorème - Couple de Bézout

A partir de l'algorithme d'Euclide, en considérant les suites (U_n) et (V_n) définies par $U_0 = 1, U_1 = 0$ et $V_0 = 0, V_1 = 1$ et

$$\forall n \in \mathbb{N}, \quad U_{n+2} = U_n - Q_{n+1}U_{n+1}, V_{n+2} = V_n - Q_{n+1}V_{n+1}$$

On a

$$\forall n \in \mathbb{N}, \quad R_n = U_n A + V_n B$$

En particulier, il existe $U, V \in \mathbb{K}[X]$ tel que $R_{N-1} = UA + VB$

$\Rightarrow$ D.E. entre
polynômes

$\Rightarrow$ PGCD de
polynômes

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

- 2.1. Multiples d'un polynôme
- 2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$
- 2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

- 3.1. Heuristique
- 3.2. Algo. d'Euclide (+Bézout)
- 3.3. PGCD

Truc & Astuce pour le calcul - Suites (U_n) et (V_n)

Avec les mêmes notations, on a finalement les suites de polynômes (U_n) et (V_n) définies par la même relation de récurrence :

$$\forall n \in \mathbb{N} \quad U_{n+2} = U_n - Q_{n+1}U_{n+1}, V_{n+2} = V_n - Q_{n+1}V_{n+1}$$

avec pour conditions initiales $U_0 = 1 = V_1$ et $U_1 = V_0 = 0$.

Comme pour le cours d'arithmétique de $\mathbb{Z}$, on peut faire le calcul au fur et à mesure dans un tableau.

Alors, pour tout $n \in \mathbb{N}$, $R_n = U_n \times A + V_n \times B$

$\Rightarrow$ D.E. entre
polynômes

$\Rightarrow$ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Truc & Astuce pour le calcul - Suites (U_n) et (V_n)

Avec les mêmes notations, on a finalement les suites de polynômes (U_n) et (V_n) définies par la même relation de récurrence :

$$\forall n \in \mathbb{N} \quad U_{n+2} = U_n - Q_{n+1}U_{n+1}, V_{n+2} = V_n - Q_{n+1}V_{n+1}$$

avec pour conditions initiales $U_0 = 1 = V_1$ et $U_1 = V_0 = 0$.

Comme pour le cours d'arithmétique de $\mathbb{Z}$, on peut faire le calcul au fur et à mesure dans un tableau.

Alors, pour tout $n \in \mathbb{N}$, $R_n = U_n \times A + V_n \times B$

Exercice

Pour tout $n \in \mathbb{N}_{N-1}$, que vaut $U_n V_{n+1} - U_{n+1} V_n$?

$\Rightarrow$ D.E. entre
polynômes

$\Rightarrow$ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

- 2.1. Multiples d'un polynôme
- 2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$
- 2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

- 3.1. Heuristique
- 3.2. Algo. d'Euclide (+Bézout)
- 3.3. PGCD

⇒ Division euclidienne entre polynômes

⇒ PGCD de polynômes

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.1. Multiples d'un polynôme

2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.1. Heuristique

3.2. Algorithme d'Euclide et coefficients de Bézout

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

3.3. PGCD

Définition - PGCD et couple de Bézout

Soit $(A, B) \in \mathbb{K}[X]^2$, A, B non nuls. Il existe un polynôme D dont les diviseurs sont exactement les diviseurs communs à A et B , c'est-à-dire tel que

$$\forall P \in \mathbb{K}[X], (P|A \text{ et } P|B) \iff P|D.$$

D est un *PGCD* de A et B et deux polynômes D_1 et D_2 vérifiant ces hypothèses sont associés.

L'unique polynôme D unitaire vérifiant ces hypothèses est noté $A \wedge B$ (on dit aussi que c'est **le** PGCD de A et B).

$\Rightarrow$ D.E. entre
polynômes

$\Rightarrow$ PGCD de
polynômes

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Définition - PGCD et couple de Bézout

Soit $(A, B) \in \mathbb{K}[X]^2$, A, B non nuls. Il existe un polynôme D dont les diviseurs sont exactement les diviseurs communs à A et B , c'est-à-dire tel que

$$\forall P \in \mathbb{K}[X], (P|A \text{ et } P|B) \iff P|D.$$

D est un *PGCD* de A et B et deux polynômes D_1 et D_2 vérifiant ces hypothèses sont associés.

L'unique polynôme D unitaire vérifiant ces hypothèses est noté $A \wedge B$ (on dit aussi que c'est **le** PGCD de A et B).

Remarque Relation d'équivalence

$\Rightarrow$ D.E. entre
polynômes

$\Rightarrow$ PGCD de
polynômes

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

- 2.1. Multiples d'un polynôme
- 2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$
- 2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

- 3.1. Heuristique
- 3.2. Algo. d'Euclide (+Bézout)
- 3.3. PGCD

Existence ?

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Avec cette définition, il faut montrer l'existence. La proposition suivante nous donne un exemple.

Proposition - Un PGCD

Le dernier reste non nul obtenu avec l'algorithme d'Euclide est un PGCD de A et B .

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

- 2.1. Multiples d'un polynôme
- 2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$
- 2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

- 3.1. Heuristique
- 3.2. Algo. d'Euclide (+Bézout)
- 3.3. PGCD

Existence ?

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Avec cette définition, il faut montrer l'existence. La proposition suivante nous donne un exemple.

Proposition - Un PGCD

Le dernier reste non nul obtenu avec l'algorithme d'Euclide est un PGCD de A et B .

Démonstration

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

- 2.1. Multiples d'un polynôme
- 2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$
- 2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

- 3.1. Heuristique
- 3.2. Algo. d'Euclide (+Bézout)
- 3.3. PGCD

Comme $A \wedge B = \lambda R_{N-1}$:

Corollaire - Couple de Bézout

Il existe des polynômes U et V tels que $AU + BV = A \wedge B$.
 (U, V) est un couple de Bézout de A et B .

$\Rightarrow$ D.E. entre
polynômes

$\Rightarrow$ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Comme $A \wedge B = \lambda R_{N-1}$:

Corollaire - Couple de Bézout

Il existe des polynômes U et V tels que $AU + BV = A \wedge B$.
 (U, V) est un couple de Bézout de A et B .

Corollaire - Autre expression du PGCD

D est un PGCD de A et B si et seulement si

$$A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$$

$\Rightarrow$ D.E. entre
polynômes

$\Rightarrow$ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

- 2.1. Multiples d'un polynôme
- 2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$
- 2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

- 3.1. Heuristique
- 3.2. Algo. d'Euclide (+Bézout)
- 3.3. PGCD

Comme $A \wedge B = \lambda R_{N-1}$:

Corollaire - Couple de Bézout

Il existe des polynômes U et V tels que $AU + BV = A \wedge B$.
 (U, V) est un couple de Bézout de A et B .

Corollaire - Autre expression du PGCD

D est un PGCD de A et B si et seulement si

$$A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$$

Démonstration

$\Rightarrow$ D.E. entre
polynômes

$\Rightarrow$ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

- 2.1. Multiples d'un polynôme
- 2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$
- 2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

- 3.1. Heuristique
- 3.2. Algo. d'Euclide (+Bézout)
- 3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Remarque Elargissement de la définition

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Remarque Elargissement de la définition

Exercice

Déterminer $PGCD(A, B)$ ainsi qu'un couple de Bezout lorsque
 $A = X^3 + X^2 + 2$ et $B = X^2 + 1$.

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

- 2.1. Multiples d'un polynôme
- 2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$
- 2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

- 3.1. Heuristique
- 3.2. Algo. d'Euclide (+Bézout)
- 3.3. PGCD

Le théorème énonce beaucoup de choses, à démontrer...

Définition - Polynômes premiers entre eux

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

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Le théorème énonce beaucoup de choses, à démontrer...

Définition - Polynômes premiers entre eux

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

Théorème - Théorème de Bezout

Soient A et B deux polynômes non nuls. Alors

$$A \wedge B = 1 \iff \exists (U, V) \in \mathbb{K}[X]^2 \text{ tel que } AU + BV = 1.$$

$\Rightarrow$ D.E. entre
polynômes

$\Rightarrow$ PGCD de
polynômes

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Le théorème énonce beaucoup de choses, à démontrer...

Définition - Polynômes premiers entre eux

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

Théorème - Théorème de Bezout

Soient A et B deux polynômes non nuls. Alors

$$A \wedge B = 1 \iff \exists (U, V) \in \mathbb{K}[X]^2 \text{ tel que } AU + BV = 1.$$

Démonstration

$\Rightarrow$ D.E. entre
polynômes

$\Rightarrow$ PGCD de
polynômes

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Le théorème énonce beaucoup de choses, à démontrer...

Définition - Polynômes premiers entre eux

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

Théorème - Théorème de Bezout

Soient A et B deux polynômes non nuls. Alors

$$A \wedge B = 1 \iff \exists (U, V) \in \mathbb{K}[X]^2 \text{ tel que } AU + BV = 1.$$

Démonstration

Exercice Sans effectuer la division euclidienne, trouver un couple de Bézout pour les polynômes $(1 - X)^5$ et $(1 + X)^4$.

$\Rightarrow$ D.E. entre
polynômes

$\Rightarrow$ PGCD de
polynômes

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Objectifs

- ⇒ Division euclidienne entre polynômes
- ⇒ PGCD de deux polynômes (en parallèle avec $\mathbb{Z}$)

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Objectifs

⇒ Division euclidienne entre polynômes

- Existence : $\forall A, B \in \mathbb{K}[X], \exists ! (Q, R)$ tel que $A = BQ + R$ avec $\deg R < \deg B$.

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Objectifs

⇒ Division euclidienne entre polynômes

- ▶ Existence : $\forall A, B \in \mathbb{K}[X], \exists ! (Q, R)$ tel que $A = BQ + R$ avec $\deg R < \deg B$.
- ▶ Il existe un algorithme de calcul de la division euclidienne (plus ou moins raffiné)

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Objectifs

⇒ Division euclidienne entre polynômes

- ▶ Existence : $\forall A, B \in \mathbb{K}[X], \exists ! (Q, R)$ tel que $A = BQ + R$ avec $\deg R < \deg B$.
- ▶ Il existe un algorithme de calcul de la division euclidienne (plus ou moins raffiné)
- ▶ Multiple ou diviseur. Éléments associés.

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

- 2.1. Multiples d'un polynôme
- 2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$
- 2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

- 3.1. Heuristique
- 3.2. Algo. d'Euclide (+Bézout)
- 3.3. PGCD

Objectifs

⇒ Division euclidienne entre polynômes

- ▶ Existence : $\forall A, B \in \mathbb{K}[X], \exists !(Q, R)$ tel que $A = BQ + R$ avec $\deg R < \deg B$.
- ▶ Il existe un algorithme de calcul de la division euclidienne (plus ou moins raffiné)
- ▶ Multiple ou diviseur. Éléments associés.
- ▶ Stabilité pour les combinaisons linéaires

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Objectifs

- ⇒ Division euclidienne entre polynômes
- ⇒ PGCD de deux polynômes (en parallèle avec $\mathbb{Z}$)

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

- 2.1. Multiples d'un polynôme
- 2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$
- 2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

- 3.1. Heuristique
- 3.2. Algo. d'Euclide (+Bézout)
- 3.3. PGCD

Conclusion

Objectifs

- ⇒ Division euclidienne entre polynômes
- ⇒ PGCD de deux polynômes (en parallèle avec $\mathbb{Z}$)
 - Plus grand diviseur commun de A et B . Définition aux associés près.

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Conclusion

Objectifs

- ⇒ Division euclidienne entre polynômes
- ⇒ PGCD de deux polynômes (en parallèle avec $\mathbb{Z}$)
 - ▶ Plus grand diviseur commun de A et B . Définition aux associés près.
 - ▶ Il existe un algorithme pour obtenir $A \wedge B$: l'algorithme d'Euclide

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Conclusion

Objectifs

- ⇒ Division euclidienne entre polynômes
- ⇒ PGCD de deux polynômes (en parallèle avec $\mathbb{Z}$)
 - ▶ Plus grand diviseur commun de A et B . Définition aux associés près.
 - ▶ Il existe un algorithme pour obtenir $A \wedge B$: l'algorithme d'Euclide
 - ▶ Il donne le couple de Bézout, caractéristique : (U, V) tq $A \wedge B = AU + BV$

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

Conclusion

Objectifs

- ⇒ Division euclidienne entre polynômes
- ⇒ PGCD de deux polynômes (en parallèle avec $\mathbb{Z}$)
 - ▶ Plus grand diviseur commun de A et B . Définition aux associés près.
 - ▶ Il existe un algorithme pour obtenir $A \wedge B$: l'algorithme d'Euclide
 - ▶ Il donne le couple de Bézout, caractéristique : (U, V) tq $A \wedge B = AU + BV$
 - ▶ Critères essentielles :

$$D = A \wedge B \iff \forall P \in \mathbb{K}[X], (P|A \text{ et } P|B) \iff P|D$$
 ou $A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

2. Division euclidienne dans $\mathbb{K}[X]$

- 2.1. Multiples d'un polynôme
- 2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$
- 2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand Commun Diviseur

- 3.1. Heuristique
- 3.2. Algo. d'Euclide (+Bézout)
- 3.3. PGCD

Conclusion

Objectifs

- ⇒ Division euclidienne entre polynômes
- ⇒ PGCD de deux polynômes (en parallèle avec $\mathbb{Z}$)
 - ▶ Plus grand diviseur commun de A et B . Définition aux associés près.
 - ▶ Il existe un algorithme pour obtenir $A \wedge B$: l'algorithme d'Euclide
 - ▶ Il donne le couple de Bézout, caractéristique : (U, V) tq $A \wedge B = AU + BV$
 - ▶ Critères essentielles :

$$D = A \wedge B \iff \forall P \in \mathbb{K}[X], (P|A \text{ et } P|B) \iff P|D$$
 ou $A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$
 - ▶ On définit les polynômes premiers entre eux.

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD

⇒ D.E. entre
polynômes

⇒ PGCD de
polynômes

Objectifs

⇒ Division euclidienne entre polynômes

⇒ PGCD de deux polynômes (en parallèle avec $\mathbb{Z}$)

Pour la prochaine fois

- ▶ Lecture du cours : chapitre 30 : Anneau euclidien des polynômes
3. (fin) & 4.PPCM
- ▶ Exercice n° 630 & 631

1. Problèmes

2. Division
euclidienne dans
 $\mathbb{K}[X]$

2.1. Multiples d'un polynôme

2.2. Existence de la division
euclidienne dans $\mathbb{K}[X]$

2.3. Nature de $\mathbb{K}[X]$

3. Plus Grand
Commun Diviseur

3.1. Heuristique

3.2. Algo. d'Euclide (+Bézout)

3.3. PGCD