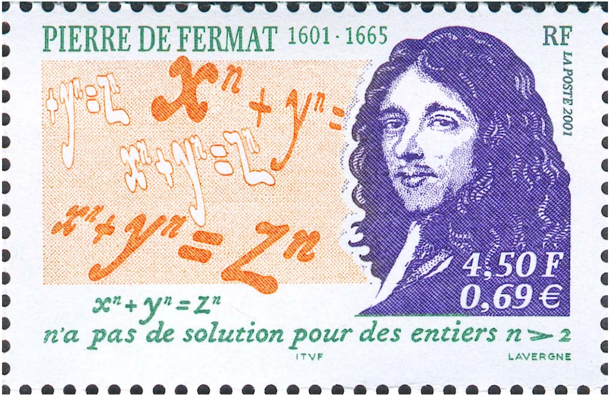

Leçon 83 - L'anneau euclidien des polynômes

3 avril 2025

⇒ Facteurs (relativement) premiers

⇒ PPCM

⇒ Facteurs (relativement) premiers

⇒ PPCM

Lemme de Gauss

Théorème - Lemme de Gauss

Soient A, B, C trois polynômes de $\mathbb{K}[X]$. Alors

$$(A \wedge B = 1 \text{ et } A|BC) \Rightarrow A|C.$$

Lemme de Gauss

Théorème - Lemme de Gauss

Soient A,B,C trois polynômes de $\mathbb{K}[X]$. Alors

$$(A \wedge B = 1 \text{ et } A|BC) \Rightarrow A|C.$$

Démonstration

Facteurs relativement premiers

Proposition - Facteurs relativement premiers

Soient A,B,C trois polynômes de $\mathbb{K}[X]$. Alors

$$(A \wedge B = 1 \text{ et } A \wedge C = 1) \Rightarrow A \wedge BC = 1 \text{ (réciproque vraie)}$$

$$(A \wedge B = 1, A|C, B|C) \Rightarrow AB|C$$

Facteurs relativement premiers

Proposition - Facteurs relativement premiers

Soient A,B,C trois polynômes de $\mathbb{K}[X]$. Alors

$$(A \wedge B = 1 \text{ et } A \wedge C = 1) \Rightarrow A \wedge BC = 1 \text{ (réciproque vraie)}$$

$$(A \wedge B = 1, A|C, B|C) \Rightarrow AB|C$$

Démonstration

Corollaires

Corollaire - Bézout avec degré minimal

Soient A, B deux polynômes non constants, premiers entre eux. Alors il existe un unique couple (U_0, V_0) tel que $AU_0 + BV_0 = 1$ avec $\deg U_0 < \deg B$, $\deg V_0 < \deg A$.
On a alors $U = U_0 + QB$ et $V = V_0 - QA$ avec $Q \in \mathbb{K}[X]$.

Corollaires

Corollaire - Bézout avec degré minimal

Soient A, B deux polynômes non constants, premiers entre eux.
Alors il existe un unique couple (U_0, V_0) tel que $AU_0 + BV_0 = 1$ avec $\deg U_0 < \deg B$, $\deg V_0 < \deg A$.
On a alors $U = U_0 + QB$ et $V = V_0 - QA$ avec $Q \in \mathbb{K}[X]$.

Démonstration

Corollaires

Corollaire - Bézout avec degré minimal

Soient A,B deux polynômes non constants, premiers entre eux.
Alors il existe un unique couple (U_0,V_0) tel que $AU_0+BV_0=1$ avec $\deg U_0<\deg B$, $\deg V_0<\deg A$.
On a alors $U=U_0+QB$ et $V=V_0-QA$ avec $Q\in\mathbb{K}[X]$.

Démonstration

Par récurrence de la proposition : Facteurs relativement premiers :

Corollaire - Facteurs premiers

Soient $A,C,B_1,\ldots,B_n$ des polynômes.

$$(\forall i\in[\![1,n]\!], A\wedge B_i=1)\Rightarrow A\wedge\prod_{i=1}^n B_i=1$$

$(\forall (i,j)\in[\![1,n]\!]^2, i\neq j\Rightarrow B_i\wedge B_j=1$ et $\forall i\in[\![1,n]\!], B_i|C)\Rightarrow \prod_{i=1}^n B_i\Big|C$

⇒ Facteurs (relativement) premiers

⇒ PPCM

Factorisation

Proposition - Factorisation (division)

Soit $P \in \mathbb{K}[X]$. Si $x_1, \ldots, x_p$ sont p racines distinctes de P de multiplicités respectives égales à $m_1, \ldots, m_p$, alors $\prod_{i=1}^{p} (X - x_i)^{m_i}$ divise P.

Factorisation

Proposition - Factorisation (division)

Soit $P \in \mathbb{K}[X]$. Si $x_1, \ldots, x_p$ sont p racines distinctes de P de multiplicités respectives égales à $m_1, \ldots, m_p$, alors $\prod_{i=1}^{p}(X - x_i)^{m_i}$ divise P.

Démonstration

Factorisation

Proposition - Factorisation (division)

Soit $P \in \mathbb{K}[X]$. Si $x_1, \ldots, x_p$ sont p racines distinctes de P de multiplicités respectives égales à $m_1, \ldots, m_p$, alors $\prod_{i=1}^{p}(X - x_i)^{m_i}$ divise P.

Démonstration

Corollaire - Nombre maximal de racines

Un polynôme non nul de degré n possède au plus n racines comptées avec leur multiplicité (c'est-à-dire comptées autant de fois que leur multiplicité).

Factorisation

Proposition - Factorisation (division)

Soit $P \in \mathbb{K}[X]$. Si $x_1, \ldots, x_p$ sont p racines distinctes de P de multiplicités respectives égales à $m_1, \ldots, m_p$, alors $\prod_{i=1}^{p}(X - x_i)^{m_i}$ divise P.

Démonstration

Corollaire - Nombre maximal de racines

Un polynôme non nul de degré n possède au plus n racines comptées avec leur multiplicité (c'est-à-dire comptées autant de fois que leur multiplicité).

Démonstration

Factorisation

Proposition - Factorisation (division)

Soit $P \in \mathbb{K}[X]$. Si $x_1, \ldots, x_p$ sont p racines distinctes de P de multiplicités respectives égales à $m_1, \ldots, m_p$, alors $\prod_{i=1}^{p}(X - x_i)^{m_i}$ divise P.

Démonstration

Corollaire - Nombre maximal de racines

Un polynôme non nul de degré n possède au plus n racines comptées avec leur multiplicité (c'est-à-dire comptées autant de fois que leur multiplicité).

Démonstration

<u>Exercice</u>

Trouver les polynômes $P \in \mathbb{R}_7[X]$ tels que

$(X+7) \times P(X) = (X-5) \times P(X+2)$

⇒ Facteurs (relativement) premiers

⇒ PPCM

Extension

La notion de PGCD peut être étendue à un nombre fini de polynômes :

Proposition - PGCD de plusieurs polynômes

Soient $k \in \mathbb{N}^*$, $k \geqslant 2$, et $(A_1, A_2, \ldots, A_k) \in \mathbb{K}[X]^k$. Il existe un unique polynôme nul ou unitaire P dont les diviseurs sont exactement les diviseurs communs à tous les A_i, c'est-à-dire tel que

$$\forall n \in \mathbb{Z}, (\forall i \in [\![1, k]\!], T | A_i) \Leftrightarrow T | P.$$

En fait, on a $\mathscr{D}(P) = \bigcap_{i=1}^{k} \mathscr{D}(A_i)$.

On l'appelle PGCD de $A_1, \ldots, A_k$, noté $A_1 \wedge \ldots \wedge A_k$ ou $\bigwedge_{i=1}^k A_i$.

On a de plus l'identité de Bézout :

$\exists (U_1, \ldots, U_k) \in \mathbb{K}[X]^k \,|\, P = \sum_{i=1}^k U_i A_i$.

Encore : $A_1\mathbb{K}[X] + \cdots + A_k\mathbb{K}[X]$ est l'idéal engendré $P\mathbb{K}[X]$.

Extension

La notion de PGCD peut être étendue à un nombre fini de polynômes :

Proposition - PGCD de plusieurs polynômes

Soient $k \in \mathbb{N}^*$, $k \geqslant 2$, et $(A_1, A_2, \ldots, A_k) \in \mathbb{K}[X]^k$. Il existe un unique polynôme nul ou unitaire P dont les diviseurs sont exactement les diviseurs communs à tous les A_i, c'est-à-dire tel que

$$\forall n \in \mathbb{Z}, (\forall i \in [\![1,k]\!], T | A_i) \Leftrightarrow T | P.$$

En fait, on a $\mathscr{D}(P) = \displaystyle\bigcap_{i=1}^{k} \mathscr{D}(A_i)$.

On l'appelle PGCD de $A_1, \ldots, A_k$, noté $A_1 \wedge \ldots \wedge A_k$ ou $\bigwedge_{i=1}^{k} A_i$.
On a de plus l'identité de Bézout :

$\exists (U_1, \ldots, U_k) \in \mathbb{K}[X]^k \,|\, P = \sum_{i=1}^{k} U_i A_i$.

Encore : $A_1\mathbb{K}[X] + \cdots + A_k\mathbb{K}[X]$ est l'idéal engendré $P\mathbb{K}[X]$.

Démonstration

Autre définition : par récurrence

La proposition suivante permet de justifier la notation associative $\wedge_{i=1}^{k} A_i$.

Autre définition : par récurrence

La proposition suivante permet de justifier la notation associative $\wedge_{i=1}^{k} A_i$.

Proposition - PGCD par récurrence

Soient $k \in \mathbb{N}^*$, $k \geqslant 2$ et $(A_1, A_2, \dots, A_k) \in (\mathbb{K}[X])^k$,

$$\bigwedge_{i=1}^{k} A_i = \left(\bigwedge_{i=1}^{k-1} A_i\right) \wedge A_k$$

Autre définition : par récurrence

La proposition suivante permet de justifier la notation associative $\wedge_{i=1}^{k} A_i$.

Proposition - PGCD par récurrence

Soient $k \in \mathbb{N}^*$, $k \geqslant 2$ et $(A_1, A_2, \ldots, A_k) \in (\mathbb{K}[X])^k$,

$$\bigwedge_{i=1}^{k} A_i = \left(\bigwedge_{i=1}^{k-1} A_i \right) \wedge A_k$$

Démonstration

Polynômes premiers entre eux

Définition - Polynômes premiers entre eux (dans leur ensemble)

Les polynômes $A_1, \ldots, A_k$ sont dits **premiers entre eux dans leur ensemble** si leur PGCD vaut 1.

Polynômes premiers entre eux

Définition - Polynômes premiers entre eux (dans leur ensemble)

Les polynômes $A_1, \ldots, A_k$ sont dits **premiers entre eux dans leur ensemble** si leur PGCD vaut 1.

Attention. Polynômes premiers entre eux

Une famille de polynômes premiers entre eux deux à deux est une famille de polynômes premiers entre eux dans leur ensemble.
La réciproque est fausse.
On peut le démontrer avec une décomposition de Bézout

Théorème de Bézout (plusieurs polynômes)

Proposition - Théorème de Bézout

Soient $A_1,\ldots,A_k$ des polynômes. Alors

$$\bigwedge_{i=1}^{k} A_i = 1 \Leftrightarrow \exists (U_1,\ldots,U_k) \in \mathbb{K}[X]^k \mid \sum_{i=1}^{k} U_i A_i = 1$$

Théorème de Bézout (plusieurs polynômes)

Proposition - Théorème de Bézout

Soient $A_1, \ldots, A_k$ des polynômes. Alors

$$\bigwedge_{i=1}^{k} A_i = 1 \Leftrightarrow \exists (U_1, \ldots, U_k) \in \mathbb{K}[X]^k \mid \sum_{i=1}^{k} U_i A_i = 1$$

Démonstration

⇒ Facteurs (relativement) premiers

⇒ PPCM

Définitions

Heuristique - PPCM

Soient A et B deux polynômes non nuls.
L'ensemble des multiples communs à A et B est non vide (contient AB) donc l'ensemble des degrés des multiples communs à A et B est une partie non vide de $\mathbb{N}$ donc admet un plus petit élément.
Un multiple de A et B de plus petit degré est appelé un $PPCM$ (Plus Petit Commun Multiple) de A et B.

Définitions

Heuristique - PPCM

Soient A et B deux polynômes non nuls.
L'ensemble des multiples communs à A et B est non vide (contient AB) donc l'ensemble des degrés des multiples communs à A et B est une partie non vide de $\mathbb{N}$ donc admet un plus petit élément.
Un multiple de A et B de plus petit degré est appelé un $PPCM$ (Plus Petit Commun Multiple) de A et B.

Définition - Caractérisation essentielle du PPCM

Soit $(A,B) \in \mathbb{K}[X]^2$. Il existe un unique polynôme M nul ou unitaire dont les multiples sont exactement les multiples communs à A et B, c'est-à-dire tel que

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

M est appelé **le** $PPCM$ de A et B, noté $A \vee B$.

Définitions

Heuristique - PPCM

Soient A et B deux polynômes non nuls.
L'ensemble des multiples communs à A et B est non vide (contient AB) donc l'ensemble des degrés des multiples communs à A et B est une partie non vide de $\mathbb{N}$ donc admet un plus petit élément.
Un multiple de A et B de plus petit degré est appelé un $PPCM$ (Plus Petit Commun Multiple) de A et B.

Définition - Caractérisation essentielle du PPCM

Soit $(A,B) \in \mathbb{K}[X]^2$. Il existe un unique polynôme M nul ou unitaire dont les multiples sont exactement les multiples communs à A et B, c'est-à-dire tel que

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

M est appelé **le** $PPCM$ de A et B, noté $A \vee B$.

Démonstration

Autre caractérisation

Une autre caractérisation essentielle

Proposition - Autre caractérisation

M est un PPCM de A et B si et seulement si

$$A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X]$$

Autre caractérisation

Une autre caractérisation essentielle

Proposition - Autre caractérisation

M est un PPCM de A et B si et seulement si

$$A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X]$$

Démonstration

⇒ Facteurs (relativement) premiers

⇒ PPCM

Relation

Proposition - Relation PGCD et PPCM

Soient $A, B \in \mathbb{K}[X]$ non nuls.

- si $A \wedge B = 1$ alors $\exists \lambda \in \mathbb{K}^* \mid AB = \lambda(A \vee B)$.
- dans le cas général, $\exists \lambda \in \mathbb{K}^* \mid AB = \lambda(A \wedge B) \times (A \vee B)$.

Relation

Proposition - Relation PGCD et PPCM

Soient $A, B \in \mathbb{K}[X]$ non nuls.

- si $A \wedge B = 1$ alors $\exists \lambda \in \mathbb{K}^* \,|\, AB = \lambda(A \vee B)$.
- dans le cas général, $\exists \lambda \in \mathbb{K}^* \,|\, AB = \lambda(A \wedge B) \times (A \vee B)$.

Démonstration

Relation

Proposition - Relation PGCD et PPCM

Soient $A, B \in \mathbb{K}[X]$ non nuls.

- si $A \wedge B = 1$ alors $\exists \lambda \in \mathbb{K}^* \,|\, AB = \lambda(A \vee B)$.
- dans le cas général, $\exists \lambda \in \mathbb{K}^* \,|\, AB = \lambda(A \wedge B) \times (A \vee B)$.

Démonstration

Heuristique. Décomposition

On peut retenir que si $A = (A \wedge B)A'$, et $B = (A \wedge B)B'$,
alors A' et B' sont premiers entre eux,
et alors $\lambda A \vee B = (A \wedge B)A'B'$.
Et donc : $A \times B = (A \wedge B)A' \times (A \wedge B)B' = (A \wedge B) \times (A \wedge B)A'B' = \lambda(A \wedge B) \times (A \vee B)$

Exercice

<u>Exercice</u>

Déterminer le PGCD, le PPCM et un couple de Bezout lorsque $A = X^3 + 3X^2 + 3X + 2$ et $B = X^5 + 3X^4 + 2X^3 - 2X^2 - 3X + 2$.

Conclusion

Objectifs

$\Rightarrow$ Facteurs (relativement) premiers

$\Rightarrow$ PPCM

Conclusion

Objectifs

$\Rightarrow$ Facteurs (relativement) premiers

- Facteurs relativement premiers : lemmes de Gauss

Conclusion

Objectifs

$\Rightarrow$ Facteurs (relativement) premiers

- Facteurs relativement premiers : lemmes de Gauss
  - $A|BC$ et $A \wedge B = 1 \Longrightarrow A|C$

Conclusion

Objectifs

$\Rightarrow$ Facteurs (relativement) premiers

- Facteurs relativement premiers : lemmes de Gauss
  - $A|BC$ et $A \wedge B = 1 \Longrightarrow A|C$
  - $A \wedge C$ et $B \wedge C = 1 \Longrightarrow AB \wedge C = 1$

Conclusion

Objectifs

$\Rightarrow$ Facteurs (relativement) premiers

- Facteurs relativement premiers : lemmes de Gauss
  - $A|BC$ et $A \wedge B = 1 \Longrightarrow A|C$
  - $A \wedge C$ et $B \wedge C = 1 \Longrightarrow AB \wedge C = 1$
  - $(A \wedge B = 1, A|C, B|C) \Rightarrow AB|C$

Conclusion

Objectifs

$\Rightarrow$ Facteurs (relativement) premiers

- Facteurs relativement premiers : lemmes de Gauss
  - $A|BC$ et $A \wedge B = 1 \Longrightarrow A|C$
  - $A \wedge C$ et $B \wedge C = 1 \Longrightarrow AB \wedge C = 1$
  - $(A \wedge B = 1, A|C, B|C) \Rightarrow AB|C$
- Une sorte de décomposition en facteurs relativement premiers : les polynômes $(X-a)^k$ pourraient jouer ce rôle

Conclusion

Objectifs

⇒ Facteurs (relativement) premiers

- Facteurs relativement premiers : lemmes de Gauss
  - $A|BC$ et $A \wedge B = 1 \Longrightarrow A|C$
  - $A \wedge C$ et $B \wedge C = 1 \Longrightarrow AB \wedge C = 1$
  - $(A \wedge B = 1, A|C, B|C) \Rightarrow AB|C$
- Une sorte de décomposition en facteurs relativement premiers : les polynômes $(X-a)^k$ pourraient jouer ce rôle
- Extension à plusieurs polynômes

Conclusion

Objectifs

$\Rightarrow$ Facteurs (relativement) premiers

$\Rightarrow$ PPCM

Conclusion

Objectifs

⇒ Facteurs (relativement) premiers

⇒ PPCM

- Plus petit multiple commun de A et B. Définition aux associés près.

Conclusion

Objectifs

$\Rightarrow$ Facteurs (relativement) premiers

$\Rightarrow$ PPCM

- Plus petit multiple commun de A et B. Définition aux associés près.
- Critères essentielles :
  $M = A \vee B \Longleftrightarrow \forall P \in \mathbb{K}[X], (A|P \text{ et } B|P) \Leftrightarrow M|P$
  ou $A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X]$

Conclusion

Objectifs

⇒ Facteurs (relativement) premiers

⇒ PPCM

- Plus petit multiple commun de A et B. Définition aux associés près.
- Critères essentielles :
  $M = A \vee B \iff \forall P \in \mathbb{K}[X], (A|P \text{ et } B|P) \Leftrightarrow M|P$
  ou $A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X]$
- Relation avec le PGCD : $A \times B = (A \wedge B) \times (A \vee B)$

Conclusion

Objectifs

⇒ Facteurs (relativement) premiers

⇒ PPCM

Pour la prochaine fois

- Lecture du cours : chapitre 19 : Anneau euclidien des polynômes
  4. Polynômes irréductibles
- Exercice n° 689 & 691