6.5 Arithmétique de $\mathbb{K}[X]$

Nous avons besoin, dans ce paragraphe, de la notion **d'idéal principal**. La notion d'idéal et d'anneau principal a déjà été donnée en 2.2.2. Nous nous proposons de la redonner dans les définitions ci-après

6.5.1 Rappel d'idéal principal

Soit $\mathcal{A}$ un anneau commutatif
On appelle idéal principal de $\mathcal{A}$ l'idéal $[b]$ des multiples d'un élément quelconque $b \in \mathcal{A}$, c'est à dire :

$$[b] = \{z \in \mathcal{A} \text{ où } z = kb \text{ où } k \in \mathcal{A}\}$$

Remarque 14 :

1. Les idéaux principaux d'un anneau intègre $\mathcal{A}$ sont liés aux propriétés de la divisibilité dans $\mathcal{A}$.
   Ainsi, pour $a \in \mathcal{A}$ et $b \in \mathcal{A}$, $[a] \subset [b]$ signifie qu'il existe $k \in \mathcal{A}$ tel que $a = kb$ et donc, b divise a
   Par exemple, dans l'anneau $\mathbb{Z}$, nous avons $6\mathbb{Z} \subset 2\mathbb{Z}$, puisque tout élément de $6\mathbb{Z}$ s'écrit $6k = 2(3k)$ avec $k \in \mathbb{Z}$; en particulier, $6 \in 2\mathbb{Z}$ puisque $6 = 2 \times 3$ et donc 2 divise 6
2. Un diviseur propre $b \in \mathcal{A}$ de $a \in \mathcal{A}$ détermine un idéal plus grand que $[a]$, c'est à dire $[a] \subset [b]$
3. Pour $a \in \mathcal{A}$ et $b \in \mathcal{A}$, nous avons $[a] = [b]$ si et seulement si a et b sont associés dans $\mathcal{A}$
4. $[a] = \mathcal{A}$ si et seulement si a est inversible dans $\mathcal{A}$

6.5.2 Rappel d'anneau principal

Un anneau $\mathcal{A}$ est dit anneau principal s'il est intègre et si tout idéal de $\mathcal{A}$ est principal

Exemple 4 :

Un exemple d'anneau principal est $\mathbb{Z}$, l'ensemble des entiers relatifs, puisque, dans $\mathbb{Z}$, tout idéal est de la forme $n\mathbb{Z}$

6.5.3 Théorème

Si $\mathbb{K}$ est un corps, alors, $\mathbb{K}[X]$ est un anneau principal, ce qui veut dire :

1. Si I est un idéal de $\mathbb{K}[X]$, alors, il existe $P \in \mathbb{K}[X]$ tel que I soit l'ensemble des multiples de P, c'est à dire tel que $I = [P] = P \times \mathbb{K}[X]$
2. P est déterminé de manière unique, à la multiplication par une constante non nulle près. *(On écrit $I = [P] = P \times \mathbb{K}[X]$; si P est unitaire, il est unique)*

Démonstration

1. Si $I = \{0\}$, alors, le théorème est évident
2. Supposons, maintenant que $I \neq \{0\}$
   Soit donc $P \neq 0$ tel que $P \in I$ et on suppose que $\deg P$ est minimal ; il est possible d'en trouver un, puisque $\deg P \in \mathbb{N}$
   (a) Par definition de ce qu'est un idéal, tous les multiples de P sont dans cet idéal I ; on peut donc écrire que $[P] \subset I$
   (b) Réciproquement, soit $B \in I$ et montrons que B est un multiple de P. Nous aurons alors $I \subset [P]$.
   Effectuons la division euclidienne de B par P.
   Nous avons alors $B = PQ + R$ avec $\deg R < \deg P$.

De $B = PQ + R$, nous déduisons que $R = B - PQ$. Comme I est un idéal, alors $PQ \in I$. Comme I, idéal est aussi un groupe, $B - PQ \in I$
Si $R \neq 0$, alors $\deg R \geqslant 0$ et donc $\deg P$ n'est pas minimal. Il y a donc contradiction.
D'où $R = 0$ et $B = PQ$, ce qui veut dire que B est un multiple de P

Ainsi $I = [P]$ et $\mathbb{K}[X]$ est un anneau principal.

3. Il est évident que si P est le polynôme de I tel que $\deg P$ soit minimal, alors, pour tout $\lambda \in \mathbb{K}^*$, $\lambda P \in I$ et $\deg(\lambda P) = \deg P$
4. Si P' est un polynôme tel que $I = [P]$ soit l'ensemble des multiples de P', c'est à dire tels que $I = [P']$, alors $P = P'Q$ et $P' = PQ_1$, c'est à dire que P et P' sont associés, c'est à dire $P' = \lambda P$

6.5.4 Définition du pgcd de 2 polynômes

$\mathbb{K}$ est un corps et $\mathbb{K}[X]$ son anneau de polynômes. Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$
Alors, $D \in \mathbb{K}[X]$ est appelé plus grand diviseur commun ou pgcd des 2 polynômes $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$ si pour tout $C \in \mathbb{K}[X]$

$$((D \div A)(D \div B)(C \div A)(C \div B)) \Longrightarrow (C \div B)$$

On note $D = \text{pgcd}(A, B)$

Remarque 15 :

1. Cette définition montre que $D = \text{pgcd}(A, B)$ est multiple de tout diviseur commun à A et B
2. 2 pgcd différents de A et B sont associés :
   En effet, $D = \text{pgcd}(A, B)$ et supposons qu'il existe $D_1 \in \mathbb{K}[X]$ tel que $D_1 = \text{pgcd}(A, B)$. Alors, de la propriété de pgcd, D divise D_1 et D_1 divise D et sont donc associés, c'est à dire qu'il existe $\lambda \in \mathbb{K}^*$ tels que $D = \lambda D_1$

6.5.5 Théorème : existence du pgcd

$\mathbb{K}$ est un corps et $\mathbb{K}[X]$ son anneau de polynômes. Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$

1. Il existe un élément $D \in \mathbb{K}[X]$ tel que D divise A et B
2. Tous les diviseurs de D sont les diviseurs communs à A et à B
3. D est donc le pgcd des 2 polynômes A et B et est déterminé de manière unique, à la multiplication par une constante près
4. Si $A \neq 0$ et si $B \neq 0$, alors le degré de D majore celui de tous les diviseurs communs à A et B
5. Il existe $U \in \mathbb{K}[X]$ et $V \in \mathbb{K}[X]$ tels que $AU + BV = D$

Démonstration

Soient donc $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$

1. (a) On appelle $\mathcal{I} = \{P \in \mathbb{K}[X] \text{ tels que il existe } Q \in \mathbb{K}[X] \text{ et } R \in \mathbb{K}[X] \text{ tels que } P = AQ + BR\}$
   i. $\mathcal{I}$ est un sous-groupe de $(\mathbb{K}[X], +)$
   ▷ $\mathcal{I} \neq \emptyset$ puisque $0 \in \mathcal{I}$.
   En effet, $0 = 0 \times A + 0 \times B$ et donc $0 \in \mathcal{I}$
   ▷ Si $P_1 \in \mathcal{I}$ et $P_2 \in \mathcal{I}$, alors :

$$P_1 - P_2 = (AQ_1 + BR_1) - (AQ_2 + BR_2) = A(Q_1 - Q_2) + B(R_1 - R_2)$$

   Donc $P_1 - P_2 \in \mathcal{I}$
   Donc $\mathcal{I}$ est un sous-groupe de $(\mathbb{K}[X], +)$
   ii. D'autre part, soit $P \in \mathcal{I}$ et $L \in \mathbb{K}[X]$, alors $P = AQ + BR$ et

$$LP = L(AQ + BR) = A(QL) + B(RL)$$

   et donc, $LP \in \mathcal{I}$

Nous en déduisons que $\mathcal{I}$ est un idéal de $\mathbb{K}[X]$

(b) $\mathbb{K}$ étant un corps, $\mathbb{K}[X]$ est un anneau principal ; il existe donc $D \in \mathbb{K}[X]$ tel que $\mathcal{I} = [D] = D \times \mathbb{K}[X]$, c'est à dire :

$$\mathcal{I} = [D] = D \times \mathbb{K}[X] = \{P \in \mathbb{K}[X] \text{ tels que } P = QD \text{ où } Q \in \mathbb{K}[X]\}$$

C'est à dire que $\mathcal{I}$ est l'ensemble des multiples d'un polynôme $D \in \mathbb{K}[X]$. Ainsi, le polynôme D divise A et B ; c'est un diviseur commun à A et B

2. Nous avons $D = \text{pgcd}(A, B)$
   - ▷ Tout diviseur commun à A et B divise D. En effet :
     Soit $C \in \mathbb{K}[X]$ un diviseur commun à A et B. Alors $A = A_1C$ et $B = B_1C$.
     Comme $D = SA + TB = S(A_1C) + T(B_1C) = C(A_1S + B_1T)$, le polynôme C divise D
   - ▷ Plus généralement, C divise tous les éléments de la forme $AP + BQ$.

   D est donc le pgcd de A et B

   Remarquons que si $H \in \mathbb{K}[X]$ divise D, alors H divise tous les éléments de $\mathcal{I} = [D]$, c'est à dire tous les polynômes de la forme $AP + BQ$. et que, si H divise tous les éléments de la forme $AP + BQ$, alors H divise D, puisque $D \in \mathcal{I}$
3. Soit C un diviseur commun à A et B. Comme $D = \text{pgcd}(A, B)$, alors C divise D et donc $\deg C \leqslant \deg D$
4. Comme $D \in \mathcal{I}$, il existe $U \in \mathbb{K}[X]$ et $V \in \mathbb{K}[X]$ tels que $D = AU + BV$

6.5.6 Proposition

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ son anneau de polynômes. Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$ 2 polynômes tels que $B \neq 0$
Alors, si $A = BQ + R$, les diviseurs communs à A et B sont aussi les diviseurs communs de B et de R
En particulier, $\text{pgcd}(A, B) = \text{pgcd}(B, R)$

Démonstration

Si $B \in \mathbb{K}[X]$ est le polynôme nul, alors tous les diviseurs de A sont aussi ceux de B, puisque si $A = \Lambda A_1$, alors $0 = \Lambda 0$.
Supposons donc $B \in \mathbb{K}[X]$ et $B \neq 0$ et effectuons donc la division euclidienne de A par B. Nous avons donc :

$$A = BQ + R \text{ avec } \deg R < \deg B$$

1. Soit $C \in \mathbb{K}[X]$ un diviseur commun à A et B.
   Alors, il existe $A_1 \in \mathbb{K}[X]$ et $B_1 \in \mathbb{K}[X]$ tels que $A = CA_1$ et $B = CB_1$ et donc, alors :

   $$A = BQ + R \iff CA_1 = B_1C + R \iff R = CA_1 - B_1C = C(A_1 - B_1)$$

   Ce qui montre que C divise B et R.
   Ainsi, les diviseurs communs à A et B sont aussi diviseurs de B et R
2. Soit $D \in \mathbb{K}[X]$ un diviseur commun à R et B.
   Alors, il existe $R_1 \in \mathbb{K}[X]$ et $B_1 \in \mathbb{K}[X]$ tels que $R = DR_1$ et $B = DB_1$ et donc, alors :

   $$A = BQ + R \iff A = B_1D + DR_1 \iff A = D(B_1 + R_1)$$

   Ce qui montre que D divise B et A.
   Ainsi, les diviseurs communs à R et B sont aussi diviseurs de B et A

6.5.7 Algorithme de recherche du pgcd

Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$ 2 polynômes tels que $B \neq 0$.

1. Effectuons la division euclidienne de A par B.
   - ▷ Nous avons alors $A = BQ + R_1$ avec $\deg R_1 < \deg B$
   - ▷ Si $R_1 = 0$, alors B divise A et $\text{pgcd}(A, B) = B$
   - ▷ Si $R_1 \neq 0$, alors, d'après la proposition précédente, $\text{pgcd}(A, B) = \text{pgcd}(B, R_1)$
2. Effectuons la division euclidienne de B par R_1
   - ▷ Nous avons alors $B = R_1Q + R_2$ avec $\deg R_2 < \deg R_1$
   - ▷ Si $R_2 = 0$, alors R_1 divise B et $\text{pgcd}(R_1, B) = R_1$. Mais nous avons aussi $\text{pgcd}(A, B) = \text{pgcd}(B, R_1)$, c'est à dire que $\text{pgcd}(A, B) = R_1$
   - ▷ Si $R_2 \neq 0$, alors, d'après la proposition précédente, $\text{pgcd}(A, B) = \text{pgcd}(B, R_1) = \text{pgcd}(R_1, R_2)$
3. Nous pouvons ainsi continuer longtemps, jusque l'étape n, où nous avons $R_{n-1} = R_nQ_n + R_{n+1}$ avec $\deg R_{n+1} < \deg R_n$ et
$$\text{pgcd}(A, B) = \text{pgcd}(B, R_1) = \text{pgcd}(R_1, R_2) = \cdots = \text{pgcd}(R_{n+1}, R_n)$$
Nous avons aussi $\deg R_{n+1} < \deg R_n < \cdots < \deg R_1 < \deg B$, c'est à dire une suite d'entiers décroissante, l'algorithme s'arrête au bout d'un nombre fini N d'étapes avec $R_{N+1} = 0$
4. **Résultat :**
   Le polynôme R_N obtenu à la fin de l'algorithme est un pgcd de A et B *(c'est le dernier reste non nul, si A et B sont différents de 0)*

Exemple 5 :

Quel est le pgcd de $X^3 + X + 1$ et de $X^2 + X + 1$?

1. On effectue la division euclidienne de $X^3 + X + 1$ par $X^2 + X + 1$:
$$X^3 + X + 1 = (X^2 + X + 1)(X - 1) + X + 2$$
2. Maintenant, nous faisons la division euclidienne de $X^2 + X + 1$ par $X + 2$:
$$X^2 + X + 1 = (X + 2)(X - 1) + 3$$
3. Et, pour terminer
$$X + 2 = 3 \times \left(\frac{1}{3}X + \frac{2}{3}\right) + 0$$

L'un des pgcd de $X^3 + X + 1$ et de $X^2 + X + 1$ est 3, et si nous considérons uniquement les polynômes unitaires, le pgcd de $X^3 + X + 1$ et de $X^2 + X + 1$ est 1

Exercice 10 :

Déterminer les pgcd des paires de polynômes A et B suivantes :

1. $A = X^6 + 2X^4 - 4X^3 - 3X^2 + 8X - 5$ et $B = X^5 + X^2 - X + 1$
2. $A = X^4 - 3X^3 + 3X^2 - 3X + 2$ et $B = X^3 - 2X^2 - X + 2$
3. $A = X^5 + X^4 - X^3 - 3X^2 - 3X - 1$ et $B = X^4 - 2X^3 - X^2 - 2X + 1$
4. $A = X^4 - 4X^3 + 1$ et $B = X^3 - 3X^2 + 1$
5. $A = X^5 + 3X^4 + X^3 + X^2 + 3X + 1$ et $B = X^4 + 2X^3 + X + 2$
6. $A = X^5 + 5X^4 + 9X^3 + 7X^2 + 5X + 3$ et $B = X^4 + 2X^3 + 2X^2 + X + 1$

6.5.8 Proposition

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ son anneau de polynômes. Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$ 2 polynômes tels que $B \neq 0$. On appelle D le pgcd de A et de B
Alors pour tout polynôme $P \in \mathbb{K}[X]$, non nul, le pgcd de AP et BP est le polynôme DP que nous pouvons écrire :
$$\text{pgcd}(PA, PB) = P \times \text{pgcd}(A, B)$$

Démonstration

On peut prendre cette démonstration comme un exercice résolu
Soit $P \in \mathbb{K}[X]$ avec $P \neq 0$.

1. D étant le pgcd de A et de B, il existe alors $A_1 \in \mathbb{K}[X]$ et $B_1 \in \mathbb{K}[X]$ tels que $A = DA_1$ et $B = DB_1$. Et donc $AP = (DA_1)P = A_1(DP)$, nous montrons, là, que DP divise AP.
   Nous démontrerions de même que DP divise BP
   DP est donc un diviseur commun à AP et BP
2. Montrons que si $Q \in \mathbb{K}[X]$ divise les polynômes AP et BP, alors Q divise aussi DP
   Si Q divise AP et BP, il existe alors $Q_1 \in \mathbb{K}[X]$ et $Q_2 \in \mathbb{K}[X]$ tels que $AP = QQ_1$ et $BP = QQ_2$.
   D étant le pgcd de A et de B il existe $U \in \mathbb{K}[X]$ et $V \in \mathbb{K}[X]$ tels que $D = AU + BV$.
   Nous avons donc $DP = APU + BPV = QQ_1U + QQ_2V = Q(Q_1U + Q_2V)$.
   Donc Q divise DP

D'après la définition 6.5.4, DP est donc le pgcd de AP et BP

Remarque 16 :

Montrons aussi que si $Q \in \mathbb{K}[X]$ divise le polynôme DP, alors Q divise aussi AP et BP
D étant le pgcd de A et de B, il existe alors $A_1 \in \mathbb{K}[X]$ et $B_1 \in \mathbb{K}[X]$ tels que $A = DA_1$ et $B = DB_1$.
Q divisant DP, il existe $Q_1 \in \mathbb{K}[X]$ tel que $DP = QQ_1$. Donc :

$$AP = (A_1D)P = A_1(DP) = A_1(QQ_1) = (A_1Q_1)Q$$

Ce qui montre que Q divise AP
Nous aurions aussi $BP = (B_1Q_1)Q$ et Q divise aussi BP
Ainsi, nous venons de démontrer que tout diviseur de DP divise aussi AP et BP
L'ensemble des diviseurs de DP est aussi celui des diviseurs communs à AP et BP

6.5.9 Proposition

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ son anneau de polynômes. Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$ 2 polynômes tels que $B \neq 0$. On appelle D le pgcd de A et de B
Soit $Q \in \mathbb{K}[X]$ tel que $A = QA_1$ et $B = QB_1$. Alors :

1. Q divise D
2. Si $D_1 \in \mathbb{K}[X]$ est tel que $D = QD_1$, alors, D_1 est le pgcd de A_1 et de B_1

Démonstration

Une nouvelle fois, on peut prendre cette démonstration comme un exercice résolu

1. Si $Q \in \mathbb{K}[X]$ tel que $A = QA_1$ et $B = QB_1$, alors, d'après la définition 6.5.4, Q est un diviseur de D.
2. Soit, maintenant, $D_1 \in \mathbb{K}[X]$ tel que $D = QD_1$.
   - ▷ D étant le pgcd de A et B, il existe $U \in \mathbb{K}[X]$ et $V \in \mathbb{K}[X]$ tels que $D = AU + BV$ et donc $QD_1 = QA_1U + QB_1V$, c'est à dire $D_1 = A_1U + B_1V$
   - ▷ Soit D_1^1 le pgcd de A_1 et B_1
     Alors, d'après la proposition 6.5.8, QD_1^1 est le pgcd de QA_1 et QB_1, c'est à dire que QD_1^1 est le pgcd de A et B et donc QD_1^1 et D sont associés.
     Nous avons alors :

$$\deg\left(QD_1^1\right) = \deg D = \deg QD_1 \Longrightarrow \deg Q + \deg D_1^1 = \deg Q + \deg D_1 \Longrightarrow \deg D_1^1 = \deg D_1$$

     D_1 et D_1^1 sont donc associés

6.5.10 Polynômes premiers entre eux

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ son anneau de polynômes. Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$ 2 polynômes
On dit que A et B sont **premiers entre eux** si et seulement si le pgcd de A et B est 1 (ou $\lambda \in \mathbb{K}^*$)
Autrement dit :
A et B sont premiers entre eux si et seulement si ils n'ont aucun diviseurs communs non triviaux

Exemple 6 :

Nous avons montré que le pgcd de X^3+X+1 et de X^2+X+1 était 1. Ce sont donc des polynômes premiers entre eux.

6.5.11 Identité de Bezout

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ son anneau de polynômes. Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$ 2 polynômes
A et B sont premiers entre eux si et seulement si il existe 2 polynômes $U \in \mathbb{K}[X]$ et $V \in \mathbb{K}[X]$ tels que $AU+BV=1$

Démonstration

1. Supposons A et B sont premiers entre eux.
   1 étant le pgcd de A et B, d'après la proposition 6.5.5, il existe $U \in \mathbb{K}[X]$ et $V \in \mathbb{K}[X]$ tels que $1 = AU+BV$
2. Réciproquement, supposons qu'il existe $U \in \mathbb{K}[X]$ et $V \in \mathbb{K}[X]$ tels que $1 = AU+BV$
   Soit $D = \text{pgcd}(A,B)$, unitaire.
   Il existe $A_1 \in \mathbb{K}[X]$ et $B_1 \in \mathbb{K}[X]$ tels que $A = DA_1$ et $B = DB_1$ et donc :
   $$1 = AU+BV = DA_1U + DB_1V = D(A_1U+B_1V)$$
   Ce qui veut dire que D divise 1 et donc $\deg D = 0$. D est donc un polynôme constant, et comme D est unitaire, $D=1$.
   Ainsi, A et B sont premiers entre eux

6.5.12 Corollaire

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ son anneau de polynômes. Soient $A \in \mathbb{K}[X]$, $B_1 \in \mathbb{K}[X]$ et $B_2 \in \mathbb{K}[X]$ 3 polynômes
Si A est premier avec B_1 et si A est premier avec B_2, alors A est premier avec le produit B_1B_2

Démonstration

- ▷ Si A est premier avec B_1, il existe donc $Q_1 \in \mathbb{K}[X]$ et $R_1 \in \mathbb{K}[X]$ tels que $AQ_1+R_1B_1=1$
- ▷ De même, si A est premier avec B_2, il existe donc $Q_2 \in \mathbb{K}[X]$ et $R_2 \in \mathbb{K}[X]$ tels que $AQ_2+R_2B_2=1$
- ▷ Alors :

$$\begin{aligned} 1 = & \ (AQ_1+R_1B_1)(AQ_2+R_2B_2) = A^2Q_1Q_2 + AQ_1R_2B_2 + R_1B_1AQ_2 + R_1B_1R_2B_2 \\ = & \ A(AQ_1Q_2 + Q_1R_2B_2 + R_1B_1Q_2) + (R_1R_2)B_1B_2 \end{aligned}$$

Il existe donc des polynômes $U \in \mathbb{K}[X]$ et $V \in \mathbb{K}[X]$ tels que $AU + B_1B_2V = 1$
A est donc premier avec le produit B_1B_2

Remarque 17 :

Il est très possible de généraliser :

1. Si $A \in \mathbb{K}[X]$ est premier avec $B_1, B_2, \ldots, B_n$, alors A est premier avec $B_1B_2\cdots B_n$
2. Si $A \in \mathbb{K}[X]$ est premier avec B, alors, pour tout $n \in \mathbb{N}^*$ A est premier avec B^n

3. Si $A \in \mathbb{K}[X]$ est premier avec B, alors, pour tout $n \in \mathbb{N}^*$ et tout $m \in \mathbb{N}^*$, A^m est premier avec B^n

Les démonstrations se font, sans difficulté, par récurrence.

6.5.13 Proposition

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ son anneau de polynômes. Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$ 2 polynômes tels que $B \neq 0$. On appelle D le pgcd de A et de B
Soient $A_1 \in \mathbb{K}[X]$ et $B_1 \in \mathbb{K}[X]$ tels que $A = DA_1$ et $B = DB_1$. Alors : A_1 et B_1 sont premiers entre eux

Démonstration

Comme $D \div A$ et $D \div B$, nous pouvons donc écrire $A = DA_1$ et $B = DB_1$ avec $A_1 \in \mathbb{K}[X]$ et $B_1 \in \mathbb{K}[X]$.
D étant le pgcd de A et de B, il existe $U \in \mathbb{K}[X]$ et $V \in \mathbb{K}[X]$ tels que $D = AU + BV$. En remplaçant, nous obtenons :

$$D = AU + BV \iff D = (DA_1)U + (DB_1V) = D(A_1U + B_1V) \iff A_1U + B_1V = 1$$

A_1 et B_1 sont donc premiers entre eux.

Remarque 18 :

Une autre façon de démontrer la proposition précédente :

Comme $D \div A$ et $D \div B$, nous pouvons écrire, comme dans la proposition, $A = DA_1$ et $B = DB_1$ avec $A_1 \in \mathbb{K}[X]$ et $B_1 \in \mathbb{K}[X]$.
Alors, d'après la proposition 6.5.8

$$D = \text{pgcd}(A, B) = \text{pgcd}(DA_1, DB_1) = D \times \text{pgcd}(A_1, B_1)$$

De $D = D \times \text{pgcd}(A_1, B_1)$, nous en déduisons que $\text{pgcd}(A_1, B_1) = 1$, c'est à dire que A_1 et B_1 sont premiers entre eux.

6.5.14 Lemme de Gauss

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ son anneau de polynômes. Soient $A \in \mathbb{K}[X]$, $B \in \mathbb{K}[X]$ et $C \in \mathbb{K}[X]$ 3 polynômes
Si A divise BC et si A est premier avec B, alors A divise C

Démonstration

Soient donc $A \in \mathbb{K}[X]$, $B \in \mathbb{K}[X]$ et $C \in \mathbb{K}[X]$ tels que A divise BC et A est premier avec B.
Si A divise BC, alors il existe $Q \in \mathbb{K}[X]$ tel que $BC = AQ$
A étant premier avec B, il existe donc $U \in \mathbb{K}[X]$ et $V \in \mathbb{K}[X]$ tels que $1 = AU + BV$ et donc $C = AUC + BVC$. Ainsi :

$$C = AUC + BVC = AUC + AQV = A(UC + QV)$$

Ainsi, A divise C

6.5.15 Proposition

$\mathbb{Z}[X]$ n'est pas un anneau principal

Démonstration

1. Puisque $\mathbb{Z}$ est un anneau et non un corps, nous nous en doutions un peu ; jusqu'ici, nous nous sommes basés sur le fait que $\mathbb{K}[X]$ était un anneau principal, justement parce que $\mathbb{K}$ est un corps
2. Considérons les 2 polynômes de $\mathbb{Z}[X]$: $A = X^2+1$ et $B = 2X$.
   A et B n'ont aucun diviseur en commun sauf 1. Ceux de B sont 1, 2, X, $2X$ et leurs opposés.
   Or, ni 2, ni X et $2X$ ne divisent $A = X^2+1$
3. Supposons que $\mathbb{Z}[X]$ soit principal
   - ▷ Soit $\mathcal{I}(A,B) = \{PA+QB \text{ où } P \in \mathbb{Z}[X] \text{ et } Q \in \mathbb{Z}[X]\}$
     Il est facile de démontrer que $\mathcal{I}(A,B)$ est un idéal de $\mathbb{Z}[X]$; c'est l'idéal engendré par A et B
   - ▷ Si $\mathbb{Z}[X]$ est principal, alors il est engendré par un polynôme $C \in \mathbb{Z}[X]$, c'est à dire que :
     $$\mathcal{I}(A,B) = [C] = C(X) \times \mathbb{Z}[X]$$
     Ce polynôme $C \in \mathbb{Z}[X]$ ne peut être qu'un diviseur commun à A et B. Ce diviseur commun est le seul polynôme $C(X) = 1$
   - ▷ Or, 1 ne peut pas appartenir à $\mathcal{I}(A,B)$
     - ⋆ Autre forme de la question : existe-t-il des polynômes $P \in \mathbb{Z}[X]$ et $Q \in \mathbb{Z}[X]$ tels que $PA+QB = 1$?
     - ⋆ Comme $\mathbb{Z}[X]$ est un sous-anneau de $\mathbb{R}[X]$, d'après le théorème de Bezout 6.5.11, il existe des polynômes $P \in \mathbb{R}[X]$ et $Q \in \mathbb{R}[X]$ tels que $PA+QB = 1$.
       Recherchons ces polynômes.
       Posons $P(X) = aX^3+bX^2+cX+d$ et $Q(X) = \alpha X^3+\beta X^2+\gamma X+\delta$
       Alors :
       $$PA+QB = 1 \iff aX^5+(b+2\alpha)X^4+(c+a+2\beta)X^3+(d+b+2\gamma)X^2+(2\delta+c)X+d = 1$$
       D'où nous tirons :
       $$\begin{cases} a = 0 \\ b+2\alpha = 0 \\ c+a+2\beta = 0 \\ d+b+2\gamma = 0 \\ 2\delta+c = 0 \\ d = 1 \end{cases} \iff \begin{cases} a = 0 \\ b = -2\alpha \\ c = -2\beta \\ b = -2\gamma-1 \\ c = -2\delta \\ d = 1 \end{cases}$$
       D'où nous tirons $\beta = \delta$ et $2\alpha = 2\gamma+1 \iff \alpha = \dfrac{2\gamma+1}{2} = \gamma+\dfrac{1}{2}$
     - ⋆ Ainsi :
       $$\begin{aligned} Q(X) = & \alpha X^3+\beta X^2+\gamma X+\delta = \left(\gamma+\frac{1}{2}\right)X^3+\beta X^2+\gamma X+\beta \\ = & \frac{X^3}{2}+\gamma\left(X^3+X\right)+\beta\left(X^2+1\right) \end{aligned}$$
       Et $P(X) = -2(\gamma+1)X^2+-2\beta X+1$
     - ⋆ Si $\gamma \in \mathbb{Z}$ et $\beta \in \mathbb{Z}$, alors $P \in \mathbb{Z}[X]$, mais $Q \notin \mathbb{Z}[X]$

   Donc $1 \notin \mathcal{I}(A,B)$ et $\mathbb{Z}[X]$ n'est pas un anneau principal

Remarque 19 :

1. Nous avons aussi $\left(X^2+1\right)-\left(\dfrac{X}{2}\right)\times(2X) = 1$. La démonstration de la proposition a l'avantage de la généralité
2. Par contre, si nous posons $A = X^2+1$ et $B = X$, alors $\left(X^2+1\right)-(X)\times(X) = 1$ et donc la polynôme 1 appartient à $\mathcal{I}(A,B)$, l'idéal engendré par A et B et, dans ce cas, $\mathcal{I}(A,B) = \mathbb{Z}[X]$

6.5.16 Théorème et définition

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ son anneau de polynômes. Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$

1. Il existe $M \in \mathbb{K}[X]$ tel que les multiples communs à A et B sont les multiples de M
2. M est déterminé de manière unique, à une constante multiplicative non nulle près
3. Si $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$ sont tels que $A \neq 0$ et $B \neq 0$ alors, le degré de M est plus petit que le degré de tout multiple commun à A et$B$
4. M est le plus petit multiple commun (PPCM) à A et B. On le note $\text{PPCM}(A, B)$

Démonstration

1. Supposons $A \neq 0$ et $B \neq 0$.
   Soient $[A] = A \times \mathbb{K}[X]$ et $[B] = B \times \mathbb{K}[X]$ les idéaux engendrés par A et B et considérons $[A] \cap [B]$
   $[A] \cap [B]$ est un idéal ; c'est l'idéal formé par les multiples communs à A et B et $[A] \cap [B] \neq \emptyset$ puisque $AB \in [A] \cap [B]$
2. $\mathbb{K}[X]$ étant un anneau principal, il existe $M \in \mathbb{K}[X]$, de degré minimal, unique à une constante multiplicative non nulle près tel que $[A] \cap [B] = [M]$
   Donc, le degré de M minore le degré de tout multiple commun à A et B
3. Si A est le polynôme nul ($A = 0$), 0 est le seul multiple commun à A et B

Remarque 20 :

En fait, M est un diviseur de tous les multiples communs à A et B

Exercice 11 :

Soit $P \in \mathbb{Z}[X]$ où $P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$.
Soit $\dfrac{p}{q} \in \mathbb{Q}$ une racine rationnelle de P avec p et q premiers entre eux.

1. Montrer que q divise a_n et que p divise a_0
2. Montrer que, pour tout $m \in \mathbb{Z}$, le nombre entier $p - mq$ divise $P(m)$
3. Déterminer les racines rationnelles des polynômes :
   (a) $P_1 = X^3 - 6X^2 + 15X - 14$
   (b) $P_2 = X^5 - 2X^4 - 4X^3 + 4X^2 - 5X + 6$
4. Déduire du 1. que si $a_n = 1$ (c'est à dire si $P \in \mathbb{Z}[X]$ est unitaire), les racines réelles de P sont soit entières, soit irrationnelles.