Chapitre 2

Arithmétique des polynômes

Dans tout le chapitre, $\mathbb{K}$ désignera l'un des ensembles $\mathbb{R}$ ou $\mathbb{C}$.

2.1 Divisibilité - Division euclidienne

Définition 2.1 *Soient* A *et* B *deux polynômes de* $\mathbb{K}[X]$. *On dit que* B ***divise*** A, *ou que* B *est un* ***diviseur*** *de* A, *ou que* A *est un* ***multiple de*** B, *et on note alors* $B|A$, *s'il existe un polynôme* Q *dans* $\mathbb{K}[X]$ *tel que* $A = BQ$.
L'ensemble $\{BQ,\ Q \in \mathbb{K}[X]\}$ *des multiples de* B *est noté* $B.\mathbb{K}[X]$.

$$\textit{Ainsi,} \qquad B|A \iff A \in B.\mathbb{K}[X].$$

Exemples.
- Tout polynôme divise 0 mais 0 ne divise que le polynôme nul.
- 1 (et d'une manière générale tout polynôme constant non nul) divise tous les polynômes.
- $X^2 + 1 | X^3 - X^2 + X - 1$ car $X^3 - X^2 + X - 1 = (X^2 + 1)(X - 1)$

Proposition 2.2 *Soit* $(A, B) \in (\mathbb{K}[X])^2$. *Si* $A \neq 0$ *et si* $B|A$ *alors* $\deg B \leqslant \deg A$.

Démonstration :
Sous ces hypothèsse, on peut en effet considérer un polynôme Q tel que $A = BQ$ et on a donc $\deg A = \deg B + \deg Q$. Comme $A \neq 0$, on a $Q \neq 0$ et par suite $\deg Q \geqslant 0$. On a donc bien $\deg A \geqslant \deg B$. □

Proposition 2.3 *Soit* $(A, B, C) \in (\mathbb{K}[X])^3$.
- $A|A$ *(la relation de divisibilité est réflexive)*
- *(*$A|B$ *et* $B|C) \Longrightarrow A|C$ *(la relation de divisibilité est transitive)*
- *(*$B|A$ *et* $A|B) \Longrightarrow \exists c \in \mathbb{K}^*,\ A = cB$

Proposition 2.4 *Pour* $(A, B, C) \in (\mathbb{K}[X])^3$ *et* $c \in \mathbb{K}^*$,
- $A|B \iff cA|B$
- $B|A \Longrightarrow B|AC$
- *(*$A|B$ *et* $A|C) \Longrightarrow A|(B + C)$

Exercice 2.1 Démontrer ces deux propositions. On pourra constater une certaine analogie avec les propriétés de la divisibilité dans $\mathbb{Z}$...

Théorème 2.5 (Division euclidienne) *Soient* A *et* B *dans* $\mathbb{K}[X]$ *avec* $B \neq 0$. *Alors, il existe un unique couple* (Q, R) *de polynômes tel que :* $A = BQ + R$ *et* $\deg R < \deg B$.

Démonstration : Commençons par démontrer l'unicité.
Supposons que nous ayons deux couples (Q_1, R_1) et (Q_2, R_2) de polynômes tels que :

$$A = BQ_1 + R_1 = BQ_2 + R_2 \quad \text{avec } \deg R_1 < \deg B \text{ et } \deg R_2 < \deg B$$

Alors $B(Q_1 - Q_2) = R_2 - R_1$.
Si $Q_1 \neq Q_2$, i.e. $Q_1 - Q_2 \neq 0$, on a $\deg\big(B(Q_1 - Q_2)\big) = \deg B + \deg(Q_1 - Q_2) \geqslant \deg B$ et

$$\deg(R_2 - R_1) \leqslant \max(\deg R_1, \deg R_2) < \deg B$$

d'où une contradiction. On a donc $Q_1 = Q_2$ et par suite aussi $R_1 = R_2$.

Pour montrer l'existence, on construit, par récurrence, une suite de couples de polynômes (Q_n, R_n) vérifiant toujours $A = BQ_n + R_n$. On initialise l'algorithme avec $Q_0 = 0$ et $R_0 = A$.
Le pas de récurrence est décrit par : Tant que $\deg R_n \geqslant \deg B$ Faire

$$Q_{n+1} = Q_n + \frac{\text{coefdom } R_n}{\text{coefdom } B} X^{\deg R_n - \deg B}$$

$$R_{n+1} = R_n - \frac{\text{coefdom } R_n}{\text{coefdom } B} X^{\deg R_n - \deg B} B$$

On a alors $\deg R_{n+1} < \deg R_n$ puisque R_n a même degré et même coefficient dominant que le polynôme $\dfrac{\text{coefdom } R_n}{\text{coefdom } B} X^{\deg R_n - \deg B} B$.
Comme la suite des $\deg R_n$ est strictement décroissante, l'algorithme s'arrête au bout d'un nombre fini d'étapes avec $\deg R_n < \deg B$. On prend alors $R = R_n$ et $Q = Q_n$. □

Le procédé décrit ci-dessus est appelé division euclidienne de A par B (ou division selon les puissances décroissantes). Q est le **quotient** et R est le **reste**.

Exemple. $A = 4X^5 - 10X^4 + 6X^3 - 7X^2 + 10X - 3$ et $B = 2X^3 + X - 1$
La division euclidienne de A par B s'écrit $A = B.(2X^2 - 5X + 2) + 3X - 1$. On a en effet :

$$\begin{array}{rl|l}
4X^5 - 10X^4 + 6X^3 - 7X^2 + 10X - 3 & & 2X^3 + X - 1 \\
\cline{3-3}
4X^5 + 2X^3 - 2X^2 & & 2X^2 - 5X + 2 \\
\cline{1-1}
-10X^4 + 4X^3 - 5X^2 + 10X - 3 & & \\
-10X^4 - 5X^2 + 5X & & \\
\cline{1-1}
4X^3 + 5X - 3 & & \\
4X^3 + 2X - 2 & & \\
\cline{1-1}
3X - 1 & &
\end{array}$$

Complément : notion d'idéal

Définition 2.6 *On dit qu'une partie* I *de* $\mathbb{K}[X]$ *est un* **idéal** *de* $\mathbb{K}[X]$ *si c'est une partie non vide qui vérifie : (i)* $\forall (A, B) \in I^2$, $A + B \in I$ *et (ii)* $\forall A \in I$, $\forall P \in \mathbb{K}[X]$, $AP \in I$.

Théorème 2.7 *Tout idéal de* $\mathbb{K}[X]$ *s'écrit* $A.\mathbb{K}[X]$ *pour un certain polynôme* A *de* $\mathbb{K}[X]$.
Plus précisément, tout idéal de $\mathbb{K}[X]$ *non réduit à* $\{0\}$ *s'écrit de manière unique* $A_0.\mathbb{K}[X]$ *où* A_0 *est un polynôme unitaire.*

Démonstration : Soit I un idéal non réduit à $\{0\}$ de $\mathbb{K}[X]$. On choisit dans $I\setminus\{0\}$ un polynôme A de plus petit degré (un tel polynôme existe puisque l'ensemble des degrés des polynômes non nuls de I est une partie non vide de $\mathbb{N}$). Si α est son coefficient dominant, remarquons que $A_0 = \frac{1}{\alpha}A$ appartient à $I\setminus\{0\}$ et est unitaire.
Prenons alors $B \in I$ et effectuons la division euclidienne de B par A_0. $B = A_0Q + R$ avec $\deg R < \deg A_0$.
Comme $R = B - A_0Q \in I$ et que A_0 est de plus petit degré, on a nécessairement $R = 0$ et donc $B \in A_0\mathbb{K}[X]$.
D'autre part, $A_0\mathbb{K}[X] \subset I$ par la propriété d'idéal. On conclut donc que $I = A_0\mathbb{K}[X]$.

Pour l'unicité, si $A_0\mathbb{K}[X] = A_1\mathbb{K}[X]$, on a $A_0|A_1$ et $A_1|A_0$, donc $A_1 = cA_0$ avec $c \in \mathbb{K}^*$. Si ils sont tous deux unitaires, on a $c = 1$ et donc $A_0 = A_1$. □

2.2 Diviseurs communs - PGCD

2.2.1 pgcd de deux polynômes

Proposition 2.8 *Soit* $(A, B) \neq (0, 0) \in (\mathbb{K}[X])^2$. *L'ensemble des degrés des diviseurs communs à* A *et* B *est une partie non vide et finie de* $\mathbb{N}$.

Démonstration : Comme 1 divise tous les polynômes, cet ensemble contient $0 = \deg 1$ et est donc non vide. D'autre part, le polynôme nul ne divisant que lui-même, il n'est pas diviseur commun et l'ensemble considéré est donc bien une partie de $\mathbb{N}$. Enfin, la proposition **??** de ce chapitre montre que le degré de tout diviseur commun est majoré par $\deg A$ ou $\deg B$. □

Définition 2.9 *Soient* A *et* B *deux polynômes de* $\mathbb{K}[X]$ *non tous deux nuls. On dit que le polynôme* D *est un plus grand commun diviseur (en abrégé, pgcd) de* A *et* B *si* D *est un polynôme de plus grand degré de l'ensemble des diviseurs communs à* A *et* B.

Exemple. Lorsque $A \neq 0$, l'ensemble des diviseurs communs à A et 0 est l'ensemble des diviseurs de A donc A est un pgcd de A et 0 et tout autre pgcd D de A et 0 a même degré que A et s'écrit par suite $D = cA$ avec $c \in \mathbb{K}^*$ (puisque D divise A). En particulier A et 0 ont un unique pgcd unitaire que l'on notera $\text{pgcd}(A, 0)$. On a donc $\text{pgcd}(A, 0) = \frac{1}{\text{coefdom A}}\,A$.

2.2.2 PGCD et algorithme de Euclide

Proposition 2.10 *Soient* A *et* B *dans* $\mathbb{K}[X]$ *avec* $B \neq 0$. *Si* R *est le reste dans la division euclidienne de* A *par* B, *alors l'ensemble des diviseurs communs à* A *et* B *est égal à l'ensemble des diviseurs commun à* B *et* R. *En particulier,* (A, B) *et* (B, R) *ont les mêmes pgcd.*

Démonstration : Si D|A et D|B, on écrit la division euclidienne de A par B : $A = BQ + R$. Soient L et M les polynômes tels que $A = DL$ et $B = DM$. Alors en remplaçant on obtient $R = A - BQ = DL - QDM = D(L - QM)$ donc D|R. Réciproquement, si $B = DL$ et $R = DL$, alors $A = BQ + R = D(QL + RM)$. □

On peut alors obtenir les *pgcd* de A et B en itérant ce procédé, comme avec les entiers.

Algorithme de Euclide

• On pose $R_0 = A$ et $R_1 = B$.
• À chaque étape n ($n \in \mathbb{N}^*$), pourvu que $R_n \neq 0$, on note R_{n+1} le reste dans la division euclidienne de R_{n-1} par R_n.
La relation $\deg(R_{n+1}) < \deg(R_n)$ assure que ce processus prend fin en un nombre fini d'étapes :

$\exists N \in \mathbb{N}^*$, $R_N \neq 0$ et $R_{N+1} = 0$. La proposition précédente montre d'autre part que les diviseurs communs de $A = R_0$ et $B = R_1$ sont les diviseurs communs de R_1 et R_2 et donc, de proche en proche, ceux de R_N et $R_{N+1} = 0$. Les *pgcd* de A et B sont donc les *pgcd* de R_N et 0 donc les cR_N ($c \in \mathbb{K}^*$). En version algorithmique cela donne :

Début
  $R_0 \leftarrow A$;
  $R_1 \leftarrow B$;
  Tant que $R_1 \neq 0$ **faire**
    $R_2 \leftarrow$ reste dans la division euclidienne de R_0 par R_1 ;
    $R_0 \leftarrow R_1$;
    $R_1 \leftarrow R_2$;
  Fin Tant que
  Afficher R_0**.**
Fin

On retiendra : **Dans l'algorithme d'Euclide, le dernier reste non nul est un pgcd de** A **et** B.

Remarque. Le pgcd n'est donc pas défini de manière unique, mais à un facteur constant non nul près : si D et E sont deux pgcd de A et B alors il existe une constante non nulle c telle que $D = cE$. En particulier, deux polynômes A et B non tous deux nuls admettent un unique pgcd unitaire que l'on notera $\text{pgcd}(A, B)$.
Par convention le pgcd de 0 et 0 est 0 : on note $\text{pgcd}(0, 0) = 0$.

Proposition 2.11 *Soient* A *et* B *deux polynômes de* $\mathbb{K}[X]$ *et* D *un pgcd de* A *et* B*. Alors il existe des polynômes* U *et* V *tels que* $D = AU + BV$.

Démonstration : Le résultat est clair si $(A, B) = (0, 0)$ puisqu'alors $D = 0$. Sinon, quitte à échanger A et B, on peut supposer $B \neq 0$. On construit alors un couple (U, V) solution en remontant l'algorithme précédent : c'est l'***algorithme d'Euclide étendu***. Cela consiste à construire, pour tout naturel $n \leqslant N$, un couple de polynômes (U_n, V_n) tel que $AU_n + BV_n = R_n$ (avec les notations précédentes).
• On pose $U_0 = 1$ et $V_0 = 0$ d'une part et $U_1 = 0$ et $V_1 = 1$ d'autre part.
• En supposant U_{n-1}, U_n, V_{n-1} et V_n construits et sachant que par définition de R_{n+1} on a $R_{n-1} = R_nQ_n + R_{n+1}$, on pose $U_{n+1} = U_{n-1} - U_nQ_n$ et $V_{n+1} = V_{n-1} - V_nQ_n$. On a alors bien $AU_{n+1} + BV_{n+1} = AU_{n-1} + BV_{n-1} - Q_n(AU_n + BV_n) = R_{n-1} - Q_nR_n = R_{n+1}$.
Quitte à diviser par une constante non nulle, on obtient alors le résultat annoncé en prenant $n = N$. □

Remarque. La détermination effective de U et V tels que $AU + BV = \text{pgcd}(A, B)$ peut donc se faire en remontant l'algorithme d'Euclide.

Exemple. Calculons le pgcd unitaire D des polynômes $A = X^4 - 4X^3 + 2X^2 + X + 6$ et $B = X^4 - 3X^3 + 2X^2 + X + 5$. L'algorithme d'Euclide (divisions euclidiennes successives) donne :

$$\begin{aligned} X^4 - 4X^3 + 2X^2 + X + 6 &= (X^4 - 3X^3 + 2X^2 + X + 5) \times 1 + (-X^3 + 1) \\ X^4 - 3X^3 + 2X^2 + X + 5 &= (-X^3 + 1)(-X + 3) + (2X^2 + 2X + 2) \\ -X^3 + 1 &= (2X^2 + 2X + 2)(-\tfrac{1}{2}X + \tfrac{1}{2}) + 0 \end{aligned}$$

Dans cet algorithme, le dernier reste non nul est un pgcd. On en déduit $D = X^2 + X + 1$.
Trouvons à présent deux polynômes U et V tels que $D = AU + BV$. En remontant l'algorithme précédent, on a successivement :

$$\begin{aligned} 2X^2 + 2X + 2 &= (-X^3 + 1)(X - 3) + B \\ 2X^2 + 2X + 2 &= (A - B)(X - 3) + B = A.(X - 3) + (-X + 4)B \end{aligned}$$

On peut donc choisir $U = \frac{1}{2}X - \frac{3}{2}$ et $V = -\frac{1}{2}X + 2$.

Théorème 2.12 (Caractérisation du pgcd) *Soient* A *et* B *deux polynômes de* $\mathbb{K}[X]$. *Le polynôme* D *est un pgcd de A et B si et seulement si :*

- *D est un diviseur commun à A et B,*
- *tout diviseur commun à A et B divise D.*

Autrement dit, D *est un pgcd de* A *et* B *si et seulement si l'ensemble des diviseurs de* D *est égal à celui des diviseurs communs à* A *et* B.

Démonstration : C'est clair si $B = 0$. Supposons donc $B \neq 0$.
• Supposons que D soit un pgcd de A et B alors D est un diviseur commun de A et B (le premier point est donc vérifié) de plus grand degré. Si E est un diviseur commun de A et B il est, d'après le résultat précédent, un diviseur commun à D et 0 donc un diviseur de D.
• Réciproquement, supposons que E soit un diviseur commun à A et B tel que tout diviseur commun à A et B divise E. Alors en particulier le pgcd D de A et B divise E et $\deg D \leqslant \deg E$. D étant de degré maximum (parmi les diviseurs communs), on déduit : $\deg D = \deg E$ et donc $E = cD$ ($c \in \mathbb{K}^*$). E est donc bien un pgcd de A et B. □

Proposition 2.13 *Soient A, B, C trois polynômes avec C unitaire. Alors :*

$$\text{pgcd}(CA, CB) = C.\text{pgcd}(A, B)$$

Démonstration : Notons $D = \text{pgcd}(A, B)$ et $\Delta = \text{pgcd}(CA, CB)$.
• On a D|A et D|B donc CD|CA et CD|CB. Par suite, CD|Δ.
• C|CA et C|CB donc C|Δ et on peut écrire $\Delta = CE$. Comme Δ|CA et Δ|CB, on peut aussi écrire $CA = \Delta A'$ et $CB = \Delta B'$. On a alors $CA = CA'E$ et $CB = CB'E$ donc $A = A'E$ et $B = B'E$. Par suite, E divise A et B donc D. $CE = \Delta$ divise donc CD.
En conclusion CD|Δ et Δ|CD et les deux polynômes CD et Δ sont unitaires donc $\Delta = CD$. □

2.2.3 Polynômes premiers entre eux

Définition 2.14 *On dit que deux polynômes* A *et* B *sont premiers entre eux si 1 est un pgcd de* A *et* B*, c'est à dire si les seuls diviseurs communs à* A *et* B *sont les polynômes constants non nuls.*

Proposition 2.15 *Soient* A *et* B *deux polynômes et* D *un pgcd de* A *et* B*. Alors on peut écrire* $A = DA_1$ *et* $B = DB_1$ *où* A_1 *et* B_1 *sont deux polynômes premiers entre eux.*

Démonstration : C'est clair (mais sans intérêt) si $(A, B) = (0, 0)$. Sinon, on peut, sans restriction aucune, supposer D unitaire. Puisque D|A et D|B, on peut écrire $A = DA_1$ et $B = DB_1$ où A_1 et B_1 sont deux polynômes. Mais alors $\text{pgcd}(A, B) = \text{pgcd}(DA_1, DB_1) = D.\text{pgcd}(A_1, B_1)$ donc $\text{pgcd}(A_1, B_1) = 1$: A_1 et B_1 sont premiers entre eux. □

Théorème 2.16 (Théorème de Bezout) *Deux polynômes A et B sont premiers entre eux si et seulement s'il existe des polynômes U et V tels que* $AU + BV = 1$.

Démonstration : Si A et B sont premiers entre eux, le résultat est donné par la proposition **??**. Supposons réciproquement que l'on puisse écrire $1 = AU + BV$ et soit $D = \text{pgcd}(A, B)$. D|A donc D|AU et de même D|BV. Par suite, D|AU + BV = 1 et D = 1 (puisque D est unitaire). □

Corollaire 2.17 *Soit* A *un polynôme premier avec chacun des polynômes* $B_1, \cdots, B_r$*. Alors* A *est premier avec le produit* $B_1B_2 \cdots B_r$.

Démonstration : Montrons le pour $r = 2$. Supposons donc A premier avec B_1 et avec B_2. Le théorème de Gauss permet alors d'écrire $AU_1 + B_1V_1 = 1$ et $AU_2 + B_2V_2 = 1$. On a alors $AB_2V_2U_1 + B_1B_2V_1V_2 = B_2V_2$ et $A(B_2V_2U_1 + U_2) + B_1B_2V_1V_2 = B_2V_2 + AU_2 = 1$. Le même théorème assure alors que A et B_1B_2 sont premiers entre eux. □

Théorème 2.18 (Lemme de Gauss) *Soient A, B et C des polynômes tels que A et B soient premiers entre eux et que A divise le produit BC. Alors A divise C.*

Démonstration : Puisque A et B sont premiers entre eux, on peut écrire $AU + BV = 1$ donc $ACU + BCV = C$. Or $A|AU$ et $A|BC$ donc $A|BCV$. Par suite $A|ACU + BCV = C$. □

Corollaire 2.19 *Soient* A_1 *et* A_2 *deux polynômes premiers entre eux divisant chacun le polynôme* B. *Alors* A_1A_2 *divise* B.

Démonstration : Puisque $A_1|B$, on peut écrire $B = A_1B_1$. Comme $A_2|B = A_1B_1$ et $\text{pgcd}(A_1, A_2) = 1$, le lemme de Gauss montre que $A_2|B_1$ et par suite $A_1A_2|A_1B_1 = B$. □

2.2.4 Complément : autre approche

Soient $A \in \mathbb{K}[X] \setminus \{0\}$ et $B \in \mathbb{K}[X]$. Alors, $A\mathbb{K}[X] + B\mathbb{K}[X] = \{AQ + BR,\ Q, R \in \mathbb{K}[X]\}$ est un idéal non réduit à $\{0\}$ de $\mathbb{K}[X]$. Donc il existe un unique polynôme unitaire D tel que

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

Cet unique polynôme est appelé plus grand diviseur commun à A et B et noté $\text{PGCD}(A, B)$. Cette définition entraîne l'existence de $(U, V) \in (\mathbb{K}[X])^2$ tels que $D = AU + BV$.
On constate que D est un diviseur commun à A et B et que tout diviseur commun à A et B divise D. D est donc le diviseur commun à A et B de plus grand degré.

2.3 Multiples communs - PPCM

Propriété. Soit $(A, B) \in (\mathbb{K}[X]\setminus\{0\})^2$. L'ensemble des degrés des multiples non nuls communs à A et B est une partie non vide de $\mathbb{N}$.

Démonstration : C'est clair puisque cette partie contient $\deg(AB)$. □

Définition 2.20 *Soient* A *et* B *deux polynômes non nuls de* $\mathbb{K}[X]$. *On dit que le polynôme M est un plus petit commun multiple (en abrégé, ppcm) de A et B si M est un polynôme de plus bas degré de l'ensemble des multiples non nuls communs à A et B.*

Proposition 2.21 *Soit* $(A, B) \in (\mathbb{K}[X]\setminus\{0\})^2$. *Si* M *et* N *sont deux ppcm de* A *et* B *alors il existe une constante non nulle c telle que* $M = cN$. *En particulier, deux polynômes* A *et* B *non nuls admettent un unique ppcm unitaire que l'on notera* $\text{ppcm}(A, B)$.

Démonstration : N est non nul par définition d'un *ppcm*. La division euclidienne de M par N permet alors d'écrire $M = NQ + R$ avec $\deg R < \deg N$. Or M et N sont des multiples communs à A et B donc $R = M - NQ$ est aussi un multiple commun à A et B. Comme $\deg R < \deg N$, la définition de *ppcm* entraîne que $R = 0$. N et M ayant d'autre part même degré, Q est une constante (non nulle). □

Remarque. Par convention, pour tout polynôme A, $\text{ppcm}(A, 0) = 0$.

Théorème 2.22 (Caractérisation du ppcm) *Un polynôme* M *est un plus petit commun multiple (ppcm) de deux polynômes A et B si et seulement si*

- M *est un multiple commun de A et B,*
- *tout multiple commun de A et B est multiple de* M*.*

Démonstration : C'est clair si $A = 0$ ou $B = 0$ puisqu'alors seul 0 est un multiple commun. Supposons donc $(A, B) \in (\mathbb{K}[X]\backslash\{0\})^2$.
• Supposons que M soit un *ppcm* de A et B alors M est un multiple (non nul) commun à A et B (le premier point est donc vérifié) de plus petit degré. Si N est un multiple commun à A et B, la division euclidienne de N par M permet d'écrire $N = MQ + R$ avec $\deg R < \deg M$. Or M et N sont des multiples communs à A et B donc $R = N - MQ$ est aussi un multiple commun à A et B. Comme $\deg R < \deg M$, la définition de *ppcm* entraîne que $R = 0$: N est bien un multiple de M.
• Réciproquement, supposons que N soit un multiple commun à A et B tel que tout multiple commun de A et B soit multiple de N. Alors en particulier le ppcm M de A et B est un multiple de N et on peut écrire $M = NQ$ et $\deg M \geqslant \deg N$. M étant de degré minimum (parmi les multiples communs non nuls), on déduit $\deg M = \deg N$ et N est bien un *ppcm* de A et B. □

Corollaire 2.23 *Les multiples communs à* A *et* B *sont les multiples de* $\mathrm{ppcm}(A, B)$.

Proposition 2.24 *Pour deux polynômes unitaires* A *et* B*, on a :* $AB = \mathrm{pgcd}(A, B)\,\mathrm{ppcm}(A, B)$.

Démonstration : Soit D le pgcd unitaire de A et B. On peut alors écrire $A = DA'$ et $B = DB'$ avec $\mathrm{pgcd}(A', B') = 1$. On cherche donc à montrer que $AB' = A'B$ est le ppcm de A et B. Or, c'est bien un multiple commun à A et B et si M est un multiple commun à A et B alors M est un multiple de D et on peut écrire $M = DM'$. M' est alors un multiple commun aux polynômes premiers entre eux A' et B'. Il est donc multiple de $A'B'$ et finalement M est multiple de $DA'B'$ donc de AB'. □

Remarque. Compte tenu des conventions adoptées, la formule précédente reste valable si $A = 0$ ou $B = 0$.

2.3.1 Autre approche

Soient A_1 et A_2 des polynômes non nuls. Leurs multiples communs sont des éléments de $A_1\mathbb{K}[X] \cap A_2\mathbb{K}[X]$. Cet ensemble est un idéal non réduit à $\{0\}$ donc il s'écrit $M\mathbb{K}[X]$ pour un unique polynôme unitaire M. Ce polynôme M est noté $ppcm(A, B)$ et appelé **plus petit multiple commun** de A et B car

- il est multiple de A et de B.
- tout multiple commun de A et B appartient à $M\mathbb{K}[X]$ donc est multiple de M (en particulier, est de degré supérieur ou égal à celui de M, sauf s'il est nul).

2.4 Polynômes irréductibles

Définition 2.25 *Un polynôme* A *de* $\mathbb{K}[X]$ *est dit irréductible s'il est de degré supérieur ou égal à 1 et si ses seuls diviseurs sont les polynômes constants non nuls et les* cA *(*$c \in \mathbb{K}^*$*).*
Un polynôme A *est donc irréductible s'il a exactement deux diviseurs unitaires (ces deux diviseurs sont alors* 1 *et* $\frac{1}{\mathrm{coefdom}(A)}A$*).*

Remarques. • Les polynômes constants ne sont, par définition, pas irréductibles.
• Soit A un polynôme non constant. Si A n'est pas irréductible alors A admet un diviseur D tel que $1 \leqslant \deg \mathrm{D} < \deg \mathrm{A}$.

Exercice 2.2 Montrer que tout polynôme de degré 1 de $\mathbb{K}[\mathrm{X}]$ est irréductible.

Remarque. Les polynômes irréductibles jouent dans $\mathbb{K}[\mathrm{X}]$ le rôle joué par les nombres premiers dans $\mathbb{N}$ (ou $\mathbb{Z}$). Le lecteur attentif mettra donc en parallèle les résultats qui suivent avec les propriétés analogues dans $\mathbb{Z}$.

Proposition 2.26

1. *Un polynôme irréductible est premier avec tout polynôme qu'il ne divise pas.*
2. *Tout polynôme irréductible qui divise un produit divise l'un de ses facteurs.*
3. *Tout polynôme non constant de* $\mathbb{K}[\mathrm{X}]$ *admet au moins un diviseur irréductible.*

Démonstration :

1. Si A est irréductible, ses seuls diviseurs sont les polynômes constants non nuls et les cA ($c \in \mathbb{K}^*$). Si de plus A ne divise pas le polynôme B, il en est de même des cA et par suite les seuls diviseurs communs à A et B sont les $c \in \mathbb{K}^*$.

2. Si A (irréductible) divise BC et si A ne divise pas B alors il est premier avec B donc (Lemme de Gauss) il divise C.

3. Parmi tous les diviseurs non constants de A (il y a au moins A), on en considère un de degré le plus petit que nous noterons Q. Si Q n'était pas irréductible, il aurait un diviseur S avec $1 \leqslant \deg \mathrm{S} < \deg \mathrm{Q}$. Ce S serait a fortiori un diviseur de A avec $\deg \mathrm{S} < \deg \mathrm{Q}$, ce qui contredit la définition de Q. Donc Q est irréductible. □

Exercice 2.3 Soient $(\mathrm{A}, \mathrm{B}) \in (\mathbb{K}[\mathrm{X}])^2$ est $n \in \mathbb{N}$. Montrer que si A est premier avec B alors il est premier avec B^n. En déduire que pour $a \neq b$, $\mathrm{X} - a$ est premier avec $(\mathrm{X} - b)^n$.

Théorème 2.27 (Décomposition en produit de facteurs irréductibles) *Tout polynôme non constant* A *s'écrit de manière unique (à l'ordre près des facteurs) sous la forme*

$$\mathrm{A} = c\mathrm{R}_1^{\alpha_1} \dots \mathrm{R}_k^{\alpha_k}$$

où $k \in \mathbb{N}^*$, $c \in \mathbb{K}^*$, $\mathrm{R}_1, \dots, \mathrm{R}_k$ *sont des polynômes unitaires irréductibles deux à deux distincts et* $\forall i \in \{1, \cdots, k\}$, $\alpha_i \in \mathbb{N}^*$.

Démonstration : (succinte). Pour l'existence, on raisonne par récurrence sur deg A. Si $\deg \mathrm{A} = 1$, c'est évident car A est irréductible.
Supposons que la décomposition existe pour tout polynôme de degré strictement inférieur à n ($n \geqslant 2$ fixé) et soit A de degré n. Si A est irréductible, il n'y a rien à faire. Sinon, par la proposition précédente, A admet un facteur irréductible R que l'on peut supposer unitaire avec $1 \leqslant \deg \mathrm{R} < \deg \mathrm{A}$. Ainsi $\mathrm{A} = \mathrm{RA}'$ et on applique ensuite l'hypothèse de récurrence à A′.

Pour l'unicité, il suffit d'adapter la démonstration faite pour les entiers. □

Proposition 2.28 *Soient* A *et* B *deux polynômes écrits sous la forme*

$$\mathrm{A} = c\,\mathrm{R}_1^{\alpha_1} \dots \mathrm{R}_k^{\alpha_k} \qquad \text{et} \qquad \mathrm{B} = d\,\mathrm{R}_1^{\beta_1} \dots \mathrm{R}_k^{\beta_k}$$

où les R_i *sont des polynômes irréductibles deux à deux distincts unitaires et les* α_i, β_i *des entiers naturels (possiblement nuls). Alors :*

$$\mathrm{pgcd}(\mathrm{A}, \mathrm{B}) = \mathrm{R}_1^{min(\alpha_1,\beta_1)} \dots \mathrm{R}_k^{min(\alpha_k,\beta_k)} \quad \text{et} \quad \mathrm{ppcm}(\mathrm{A}, \mathrm{B}) = \mathrm{R}_1^{max(\alpha_1,\beta_1)} \dots \mathrm{R}_k^{max(\alpha_k,\beta_k)}$$

Exercice 2.4 Démontrer cette proposition.

2.5 Division des polynômes suivant les puissances croissantes.

Proposition 2.29 *Soient* A *et* B *deux polynômes et* n *un entier naturel. On suppose que le coefficient constant de* B *n'est pas nul. Alors il existe un unique couple* $(\mathrm{Q}_n, \mathrm{R}_n)$ *de polynômes tel que*

$$\mathrm{A} = \mathrm{BQ}_n + \mathrm{X}^{n+1}\mathrm{R}_n \quad \textit{et} \quad \deg \mathrm{Q}_n \leqslant n.$$

Q_n *et* $\mathrm{X}^{n+1}\mathrm{R}_n$ *sont appelés respectivement quotient et reste dans la division suivant les puissances croissantes de* A *par* B *à l'ordre* n.

Démonstration : On part de $\mathrm{A} = a_0 + \cdots + a_m\mathrm{X}^m$ et $\mathrm{B} = b_0 + b_1\mathrm{X} + \cdots + b_d\mathrm{X}^d$ avec $b_0 \neq 0$ et on construit Q_n et R_n par récurrence sur n.

- Pour $n = 0$, on pose $\mathrm{Q}_0 = \frac{a_0}{b_0}$ et $\mathrm{XR}_0 = \mathrm{A} - \frac{a_0}{b_0}\mathrm{B}$ (ce polynôme est bien divisible par X).
- On suppose Q_n et R_n construits. On écrit $\mathrm{R}_n = r_0 + \cdots + r_p\mathrm{X}^p$. Le polynôme $\mathrm{R}_n - \frac{r_0}{b_0}\mathrm{B}$ a alors son coefficient constant nul donc est factorisable par X et on pose $\mathrm{R}_n - \frac{r_0}{b_0}\mathrm{B} = \mathrm{XR}_{n+1}(\mathrm{X})$. Comme $\mathrm{A} = \mathrm{BQ}_n + \mathrm{X}^{n+1}\mathrm{R}_n = \mathrm{BQ}_n + \mathrm{X}^{n+1}(\mathrm{R}_n - \frac{r_0}{b_0}\mathrm{B} + \frac{r_0}{b_0}\mathrm{B})$, on a :
  $\mathrm{A} = \mathrm{B}[\mathrm{Q}_n + \frac{r_0}{b_0}\mathrm{X}^{n+1}] + \mathrm{X}^{n+1}[\mathrm{R}_n - \frac{r_0}{b_0}\mathrm{B}]$ soit $\mathrm{A} = \mathrm{BQ}_{n+1} + \mathrm{X}^{n+2}\mathrm{R}_{n+1}$ où l'on a posé $\mathrm{Q}_{n+1} = \mathrm{Q}_n + \frac{r_0}{b_0}\mathrm{X}^{n+1}$ qui est bien de degré au plus $n+1$.

Montrons à présent l'unicité. Supposons donc que $(\mathrm{S}_n, \mathrm{T}_n)$ est une autre solution. On a alors $\mathrm{B}(\mathrm{Q}_n - \mathrm{S}_n) = \mathrm{X}^{n+1}(\mathrm{T}_n - \mathrm{R}_n)$. Comme $b_0 \neq 0$, B est premier avec X donc avec X^{n+1}. Le lemme de Gauss entraîne alors que X^{n+1} divise $\mathrm{Q}_n - \mathrm{S}_n$. Ce dernier polynôme étant de degré au plus n, il est nul. On a donc $\mathrm{Q}_n = \mathrm{S}_n$ et aussi $\mathrm{T}_n = \mathrm{R}_n$. □

Exemple. $\mathrm{A} = 4\mathrm{X} + 6\mathrm{X}^2 + \mathrm{X}^3$, $\mathrm{B} = 2 + 3\mathrm{X} + 2\mathrm{X}^2$, $n = 3$. Cette division suivant les puissances croissantes s'écrit $\mathrm{A} = \mathrm{B}.(2\mathrm{X} - \frac{3}{2}\mathrm{X}^3) + \mathrm{X}^4(\frac{9}{2} + 3\mathrm{X})$. On a en effet :

$$\begin{array}{l|l}
4\,\mathrm{X} + 6\,\mathrm{X}^2 + \mathrm{X}^3 & 2 + 3\mathrm{X} + 2\mathrm{X}^2 \\
\cline{2-2}
4\,\mathrm{X} + 6\,\mathrm{X}^2 + 4\mathrm{X}^3 & 2\mathrm{X} - \frac{3}{2}\mathrm{X}^3 \\
\cline{1-1}
-3\,\mathrm{X}^3 & \\
-3\mathrm{X}^3 - \frac{9}{2}\mathrm{X}^4 - 3\mathrm{X}^5 & \\
\cline{1-1}
\frac{9}{2}\mathrm{X}^4 + 3\mathrm{X}^5 &
\end{array}$$