Polynômes & Fractions Rationnelles

0.1 Polynômes, opérations sur les polynômes

Dans tout ce chapitre, on notera $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Définition 0.1. Un **polynôme** (à une indéterminée) à coefficients dans $\mathbb{K}$ est une suite $P = (a_k)_{k\geq 0}$ d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang, c'est-à-dire telle qu'il existe $n \in \mathbb{N}$ tel que $a_k = 0$ pour tout $k > n$. Les nombres a_k s'appellent les **coefficients** de P.

Remarque 0.2.
1. Deux polynômes sont égaux si et seulement si leurs coefficients respectifs sont égaux.
2. Lorsque tous les coefficients de P sont nuls, on dit que P est **le polynôme nul** et on note $P = 0$.

Définition 0.3. Soit P un polynôme non nul. Le plus grand entier k tel que $a_k \neq 0$ est appelé le **degré** de P. On le note $\deg P$. Par convention $\deg 0 = -\infty$.

Soit $P = (a_k)_{k\geq 0}$ un polynôme non nul et $n \in \mathbb{N}$ tel que $a_k = 0$ pour tout $k > n$. On notera désormais :

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

Si $\deg P = n$, le terme $a_n X^n$ est appelé monôme de plus haut degré de P. Le coefficient a_n est appelé le **coefficient dominant** de P. Si $a_n = 1$, P est appelé un **polynôme unitaire**.

On appelle **polynôme constant** tout polynôme de la forme a_0, c'est-à-dire tout polynôme dont les coefficients sont nuls à partir du rang 1.

Notation. *On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$. Pour $N \in \mathbb{N}$, on note aussi $\mathbb{K}_N[X]$ l'ensemble des polynômes de degré $\leq N$:*

$$\mathbb{K}_N[X] = \left\{a_N X^N + \cdots + a_0 : a_i \in \mathbb{K}\right\}.$$

Remarque 0.4. On peut identifier l'ensemble des polynômes constants à $\mathbb{K}$ et donc identifier $\mathbb{K}$ à un sous-ensemble de $\mathbb{K}[X]$: $\mathbb{K} \subset \mathbb{K}[X]$.

Définition 0.5 (Opérations élémentaires)**.** Soient $P, Q \in \mathbb{K}[X]$ deux polynômes, $\lambda \in \mathbb{K}$. On note :

$$P = \sum_{k=0}^{p} a_k X^k, \qquad Q = \sum_{k=0}^{q} b_k X^k.$$

On note $a_k = 0$ pour tout $k > p$ et $b_k = 0$ pour tout $k > q$. On définit alors :

$$P + Q = \sum_{k=0}^{\max(p,q)} (a_k + b_k) X^k$$

la **somme** des polynômes P et Q. C'est le polynôme associé à la suite $(a_k + b_k)_{k \geq 0}$.

$$PQ = \sum_{k=0}^{p+q} \Big(\sum_{i+j=k} a_i b_j \Big) X^k,$$

le **produit** des polynômes P et Q. C'est le polynôme associé à la suite $(\sum_{i+j=k} a_i b_j)_{k \geq 0}$.

$$\lambda P = \sum_{k=0}^{p} \lambda a_k X^k,$$

le **produit** du scalaire λ et du polynôme P. C'est le polynôme associé à la suite $(\lambda a_k)_{k \geq 0}$.

Exemple. $(X^2 + 2X) + (X^3 + X^2 + 1) = X^3 + 2X^2 + 2X + 1$
$(X^2 + X)(X + 1) = X^3 + 2X^2 + X$
$3(X^2 + 2X + 5) = 3X^2 + 6X + 15$

On définit alors les puissances d'un polynôme P par récurrence en posant :

$$P^0 = 1 \text{ et } P^n = P^{n-1}P \text{ pour tout } n \geq 1$$

Le monôme $X = (0, 1, 0, 0, \dots,)$ est appelée **l'indéterminée**. On a alors $X^n = (\delta_{kn})_{k \geq 0}$ où $\delta_{kn} = 1$ si $k = n$ et $\delta_{kn} = 0$ si $k \neq n$. Ceci justifie le choix de l'écriture $a_n X^n + \cdots + a_1 X + a_0$ pour un polynôme $(a_k)_{k \geq 0}$ de degré au plus n.

Soient P, Q, et R des polynômes. On a :
- ⋄ $(P + Q) + R = P + (Q + R)$: la loi + est associative,
- ⋄ $P + Q = Q + P$: la loi + est commutative,
- ⋄ $0 + P = P$: 0 est un neutre pour la loi +,
- ⋄ $P + (-1)P = 0$: tout élément de $\mathbb{K}[X]$ admet un inverse pour la loi +.

On dit alors que $(\mathbb{K}[X], +)$ est un groupe commutatif.

- ⋄ $(PQ)R = P(QR)$: la loi x est associative,
- ⋄ $PQ = QP$: la loi x est commutative,
- ⋄ $1 \cdot P = P$: 1 est un neutre pour pour la loi x,
- ⋄ $P(Q + R) = PQ + PR$: la loi x est distributive par rapport à la loi +.

On dit alors que $(\mathbb{K}[X], +, \times)$ est un anneau commutatif.

Proposition 0.6. *(Formule du binôme de Newton) Soient $P, Q \in \mathbb{K}[X]$ et $n \in \mathbb{N}$. Alors :*

$$(P + Q)^n = \sum_{k=0}^{n} \binom{n}{k} P^{n-k} Q^k\,.$$

Démonstration. La preuve est la même que pour la formule du binôme de Newton dans $\mathbb{K}$: par récurrence sur $n \geq 0$ en utilisant les règles de calcul sur les opérations dans $\mathbb{K}[X]$. □

Proposition 0.7. *Soient $P, Q \in \mathbb{K}[X]$. On a :*

$$\deg(P + Q) \leq \max(\deg P, \deg Q) \;\; \textit{et} \;\; \deg(PQ) = \deg P + \deg Q\,.$$

De plus, si $\deg P \neq \deg Q$*, on a* $\deg(P + Q) = \max(\deg P, \deg Q)$.

Démonstration. Prouvons d'abord l'inégalité pour le degré de la somme. Si $P = Q = 0$, alors $P+Q = 0$ et on a $\deg(P+Q) = \max(\deg P, \deg Q) = -\infty$. Supposons à présent que au moins un des deux polynômes P ou Q est non nul. On note $n = \max(\deg P, \deg Q)$ et on a $n \in \mathbb{N}$. On peut écrire :

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

On obtient $P + Q = \sum_{k=0}^{n}(a_k + b_k)X^k$, ce qui prouve $\deg(P + Q) \leq n$. Le coefficient de degré n de $P + Q$ est $a_n + b_n$. Supposons par exemple $\deg P \neq \deg Q$. Si $\deg P > \deg Q$, on a $a_n \neq 0$ et $b_n = 0$ donc $a_n + b_n = a_n \neq 0$ et $\deg(P + Q) = n$. Le cas $\deg P < \deg Q$ est similaire.

Montrons à présent l'égalité pour le degré du produit. Si $P = 0$ ou $Q = 0$, alors $PQ = 0$ et on a $\deg(PQ) = -\infty = \deg P + \deg Q$, où la dernière égalité vient du fait que la somme de $-\infty$ et de $N \in \{-\infty\} \cup \mathbb{N}$ vaut $-\infty$. Supposons à présent que P et Q sont non nuls. On écrit :

$$P = \sum_{k=0}^{p} a_k X^k\,, \qquad Q = \sum_{k=0}^{q} b_k X^k\,,$$

où p et q sont les degrés respectifs de P et Q (en particulier a_p et b_q sont non nuls). On a alors $PQ = \sum_{k=0}^{p+q}\left(\sum_{i+j=k} a_i b_j\right)X^k$, ce qui prouve $\deg(PQ) \leq p+q = \deg P + \deg Q$. Le coefficient de degré $p+q$ de PQ est $a_p b_q \neq 0$, et donc $\deg(PQ) = p+q = \deg P + \deg Q$. □

L'inégalité dans la proposition précédente peut être stricte comme le montre l'exemple suivant. Avec $P = X$, $Q = -X + 1$, $P + Q = 1$, on a :

$$\deg(P + Q) = 0 \neq 1 = \max(\deg P, \deg Q)\,.$$

Corollaire 0.8.
1. *$\forall A, B \in \mathbb{K}[X], AB = 0 \Rightarrow (A = 0$ ou $B = 0)$*
2. *$\forall A, B, C \in \mathbb{K}[X], (AC = BC$ et $C \neq 0) \Rightarrow A = B$*

Démonstration.
1. Par contraposée. Si A et B sont non nuls, alors $\deg A \in \mathbb{N}$ et $\deg B \in \mathbb{N}$. La proposition précédente donne donc $\deg(AB) = \deg A + \deg B \in \mathbb{N}$ et donc $AB \neq 0$.
2. Si $AC = BC$, on a $(A - B)C = 0$ et il suffit d'utiliser le point précédent pour obtenir $A - B = 0$.

□

Définition 0.9. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$. La fonction

$$\begin{aligned} f_P \colon \mathbb{K} &\to \mathbb{K} \\ x &\mapsto \sum_{k=0}^{n} a_k x^k = a_0 + a_1 x + \cdots + a_n x^n. \end{aligned}$$

est appelée **application polynomiale** associée au polynôme P.

On appellera application polynomiale sur $\mathbb{K}$ toute application $f : \mathbb{K} \to \mathbb{K}$ telle qu'il existe $P \in \mathbb{K}[X]$ tel que $f = f_P$. Dans la pratique, on écrira souvent $P(x)$ pour $f_P(x)$.

Remarque 0.10. Lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, si l'application polynomiale f_P est identiquement nulle alors on peut montrer que tous les coefficients a_k sont nuls et donc $P = 0$ (exercice : le faire). En particulier, un polynôme non nul définit une application non nulle.

Proposition 0.11. *Soient $P, Q \in \mathbb{K}[X]$ et $\lambda, x \in \mathbb{K}$. Alors :*

$$(P+Q)(x) = P(x) + Q(x)\,,\ (PQ)(x) = P(x)Q(x)\ \textit{ et } (\lambda P)(x) = \lambda P(x)\,.$$

Démonstration. Immédiat. □

Définition 0.12. (Composée de deux polynômes) Soient $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$. On définit :

$$P \circ Q = P(Q) = \sum_{k=0}^{n} a_k Q^k\,.$$

Exemple. *Si $P = X^5 + X + 1$ et $Q = X^2$, on a $P(Q) = X^{10} + X^2 + 1$.*

Proposition 0.13. *Soient P et Q deux polynômes non constants. Alors on a :*

$$\deg(P \circ Q) = \deg(P) \cdot \deg(Q)\,.$$

Démonstration. Exercice. □

0.2 Dérivation et formule de Taylor

Définition 0.14. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$. On appelle **polynôme dérivé de** P le polynôme P' suivant :

$$P' = \sum_{k=1}^{n} k a_k X^{k-1} \text{ si } \deg P \geq 1 \text{ et } P' = 0 \text{ sinon }\,.$$

Proposition 0.15. *Soit $P \in \mathbb{K}[X]$.*

1. *si* $\deg P \geq 1$*, alors on a :* $\deg(P') = \deg(P) - 1$
2. *si* $\deg P < 1$*, alors* $P' = 0$ *et* $\deg(P') = -\infty$

Démonstration. Immédiat. □

Proposition 0.16. *Soient $P, Q \in \mathbb{K}[X]$ et $\lambda, \mu \in \mathbb{K}$. Alors on a :*

1. $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$
2. $(PQ)' = P'Q + PQ'$

Démonstration. Exercice. □

On définit par récurrence les polynômes dérivés successifs de P. Par convention, $P^{(0)} = P$ et $P' = P^{(1)}$. Pour $k \geq 2$, on note $P^{(k)} = (P^{(k-1)})'$.

Proposition 0.17. *Soit $P = \sum_{j=0}^{n} a_j X^j$ un polynôme de degré n.*

Si $k \leq n$, $P^{(k)} = \sum_{j=k}^{n} a_j j(j-1)\cdots(j-k+1)X^{j-k} = \sum_{j=k}^{n} a_j \frac{j!}{(j-k)!} X^{j-k}$

Si $k > n$, $P^{(k)} = 0$.

Démonstration. Immediat par récurrence. □

Proposition 0.18. *Soient $P \in \mathbb{K}[X]$ et $k \in \mathbb{N}$. Alors on a :*

1. *si* $\deg P \geq k$*, alors on a :* $\deg(P^{(k)}) = \deg(P) - k$
2. *si* $\deg P < k$*, alors* $P^{(k)} = 0$ *et* $\deg(P^{(k)}) = -\infty$

Démonstration. Immédiat. □

Proposition 0.19. *Soient $P, Q \in \mathbb{K}[X]$, $\lambda, \mu \in \mathbb{K}$ et $n \in \mathbb{N}$. Alors on a :*

1. $(\lambda P + \mu Q)^{(n)} = \lambda P^{(n)} + \mu Q^{(n)}$
2. *(Formule de Leibniz)*

$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$$

Démonstration.
1. Immédiat.
2. Par récurrence sur n (exercice).

□

Proposition 0.20. *(Formule de Taylor) Soient $P \in \mathbb{K}[X]$ de degré $n \geq 0$ et $\alpha \in \mathbb{K}$. On a alors :*

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

Démonstration. On commence par montrer la formule pour le monôme X^n. On a :

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

$$= \sum_{k=0}^{n} \binom{n}{k} \alpha^{n-k} (X - \alpha)^k = (X - \alpha + \alpha)^n = X^n$$

en utilisant la formule du binôme de Newton. Considérons maintenant $P = \sum_{p=0}^{n} a_p X^p \in \mathbb{K}[X]$. En utilisant le cas précédent, on obtient :

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

$$= \sum_{p=0}^{n} a_p \sum_{k=0}^{n} \frac{(X^p)^{(k)}(\alpha)}{k!} (X - \alpha)^k = \sum_{p=0}^{n} a_p X^p = P\,.$$

□

0.3 Arithmétique sur les polynômes

Définition 0.21. Soient $A, B \in \mathbb{K}[X]$. On dit que B divise A (et on note $B \mid A$) s'il existe $C \in \mathbb{K}[X]$ tel que $A = BC$.

Exemple. *$B = X^2$ divise $A = (X-1)X^3(X+2)$. En effet, $A = BC$ où on note $C = (X-1)X(X+2)$.*

Remarque.

1. *Si $B \mid A$ avec $A \neq 0$, alors $\deg B \leq \deg A$. En effet, il existe alors $C \in \mathbb{K}[X]$ non nul tel que $A = BC$ et donc :*

$$\deg A = \deg B + \deg C \geq \deg B \,.$$

2. *Soient $A, B, C \in \mathbb{K}[X]$. Si $C \mid A$ et $C \mid B$, alors $C \mid AP + BQ$ pour tous $P, Q \in \mathbb{K}[X]$.*
3. *Soient $A, B \in \mathbb{K}[X]$. Alors on a : ($A \mid B$ et $B \mid A$) ssi il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$ (exercice : le prouver). On dit alors que A et B sont associés.*

Théorème 0.22 (Division euclidienne)**.** *Soient $A, B \in \mathbb{K}[X]$ tels que $B \neq 0$. Il existe alors un unique couple $(Q, R) \in (\mathbb{K}[X])^2$ tel que :*

$$A = QB + R \qquad \text{et} \qquad \deg R < \deg B.$$

Les polynômes Q et R sont appelés les **quotient** *et* **reste** *de la* **division euclidienne** *de A par B.*

Démonstration. Commençons par prouver l'unicité. Supposons qu'il existe $Q, \widetilde{Q}, R, \widetilde{R} \in \mathbb{K}[X]$ tels que :

$$A = QB + R = \widetilde{Q}B + \widetilde{R} \text{ avec } \deg R < \deg B \text{ et } \deg \widetilde{R} < \deg B \,.$$

On en déduit que $(Q - \widetilde{Q})B = \widetilde{R} - R$. Par l'absurde, supposons que $Q \neq \widetilde{Q}$. Alors $\deg((Q - \widetilde{Q})B) \geq \deg B$, tandis que $\deg(\widetilde{R} - R) < \deg B$, contradiction. Ainsi $Q = \widetilde{Q}$ et on déduit que $R = \widetilde{R}$.

On montre à présent l'existence. Notons $B = \sum_{k=0}^{p} b_k X^k$ où $p = \deg B \geq 0$ (puisque $B \neq 0$). Si $\deg B = 0$, le polynôme B est un polynôme constant non nul et il suffit de prendre $Q = A/b_0$ et $R = 0$. On peut donc supposer $p > 0$ dans la suite. On montre par récurrence sur $n \geq 0$ la propriété (H_n) suivante.

(H_n) : Pour tout $A \in \mathbb{K}_n[X]$, il existe $(Q, R) \in (\mathbb{K}[X])^2$ tel que $A = QB + R$ et $\deg R < p$.

- ◇ **Initialisation.** (H_n) est vraie pour tout $n < p$: en effet, si $\deg A \leq n < p$, il suffit de prendre $Q = 0$ et $R = A$.
- ◇ **Hérédité.** Supposons à présent que (H_n) est vraie pour un certain entier $n \geq p-1$ et montrons que (H_{n+1}) est vraie.

  Soit $A = \sum_{k=0}^{n+1} a_k X^k \in \mathbb{K}_{n+1}[X]$. On considère alors le polynôme suivant :

$$\widetilde{A} = A - \frac{a_{n+1}}{b_p} \cdot X^{n+1-p} \cdot B \,.$$

On remarque que $\widetilde{A} \in \mathbb{K}_n[X]$. On peut donc appliquer l'hypothèse de recurrence (H_n) au polynôme $\widetilde{A}$: il existe $(\widetilde{Q}, \widetilde{R}) \in (\mathbb{K}[X])^2$ tel que $\widetilde{A} = \widetilde{Q}B + \widetilde{R}$ et $\deg \widetilde{R} < p$. On pose alors :

$$Q = \widetilde{Q} + \frac{a_{n+1}}{b_p} \cdot X^{n+1-p} \text{ et } R = \widetilde{R}\,,$$

et on a alors $A = BQ + R$. On a prouvé que (H_{n+1}) est vraie.

Par application du principe de récurrence, la propriété (H_n) est vraie pour tout $n \geq 0$. □

Corollaire 0.23. *Pour tous $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$, on a :*

$$P(\alpha) = 0 \textit{ si et seulement si } X - \alpha \mid P\,.$$

Démonstration. La division euclidienne de P par $X - \alpha$ s'écrit :

$$P = (X - \alpha)Q + R \text{ avec } \deg R < 1$$

En particulier R est un polynôme constant. On évalue en $x = \alpha$ et on obtient $P(\alpha) = R$. On en déduit que $P(\alpha) = 0$ ssi $R = 0$ ssi $X - \alpha \mid P$. □

Exemple. *On peut effectuer la division euclidienne de deux polynômes en la posant, comme une division d'entiers. Dans l'exemple suivant, on calcule la division euclidienne de $A = 6X^3 - 2X^2 + X + 3$ par $B = X^2 - X + 1$.*

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

On obtient le quotient $Q = 6X + 4$ et le reste $R = -X - 1$.

Proposition 0.24. *Soient $A, B \in \mathbb{K}[X]$ tels que $(A, B) \neq (0, 0)$. L'ensemble des degrés des diviseurs communs à A et B est une partie non vide et majorée de $\mathbb{N}$.*

Démonstration. Comme 1 divise tous les polynômes, cet ensemble contient $\deg 1 = 0$ et est donc non vide. De plus, comme le polynôme nul ne divise que lui-même, il n'est pas diviseur commun, et l'ensemble considéré est donc inclus dans $\mathbb{N}$. Enfin, le degré de tout diviseur commun est majoré par $\max(\deg A, \deg B)$. □

Il existe donc un diviseur commun à A et B de degré maximal. Ceci conduit à la définition suivante :

Définition 0.25. Soient A et B deux polynômes de $\mathbb{K}[X]$ tels que $(A, B) \neq (0, 0)$. Tout diviseur commun à A et B de degré maximal est appelé un **plus grand diviseur commun (PGCD)** de A et B.

Remarque 0.26. Un PGCD de deux polynômes non tous deux nuls est non nul, car son degré est un entier naturel.

Remarque 0.27. Si D est un PGCD de A et B, alors λD est aussi un PGCD de A et B pour tout $\lambda \in \mathbb{K}^*$. On montrera qu'en fait, tout PGCD de A et B est de cette forme.

Proposition 0.28. *Soient $A, B \in \mathbb{K}[X]$ tel que $B \neq 0$. Si R est le reste de la division euclidienne de A par B, alors l'ensemble des diviseurs communs à A et B est égal à l'ensemble des diviseurs communs à B et R. En particulier, tout PGCD de A et B est aussi un PGCD de B et R et vice versa.*

Démonstration. On écrit la division euclidienne de A par B : $A = BQ + R$. Soit D un diviseur commun à A et B : $D \mid A$ et $D \mid B$. Il existe des polynômes $\tilde{A}$ et $\tilde{B}$ tels que $A = D\tilde{A}$ et $B = D\tilde{B}$. En remplaçant, on obtient :

$$R = A - BQ = D\tilde{A} - QD\tilde{B} = D(\tilde{A} - Q\tilde{B}),$$

donc $D \mid R$. Réciproquement, si $B = D\tilde{B}$ et $R = D\tilde{R}$, alors $A = BQ + R = D(Q\tilde{B} + \tilde{R})$, donc $D \mid A$. □

Proposition 0.29. *Soient $A, B \in \mathbb{K}[X]$ tels que $(A, B) \neq (0, 0)$. Soit D un PGCD de A et B. On a alors :*

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

Démonstration. Pour un polynôme P, notons $\mathcal{D}(P)$ l'ensemble des diviseurs de P. Montrons par récurrence sur $n \in \mathbb{N}$ la propriété suivante :

(H_n) : Si $A, B \in \mathbb{K}[X]$ sont tels que $(A, B) \neq (0, 0)$ et $\min(\deg A, \deg B) < n$ et si D est un PGCD de A et B, alors $\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(D)$.

Initialisation : Montrons tout d'abord (H_0). Soient $A, B \in \mathbb{K}[X]$ tels que $(A, B) \neq (0, 0)$ et $\min(\deg A, \deg B) < 0$. Alors exactement un des deux polynômes A et B est nul. Par exemple, $A \neq 0$ et $B = 0$. On a alors $\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(A)$ et donc (H_0) est vérifiée puisque tout PGCD de A et $B = 0$ est de la forme λA avec $\lambda \in \mathbb{K}^*$ (exo : le montrer).

Hérédité : Supposons à présent (H_n) vérifiée pour un certain $n \geq 0$ donné. Soient $A, B \in \mathbb{K}[X]$ tels que $(A, B) \neq (0, 0)$ et $\min(\deg A, \deg B) < n + 1$ et soit D un PGCD de A et B. On peut supposer par exemple que $\deg B \leq \deg A$. Si $\deg B < n$, alors on peut conclure par (H_n). Si $\deg B = n$, on a $B \neq 0$ et donc on peut écrire la division euclidienne de A par B : $A = BQ + R$ avec $\deg R < \deg B$. En particulier, on a $\deg R < \deg B = n$. En utilisant la proposition précédente, on a $\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(B) \cap \mathcal{D}(R)$ et D est donc aussi un PGCD de B et R. En utilisant l'hypothèse de récurrence (H_n), on obtient alors $\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(D)$. Ceci montre que (H_{n+1}) est vraie. Par application du principe de récurrence, la propriété est vérifiée pour tout n, ce qui montre la propriété désirée. □

Proposition-Définition 0.1. Soient $A, B \in \mathbb{K}[X]$ tels que $(A, B) \neq (0, 0)$. Soient D_1 et D_2 deux PGCD de A et B. Alors, D_1 et D_2 sont associés, c'est-à-dire qu'il existe $\lambda \in \mathbb{K}^*$ tel que $D_1 = \lambda D_2$. En particulier, il existe un unique PGCD unitaire de A et B. On l'appelle **le PGCD de A et B, et on le note** $PGCD(A, B)$.

Démonstration. D'après la proposition précédente, on a $\mathcal{D}(A)\cap\mathcal{D}(B) = \mathcal{D}(D_1) = \mathcal{D}(D_2)$, où on note encore $\mathcal{D}(P)$ l'ensemble des diviseurs de P. On a donc en particulier $D_1 \mid D_2$ et $D_2 \mid D_1$. Il existe donc des polynômes P et Q tels que $D_1 = PD_2$ et $D_2 = QD_1$, et alors $D_1 = PQD_1$. Comme $(A, B) \neq (0, 0)$, on a $D_1 \neq 0$ et donc $PQ = 1$. Les polynômes P et Q sont donc des polynômes constants non nuls.

En particulier, on en déduit l'existence d'un PGCD unitaire de A et B (il suffit de prendre un PGCD et de le diviser par son coefficient dominant). L'unicité vient du fait que deux polynômes unitaires associés sont égaux. □

On peut alors obtenir le pgcd de A et B en faisant des divisions euclidiennes successives, comme avec les entiers : c'est **l'algorithme d'Euclide**.

Algorithme d'Euclide.

1. Poser $R_0 = A$ et $R_1 = B$.
2. Tant que $R_1 \neq 0$:

$$R_2 = \text{reste de la division euclidienne de } R_0 \text{ par } R_1; \quad R_0 \leftarrow R_1, \quad R_1 \leftarrow R_2.$$

3. Le dernier reste non nul normalisé est le pgcd de A et B.

Lemme 0.30 (Bézout)**.** *Soient $A, B \in \mathbb{K}[X]$ tels que $(A, B) \neq (0, 0)$. Alors il existe deux polynômes $U, V \in \mathbb{K}[X]$ tels que :*

$$AU + BV = PGCD(A, B)$$

Démonstration. On montre par récurrence sur $n \in \mathbb{N}$ la propriété suivante :

(H_n) : Si $A, B \in \mathbb{K}[X]$ sont tels que $(A, B) \neq (0, 0)$ et $\min(\deg A, \deg B) < n$, alors il existe deux polynômes $U, V \in \mathbb{K}[X]$ tels que $AU + BV = PGCD(A, B)$.

Initialisation : Soient $A, B \in \mathbb{K}[X]$ tels que $(A, B) \neq (0, 0)$ et $\min(\deg A, \deg B) < 0$. Alors un des deux polynômes A et B est nul et l'autre non. Par exemple, supposons $A \neq 0$ et $B = 0$. Notons $a \neq 0$ le coefficient dominant de A. En posant $U = \frac{1}{a}$ et $V = 0$, on a alors que $AU + BV = \frac{1}{a}A$ est le polynôme unitaire associé à A, c'est-à-dire $PGCD(A, 0)$. La propriété (H_0) est donc vraie.

Hérédité : Supposons la propriété (H_n) vérifiée pour un entier $n \geq 0$ donné et montrons que (H_{n+1}) est vraie. Soient A, B deux polynômes tels que $(A, B) \neq (0, 0)$ et $\min(\deg A, \deg B) < n + 1$. Supposons par exemple $\deg(A) \geq \deg(B)$.

Si $\min(\deg A, \deg B) < n$, il suffit d'appliquer (H_n) pour conclure. Sinon, $\deg B = n$. En particulier, B est non nul. On effectue la division euclidienne de A par B :

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

On peut alors appliquer (H_n) au couple (B, R) : il existe $\tilde{U}, \tilde{V} \in \mathbb{K}[X]$ tels que

$$B\tilde{U} + R\tilde{V} = PGCD(B, R)\,.$$

Mais on a vu précédemment que $PGCD(A, B) = PGCD(B, R)$. On a donc :

$$PGCD(A, B) = B\tilde{U} + R\tilde{V} = B\tilde{U} + (A - BQ)\tilde{V} = A\tilde{V} + B(\tilde{U} - Q\tilde{V})\,.$$

On pose $U = \tilde{V}$ et $V = \tilde{U} - Q\tilde{V}$ et on a donc $PGCD(A,B) = AU + BV$. Ceci montre que (H_{n+1}) est vraie. Par application du principe de récurrence, la propriété (H_n) est vérifiée pour tout $n \in \mathbb{N}$, ce qui permet de conclure. $\square$

Exemple. *On veut calculer $PGCD(A,B)$ pour $A = X^4 - 4X^3 + 2X^2 + X + 6$ et $B = X^4 - 3X^3 + 2X^2 + X + 5$. L'algorithme d'Euclide donne successivement :*

$$X^4 - 4X^3 + 2X^2 + X + 6 = (X^4 - 3X^3 + 2X^2 + X + 5) \times 1 + (-X^3 + 1)$$
$$X^4 - 3X^3 + 2X^2 + X + 5 = (-X^3 + 1)(-X + 3) + (2X^2 + 2X + 2)$$
$$-X^3 + 1 = (2X^2 + 2X + 2)(-X/2 + 1/2)$$

Le dernier reste non nul est un PGCD de A et B donc $PGCD(A,B) = X^2 + X + 1$. En remontant l'algorithme précédent, on obtient :

$$(2X^2 + 2X + 2) = (-X^3 + 1)(X - 3) + B$$
$$(2X^2 + 2X + 2) = (A - B)(X - 3) + B$$
$$(2X^2 + 2X + 2) = (X - 3)A + (4 - X)B$$
$$X^2 + X + 1 = AU + BV \text{ avec } U = \frac{1}{2}X - \frac{3}{2} \text{ et } V = 2 - \frac{1}{2}X$$

Définition 0.31. On dit que deux polynômes P et Q de $\mathbb{K}[X]$ non tous les deux nuls sont **premiers entre eux** si $\mathrm{PGCD}(P,Q) = 1$, c'est-à-dire si leurs seuls diviseurs communs sont les polynômes constants non nuls.

Remarque 0.32. Soient $A, B, C \in \mathbb{K}[X]$ non nuls. On a alors : $\mathrm{PGCD}(A,B) = C$ si et seulement si il existe des polynômes $\tilde{A}$ et $\tilde{B}$ tels que $A = \tilde{A}C$, $B = \tilde{B}C$ avec $\tilde{A}$ et $\tilde{B}$ premiers entre eux (exercice : le montrer).

Exemple. *$X^2 - 1$ et $(X+1)(X+2)$ ne sont pas premiers entre eux puisque leur PGCD unitaire est $X + 1$. A l'inverse $X^2 + 1$ et $(X+1)(X+2)$ sont premiers entre eux.*

Proposition 0.33. *Soient $A, B \in \mathbb{K}[X]$. Alors A et B sont premiers entre eux si et seulement si il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$.*

Démonstration. Le sens direct est une conséquence immédiate du lemme de Bézout. Montrons la réciproque. Supposons qu'il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$. Alors tout diviseur commun à A et B divise aussi AU et BV et donc $AU + BV = 1$. Le polynôme D est donc constant non nul, ce qui permet de conclure. $\square$

Corollaire 0.34. *Soient $A, B, C \in \mathbb{K}[X]$ tels que A et B sont premiers entre eux, et A et C sont premiers entre eux. Alors A et BC sont premiers entre eux.*

Démonstration. Si A et B sont premiers entre eux et A et C sont premiers entre eux, alors d'après la proposition précédente il existe $U, V, \tilde{U}, \tilde{V} \in \mathbb{K}[X]$ tels que $AU + BV = 1$ et $A\tilde{U} + C\tilde{V} = 1$. En multipliant les deux égalités précédentes, on obtient :

$$1 = (AU + BV)(A\tilde{U} + C\tilde{V}) = A\hat{U} + BC\hat{V}$$

où l'on a noté $\hat{U} = U\tilde{U}A + BV\tilde{U} + UC\tilde{V}$ et $\hat{V} = V\tilde{V}$. Alors, toujours d'après la proposition précédente, les polynômes A et BC sont premiers entre eux. $\square$

Lemme 0.35 (Lemme de Gauss)**.** *Soient $A, B, C \in \mathbb{K}[X]$. Si A divise BC et si A et B sont premiers entre eux, alors A divise C.*

Démonstration. Supposons que A divise BC et que A et B sont premiers entre eux. Il existe donc deux polynômes U et V tels que $AU + BV = 1$. En particulier, on a alors $AUC + BVC = C$. Comme $A \mid BC$, il existe $Q \in \mathbb{K}[X]$ tel que $BC = AQ$. On a donc $AUC + BVC = A(UC + VQ) = C$ et donc $A \mid C$. $\square$

0.4 Racines d'un polynôme

Définition 0.36. Soient $P \in \mathbb{K}[X]$ et $r \in \mathbb{K}$. On dit que r est **racine** de P si $P(r) = 0$.

Définition 0.37. Soient $P \in \mathbb{K}[X]$ et $r \in \mathbb{K}$. **L'ordre de multiplicité** de r dans P est l'unique entier $m \geq 0$ tel que $(X - r)^m$ divise P et $(X - r)^{m+1}$ ne divise pas P. Par convention, l'ordre de multiplicité de tout r dans $P = 0$ est égal à $+\infty$.

Notons que r est une racine de P si et seulement si $m \geq 1$. Si l'ordre de multiplicité m est 1 (resp. 2, resp. ≥ 2), on dit que la racine r est **simple** (resp. **double**, resp. **multiple**).

Exemple. *Le polynôme* $(X-1)^2(X-2)(X-3)$ *a* 1 *comme racine double et* 2 *et* 3 *comme racines simples.*

Proposition 0.38. *Un polynôme non nul de degré n a au plus n racines dans $\mathbb{K}$.*

Démonstration. On procède par récurrence sur l'entier n. Un polynôme constant non nul P de degré $n = 0$ n'a pas de racines. Supposons la propriété vérifiée pour les polynômes de degré $\leq n$, où $n \geq 0$. Soit P un polynôme non nul de degré $n + 1$. Si P n'a pas de racine, la propriété est vérifiée. Sinon, soit r une racine de P. Le polynôme P peut donc s'écrire $P = (X - r)Q$, où Q est un polynôme de degré $\deg Q = n$. Par hypothèse de récurrence Q a au plus n racines, on en déduit que P a au plus $n + 1$ racines. □

Proposition 0.39. *Soit $P \in \mathbb{K}[X]$ non nul et soit $r \in \mathbb{K}$ une racine de P. La multiplicité m de la racine r est l'unique entier m tel que :*

$$P(r) = P'(r) = \cdots = P^{(m-1)}(r) = 0 \qquad \textit{et} \qquad P^{(m)}(r) \neq 0.$$

Démonstration. Soit r une racine de multiplicité m de P. Alors $P = (X - r)^m Q$ avec $Q(r) \neq 0$. En dérivant P, on obtient :

$$P' = m(X - r)^{m-1}Q + (X - r)^m Q' = (X - r)^{m-1}(mQ + (X - r)Q')\,.$$

P' est de la forme $(X - r)^{m-1}Q_1$ avec $Q_1 = mQ + (X - r)Q'$. En particulier $Q_1(r) = mQ(r) \neq 0$. Donc $P(r) = P'(r) = 0$ si et seulement si $m > 1$.

En dérivant k fois en utilisant la formule de Leibniz, on obtient que pour tout $k < m$,

$$P^{(k)} = (X - r)^{m-k}Q_k$$

avec $Q_k(r) = m(m - 1)\ldots(m - k + 1)Q(r) \neq 0$, et

$$P^{(m)} = Q_m \quad \text{avec} \quad Q_m(r) = m!\,Q(r) \neq 0.$$

Donc pour tout $k < m$, $P^{(k)}(r) = 0$, alors que $P^{(m)}(r) = m!Q(r) \neq 0$.

Réciproquement, supposons que $P(r) = P'(r) = \cdots = P^{(m-1)}(r) = 0$ et $P^{(m)}(r) \neq 0$. Soit n la multiplicité de r. D'après ce qui précède, on a :

$$P(r) = \cdots = P^{(n-1)}(r) = 0 \quad \text{et} \quad P^{(n)}(r) \neq 0.$$

Ceci montre que $m = n$. □

Exemple. *Soit* $P = X^5 - X^4 - 6X^3 + 14X^2 - 11X + 3$. *On a alors* $P' = 5X^4 - 4X^3 - 18X^2 + 28X - 11$, $P'' = 20X^3 - 12X^2 - 36X + 28$, $P^{(3)} = 60X^2 - 24X - 36$, $P^{(4)} = 120X - 24$. *On a donc* $P(1) = 1 - 1 - 6 + 14 - 11 + 3 = 0$, $P'(1) = 5 - 4 - 18 + 28 - 11 = 0$, $P''(1) = 20 - 12 - 36 + 28 = 0$, $P^{(3)}(1) = 60 - 24 - 36 = 0$ *et* $P^{(4)}(1) = 120 - 24 = 96 \neq 0$. *Ceci montre que 1 est racine de P de multiplicité 4.*

0.5 Décomposition en produit de polynômes irréductibles

Définition 0.40. Un polynôme non constant $P \in \mathbb{K}[X]$ est **irréductible** (sur $\mathbb{K}$) si les seuls diviseurs de P sont les polynômes constants non nuls λ (où $\lambda \in \mathbb{K}^*$) et les polynômes λP associés à P (où $\lambda \in \mathbb{K}^*$). Ainsi un polynôme irréductible est un polynôme non constant P tel que :

$$\forall A, B \in \mathbb{K}[X]\,, P = AB \Rightarrow (\deg A = 0 \text{ ou } \deg B = 0)$$

Remarque 0.41. La définition précédente est l'analogue des nombres premiers pour l'arithmétique dans $\mathbb{Z}$.

Exemple. *Tout polynôme de degré 1 est irréductible. En effet, si P de degré 1 se factorise $P = AB$, alors on a : $1 = \deg P = \deg A + \deg B$. Comme $\deg A$ et $\deg B$ sont des entiers, on en déduit que $\deg A = 0$ ou $\deg B = 0$, c'est-à-dire A est constant ou B est constant.*

Exemple. *$X^2 + 1$ n'est pas irréductible sur $\mathbb{C}$ puisque $X^2 + 1 = (X - i)(X + i)$.*

Exemple. *En revanche, $X^2 + 1$ est irréductible sur $\mathbb{R}$. En effet, $X^2 + 1$ n'a pas de racine réelle donc n'admet aucun diviseur de degré 1 dans $\mathbb{R}[X]$. Les seuls diviseurs de $X^2 + 1$ sont donc les polynômes constants non nuls et les polynômes de la forme $\lambda(X^2 + 1)$ avec $\lambda \in \mathbb{R}^*$. Le polynôme $X^2 + 1$ est donc irréductible. Plus généralement, tout polynôme réel de degré 2 avec discriminant strictement négatif (donc sans racine réelle) est irréductible.*

Lemme 0.42 (Lemme d'Euclide)**.** *Soit $P \in \mathbb{K}[X]$ irréductible et $A, B \in \mathbb{K}[X]$. Si $P \mid AB$ alors $P \mid A$ ou $P \mid B$.*

Démonstration. Si $P \mid A$, alors la conclusion est vérifiée. Si $P \nmid A$ alors les polynômes A et P sont premiers entre eux. Par le lemme de Bézout il existe U, V tels que $AU + PV = 1$. Multiplier par B donne $AUB + PVB = B$. Comme $P \mid AB$, on obtient que $P \mid AUB$. Comme P divise aussi PVB, le polynôme P divise la somme $AUB + PVB = B$. □

Le théorème suivant est l'analogue du théorème fondamental de l'arithmétique :

Théorème 0.43 (Factorisation en produit de polynômes irréductibles)**.** *Tout polynôme $P \in \mathbb{K}[X] \setminus \{0\}$ s'écrit*

$$P = \lambda P_1^{\alpha_1} \cdots P_N^{\alpha_N},$$

où $\lambda \in \mathbb{K}^*$, $N \in \mathbb{N}$, les P_i sont des polynômes irréductibles unitaires deux à deux distincts et les α_i sont des entiers strictement positifs.

Cette décomposition est unique à réarrangement près.

Démonstration. On prouve par récurrence sur $n \in \mathbb{N}$ la propriété suivante :

(H_n) : Pour tout polynôme P non nul tel que $\deg P \leq n$, il y a existence et unicité d'une factorisation en produit de polynômes irréductibles.

Initialisation : Si $P = a_0$ où $a_0 \neq 0$, il suffit de prendre $\lambda = a_0$ et $N = 0$ et on a bien $P = \lambda$. L'unicité est claire. Ceci montre (H_0).

Hérédité : Supposons (H_n) vraie. Montrons (H_{n+1}). Soit un polynôme P de degré $\leq n+1$. Si $\deg P < n$, il suffit d'utiliser (H_n). Supposons à présent $\deg P = n+1$. Commençons par prouver l'existence d'une factorisation.

Si P est irréductible, on choisit λ égal au coefficient dominant de P, on prend $N=1$, $P_1 = \frac{1}{\lambda}P$ et $\alpha_1 = 1$.

Supposons à présent P non irréductible. Il peut donc être écrit sous la forme $P = QR$ où Q et R sont non constants. Comme $\deg P = \deg Q + \deg R$, on a $\deg Q \leq n$ et $\deg R \leq n$. On applique alors l'hypothèse de récurrence (H_n) à Q et à R, et on peut donc factoriser Q et R :

$$Q = \lambda_Q Q_1^{\beta_1} \cdots Q_L^{\beta_L} \text{ et } R = \lambda_R R_1^{\gamma_1} \cdots R_M^{\gamma_M}$$

où $\lambda_Q, \lambda_R \in \mathbb{K}^*$, $L, M \geq 1$, les Q_i et R_j sont irréductibles unitaires et les β_i et γ_j sont des entiers strictement positifs. On a alors :

$$P = (\lambda_Q Q_1^{\beta_1} \cdots Q_L^{\beta_L})\,(\lambda_R R_1^{\gamma_1} \cdots R_M^{\gamma_M}),$$

En regroupant les facteurs communs, on obtient bien une décomposition de la forme :

$$P = \lambda P_1^{\alpha_1} \cdots P_N^{\alpha_N}.$$

où $\lambda = \lambda_Q \cdot \lambda_R \in \mathbb{K}^*$, $N \geq 1$, les P_i sont irréductibles unitaires deux à deux distincts avec $\{P_1, \ldots, P_N\} = \{Q_1, \ldots, Q_L, R_1, \ldots, R_M\}$ et les α_i sont des entiers strictement positifs. Ceci prouve l'existence.

Montrons maintenant l'unicité. Supposons que P admette deux factorisations en produits de polynômes irréductibles :

$$P = \lambda P_1^{\alpha_1} \cdots P_N^{\alpha_N} = \mu S_1^{a_1} \cdots S_K^{a_K}$$

où $\lambda, \mu \in \mathbb{K}^*$, $N, K \geq 1$, les P_i et S_j sont irréductibles unitaires et les α_i et a_j sont des entiers positifs. Alors S_1 divise le produit $P_1^{\alpha_1} \cdots P_N^{\alpha_N}$. Par le lemme d'Euclide, S_1 divise un des polynômes P_i. Comme S_1 et P_i sont irréductibles et unitaires, on en déduit que $S_1 = P_i$. On peut alors diviser les deux décompositions ci-dessus par $P_i = S_1$. L'hypothèse de récurrence (H_n) donne l'unicité de la factorisation pour le quotient de P par $P_i = S_1$. En multipliant par $P_i = S_1$, on obtient l'unicité de la factorisation pour P.

Ceci prouve (H_{n+1}). Par application du principe de récurrence, la propriété (H_n) est vérifiée pour tout $n \in \mathbb{N}$, ce qui permet de conclure. □

Remarque 0.44. Les diviseurs de P dans $\mathbb{K}[X]$ sont alors les polynômes de la forme $\mu P_1^{\beta_1} \cdots P_N^{\beta_N}$, où $\mu \in \mathbb{K}^*$ et les β_i sont des entiers tels que $0 \leq \beta_i \leq \alpha_i$.

On admettra le théorème suivant, appelé théorème de d'Alembert-Gauss ou encore théorème fondamental de l'algèbre :

Théorème 0.45 (Théorème de d'Alembert-Gauss)**.** *Tout polynôme non constant de* $\mathbb{C}[X]$ *admet une racine dans* $\mathbb{C}$.

Corollaire 0.46. *Les polynômes irréductibles dans* $\mathbb{C}[X]$ *sont les polynômes de degré* 1.

Démonstration. On a déjà vu que les polynômes de degré 1 sont irréductibles. Réciproquement, soit $P \in \mathbb{C}[X]$ irréductible. D'après le théorème de d'Alembert-Gauss, P admet une racine r dans $\mathbb{C}$. Alors $X - r$ divise P. Comme P est irréductible, il existe $\lambda \in \mathbb{C}^*$ tel que $P = \lambda(X - r)$. □

Corollaire 0.47. *Tout polynôme non constant $P \in \mathbb{C}[X]$ s'écrit sous la forme :*

$$P = \lambda \prod_{i=1}^{N} (X - r_i)^{\alpha_i}$$

où $\lambda \in \mathbb{C}^*$ est le coefficient dominant de P, $N \geq 1$, $r_1, \ldots, r_N \in \mathbb{C}$ sont les racines deux à deux distinctes de P dans $\mathbb{C}$ de multiplicités respectives $\alpha_1, \ldots, \alpha_N \geq 1$.

Démonstration. C'est une conséquence immédiate du corollaire précédent et du théorème de factorisation en produit de polynômes irréductibles. □

Corollaire 0.48. *Les polynômes irréductibles dans $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 avec discriminant strictement négatif.*

Démonstration. On a déjà vu que les polynômes de degré 1 et les polynômes de degré 2 avec discriminant strictement négatif sont irréductibles sur $\mathbb{R}$.

Soit $P \in \mathbb{R}[X]$ irréductible sur $\mathbb{R}$, et supposons que $\deg P \geq 2$. D'après le théorème de d'Alembert-Gauss, P admet une racine r dans $\mathbb{C}$. Mais puisque P est un polynôme réel, on a $P = \overline{P}$ et donc :

$$P(\overline{r}) = \overline{P}(\overline{r}) = \overline{P(r)} = \overline{0} = 0$$

et donc $\overline{r}$ est aussi une racine de P. Comme P est irréductible, on a $r \notin \mathbb{R}$ (sinon $X - r$ diviserait P dans $\mathbb{R}[X]$. Comme P est irréductible et de degré ≥ 2, on obtiendrait une contradiction). Ceci montre $r \neq \overline{r}$. Finalement, P admet dans $\mathbb{C}[X]$ comme diviseur le polynôme $(X - r)(X - \overline{r})$. Il existe donc $Q \in \mathbb{C}[X]$ tel que :

$$P = (X - r)(X - \overline{r})Q = (X^2 - (r + \overline{r})X + r\overline{r})Q = (X^2 - 2\mathrm{Re}(r)X + |r|^2)Q$$

Comme P est un polynôme réel, on obtient que Q est aussi réel. Finalement, comme P est irréductible, Q est un polynôme constant : $Q = \lambda \in \mathbb{R}^*$. On a donc :

$$P = \lambda(X^2 - 2\mathrm{Re}(r)X + |r|^2)$$

Le polynôme P est donc de degré 2 de discriminant $\Delta = 4\lambda^2(\mathrm{Re}(r)^2 - |r|^2) < 0$. □

Corollaire 0.49. *Tout polynôme non constant $P \in \mathbb{R}[X]$ s'écrit sous la forme :*

$$P = \lambda \cdot \prod_{i=1}^{N} (X - r_i)^{\alpha_i} \cdot \prod_{j=1}^{M} (X^2 + a_j X + b_j)^{\beta_j}$$

avec $\lambda \in \mathbb{R}^*$, $N \in \mathbb{N}$, $r_1, \ldots, r_N \in \mathbb{R}$ sont les racines deux à deux distinctes de P dans $\mathbb{R}$ de multiplicités respectives $\alpha_1, \ldots, \alpha_N \geq 1$, $M \in \mathbb{N}$, les couples $(a_1, b_1), \ldots, (a_M, b_M) \in \mathbb{R}^2$ deux à deux distincts sont tels que $a_j^2 - 4b_j < 0$ pour tout $1 \leq j \leq M$ et $\beta_1, \ldots, \beta_M \geq 1$.

Démonstration. C'est une conséquence immédiate du corollaire précédent et du théorème de factorisation en produit de polynômes irréductibles. □

Exemple. *On obtient les décompositions en produits de facteurs irréductibles suivantes pour $X^4 - 1$:*

$$X^4 - 1 = (X-1)(X-i)(X+1)(X+i) \text{ dans } \mathbb{C}[X]$$

$$= (X-1)(X+1)(X^2+1) \text{ dans } \mathbb{R}[X]$$

Exemple. *On obtient les décompositions en produits de facteurs irréductibles suivantes pour $X^4 + 1$:*

$$X^4 + 1 = (X - \exp(i\frac{\pi}{4}))(X - \exp(i\frac{3\pi}{4}))(X - \exp(i\frac{5\pi}{4}))(X - \exp(i\frac{7\pi}{4})) \text{ dans } \mathbb{C}[X]$$

$$= (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1) \text{ dans } \mathbb{R}[X]$$

0.6 Fractions rationnelles et décomposition en éléments simples

0.6.1 Fractions rationnelles

Définition 0.50. Une **fraction rationnelle** (à coefficients dans $\mathbb{K}$) est le quotient de deux polynômes, c'est à dire

$$F = \frac{P}{Q} \quad \text{avec } P \in \mathbb{K}[X],\ Q \in \mathbb{K}[X] \setminus \{0\}.$$

Remarque 0.51. Voici comment définir rigoureusement la fraction rationnelle $F = P/Q$. On peut vérifier que la relation $\sim$ définie par $(P,Q) \sim (R,S)$ ssi $P\,S = Q\,R$ est une relation d'équivalence sur $\mathbb{K}[X] \times \mathbb{K}[X] \setminus \{0\}$. La fraction rationnelle $F = P/Q$ est alors la classe d'équivalence de (P,Q).

Notation. *On note $\mathbb{K}(X)$ l'ensemble des fractions rationnelles à coefficients dans $\mathbb{K}$.*

On définit l'addition et la multiplication de fractions rationnelles par :

$$\frac{P}{Q} + \frac{R}{S} = \frac{P\,S + Q\,R}{Q\,S}, \qquad \frac{P}{Q} \times \frac{R}{S} = \frac{P\,R}{Q\,S}.$$

Remarque 0.52. Muni de ces deux opérations, on peut vérifier que $\mathbb{K}(X)$ est un corps.

Définition 0.53. Le **degré** d'une fraction rationnelle $F = \frac{P}{Q}$ est par définition :

$$\deg(F) = \deg(P) - \deg(Q)$$

Notons que $\deg(F)$ est un élément de $\mathbb{Z} \cup \{-\infty\}$.

Soit $F \in \mathbb{K}(X)$ une fraction rationnelle. Alors F peut s'écrire $\frac{P}{Q}$ où $P \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X] \setminus \{0\}$ sont premiers entre eux. Cette écriture est unique, à une constante multiplicative près. Elle s'appelle la **représentation irréductible** de F.

Définition 0.54. Soit $F \in \mathbb{K}(X)$ donnée sous forme irréductible $\frac{P}{Q}$. On appelle **zéros** de F les zéros de P. On appelle **pôles** de F les zéros de Q. La multiplicité d'un zéro ou d'un pôle de F est sa multiplicité en tant que zéro de P ou de Q.

Soit $F = \frac{P}{Q}$ une fraction rationnelle donnée sous forme irréductible. Soit $\mathcal{P} \subset \mathbb{K}$ l'ensemble des pôles de F. On associe à F la fonction suivante :

$$\begin{aligned} f_F \colon \mathbb{K} \setminus \mathcal{P} &\to \mathbb{K} \\ x &\mapsto \frac{P(x)}{Q(x)}. \end{aligned}$$

Cette fonction s'appelle **l'application rationnelle associée** à F. On écrira souvent $F(x)$ à la place de $f_F(x)$.

0.6.2 Décomposition en éléments simples

Voici le résultat principal de cette section :

Théorème 0.55 (Décomposition en éléments simples dans $\mathbb{C}(X)$)**.** *Soit*

$$F = \frac{A}{B} \in \mathbb{C}(X).$$

Étant donnée la décomposition en produit de polynômes irréductibles de B :

$$B = \lambda(X - r_1)^{\alpha_1} \times \cdots \times (X - r_N)^{\alpha_N},$$

on peut écrire F de manière unique comme somme :

- *d'un polynôme E, appelé la partie entière de F, qui est le quotient de la division euclidienne de A par B,*
- *d'éléments simples $\dfrac{c_{ij}}{(X - r_i)^j}$ où $1 \leq i \leq N$, $1 \leq j \leq \alpha_i$, $c_{ij} \in \mathbb{C}$.*

On a alors :

$$F = E + \sum_{i=1}^{N} \sum_{j=1}^{\alpha_i} \frac{c_{ij}}{(X - r_i)^j}.$$

Pour prouver le théorème précédent, commençons par prouver le résultat suivant :

Lemme 0.56 (Division suivant les puissances croissantes)**.** *Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$ tel que $B(0) \neq 0$. Pour tout $n \geq 0$ il existe $(Q, R) \in \mathbb{K}_n[X] \times \mathbb{K}[X]$ unique tel que :*

$$A = BQ + X^{n+1}R.$$

Démonstration. On démontre le lemme par récurrence sur n. Si $n = 0$, en écrivant :

$$A = a_N X^N + \cdots + a_0 \quad \text{et} \quad B = b_M X^M + \cdots + b_0,$$

par hypothèse, on a $b_0 = B(0) \neq 0$. On cherche un polynôme Q de degré au plus 0, donc constant. Le seul possible est

$$Q = \frac{a_0}{b_0}$$

car on a alors $(A-BQ)(0) = a_0-b_0\cdot(a_0/b_0) = 0$, donc $X \mid (A-BQ)$, et donc $A-BQ = XR$ pour un certain polynôme $R \in \mathbb{K}[X]$.

Supposons l'hypothèse satisfaite jusqu'à l'ordre $n-1$, avec $n \geq 1$. Il existe donc $Q_{n-1} \in \mathbb{K}_{n-1}[X]$ et $R_{n-1} \in \mathbb{K}[X]$ tels que

$$A = BQ_{n-1} + X^n R_{n-1}.$$

Procédant comme ci-dessus, on peut écrire :

$$R_{n-1} = \lambda B + XR,$$

où $\lambda = R_{n-1}(0)/b_0$ et $R \in \mathbb{K}[X]$. On a donc :

$$A = B(Q_{n-1} + \lambda X^n) + X^{n+1}R,$$

ce qui prouve l'existence de la décomposition à l'ordre n en posant :

$$Q = Q_{n-1} + \lambda X^n \in \mathbb{K}_n[X]\,.$$

Supposons qu'il y ait un autre couple $(\tilde{Q}, \tilde{R})$ convenant. On a alors :

$$B(Q-\tilde{Q}) = X^{n+1}(\tilde{R}-R).$$

Comme $B(0) \neq 0$, les polynômes X^{n+1} et B sont premiers entre eux. D'après le lemme de Gauss, X^{n+1} divise donc $Q-\tilde{Q}$. Mais comme $Q-\tilde{Q}$ est de degré au plus n, ceci implique que $Q = \tilde{Q}$ et donc $R = \tilde{R}$. Ceci prouve l'unicité de la décomposition à l'ordre n. □

Corollaire 0.57. *Soient $r \in \mathbb{K}$, $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$ tel que $B(r) \neq 0$. Pour tout $n \geq 0$, il existe $(Q,R) \in \mathbb{K}_n[X] \times \mathbb{K}[X]$ unique tel que :*

$$A = BQ + (X-r)^{n+1}R.$$

On peut maintenant conclure la preuve du théorème 0.55 :

Preuve du théorème 0.55. On montre l'existence de la décomposition dans $\mathbb{C}(X)$ par récurrence sur le nombre N de racines distinctes du dénominateur B.

Quand $N = 0$, $F \in \mathbb{C}[X]$. On prend $E = F$.

Supposons l'existence établie pour $N-1$ pôles distincts, où $N \geq 1$. Supposons que :

$$B = \lambda(X-r_1)^{\alpha_1} \times \cdots \times (X-r_N)^{\alpha_N}.$$

où les r_i sont distincts deux à deux. D'après le corollaire 0.57 appliqué aux polynômes A et $\tilde{B} = \lambda(X-r_1)^{\alpha_1} \times \cdots \times (X-r_{N-1})^{\alpha_{N-1}}$ avec $r = r_N$ et $n = \alpha_N - 1$, on a :

$$A = \tilde{B}Q + (X-r_N)^{\alpha_N}R\,,$$

où $Q \in \mathbb{C}_{\alpha_N-1}[X]$ et $R \in \mathbb{C}[X]$. On obtient alors :

$$F = \frac{A}{B} = \frac{A}{\tilde{B}\cdot(X-r_N)^{\alpha_N}} = \frac{Q}{(X-r_N)^{\alpha_N}} + \frac{R}{\tilde{B}}.$$

Comme $\deg Q \leq \alpha_N - 1$, on peut l'écrire (exercice : le vérifier) :

$$Q = c_{N1}(X-r_N)^{\alpha_N-1} + \cdots + c_{N\alpha_N-1}(X-r_N) + c_{N\alpha_N},$$

et on obtient donc :

$$F = \sum_{j=1}^{\alpha_N} \frac{c_{Nj}}{(X - r_N)^j} + \frac{R}{\tilde{B}}.$$

On applique maintenant l'hypothèse de récurrence à $R/\tilde{B}$, et la preuve de l'existence est complète.

Pour prouver l'unicité, on peut se ramener au cas où

$$E + \sum_{i=1}^{N} \sum_{j=1}^{\alpha_i} \frac{c_{ij}}{(X - r_i)^j} = 0,$$

et on montre que le polynôme E et les coefficients c_{ij} sont nuls.

En multipliant cette égalité par $(X - r_N)^{\alpha_N}$ puis en évaluant en $x = r_N$, on obtient $c_{N\alpha_N} = 0$. On réitère en multipliant successivement par $(X - r_N)^{\alpha_N - 1}$, …, $(X - r_N)$ puis en évaluant en $x = r_N$, on obtient $c_{N\alpha_N} = c_{N\alpha_N - 1} = \cdots = c_{N1} = 0$. En réitérant successivement le même procédé avec les autres pôles r_i, on trouve que tous les coefficients c_{ij} sont nuls. On obtient donc $E = 0$. Ceci montre l'unicité. □

Théorème 0.58 (Décomposition en éléments simples dans $\mathbb{R}(X)$)**.** *Soit*

$$F = \frac{A}{B} \in \mathbb{R}(X).$$

Étant donnée la décomposition en produit de polynômes irréductibles de B :

$$B = \lambda(X - r_1)^{\alpha_1} \times \cdots \times (X - r_N)^{\alpha_N} \times (X^2 + a_1 X + b_1)^{\beta_1} \times \cdots \times (X^2 + a_M X + b_M)^{\beta_M},$$

on peut écrire F de manière unique comme somme :

- *d'un polynôme E, appelé la partie entière de F, qui est le quotient de la division euclidienne de A par B,*

- *d'éléments simples de première espèce :*

$$\frac{c_{ij}}{(X - r_i)^j},$$

  où $1 \leq i \leq N$, $1 \leq j \leq \alpha_i$, $c_{ij} \in \mathbb{R}$,

- *d'éléments simples de seconde espèce*

$$\frac{d_{ij} X + e_{ij}}{(X^2 + a_i X + b_i)^j},$$

  où $1 \leq i \leq M$, $1 \leq j \leq \beta_i$, $d_{ij}, e_{ij} \in \mathbb{R}$.

On a alors :

$$F = E + \sum_{i=1}^{N} \sum_{j=1}^{\alpha_i} \frac{c_{ij}}{(X - r_i)^j} + \sum_{i=1}^{M} \sum_{j=1}^{\beta_i} \frac{d_{ij} X + e_{ij}}{(X^2 + a_i X + b_i)^j}.$$

Démonstration. Admis □

En pratique, pour décomposer une fraction rationnelle F en éléments simples :

- on commence par écrire F sous forme irréductible $F = P/Q$
- on calcule d'abord la partie entière E de F : c'est le quotient de la division euclidienne de P par Q
- on factorise Q en produit de polynômes irréductibles
- on écrit la forme a priori de la décomposition en éléments simples cherchée (cf les théorèmes 0.55 et 0.58)
- pour un pôle r d'ordre α, le coefficient de $\frac{1}{(X-r)^\alpha}$ s'obtient en multipliant par $(X-r)^\alpha$ et en évaluant en $X = r$

Remarque 0.59. Si r est un pôle simple de F, alors le coefficient de $\frac{1}{X-r}$ est $\dfrac{P(r)}{Q'(r)}$.

Remarque 0.60. Pour déterminer les autres coefficients, on peut évaluer en un point, multiplier par X^k et regarder la limite en $+\infty$...

Remarque 0.61. Si on calcule la décomposition en éléments simples sur $\mathbb{R}$ et qu'il y a un polynôme de degré 2 irréductible dans la factorisation de Q, on peut commencer par calculer la décomposition en éléments simples sur $\mathbb{C}$ et ensuite regrouper les parties polaires correspondant aux pôles conjugués.

Exemple 1 : $F = \dfrac{X^4+1}{X^3-1}$ dans $\mathbb{C}(X)$

On calcule la partie entière de F en calculant le quotient de la division euclidienne de X^4+1 par X^3-1. On trouve que la partie entière de F est X. Ensuite on factorise :

$$X^3 - 1 = (X-1)(X-j)(X-j^2)$$

On en déduit que F se décompose sous la forme :

$$F = X + \frac{a}{X-1} + \frac{b}{X-j} + \frac{c}{X-j^2}$$

où a, b et c sont trois nombres complexes à déterminer.

On multiplie F par $(X-1)$. On obtient alors :

$$\frac{X^4+1}{(X-j)(X-j^2)} = X(X-1) + a + \frac{b}{X-j} + \frac{c}{X-j^2}$$

puis on évalue en $x = 1$. On trouve : $a = \frac{2}{3}$.

On multiplie de même par $(X-j)$ puis on évalue en $x = j$. Ceci donne $b = -\frac{1}{3}$.

On remarque que $F = \overline{F}$. Par unicité de la décomposition, on a alors $a = \overline{a}$, $b = \overline{c}$ et $c = \overline{b}$. On a donc $c = \overline{b} = -\frac{1}{3}$. On obtient donc la décomposition suivante :

$$F = X + \frac{2}{3}\frac{1}{X-1} - \frac{1}{3}\frac{1}{X-j} - \frac{1}{3}\frac{1}{X-j^2}.$$

Exemple 2 : $F = \dfrac{X^3+1}{X(X-1)(X^2+1)^2}$ dans $\mathbb{R}(X)$

La partie entière de F est nulle. La décomposition a priori s'écrit :

$$F = \frac{a}{X} + \frac{b}{X-1} + \frac{cX+d}{X^2+1} + \frac{eX+f}{(X^2+1)^2}$$

où a, b, c, d, e, f sont des nombres réels à déterminer.

On multiplie F par $(X^2+1)^2$ puis on évalue en $x = i$. On obtient $e = 1$ et $f = 0$. On simplifie et on obtient :

$$\frac{1}{X(X-1)(X^2+1)} = \frac{a}{X} + \frac{b}{X-1} + \frac{cX+d}{X^2+1}.$$

On multiplie alors par X^2+1 et on évalue en $x = i$. On obtient : $c = \frac{1}{2}$ et $d = -\frac{1}{2}$.

On multiplie les deux membres par X puis on passe à la limite quand $x \to +\infty$. Ceci donne : $a + b + c = 0$. De même, si on multiplie les deux membres par X puis on évalue en $x = 0$, on trouve $a = -1$. On en déduit que $b = 1/2$.

On obtient donc la décomposition suivante :

$$F = -\frac{1}{X} + \frac{1}{2(X-1)} + \frac{X-1}{2(X^2+1)} + \frac{X}{(X^2+1)^2}.$$