Cours : Arithmétique des polynômes

Antoine Boivin

29 septembre 2024

Table des matières

1 Généralités sur les polynômes

Définition 1.1 (Une construction des polynômes)**.** Soit $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p \coloneqq \mathbb{Z}/p\mathbb{Z}$... un corps commutatif. Un polynôme (à une indéterminée) à coefficients dans $\mathbb{K}$ est une suite d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang i.e. une suite $(a_n)_{n\in\mathbb{N}}$ telle qu'il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$, $a_n = 0$.
On note $\mathbb{K}^{(\mathbb{N})}$ l'ensemble des polynômes.

Exemple 1.2.
— $0_{\mathbb{K}^{(\mathbb{N})}} \coloneqq (0, 0, \ldots)$ et $1_{\mathbb{K}^{(\mathbb{N})}} \coloneqq (1, 0, 0, \ldots)$
— $(1, 2, 4, 0, 0, \ldots)$ « correspond » au polynôme $1 + 2X + 4X^2$

Définition 1.3. Soient $P = (a_k)_{k\in\mathbb{N}}, Q = (b_k)_{k\in\mathbb{N}}$ deux polynômes et $\lambda \in \mathbb{K}$. On peut définir la somme de P et Q :

$$P + Q \coloneqq (a_k + b_k)_{k\in\mathbb{N}},$$

la multiplication de P par le scalaire λ :

$$\lambda \cdot P = \lambda P \coloneqq (\lambda a_k)_{k\in\mathbb{N}},$$

et le produit de P et Q :

$$P \times Q = PQ \coloneqq \left(\sum_{i+j=k} a_i b_j \right)_{k\in\mathbb{N}}$$

Exemple 1.4.
— Pour tout $k \in \mathbb{N} \setminus \{0\}$, $(0,1,0,\dots)^k = (0,\dots,0,1,0,\dots)$ où le 1 est à la kème place.
— $(1,2,4,0,\dots) + (2,3,5,1,0,\dots) = (3,5,9,1,0,\dots)$
— $(1,2,3,0,\dots) \times (2,4,5,0,\dots) = (1,8,19,22,15,0,\dots)$

Proposition 1.5. *Soient P, Q, R trois polynômes et $\lambda, \mu \in \mathbb{K}$. Alors*
— $P + Q = Q + P$ *(commutativité de $+$);*
— $P + (Q + R) = (P + Q) + R$ *(associativité de $+$);*
— $P + 0 = P$ *(0 est l'élément neutre de $+$);*
— $P(Q + R) = PQ + PR$ *(distributivité de $\times$ par rapport à $+$);*
— $P(QR) = (PQ)R$ *(associativité de $\times$);*
— $P \times 1_{\mathbb{K}^{(\mathbb{N})}} = 1_{\mathbb{K}^{(\mathbb{N})}} \times P = P$ *($1_{\mathbb{K}^{(\mathbb{N})}}$ est l'élément neutre de $\times$)*
— $PQ = QP$ *(commutativité de $\times$);*
— $\lambda 1_{\mathbb{K}^{(\mathbb{N})}} \times P = \lambda P$;
— $(\lambda + \mu)P = \lambda P + \mu P$
— $(\lambda\mu)P = \lambda(\mu P)$
— $\lambda(P + Q) = \lambda P + \lambda Q$

Remarque 1.6. On dit que $(\mathbb{K}^{(\mathbb{N})}, +)$ est un groupe commutatif, $(\mathbb{K}^{(\mathbb{N})}, +, \times)$ est un anneau commutatif, $(\mathbb{K}^{(\mathbb{N})}, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel et $(\mathbb{K}^{(\mathbb{N})}, +, \times, \cdot)$ est une $\mathbb{K}$-algèbre commutative.

Remarque 1.7. Notons $X = (0,1,0,\dots)$ alors $X^k = (0,\dots,0,1,0,\dots)$. Alors tout polynôme $P = (a_k)_{k\in\mathbb{N}}$ s'écrit

$$P = (a_k)_{k\in\mathbb{N}} = \sum_{k\in\mathbb{N}} a_k(0,\dots,0,1,0,\dots) = \sum_{k\in\mathbb{N}} a_k X^k.$$

où, par convention, $X^0 = 1_{\mathbb{K}^{(\mathbb{N})}}$.

Remarque 1.8. Le symbole "X" est muet. On aurait pu le remplacer par $x, t, \diamondsuit, \spadesuit, \text{☺} \dots$

Remarque 1.9. Il n'est pas nécessaire de se placer sur un corps $\mathbb{K}$ pour définir les polynômes, les opérations ou pour avoir toutes ces propriétés. On peut reprendre les constructions et les résultats précédents avec $\mathbb{K} = \mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, k[t], \dots$ (et même d'objets encore plus généraux). Le fait de se placer sur un corps deviendra crucial dans la suite du cours.

Notation 1.10. On notera $\mathbb{K}[X]$ l'ensemble des polynômes à une indéterminée à coefficients dans $\mathbb{K}$ muni de la somme, la multiplication par un scalaire et du produit.

Remarque 1.11. Si $\mathbb{K} \subset \mathbb{L}$ (par exemple, $\mathbb{Q} \subset \mathbb{R}$ ou $\mathbb{R} \subset \mathbb{C}$) alors $\mathbb{K}[X] \subset \mathbb{L}[X]$

Définition 1.12. Soit $P = \sum a_k X^k \in \mathbb{K}[X]$ un polynôme. Alors
- le degré $\deg(P)$ de $P \neq 0$ est le plus grand $k \in \mathbb{N}$ tel que a_k soit non nul (par convention, $\deg(0) = -\infty$) ;
- le coefficient dominant de P est $\mathrm{cd}(P) := a_{\deg(P)}$;
- le coefficient constant de P est a_0.

Un polynôme est dit unitaire si son coefficient dominant est 1.

Notation 1.13. On notera $\mathbb{K}[X]_{\leq n}$ le sous-ensemble (sous-espace vectoriel) des polynômes de degré $\leq n$

Exemple 1.14.
- $\deg(1 + 2X + 4X^2) = 2$
- Son terme dominant est 4 et son terme constant est 1.

Proposition 1.15. *Soient $P, Q \in \mathbb{K}[X]$. Alors*
- $\deg(PQ) = \deg(P) + \deg(Q)$;
- $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$ *avec égalité lorsque* $\deg(P) \neq \deg(Q)$.
- *le coefficient dominant (resp. constant) de PQ est le produit des coefficients dominants (resp. constants) de P et Q.*

Exemple 1.16. Si deux polynômes de même degré ont des coefficients dominants opposés alors leur somme est de degré strictement inférieur (eg. X et $-X$).

Définition 1.17. Soit $P = \sum_k a_k X^k$ un polynôme de $\mathbb{K}[X]$ et $x \in \mathbb{K}$. L'évaluation du polynôme P en x est

$$P(x) := \sum_k a_k x^k \in \mathbb{K}.$$

La fonction polynomiale associée à P est la fonction $f_P : x \in \mathbb{K} \mapsto P(x) \in \mathbb{K}$.

Remarque 1.18. Si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ alors f_P est une fonction infiniment dérivable (ou lisse).

Remarque 1.19. Si $\mathbb{K}$ est infini alors les polynômes et les fonctions polynomiales sont en correspondance. Ce n'est pas le cas si $\mathbb{K} = \mathbb{F}_p$ (penser au polynôme $X^p - X$ qui est nul pour tout $x \in \mathbb{F}_p$ par le théorème de Fermat).

Définition 1.20. Soient A, B deux polynômes de $\mathbb{K}[X]$. On dit que A divise B ou que B est un multiple de A s'il existe $C \in \mathbb{K}[X]$ tel que $B = AC$.
On note alors $A|B$.

Avertissement 1.21. Contrairement au cas sur $\mathbb{N}$, $A|B$ et $B|A$ n'impliquent pas $A = B$ (i.e. la divisibilité n'est pas une relation antisymétrique).

Avertissement 1.22. Contrairement au cas sur $\mathbb{Z}$, $A|B$ et $B|A$ n'impliquent pas $A = \pm B$

Lemme 1.23. *Soient A, B deux polynômes de $\mathbb{K}[X]$. Si $A|B$ et $B|A$ alors il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$.*

Démonstration. Si $A|B$ et $B|A$ alors il existe $Q_1, Q_2 \in \mathbb{K}[X]$ tel que

$$A = BQ_1,\ B = AQ_2$$

On en déduit donc que $A = Q_1 Q_2 A$ et

$$\deg(A) = \deg(Q_1) + \deg(Q_2) + \deg(A)$$

Autrement dit que $\deg(Q_1) = \deg(Q_2) = 0$ i.e. $Q_1, Q_2 \in \mathbb{K}^*$. □

Définition 1.24. A et B sont alors dits associés.

Proposition 1.25.
- *Pour tout $A \in \mathbb{K}[X]$, $A|A$ (la divisibilité est réflexive) ;*
- *Pour tout $A, B, C \in \mathbb{K}[X]$, $(A|B$ et $B|C) \Rightarrow A|C$ (la divisibilité est transitive) ;*
- *Pour tout $A, B, C \in \mathbb{K}[X]$, $A|B \Rightarrow A|BC$;*
- *Pour tout $A, B, C \in \mathbb{K}[X]$, $(A|B$ et $A|C) \Rightarrow A|(B + C)$;*
- *Pour tout $A, B, P, Q \in \mathbb{K}[X]$, $(A|B$ et $P|Q) \Rightarrow AP|BQ$;*

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

Lemme 2.1. *Soient $(u_n)_{n\in\mathbb{N}}$ une suite strictement décroissante d'entiers et $b \in \mathbb{N}$. Alors il existe un rang N pour lequel $u_N < b$.*

Démonstration. Si $u_0 < b$ alors $N = 0$ convient. Sinon, on montre par récurrence que

$$\forall n \in \mathbb{N}, u_n < u_0 - (n-1)$$

On en déduit que $N = u_0 - b + 1$ convient.

□

Théorème 2.2. *Soient $A, B \in \mathbb{K}[X]$ deux polynômes de $\mathbb{K}[X]$ avec $B \neq 0$. Alors il existe un unique couple (Q, R) de polynômes tel que*

$$A = BQ + R$$

où $\deg(R) < \deg(B)$.
On dit que Q est le quotient de la division euclidienne de A par B et R est le reste.

Démonstration. **Existence** :

— Si $\deg(A) < \deg(B)$ alors $Q = 0$ et $R = A$ convient

— Supposons que $\deg(A) \geq \deg(B)$. Notons $n \coloneqq \deg(A)$ et $d \coloneqq \deg(B)$.
On va considérer la suite de polynômes $(A_k)_k$ définie par itération comme suit :

$$\begin{cases} A_0 = A \\ A_{k+1} = A_k - \frac{cd(A_k)}{b_k} X^{\deg(A_k)-d} B \text{ si } \deg(A_k) \geq d \end{cases}$$

où les b_k sont les coefficients de B.
Par le lemme 2.1, la suite des degrés $(\deg(A_k))$ devient strictement inférieure à $d = \deg(B)$ à un certain rang N. On en déduit que $Q = \sum_k \frac{cd(A_k)}{b_d} X^{\deg(A_k)-d}$ et $R = A_N$

Unicité :
Supposons que (Q, R) et (Q', R') vérifient tous les deux l'égalité du théorème et $Q \neq Q'$ (et donc $\deg(Q - Q') \geq 0$). Alors

$$B(Q - Q') = R' - R$$

On en déduit que

$$\deg(B) \leq \deg(B(Q - Q')) = \deg(R' - R) < \deg(B).$$

autrement dit une contradiction. On en déduit donc $Q = Q'$ et

$$BQ + R = A = BQ' + R' = BQ + R'$$

On a donc $R = R'$ et par conséquent, l'unicité du couple (Q, R). □

Exemple 2.3. Si on prend $A = 2X^4 + X^3 + 5X^2 + 7X + 7$ et $B = X^2 + 1$ alors $Q = 2X^2 + X + 3$ et $R = 6X + 4$.

Exemple 2.4. Si $\deg(B) = 1$ i.e. $B = \lambda(X - \alpha)$ alors le reste de la division euclidienne est $P(\alpha)$.

Proposition 2.5. *Soient $A, B \in \mathbb{K}[X]$ deux polynômes sur $\mathbb{K}$. B divise A si, et seulement si, le reste de la division euclidienne de A par B est nul.*

Démonstration. Si B divise A alors il existe Q tel que $A = BQ$. Par unicité de la division euclidienne, le reste de la division euclidienne de A par B est nul. Réciproquement, si le reste de la division euclidienne de A par B alors il existe $\in \mathbb{K}[X]$, $A = BQ$ □

3 Racine et divisibilité

3.1 Définitions

Définition 3.1. Soient P un polynôme sur $\mathbb{K}$ et $\alpha \in \mathbb{K}$. L'élément α est une racine de P si $P(x) = 0$.

Exemple 3.2. 1 est une racine de $X^2 - 3X + 2$.

Lemme 3.3. *Soient P un polynôme sur $\mathbb{K}$. α est une racine sur $\mathbb{K}$ si, et seulement si, le polynôme $X - \alpha$ divise P*

Démonstration. Cela vient du fait que le reste de la division euclidienne de P par $(X - \alpha)$ est $P(\alpha)$. □

Proposition 3.4. *Soient P un polynôme sur $\mathbb{K}$ et $\alpha_1, \ldots, \alpha_n$ des racines distinctes de P. Le polynôme $\prod_{i=1}^{n}(X - \alpha_i)$ divise P.*

Définition 3.5. Soient P un polynôme sur $\mathbb{K}$ et α une racine sur $\mathbb{K}$. On dit que α est une racine d'ordre $r \geq 1$ de P si $(X - a)^r$ divise P et $(X - a)^{r+1}$ ne divise pas P.

Exemple 3.6. $P = (X-1)^2(X-2)$ a 1 comme racine double et 2 comme racine simple.

Théorème 3.7 (d'Alembert-Gauß, théorème fondamental de l'algèbre)**.** *Tout polynôme non-constant de $\mathbb{C}[X]$ a une racine. On dit aussi que $\mathbb{C}$ est algébriquement clos.*

Corollaire 3.8. *Tout polynôme $P \in \mathbb{C}[X]$ s'écrit comme le produit*

$$P = \mathrm{cd}(P) \prod_{i=1}^{n} (X - \alpha_i)^{m_i}$$

où $\alpha_1, \ldots, \alpha_n$ sont les racines de multiplicité respective $m_1, \ldots, m_n$ de P.

3.2 Polynôme dérivé et multiplicité

Dans cette sous-section, nous allons supposer que $\mathbb{Q} \subset \mathbb{K}$.

Définition 3.9. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ un polynôme. Le polynôme dérivé de P est

$$P' = \sum_{k=1}^{n} a_k k X^{k-1} = \sum_{k=0}^{n-1} a_{k+1}(k+1)X^k$$

Notation 3.10. On note $P^{(k)}$ le kème dérivé de P i.e. $P^{(2)} = P''$, $P^{(3)} = P'''$...

Proposition 3.11. *Soit $P \in \mathbb{K}[X]$ un polynôme sur $\mathbb{K}$. Alors*
- $\deg(P') = \deg(P) - 1$
- $P' = 0$ *si, et seulement si, P est constant.*

Proposition 3.12. *Soient P et Q deux polynômes et $\lambda \in \mathbb{K}$. Alors*

$$(P + \lambda Q)' = P' + \lambda Q'$$

Remarque 3.13. On dit que la dérivation est une application $\mathbb{K}$-linéaire $\mathbb{K}[X] \to \mathbb{K}[X]$.

Proposition 3.14 (Formule de Leibniz)**.** *Soient P et Q deux polynômes. Alors*

$$(PQ)' = P'Q + PQ'$$

Corollaire 3.15. *Soient* P *et* Q *deux polynômes et* $n \in \mathbb{N}$. *Alors*

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

Proposition 3.16. *Soient* $P \in \mathbb{K}[X]$ *et* $x \in \mathbb{K}$. *Alors* x *est une racine d'ordre* $r \geq 2$ *de* P *alors* x *est une racine d'ordre* $r-1$ *de* P'.

Démonstration. Supposons que x est une racine d'ordre r de P i.e. il existe Q tel que $P = (X-x)^r Q$ et $Q(x) \neq 0$. Alors

$$P' = r(X-x)^{r-1}Q + (X-x)^r Q' = (X-x)^{r-1}\left(rQ + (X-x)Q'\right)$$

Comme $\left(rQ + (X-x)Q'\right)(x) = rQ(x) = 0$ alors x est une racine d'ordre $r-1$ de P'. □

Lemme 3.17. *Soient* k *et* n *deux entiers naturels. Alors*

$$(X^n)^{(k)} = \begin{cases} \frac{n!}{(n-k)!} X^{n-k} & \text{si } n \geq k \\ 0 & \text{sinon} \end{cases}$$

Démonstration. $(X^n)^{(k)} = (nX^{n-1})^{(k-1)} = \ldots = n(n-1)\cdots(n-k+1)X^{n-k}$. □

Théorème 3.18 (Développement de Taylor)**.** *Soient* $P \in \mathbb{K}[X]$ *et* $a \in \mathbb{K}$. *Alors*

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

Démonstration. Si P est nul, le résultat est évident. Supposons que $\deg(P) \geq 0$.
Posons $n \coloneqq \deg(P)$. Par itération de la division euclidienne, on montre qu'il existe une unique famille $(c_0, \ldots, c_n)$ telle que

$$P = \sum_{k=0}^{n} c_k (X-a)^k$$

Soit $l \in \{0, \ldots, n\}$. Alors

$$P^{(l)} = \sum_{k \geq l}^{n} c_k \frac{k!}{(k-l)!}(X-a)^{k-l}$$

On en déduit donc que

$$P^{(l)}(a) = l! c_l$$

et donc comme $l! \neq 0$ (car $\mathbb{Q} \subset \mathbb{K}$), on a

$$c_l = \frac{P^{(l)}(a)}{l!}.$$

□

Remarque 3.19. On dit que $(1, X-a, \ldots, (X-a)^n)$ est une base de $\mathbb{K}[X]_{\leq n}$.

L'unicité des coefficients (c_l) entraîne que :

Corollaire 3.20. *Soit* $P \in \mathbb{K}[X]$ *et* $x \in \mathbb{K}$. x *est une racine d'ordre* r *si, et seulement si,* $P(x) = 0$, $P'(x) = 0$, ..., $P^{(r-1)}(x) = 0$ *et* $P^{(r)}(x) \neq 0$.

Remarque 3.21. Les fonctions lisses $\mathbb{R} \to \mathbb{R}$ vérifiant la condition suivante

$$\forall x \in \mathbb{R}, \exists n_0 \in \mathbb{N}, f^{(n_0)}(x) = 0$$

sont polynomiales.

4 PGCD et PPCM dans $\mathbb{K}[X]$

4.1 Définitions

Lemme 4.1. *Soient A et B deux polynômes de $\mathbb{K}[X]$ avec $B \neq 0$. Soient Q et R le quotient et le reste de la division euclidienne de A par B. Les diviseurs communs de A et B sont les mêmes que les diviseurs communs de B et R.*

Démonstration. Soit D un diviseur commun de A et B. Alors D divise BQ (compatibilité avec la multiplication) et donc $R = A - BQ$ (compatibilité avec la somme). Réciproquement, si D divise B et R alors il divise aussi $A = BQ + R$. □

Théorème 4.2. *Soient A et B deux polynômes dans $\mathbb{K}[X]$. Il existe un unique polynôme D nul ou unitaire dont les diviseurs sont les diviseurs communs de A et B, c'est-à-dire tel que pour tout polynôme $P \in \mathbb{K}[X]$,*

$$P \mid D \Leftrightarrow P \mid A \text{ et } P \mid B$$

De plus, il existe deux polynômes U et V tels que $AU + BV = D$

Démonstration. **Existence** :
Démontrons par récurrence sur n que si $\deg(B) < n$ alors pour tout polynôme A, il existe un polynôme D dont les diviseurs sont les diviseurs communs à A et B et tel qu'il existe U et V tels que $AU + BV = D$.
Initialisation : Si $n = 0$ alors $B = 0$ alors $D = A$, $U = 1$ et $V = 0$ conviennent.
Hérédité : Soit $n \in \mathbb{N}$ et supposons le résultat vrai au rang n. Soient $A, B \in \mathbb{K}[X]$ et $\deg(B) < n + 1$. Si $\deg(B) < n$ alors le résultat est vrai (par hypothèse de récurrence). Sinon, B est nul et donc on peut faire la division euclidienne de A par B (on notera Q le quotient et R le reste). Comme $\deg(R) < \deg(B)$ alors $\deg(R) < n$. On peut donc appliquer l'hypothèse de récurrence avec R (et B) : il existe un polynôme D dont les diviseurs sont les diviseurs communs de B et R et des polynômes U_0, V_0 tels que

$$BU_0 + RV_0 = D$$

Par le lemme précédent, les diviseurs de D sont également les diviseurs de A et B. On a aussi l'égalité suivante :

$$D = BU_0 + RV_0 = BU_0 + (A - BQ)V_0 = B(U_0 - QV_0) + AV_0$$

Le triplet $(D, V_0, U_0 - QV_0)$ convient.
Conclusion : Si $D \neq 0$, il ne reste qu'à diviser D par son coefficient pour conclure.
Unicité
Supposons qu'il existe D_1 et D_2 qui vérifient le problème. Alors D_1 divise A et B et donc divise D_2. De la même façon, D_2 divise D_1. D_1 et D_2 sont associés. Si l'un est nul, l'autre aussi. Si les deux sont unitaires alors ils sont égaux. □

Définition 4.3. Le polynôme D est alors appelé PGCD de A et B et est noté $\mathrm{PGCD}(A, B)$ ou $A \wedge B$. Le couple (U, V) est appelé couple de coefficients de Bézout de A et B.

Remarque 4.4.
- La condition d'unitarité permet d'avoir l'unicité ; si on ne l'a pas le PGCD serait défini à multiplication par un scalaire non nul.
- Le PGCD est le plus grand (pour la divisibilité) des diviseurs unitaires communs de A et de B.
- On peut remplacer la condition de divisibilité par la condition suivante : Pour tout couple de polynômes (P, Q), D divise $PA + QB$.

On va maintenant donner une version effective de ce théorème :
Pour cela, on va utiliser le résultat suivant (montré dans la preuve du théorème précédent)

Corollaire 4.5. *Soit* A *un polynôme non nul de* $\mathbb{K}[X]$*. Alors*

$$A \wedge 0 = \frac{1}{\mathrm{cd}(A)} A.$$

De la même façon, si P *et* Q *sont deux polynômes non nuls de* $\mathbb{K}[X]$ *tels que* P *divise* Q *alors*

$$P \wedge Q = \frac{1}{\mathrm{cd}(P)} P$$

.

Proposition 4.6 (Algorithme d'Euclide)**.** *Soient* A, B *deux polynômes non nuls de* $\mathbb{K}[X]$*. Notons* (A_n) *la suite de polynôme définie comme suit :*

— $A_0 = A$ *et* $A_1 = B$*;*

— *pour tout* $n \in \mathbb{N}$, A_{n+2} *est le reste de la division euclidienne de* A_n *par* A_{n+1}*.*

La suite (A_n) *finit par devenir nulle et le PGCD de* A *et* B *est le dernier* A_n *non nul.*

Démonstration. Comme la suite d'entiers $(\deg(A_n))$ est strictement décroissante alors elle finit par devenir strictement négative et donc la suite (A_n) devient nulle à partir d'un certain rang (que l'on notera N). Par itération du lemme 4.1, les diviseurs communs de $A = A_0$ et $B = A_1$ sont les diviseurs communs de A_N et A_{N+1} et donc

$$\mathrm{PGCD}(A, B) = \mathrm{PGCD}(A_N, A_{N+1}) = \mathrm{PGCD}(A_N, 0) = \frac{1}{\mathrm{cd}(A_N)} A_N$$

□

Remarque 4.7. On trouve les coefficients de Bézout en « remontant » cette algorithme : les égalités $\begin{cases} A_{N-3} = Q_{N-1} A_{N-2} + A_{N-1} \\ A_{N-2} = Q_{N-2} A_{N-1} + A_N \end{cases}$ deviennent

$$\begin{aligned} A_N &= A_{N-2} - Q_{N-2} A_{N-1} = A_{N-2} - Q_{N-2}(A_{N-3} - Q_{N-1} A_{N-2}) \\ &= (1 + Q_{N-2} Q_{N-1}) A_{N-2} - Q_{N-2} A_{N-3} \end{aligned}$$

Et ainsi jusqu'à $A = A_0$ et $B = A_1$.

Exemple 4.8. Prenons $A = X^3 - 4X^2 + 4X$ et $B = X^3 - X$. Alors

— $X^3 - 3X^2 + 3X = 1(X^3 - X) + (-3X^2 + 4X)$

— $X^3 - X = \left(\frac{-1}{3} X - \frac{4}{9}\right)(-3X^2 + 4X) + \frac{7}{9} X$

— $-3X^2 + 4X = \left(\frac{-27}{7} X - \frac{36}{7}\right) \frac{7}{9} X$

On en déduit que $A \wedge B = X$ et

$$\frac{7}{9} X = B - \left(\frac{-1}{3} X - \frac{4}{9}\right)(-3X^2 + 4X) = B - \left(\frac{-1}{3} X - \frac{4}{9}\right)(A - B) = \left(\frac{1}{3} X + \frac{4}{9}\right) A + \left(\frac{-1}{3} X + \frac{4}{9}\right) B$$

Proposition 4.9. *Soient* A *et* B *deux polynômes dans* $\mathbb{K}[X]$*. Il existe un unique polynôme* M *nul ou unitaire dont les multiples sont les multiples communs de* A *et* B*, c'est-à-dire tel que pour tout polynôme* $P \in \mathbb{K}[X]$*,*

$$M \mid P \Leftrightarrow A \mid P \text{ et } B \mid P$$

Démonstration. **Existence :**
Si A ou B sont nuls alors $M = 0$ convient. Supposons donc $A \neq 0 \neq B$. Il existe alors des multiples non-nuls communs de A et de B (i.e. AB). Soit M un multiple commun non nul de degré minimal [1]. Par construction, les multiples de M sont des multiples de A et de B. Réciproquement, soient P est un multiple commun de A et de B et Q, R le quotient et le reste de la division euclidienne de P par M. Le polynôme $R = P - MQ$ est divisible par A et par B. Comme M est de degré minimal parmi les multiples non nuls communs de A et de B et $\deg(R) < \deg(B)$ alors $R = 0$. On en déduit donc P est un multiple de M.
Unicité : Même preuve que pour le PGCD. □

Définition 4.10. Le polynôme P est alors appelé PPCM de A et B et est noté $\text{PPCM}(A, B)$ ou $A \vee B$.

4.2 Propriétés du PGCD et du PPCM

Proposition 4.11. *Soient A, B des polynômes de $\mathbb{K}[X]$. Si $P = AP_1$ et $B = PB_1$ avec $P, A_1, B_1 \in \mathbb{K}[X]$ et P unitaire. Alors*

$$A \wedge B = P(A_1 \wedge B_1) \text{ et } A \vee B = P(A_1 \vee B_1)$$

Démonstration. Si A et B sont nuls alors les résultats sont immédiats. Supposons que $A \neq 0 \neq B$. Soit Q un polynôme de $\mathbb{K}[X]$. Les assertions suivantes sont équivalentes :

1. $Q \mid A_1 \wedge B_1$
2. $Q \mid A_1$ et $Q \mid B_1$
3. $PQ \mid A$ et $PQ \mid B$
4. $PQ \mid A \wedge B$

En particulier, en prenant $Q = A_1 \wedge B_1$, on obtient que $P(A_1 \wedge B_1)$ divise $A \wedge B$. De plus, comme P est un diviseur commun de A et B alors P divise $A \wedge B$ i.e. il existe R tel que $A \wedge B = PR$. On déduit des équivalences précédentes avec $Q = R$ que $R \mid A_1 \wedge B_1$ et donc $A \wedge B = PR \mid P(A_1 \wedge B_1)$ et donc $A \wedge B$ et $P(A_1 \wedge B_1)$ sont associés. Comme P, $A \wedge B$ et $A_1 \wedge B_1$ sont unitaires alors on en déduit que

$$A \wedge B = P(A_1 \wedge B_1).$$

Le cas du PPCM se fait de la même façon. □

Définition 4.12. Deux polynômes A, B sont dits premiers entre eux si leur PGCD vaut 1.

Exemple 4.13. Les polynômes $X^2 + X$ et $X^2 - 2X + 1$ sont premiers entre eux.

Corollaire 4.14. *Soient A, B deux polynômes de $\mathbb{K}[X]$. Il existe deux polynômes $A_1, B_1 \in \mathbb{K}[X]$ tels que $A_1 \wedge B_1 = 1$ et tels que $A = (A \wedge B)A_1$ et $B = (A \wedge B)B_1$.*

Démonstration. On utilise la proposition précédente avec $P = A \wedge B$. □

1. Tout sous-ensemble non vide de $\mathbb{N}$ est minoré

4.3 Théorème de Bézout et théorème de Gauß

Proposition 4.15 (Identité de Bézout)**.** *Deux polynômes* A, B *de* $\mathbb{K}[X]$ *sont premiers entre eux si, et seulement si, il existe* $U, V \in \mathbb{K}[X]$ *tels que* $AU + BV = 1$.

Démonstration. L'implication vient de la définition du PGCD. Réciproquement, supposons qu'il existe U, V tel que $AU + BV = 1$. Si D divise A et B alors D divise $AU + BV = 1$ et donc D est constant. On en déduit donc que $PGCD(A, B) = 1$. □

Théorème 4.16 (Gauß)**.** *Soient* A, B, C *des polynômes de* $\mathbb{K}[X]$*. Si* A *et* B *sont premiers entre eux et* A *divise* BC *alors* A *divise* C*.*

Démonstration. Comme A et B sont premiers entre eux alors il existe deux polynômes U, V tels que $AU + BV = 1$. On en déduit donc $AUC + BVC = C$. Comme A divise BC alors A divise C. □

Corollaire 4.17. *Si* A *et* B *sont deux polynômes de* $\mathbb{K}[X]$ *premiers entre eux, alors il existe* $\lambda \in \mathbb{K}^*$ *tel que*

$$A \vee B = \lambda AB$$

Démonstration. Les multiples de AB sont des multiples de A et de B. Réciproquement, soit P un multiple commun de A et B. Il existe un polynôme Q tel que $P = BQ$. Comme A divise $P = BQ$ et $A \wedge B = 1$ alors A divise Q. On en déduit que AB divise P.
On en déduit que les multiples de AB sont les multiples communs de A et de B. On en déduit donc que $A \vee B$ et AB sont associés. □

Corollaire 4.18. *Soient* A, B *deux polynômes de* $\mathbb{K}[X]$*. Les polynômes* $(A \wedge B)(A \vee B)$ *et* AB *sont associés, c'est-à-dire qu'il existe* $\lambda \in \mathbb{K}^*$ *tel que* $AB = \lambda(A \wedge B)(A \vee B)$

Démonstration. Soient A, B deux polynômes de $\mathbb{K}[X]$. Si $A = 0$ ou $B = 0$ alors le résultat est immédiat. Supposons donc que $A \neq 0 \neq B$. Par définition du PGCD, il existe A_1 et B_1 deux polynômes tels que

$$\begin{cases} A = A_1 A \wedge B \\ B = B_1 A \wedge B \end{cases}$$

Les polynômes A_1 et B_1 sont premiers entre eux. On en déduit donc qu'il existe $\lambda \in \mathbb{K}^*$ tel que

$$A_1 \vee B_1 = \lambda A_1 B_1$$

On en déduit donc que

$$\lambda AB = \lambda(A \wedge B)^2 A_1 B_1 = (A \wedge B)^2 A_1 \vee B_1 = (A \wedge B)(A \wedge BA_1) \vee (A \wedge BB_1) = (A \wedge B)A \vee B$$

□

Proposition 4.19. *Soient* A, B *deux polynômes de* $\mathbb{K}[X]$ *non constants et premier entre eux. Il existe un unique couple* (U_0, V_0) *de polynôme dans* $\mathbb{K}[X]$ *tels que*

$$AU_0 + BV_0 = 1 \ \textit{avec} \ \ \deg(U_0) < \deg(B),\ \deg(V_0) < \deg(A)$$

Démonstration. **Existence :** Par Bézout, comme A et B sont premiers entre eux, il existe un couple (U, V) de polynômes de $\mathbb{K}[X]$ tels que $AU + BV = 1$. On fait la division euclidienne de U par B i.e. $U = Q_1 B + U_0$ (avec $\deg(U_0) < \deg(B)$). On obtient alors l'égalité

$$1 = A(Q_1 B + U_0) + BV = AU_0 + B(AQ_1 + V)$$

Comme $0 = \deg(1) \neq \max(\deg(AU_0), \deg(B(AQ_1 + V)))$ (et donc on n'est pas dans le cas d'égalité du lemme 8.16) alors $\deg(A) + \deg(U_0) = \deg(AU_0) = \deg(B(AQ_1 + V)) = \deg(B) + \deg(AQ + V)$. On en déduit :

$$\deg(AQ + V) = \deg(A) + \deg(U_0) - \deg(B) < \deg(A)$$

Le couple $(U_0, AQ + V)$ convient donc.
Unicité : Soient (U_0, V_0) et (U_1, V_1) deux polynômes vérifiant la proposition i.e.

$$AU_i + BV_i = 1 \text{ avec } \deg(U_i) < \deg(B),\ \deg(V_i) < \deg(A)$$

pour $i = 0, 1$. On en déduit que

$$AU_1 + BV_1 = AU_0 + BV_0$$

ou encore

$$A(U_1 - U_0) = B(V_0 - V_1).$$

Comme A et B sont premiers entre eux alors, par le théorème de Gauß, on en déduit que B divise $U_1 - U_0$. Ce dernier polynôme étant de degré strictement inférieur à $\deg(B)$, on en déduit qu'il est nul i.e. $U_1 = U_0$. On en déduit alors que $V_1 = V_0$. □

5 Irréductibilité

Définition 5.1. Un polynôme P de $\mathbb{K}[X]$ est dit irréductible si
— $\deg(P) \geq 1$
— les seuls diviseurs (à coefficient multiplicatif non nul près) de P sont 1 et P

Exemple 5.2.
— Un polynôme de degré 1 est irréductible.
— Un polynôme de degré 2 et 3 sans racine dans $\mathbb{K}$ est irréductible.
— Tout polynôme de degré ≥ 2 ayant une racine est réductible.

Exemple 5.3.
— Le polynôme $X^2 + 1$ est irréductible sur $\mathbb{Q}, \mathbb{R}$ et $\mathbb{F}_p$ avec $p \equiv 3[4]$ mais réductible sur $\mathbb{C}, \mathbb{F}_2$ et $\mathbb{F}_p$ pour $p \equiv 1[4]$.
— Soient $a_1, \ldots, a_n \in \mathbb{Z}$. Alors le polynôme $\prod_{k=1}^{n}(X - a_k) - 1$ est irréductible sur $\mathbb{Q}$.
— Il existe des polynômes irréductibles dans $\mathbb{F}_p$ de tout degré. Ce résultat permet la construction de tous les corps finis.

Proposition 5.4. *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*

Démonstration. Par d'Alembert-Gauß, tout polynôme non-constant à coefficients complexes a une racine. Grâce à l'exemple 5.2, on en déduit qu'un polynôme complexe irréductible est de degré 1. □

Définition 5.5. Soit $P = \sum a_k X^k \in \mathbb{C}[X]$. Le conjugué de P est le polynôme

$$\overline{P} = \sum \overline{a_k} X^k$$

Proposition 5.6. *Soient $P, Q \in \mathbb{C}[X]$ et $\lambda \in \mathbb{C}$. Alors*
— $\overline{P + Q} = \overline{P} + \overline{Q}$
— $\overline{PQ} = \overline{P}\ \overline{Q}$
— $\overline{\lambda P} = \overline{\lambda}\overline{P}$
— $\forall k \in \mathbb{N}, \overline{P^{(k)}} = \overline{P}^{(k)}$
— $\forall z \in \mathbb{C}, \overline{P(z)} = \overline{P}(\overline{z})$

— *Si* $P \in \mathbb{R}[X]$ *alors pour tout* $z \in \mathbb{C}$, $\overline{P(z)} = P(\overline{z})$
— $P \in \mathbb{R}[X]$ *si, et seulement si,* $P = \overline{P}$.

Grâce au théorème de d'Alembert-Gauß et cette proposition, on déduit le résultat suivant :

Corollaire 5.7. *Les racines complexes d'un polynôme* $P \in \mathbb{R}[X]$ *sont*
— *soit des réels,*
— *soit des paires de complexes conjugués de même ordre.*

Corollaire 5.8. *Les polynômes irréductibles de* $\mathbb{R}[X]$ *sont*
— *les polynômes de degré 1 ;*
— *les polynômes de degré 2 de discriminant strictement négatif.*

Démonstration. Soit P un polynôme de $\mathbb{R}[X]$.
— si $\deg(P) = 1$ alors il est irréductible.
— si $\deg(P) = 2$ alors il est irréductible si, et seulement si, il n'a pas de racine réelle i.e. si, et seulement si, son discriminant est négatif.
— si $\deg(P) \geq 3$ alors soit il a une racine réelle (et donc il n'est pas irréductible) soit il a une racine complexe (non réelle) ω. Dans ce cas là, son conjugué $\overline{\omega}$ est aussi une racine de P car P est un polynôme réel. On en déduit donc que P est divisible par $(X-\omega)(X-\overline{\omega}) = X^2 - 2\mathrm{Re}(\omega)X + |\omega|^2 \in \mathbb{R}[X]$. Autrement dit, P est réductible.

□

Proposition 5.9. *Un polynôme irréductible* P *est premier avec tous les polynômes qu'il ne divise pas.*

Démonstration. Soit Q un polynôme de $\mathbb{K}[X]$. Comme $P \wedge Q$ divise P et P est irréductible alors

$$P \wedge Q = \begin{cases} 1 & \text{ou} \\ \frac{P}{cd(P)} & \end{cases}$$

Alors soit P et Q sont premiers entre eux soit P divise Q. □

Corollaire 5.10. *Un polynôme irréductible divise un produit de polynômes si, et seulement si, il divise l'un des facteurs.*

Démonstration. Soient $P_1, \ldots, P_n$ des polynômes non constants de $\mathbb{K}[X]$. Soit $P \in \mathbb{K}[X]$ un polynôme irréductible qui divise $\prod_{i=1}^{n} P_i$. Supposons, par l'absurde que P ne divise aucun des P_i. Alors par la proposition précédente, pour tout i, $P \wedge P_i = 1$. Comme P divise $\prod_{i=1}^{n} P_i$ alors par itération du théorème de Gauß, P divise $\prod_{i>k} P_i$ pour tout $k \geq 0$. En particulier, P divise 1 i.e. P n'est pas irréductible, contradiction ! □

Théorème 5.11. *Tout polynôme non-constant de* $\mathbb{K}[X]$ *est le produit d'un scalaire par un produit de polynômes irréductibles unitaires de* $\mathbb{K}[X]$. *De plus, cette décomposition est unique à l'ordre près des facteurs.*

Démonstration. **Existence** : Démontrons, par récurrence, pour $n \geq 1$, la propriété suivante : « Tout polynôme non constant de $\mathbb{K}[X]$ de degré inférieur ou égal à n peut s'écrire sous la forme d'un produit de polynômes irréductibles ».
Initialisation : si $n = 1$ alors c'est vrai car tout polynôme de degré 1 est irréductible et est donc le produit d'un seul polynôme irréductible.
Hérédité : Soit $n \in \mathbb{N}, n \geq 1$ et supposons la propriété vraie au rang n. Soit A un polynôme de degré $n+1$. Si A est irréductible alors c'est le produit d'un seul polynôme irréductible. Sinon, c'est le produit $A = BC$ de deux polynômes non-constant de degré.

Les polynômes B et C sont de degré inférieur ou égal à n. Par l'hypothèse de récurrence, les polynômes B et C s'écrivent comme le produit de polynômes irréductibles.
Unicité : Soit $A = \lambda A_1 \dots A_n$ une telle décomposition du polynôme A. Le scalaire λ est le coefficient dominant du polynôme A. Les polynômes irréductibles unitaires A_i divise A et réciproquement, les polynômes irréductibles unitaires qui divise A divise l'un des Q_i qui sont égaux car irréductibles et unitaires. Les polynômes apparaissant dans la décomposition sont donc tous les polynômes irréductibles unitaires de A.
Soient A deux décompositions de A :

$$A = \lambda P_1^{\alpha_1} \dots P_r^{\alpha_r} = \lambda P_1^{\beta_1} \dots P_r^{\beta_r}$$

où les P_i sont irréductibles unitaires distincts deux à deux. Supposons qu'il existe un i tel que $\alpha_i \neq \beta_i$ (supposons que $\alpha_i < \beta_i$). Alors

$$\prod_{j \neq i} P_j^{\alpha_j} = P_i^{\beta_i - \alpha_i} \prod_{j \neq i} P_j^{\beta_j}$$

Alors P_i divise $\prod_{j \neq i} P_j^{\alpha_j}$, ce qui absurde puisque P_i est premier avec les P_j, $j \neq i$. On en déduit que, pour tout i, $\alpha_i = \beta_i$ et donc la décomposition est unique à permutation près. □

Corollaire 5.12. *Soient* A, B *deux polynômes non-nuls de* $\mathbb{K}[X]$. *Si*

$$A = \lambda P_1^{\alpha_1} \dots P_n^{\alpha_n} \text{ et } B = \mu P_1^{\beta_1} \dots P_n^{\beta_n}$$

où $P_1, \dots, P_n$ *sont des polynômes unitaires irréductibles distincts deux-à-deux, alors on a :*

$$A \mid B \Leftrightarrow (\forall 1 \leq i \leq n, \alpha_i \leq \beta_i).$$

De plus,

$$A \wedge B = \prod_{i=1}^{n} P_i^{\min(\alpha_i, \beta_i)} \text{ et } A \vee B = \prod_{i=1}^{n} P_i^{\max(\alpha_i, \beta_i)}$$

Démonstration. Si $A \mid B$ alors pour tout i, $P_i^{\alpha_i}$ divise A et donc divise B. On en déduit que $\alpha_i \leq \beta_i$. Réciproquement, si pour tout i, $\alpha_i \leq \beta_i$ alors $P_i^{\alpha_i}$ divise $P_i^{\beta_i}$ et donc $\prod_i P_i^{\alpha_i}$ divise $\prod_i P_i^{\beta_i}$ i.e. A divise B.
Les diviseurs unitaires communs de A et de B sont de la forme

$$D = P_1^{\delta_1} \dots P_n^{\delta_n}$$

avec $\delta_i \leq \alpha_i$ et $\delta_i \leq \alpha_i$ (i.e. $\delta_i \leq \min(\alpha_i, \beta_i)$) pour $1 \leq i \leq n$. On en déduit que le PGCD de A et B est

$$A \wedge B = P_1^{\min(\alpha_1, \beta_1)} \dots P_n^{\min(\alpha_n, \beta_n)}.$$

De la même façon, les multiples unitaires communs de A et de B sont de la forme

$$D = P_1^{\mu_1} \dots P_n^{\mu_n}$$

avec $\mu_i \geq \alpha_i$ et $\mu_i \geq \alpha_i$ (i.e. $\mu_i \geq \max(\alpha_i, \beta_i)$) pour $1 \leq i \leq n$. On en déduit que le PGCD de A et B est

$$A \wedge B = P_1^{\max(\alpha_1, \beta_1)} \dots P_n^{\max(\alpha_n, \beta_n)}.$$

□

6 Relation entre coefficients et racines

Définition 6.1. Un polynôme est dit scindé sur $\mathbb{K}$ s'il peut s'écrire sous la forme

$$A = \lambda \prod_{i=1}^{n} (X - \alpha_i)$$

où $\alpha_1, \ldots, \alpha_n$ sont dans $\mathbb{K}$ et $\lambda \in \mathbb{K}^*$.

Exemple 6.2.
— Un polynôme de degré n avec n racines distinctes est scindé.
— Un polynôme de degré n avec n racines comptés avec multiplicités est scindé. En particulier, tout polynôme complexe est scindé.

Exemple 6.3.
— Soit $P = a_2X^2 + a_1X + a_0$ un polynôme scindé de degré 2 de racines α_1, α_2 i.e.

$$\begin{aligned} P &= a_2(X - \alpha_1)(X - \alpha_2) \\ &= a_2X^2 - a_2(\alpha_1 + \alpha_2)X + a_2\alpha_1\alpha_2 \end{aligned}$$

On en déduit que $\frac{a_1}{a_2} = -(\alpha_1 + \alpha_2)$ et $\frac{a_0}{a_2} = \alpha_1\alpha_2$

— Soit $P = a_3X^3 + a_2X^2 + a_1X + a_0$ un polynôme scindé de degré 3 de racines $\alpha_1, \alpha_2, \alpha_3$ i.e.

$$\begin{aligned} P &= a_3(X - \alpha_1)(X - \alpha_2)(X - \alpha_3) \\ &= a_3X^2 - a_3(\alpha_1 + \alpha_2 + \alpha_3)X^2 + a_3(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)X - a_3\alpha_1\alpha_2\alpha_3 \end{aligned}$$

On en déduit que $\frac{a_1}{a_3} = -(\alpha_1 + \alpha_2 + \alpha_3)$, $\frac{a_2}{a_3} = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3$ et $\frac{a_0}{a_3} = -\alpha_1\alpha_2\alpha_3$

Exemple 6.4. Considérons le polynôme $P = X^2 - 2X + 2$. Ses racines sont $1 + i$ et $1 - i$. On a bien $\begin{cases} (1+i) + (1-i) = 2 \\ (1+i)(1-i) = 2 \end{cases}$

Plus généralement, pour $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$, on définit

— $\sigma_1 = \displaystyle\sum_{i=1}^{n} \alpha_i$

— $\sigma_2 = \displaystyle\sum_{1 \le i < j \le n} \alpha_i\alpha_j$

— $\sigma_k = \displaystyle\sum_{1 \le i_1 < \ldots < i_k \le n} \alpha_{i_1} \ldots \alpha_{i_k}$ pour $1 \le k \le n$.

— $\sigma_n = \displaystyle\prod_{i=1}^{n} \alpha_i$.

Définition 6.5. Les quantités σ_i sont appelés fonctions symétriques élémentaires des racines du polynôme scindé $\prod_{i=1}^{n}(X - \alpha_i)$.

Proposition 6.6 (Formules de Viète)**.** *Soit $A = \sum_{i=0}^{n} a_kX^k$ un polynôme scindé sur $\mathbb{K}$ et $\sigma_1, \ldots, \sigma_n$ les fonctions symétriques élémentaires de ses racines. Alors*

$$\forall 1 \le p \le n, \sigma_p = (-1)^p \frac{a_{n-p}}{a_n}$$

7 Résolutions d'équations

7.1 Équations diophantiennes

Soient $A, B, R \in \mathbb{K}[X]$. On veut résoudre des équations de la forme

$$AU + BV = R \tag{1}$$

avec $U, V \in \mathbb{K}[X]$.

On commence par calculer le PGCD $A \wedge B$. Si $A \wedge B$ ne divise pas R alors (1) n'a pas de solution (car $A \wedge B$ divise $AU + BV$). Supposons maintenant que c'est le cas et écrivons $R = (A \wedge B)R_1$, $A = (A \wedge B)A_1$ et $B = (A \wedge B)B_1$. L'équation (1) devient

$$A_1U + B_1V = R_1 \tag{2}$$

(et $A_1 \wedge B_1 = 1$).
Par le théorème de Bézout, il existe $\widetilde{U_0}$ et $\widetilde{V_0}$ tel que

$$A\widetilde{U_0} + B\widetilde{V_0} = 1$$

On obtient ainsi une solution particulière $(U_0 = \widetilde{U_0}R_1, V_0 = \widetilde{V_0}R_1)$ de (2). L'équation (2) se réécrit

$$A_1U + B_1V = A_1U_0 + B_1V_0$$

ou encore

$$A_1(U - U_0) + B_1V = B_1(V_0 - V). \tag{3}$$

Comme A_1 et B_1 sont premier entre eux alors B_1 divise $U - U_0$. Il existe donc $K \in \mathbb{K}[X]$ tel que $U = U_0 + KB_1$. On en déduit ensuite que $V = V_0 + A_1K$.
Réciproquement, tous ces polynômes sont solutions de (1).

7.2 Théorème des restes chinois et systèmes d'équations

Notation 7.1. Deux polynômes sont congrus modulo $P \in \mathbb{K}[X]$ s'ils ont le même reste pour la division euclidienne modulo P, noté $A \equiv B[P]$

Théorème 7.2 (des restes chinois)**.** *Soient P, Q deux polynômes premiers entre eux. Alors pour tout polynôme A de degré $< \deg(PQ)$, il existe un unique couple de polynômes (A_1, A_2) de degré, respectivement, $< \deg(P)$ et $< \deg(Q)$ tel que*

$$\{S \in \mathbb{K}[X] \mid S \equiv A[PQ]\} = \{S \in \mathbb{K}[X] \mid S \equiv A_1[P], S \equiv A_2[Q]\}$$

Démonstration. Si S est congru à A modulo PQ alors si on note R_1 le reste de la division euclidienne de S par A et R_2 celui de A alors $S \equiv R_1[P]$ et $S \equiv R_2[Q]$. Réciproquement, supposons que $S \equiv R_1[P]$ et $S \equiv R_2[Q]$. On va retrouver A.
Comme P et Q sont premiers entre eux alors il existe $U, V \in \mathbb{K}[X]$ tels que

$$PU + QV = 1$$

Alors $\begin{cases} PU \equiv 1[Q] \\ PU \equiv 0[P] \end{cases}$ et $\begin{cases} QV \equiv 0[Q] \\ QV \equiv 1[P] \end{cases}$.

On en déduit que $\begin{cases} A_2PU + A_1QV \equiv A_2 \times 1 + A_1 \times 0 \equiv A_2[Q] \\ A_2PU + A_1QV \equiv A_2 \times 0 + A_1 \times 1 \equiv A_1[P] \end{cases}$.

On en déduit que le reste de la division euclidienne de $A_2PU + A_1QV$ par PQ est le polynôme A recherché. □

Exemple 7.3. Considérons les solutions du système

$$\begin{cases} P \equiv 8[X-1] \\ P \equiv 3X+1[X^2] \end{cases} \tag{4}$$

On écrit une identité de Bézout pour X^2 et $X-1$:

$$X^2 - (X-1)(X+1) = 1$$

On en déduit que $8X^2 - (3X+1)(X+1)(X-1)$ vérifie les congruences (4). On en déduit que les solutions du système (4) sont les polynômes congrus à $4X^2+3X+1$ modulo $X^2(X-1)$

Soient $B_0 = \prod_{j=1}^{p} B_j^{p_j} \prod_{k=1}^{n} B_{0,k}^{m_k}$, $B_1 = \prod_{j=1}^{p} B_j^{q_j} \prod_{k=1}^{m} B_{1,k}^{n_k}$ deux polynômes écrits comme un produit de polynômes irrédutibles (si $p = 0$, B_0 et B_1 sont premier entre eux) et R_0, R_1 deux autres polynômes. On veut résoudre les équations de la forme

$$\begin{cases} P \equiv R_0[B_0] \\ P \equiv R_1[B_1] \end{cases} \tag{5}$$

(le cas à plus que deux congruences se fait de la même façon). Par le théorème des restes chinois, les congruences (5) deviennent

$$\begin{cases} P \equiv R_{0,0}[\prod_{k=1}^{n} B_{0,k}^{m_k}] \\ P \equiv R_{k,0}[B_j^{p_j}] \text{ pour } 1 \leq j \ \leq p \\ P \equiv R_{0,1}[\prod_{k=1}^{m} B_{1,k}^{n_k}] \\ P \equiv R_{k,1}[B_j^{q_j}] \text{ pour } 1 \leq j \ \leq p \end{cases} \tag{6}$$

Pour tout $1 \leq j \leq p$, on vérifie si les équations sont compatibles i.e.

$$R_{k,0} \equiv R_{k,1}[B_j^{\min(p_j,q_j)}]$$

Supposons $q_j \geq p_j$. Alors

$$\begin{aligned} P =& R_{k,1} + B_k^{q_k} Q_k \\ =& R_{k,1} + B_k^{p_k}(B_k^{q_k-p_k} Q_k) \end{aligned}$$

Si ce n'est pas le cas, il n'y a pas de solution. Sinon, on supprime la congruence correspondant à la plus petite puissance. On obtient alors un système de congruences où tous les polynômes sont premiers entre eux. Cela permet de finir de résoudre ce système.

Exemple 7.4. On va résoudre le système

$$\begin{cases} P \equiv 7X+1[X(X-1)] \\ P \equiv 3X+1[X^2] \end{cases} \tag{7}$$

Par le théorème des restes chinois, la première congruence est équivalente aux deux congruences $\begin{cases} P \equiv 1[X] \\ P \equiv 8[X-1] \end{cases}$.
Comme $3X+1 \equiv 1[X]$ alors la congruence $P \equiv 1[X]$ et la deuxième congruence de (7) sont compatibles. On en déduit que le système (7) devient : $\begin{cases} P \equiv 3X+1[X^2] \\ P \equiv 8[X-1] \end{cases}$.
On déduit du lemme précédent que $P \equiv 4X^2+3X+1[X^2(X-1)]$.

8 Fractions rationnelles

8.1 Généralités sur les fractions rationnelles

Slogan 8.1. Les fraction rationnelles sont aux polynômes ce que sont les rationnels pour les entiers.

Définition 8.2. Une fraction rationnelle à une indéterminée sur $\mathbb{K}$ est le quotient $\frac{P}{Q}$ de deux polynômes avec $Q \neq 0_{\mathbb{K}[X]}$. On identifie deux fractions rationnelles $\frac{P}{Q}$ et $\frac{R}{S}$ si $SP = QR$.

Remarque 8.3.
— De façon plus formelle, on munit $\mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$ de la relation binaire $\sim$ définie par :
$$(P, Q) \sim (R, S) \text{ si } SP = QR$$
C'est une relation d'équivalence. Une fraction rationnelle est une classe d'équivalence de $\sim$.
— On écrira de la même façon la fraction rationnelle $\frac{P}{1}$ et le polynôme P (de la même façon que l'on identifie, dans $\mathbb{Q}$, $\frac{n}{1}$ et n.

En particulier, si S est un polynôme non nul et $\frac{P}{Q}$ est une fraction rationnelle alors
$$\frac{SP}{SQ} = \frac{P}{Q}.$$

Proposition 8.4. *Pour tout fraction rationnelle F, il existe un unique (à multiplication par un élément de $\mathbb{K}^*$ près) couple de polynômes premiers entre eux P, Q tels que*
$$F = \frac{P}{Q}.$$

Démonstration. Soit $F = \frac{P}{Q}$ une fraction rationnelle.
Existence : Notons P_0 et Q_0 les polynômes tels que $P = (P \wedge Q)P_0$ et $Q = (P \wedge Q)Q_0$. Alors
$$\frac{P}{Q} = \frac{(P \wedge Q)P_0}{(P \wedge Q)Q_0} = \frac{P_0}{Q_0}$$
et $P_0 \wedge Q_0 = 1$.
Unicité : Soient (P_1, Q_1) et (P_2, Q_2) deux couples de polynômes premiers entre eux tels que
$$F = \frac{P_1}{Q_1} = \frac{P_2}{Q_2}.$$
Alors $P_1Q_2 = P_2Q_1$. Comme P_1 et Q_1 sont premiers entre eux alors par le lemme de Gauß, P_1 divise P_2. De la même façon, comme P_2 et Q_2 sont premiers entre eux, P_2 divise P_1. On en déduit qu'il existe $\lambda \in \mathbb{K}^*$ tel que $P_2 = \lambda P_1$. De même, $Q_2 = \lambda Q_1$. □

Définition 8.5. On appelle cette écriture forme/représentation irréductible de F

Corollaire 8.6. *Soit F une fraction rationnelle et $F = \frac{P}{Q}$ sa représentation irréductible. Alors si $\frac{R}{S} = F$ alors il existe un polynôme non nul T tel que* $\begin{cases} R = TP \\ S = TQ \end{cases}$

Démonstration. Si $\frac{R}{S} = \frac{P}{Q}$ alors $RQ = PS$. Comme P et Q sont premiers entre eux alors P divise R. Ainsi il existe T tel que $R = TP$ et donc $TPQ = PS$ i.e. $S = QT$. □

On va maintenant définir des lois de compositions sur l'ensemble des fractions rationnelles. Cela se fait de la même façon que sur $\mathbb{Q}$: pour tout quadruplet de polynômes P_1, P_2, Q_1, Q_2

$$\frac{P_1}{Q_1} + \frac{P_2}{Q_2} = \frac{P_1Q_2 + P_2Q_1}{Q_1Q_2}$$

et

$$\frac{P_1}{Q_1} \times \frac{P_2}{Q_2} = \frac{P_1P_2}{Q_1Q_2}$$

Cependant avant de pouvoir faire ça, il faut tout d'abord vérifier que tout cela est bien défini, c'est-à-dire montrer que si on multiplie le numérateur et le dénominateur par un même polynôme, on obtient le même résultat.

Lemme 8.7. *Soient* $F = \frac{P_1}{Q_1}$ *et* $G = \frac{P_2}{Q_2}$ *deux fractions rationnelles et* S *et* T *deux polynômes non nuls. Alors*

$$\frac{(SP_1)(TQ_2) + (TP_2)(SQ_1)}{(SQ_1)(TQ_2)} = \frac{P_1Q_2 + P_2Q_1}{Q_1Q_2}$$

et

$$\frac{(SP_1)(TP_2)}{(SQ_1)(TQ_2)} = \frac{P_1P_2}{Q_1Q_2}$$

Remarque 8.8. — Cela revient à dire que

$$\frac{P_1}{Q_1} + \frac{P_2}{Q_2} = \frac{SP_1}{SQ_1} + \frac{TP_2}{TQ_2}$$

et

$$\frac{P_1}{Q_1} \times \frac{P_2}{Q_2} = \frac{SP_1}{SQ_1} \times \frac{TP_2}{TQ_2}$$

— Ces deux opérations sont compatibles avec celles définies sur les polynômes dans le sens où

$$\frac{P_1}{1} + \frac{P_2}{1} = \frac{P_1 + P_2}{1}$$

et

$$\frac{P_1}{1} \times \frac{P_2}{1} = \frac{P_1P_2}{1}.$$

On a ainsi deux opérations sur l'ensemble des fonctions rationnelles (et une troisième qui est la multiplication par un scalaire qui est la multiplication par $\frac{\lambda}{1}$).

Ces opérations héritent des propriétés de celles sur $\mathbb{K}[X]$:

Proposition 8.9. *Soient* F, G, H *trois fractions rationnelles et* $\lambda, \mu \in \mathbb{K}$*. Alors*

— $F + G = G + F$ *(commutativité de +);*
— $F + (G + H) = (F + G) + H$ *(associativité de +);*
— $F + 0 = F$ *(0 est l'élément neutre de +);*
— $F(G + H) = FG + FH$ *(distributivité de × par rapport à +);*
— $F(GH) = (FG)H$ *(associativité de ×);*
— $F \times \frac{1}{1} = \frac{1}{1} \times F = F$ *($\frac{1}{1}$ est l'élément neutre de ×)*
— $FG = GF$ *(commutativité de ×);*
— $\lambda 1_{\mathbb{K}[X]} \times F = \lambda F$*;*
— $(\lambda + \mu)F = \lambda P + \mu F$
— $(\lambda\mu)F = \lambda(\mu F)$
— $\lambda(F + G) = \lambda F + \lambda G$

Notation 8.10. On note $\mathbb{K}(X)$ l'ensemble des fractions rationnelles muni de ses trois opérations.

Remarque 8.11. $\mathbb{K}(X)$ est aussi une $\mathbb{K}$-algèbre commutative et $\mathbb{K}[X]$ est une sous $\mathbb{K}$-algèbre de $\mathbb{K}(X)$.

Proposition 8.12. *Toute fraction rationnelle non nulle* F *a un (unique) inverse i.e. il existe une fraction rationnelle* G *telle que* $FG = GF = 1$.

Démonstration. Si $F = \frac{P}{Q}$ alors $G = \frac{Q}{P}$ convient □

Remarque 8.13. Avec cette propriété, on dit que l'anneau $(\mathbb{K}(X), +, \times)$ est un corps (c'est même le corps des fractions de $\mathbb{K}[X]$).

Définition 8.14. Le degré d'une fraction rationnelle $F = \frac{P}{Q}$ est

$$\deg(F) \coloneqq \deg(P) - \deg(Q) = \mathbb{Z} \cup \{-\infty\}$$

Remarque 8.15.
— Le degré est bien définie car $\deg(PS) = \deg(P) + \deg(S)$
— Comme le degré de 1 est nul alors cela étend bien le degré des polynômes.
— On remarquera que $\deg(F) \geq 0$ n'implique pas que F est un polynôme (e.g. $F = \frac{X^3}{X^2+1}$ n'est pas un polynôme).

Proposition 8.16. *Soient* $F, G \in \mathbb{K}(X)$. *Alors*
— $\deg(FG) = \deg(F) + \deg(G)$;
— $\deg(F + G) \leq \max(\deg(F), \deg(G))$ *avec égalité lorsque* $\deg(F) \neq \deg(G)$.

Démonstration. On se concentre sur le deuxième point. Soient $F = \frac{P}{Q}$ et $G = \frac{R}{S}$ deux fractions rationnelles.

$$\begin{aligned}
\deg(F + G) &= \deg\left(\frac{SP + QR}{SQ}\right) \\
&= \deg(SP + QR) - \deg(SQ) \\
&\leq \max(\deg(SP), \deg(QR)) - \deg(SQ) \\
&\leq \max(\deg(SP) - \deg(SQ), \deg(QR) - \deg(SQ)) \\
&\leq \max(\deg(P) - \deg(Q), \deg(R) - \deg(S)) \\
&\leq \max(\deg(F), \deg(G))
\end{aligned}$$

Si $\deg(F) \neq \deg(G)$ alors $\deg(P) - \deg(Q) \neq \deg(R) - \deg(S)$ et donc $\deg(SP) \neq \deg(QR)$. On en déduit donc toutes les inégalités ci-dessus sont des égalités. □

Définition 8.17. La dérivée d'une fraction rationnelle $F = \frac{P}{Q}$ est la fraction rationnelle

$$F' \coloneqq \frac{P'Q - PQ'}{Q^2}.$$

Lemme 8.18.
— *Pour tout* $F, G \in \mathbb{K}(X)$ *et* $\lambda \in \mathbb{K}$, *on a :*

$$(F + \lambda G)' = F' + \lambda G'$$

— *Pour tout* $F, G \in \mathbb{K}(X)$, *on a :*

$$(FG)' = F'G + FG'$$

— *La dérivée définie pour les polynômes et celle définie pour les fractions rationnelles coïncident sur les polynômes.*

Définition 8.19. Soit $F = \frac{P}{Q}$ une fraction rationnelle écrite sous forme irréductible. La fonction associée à F est la fonction (dite « rationnelle »)

$$f_F : x \in \mathbb{K} \setminus \{x \in \mathbb{K} \mid Q(x) = 0\} \mapsto F(x) \coloneqq \frac{P(x)}{Q(x)} \in \mathbb{K}$$

On appelle pôle de F les racines de Q et racine de F les racines de P (ou les zéros de f_F)

Remarque 8.20.
— Si $\mathbb{K} = \mathbb{R}$ alors a est un pôle de F si

$$\lim_{x \to a} f_F(x) = \pm\infty.$$

— Si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, f_F est infiniment dérivable et $f_F' = f_{F'}$.
— si $\mathbb{K} = \mathbb{F}_p$, f_F peut être définie nulle part (e.g. $F = \frac{1}{X^p - X}$)

8.2 Décomposition en éléments simples

8.2.1 Résultats généraux de décomposition

Le but de cette subsection va être d'expliquer comment intégrer les fonctions rationnelles associées à une fraction rationnelle de $\mathbb{R}(X)$. Pour cela, on va décomposer cette dernière en une somme de fractions rationnelles que l'on pourra facilement intégrer.

Lemme 8.21. *Soit F une fraction rationnelle. Il existe un unique couple (E, G) où $E \in \mathbb{K}[X]$ et $G \in \mathbb{K}(X)$ tel que*

$$F = E + G$$

et $\deg(G) < 0$. Le polynôme E est appelé partie entière de la fraction rationnelle F.

Démonstration. Soit $F = \frac{P}{Q}$ une fraction rationnelle écrite sous forme irréductible. Soit E, R le quotient et le reste de la division euclidienne de P par Q. Alors

$$F = \frac{P}{Q} = \frac{EQ + R}{Q} = E + \frac{R}{Q}$$

Comme $\deg(R) < \deg(Q)$ (par définition du reste) alors $\deg\left(\frac{R}{Q}\right) < 0$.
L'unicité vient de l'unicité de la division euclidienne. □

Lemme 8.22. *Soit $F = \frac{A}{B}$ une fraction rationnelle de degré strictement négatif. Soient B_1, B_2 deux polynômes premiers entre eux tels que $B = B_1 B_2$. Alors il existe une unique paire de polynômes (A_1, A_2) tels que $\deg(A_i) < \deg(B_i)$ pour $i = 1, 2$ et*

$$F = \frac{A_1}{B_1} + \frac{A_2}{B_2}.$$

Démonstration. **Existence** :
Comme B_1 et B_2 sont premiers entre eux alors, par le théorème de Bézout, il existe des polynômes U et V tels que

$$B_1 U + B_2 V = 1$$

et donc tels que $AB_1U + AB_2V = B$. On obtient alors les égalités suivantes

$$\begin{aligned} \frac{A}{B} &= \frac{AB_1U + AB_2V}{B_1B_2} = \frac{AU}{B_2} + \frac{AV}{B_1} \\ &= E_2 + \frac{A_2}{B_2} + E_1 + \frac{A_1}{B_1} \qquad (8.21), \deg(A_i) < \deg(B_i) \end{aligned}$$

Par unicité de la partie entière, $E_1 + E_2 = 0$ et donc

$$F = \frac{A_1}{B_1} + \frac{A_2}{B_2}.$$

Unicité :
Soient (A_1, A_2) et (C_1, C_2) deux paires de polynômes vérifiant les hypothèses de l'énoncé. Alors

$$\frac{A_1}{B_1} + \frac{A_2}{B_2} = \frac{C_1}{B_1} + \frac{C_2}{B_2}$$

On en déduit que $\frac{A_1 - C_1}{B_1} = \frac{C_2 - A_2}{B_2}$ et donc $B_2(A_1 - C_1) = B_1(C_2 - A_2)$. Comme B_1 et B_2 sont premiers entre eux alors par le théorème de Gauß, B_2 divise $C_2 - A_2$. Autrement dit, il existe $K \in \mathbb{K}[X]$ tel que $C_2 = KB_2 + A_2$. Comme $\deg(A_2) < \deg(B_2)$ et $\deg(C_2) < \deg(B_2)$ (par hypothèse) alors $K = 0$ et donc $A_2 = C_2$. De la même façon, $A_1 = C_1$. □

En utilisant ce lemme de façon répétée, on obtient :

Lemme 8.23. *Soit $F = \frac{A}{B}$ une fraction rationnelle de degré strictement négatif. Soient $B_1, \dots, B_n$ des polynômes premiers entre eux deux à deux tels que $B = \prod_{i=1}^{n} B_i$. Alors il existe une unique famille $(A_1, \dots, A_2)$ de polynômes tels que $\deg(A_i) < \deg(B_i)$, $1 \leq i \leq n$ et*

$$F = \sum_{i=1}^{n} \frac{A_i}{B_i}.$$

Lemme 8.24. *Soient A, B deux polynômes tels que $\deg(A) < n \deg(B) = \deg(B^n)$. Il existe une unique famille $(A_1, \dots, A_n)$ tels que $\deg(A_i) < \deg(B)$ et*

$$\frac{A}{B^n} = \sum_{i=1}^{n} \frac{A_i}{B^i}$$

Démonstration. On procède par récurrence sur n. Si $n = 1$ alors $A_1 = A$ est le seul à convenir.
Soit $n \in \mathbb{N}^*$ et supposons la propriété vraie au rang n. Soient Q, R le quotient et le reste de la division euclidienne de A par B. Alors

$$\frac{A}{B^{n+1}} = \frac{QB + R}{B^{n+1}} = \frac{Q}{B^n} + \frac{R}{B^{n+1}}$$

Comme $\deg(R) < \deg(B)$, il reste à montrer que $\deg(Q) < n \deg(B)$. On peut supposer $Q \neq 0$ (car ce cas-là est évident). Alors $\deg(A) = \deg(BQ) = \deg(BQ) = \deg(B) + \deg(Q)$. Comme $\deg(A) < (n+1)\deg(B)$ alors $\deg(Q) = \deg(A) - \deg(B) < n \deg(Q)$. La propriété est donc vraie au rang $n + 1$. □

Théorème 8.25 (décomposition en éléments simples sur $\mathbb{C}$)**.** *Soit $F = \frac{P}{Q}$ une fraction rationnelle de $\mathbb{C}(X)$ écrite sous forme irréductible de partie entière E et Q unitaire. Si la décomposition en facteurs irréductibles de Q est*

$$Q = \prod_{i=1}^{n} (X - \alpha_i)^{m_i}$$

alors il existe une unique famille de coefficients $(x_{ij})_{1 \leq i \leq n, 1 \leq j \leq m_i}$ de nombres complexes tels que

$$F = E + \sum_{i=1}^{n} \sum_{j=1}^{m_i} \frac{x_{ij}}{(X - \alpha_i)^j}$$

Lemme 8.26. *Soit* $F = \frac{P}{Q} \in \mathbb{R}(X) \subset \mathbb{C}(X)$ *une fraction rationnelle écrite sous forme irréductible. Soit* α *une racine complexe d'ordre* r *de* Q*. Notons* $\lambda_1, \dots, \lambda_n$ *les coefficients devant les* $\frac{1}{(X-\alpha)^i}$ *dans leur décomposition en éléments simples. Alors les coefficients devant* $\frac{1}{(X-\alpha)^i}$ *sont* $\overline{\lambda_1}, \dots, \overline{\lambda_n}$*. En particulier, si* $\alpha \in \mathbb{R}$ *alors* $\lambda_i \in \mathbb{R}$ *pour tout* i*.*

Démonstration. On va supposer dans un premier temps que $r = 1$ (on notera λ le complexe λ_1).
On sait que $\lambda = [(X-\alpha)F](\alpha)$. Soit $\widetilde{Q}$ le polynôme tel que $Q = (X-\alpha)\widetilde{Q}$ (et donc $Q = \overline{Q} = (X-\overline{\alpha})\overline{\widetilde{Q}}$). Alors

$$\lambda = \frac{P(\alpha)}{\widetilde{Q}(\alpha)}$$

Comme $P \in \mathbb{R}[X]$, on en déduit donc

$$\overline{\lambda} = \frac{\overline{P(\alpha)}}{\overline{\widetilde{Q}(\alpha)}} = \frac{\overline{P(\alpha)}}{\overline{\widetilde{Q}}(\overline{\alpha})} = \frac{P(\overline{\alpha})}{\overline{\widetilde{Q}}(\overline{\alpha})} = [(X-\overline{\alpha})F](\overline{\alpha})$$

Ce dernier complexe est le coefficient devant $\frac{1}{X-\overline{\alpha}}$. Le cas général se fait en considérant $(X-\alpha)^n F$ et ses dérivées. □

Lemme 8.27. *Soient* $\alpha, \lambda \in \mathbb{C}$*. Alors*

$$\frac{\lambda}{(X-\alpha)^n} + \frac{\overline{\lambda}}{(X-\overline{\alpha})^n} \in \mathbb{R}(X)$$

Démonstration. On a l'égalité suivante

$$\frac{\lambda}{(X-\alpha)^n} + \frac{\overline{\lambda}}{(X-\overline{\alpha})^n} = \frac{\lambda(X-\overline{\alpha})^n + \overline{\lambda}(X-\alpha)^n}{(X-\alpha)^n(X-\overline{\alpha})^n}$$

Le numérateur et le dénominateur sont égaux à leur conjugué et sont donc dans $\mathbb{R}[X]$. □

Théorème 8.28 (décomposition en éléments simples sur $\mathbb{R}$)**.** *Soit* $F = \frac{P}{Q}$ *une fraction rationnelle de* $\mathbb{R}(X)$ *écrite sous forme irréductible de partie entière* E *et* Q *unitaire. Si la décomposition en facteurs irréductibles de* Q *est*

$$Q = \prod_{i=1}^{n} (X-\alpha_i)^{m_i} \prod_{k=1}^{p} (X^2 - \beta_k X + \gamma_k)^{n_k}$$

alors il existe un unique triplet de familles de réels $(x_{ij})_{1 \le i \le n, 1 \le j \le m_i}$, $(y_{kl})_{1 \le k \le p, 1 \le l \le n_k}$, $(z_{kl})_{1 \le k \le p, 1 \le l \le n_k}$ *tel que*

$$F = E + \sum_{i=1}^{n} \sum_{j=1}^{m_i} \frac{x_{ij}}{(X-\alpha_i)^j} + \sum_{k=1}^{p} \sum_{l=1}^{n_k} \frac{y_{kl}X + z_{kl}}{(X^2 - \beta_k X + \gamma_k)^l}$$

On peut démontrer ce théorème comme dans le cas complexe. Dans la démonstration qui suit, on va partir de la décomposition sur $\mathbb{C}$ pour trouver celle sur $\mathbb{R}$ dans le cas des racines complexes simples (i.e. $n_k = 1$) afin d'avoir un moyen calculatoire simple de le faire.

Démonstration. Quitte à retirer la partie entière, on suppose que F est de degré strictement négatif.
On peut décomposer en facteurs irréductibles le polynôme Q sur $\mathbb{C}$:

$$Q = \prod_{i=1}^{n} (X-\alpha_i)^{m_i} \prod_{k=1}^{p} (X-\lambda_k)(X-\overline{\lambda_k})$$

où λ_k et $\overline{\lambda}_k$ sont les racines de $X^2 - \beta_k X + \gamma_k$.
On a donc une décomposition en éléments simples sur $\mathbb{C}$ (on utilise 8.26 pour avoir le coefficient des racines complexes conjuguées) :

$$F = \sum_{i=1}^{n} \sum_{j=1}^{m_i} \frac{x_{ij}}{(X-\alpha_i)^j} + \sum_{k=1}^{p} \frac{w_k}{(X-\lambda_k)} + \frac{\overline{w_k}}{(X-\overline{\lambda_k})}$$

Ensuite, on a :

$$\frac{w_k}{X-\lambda_k} + \frac{\overline{w_k}}{X-\overline{\lambda_k}} = \frac{w_k(X-\overline{\lambda}) + \overline{w_k}(X-\lambda)}{X^2 - \beta_k + \gamma_k} = \frac{2\mathrm{Re}(w_k)X - 2\mathrm{Re}\left(w_k\overline{\lambda}\right)}{X^2 - \beta_k + \gamma_k}$$

On en déduit que $y_k = 2\mathrm{Re}(w_k)$ et $z_k = -2\mathrm{Re}\left(w_k\overline{\lambda}\right)$.

□

8.2.2 Méthode de calculs

Soit $F = \frac{P}{Q}$ une fraction rationnelle écrite sous forme irréductible et

$$Q = \prod_{i=1}^{n} (X-\alpha_i)^{m_i} \prod_{k=1}^{p} (X^2 - \beta_k X + \gamma_k)^{n_k}$$

la décomposition en facteurs irréductibles de Q. On en déduit l'existence d'une écriture de la forme

$$F = E + \sum_{i=1}^{n} \sum_{j=1}^{m_i} \frac{x_{ij}}{(X-\alpha_i)^j} + \sum_{k=1}^{p} \sum_{l=1}^{n_k} \frac{y_{kl}X + z_{kl}}{(X^2 - \beta_k X + \gamma_k)^l}$$

Pour trouver les différents coefficients, on peut procéder comme suit :

- E est le quotient de la division euclidienne de P par Q (on peut supposer dans la suite que $E = 0$).
- Soit α_i une racine réelle de Q. Alors α_i n'est pas une racine de $(X-\alpha_i)^{m_i}F$ et

  $$x_{i,m_i} = [(X-\alpha_i)^{m_i}F](\alpha_i)$$

  On ne peut pas trouver les coefficients plus petits avec cette méthode.
- Soit λ_k une racine simple non réelle de Q (et de $X^2 - \beta_k X + \gamma_k$). On trouve de la même façon que dans le cas réel le coefficient (complexe) ω_k devant $\frac{1}{X-\lambda_k}$. Celui devant $\frac{1}{X-\overline{\lambda}_k}$ est $\overline{\omega_k}$ et on retrouve ainsi y_{k1} et z_{k1} en faisant la somme.
- Pour trouver les coefficients qui manquent, on peut ensuite
  - évaluer en des points bien choisis (e.g. 0 ou des zéros de F) ;
  - calculer $\lim_{x\to\infty} [X^n F](x)$ de deux façons différentes (avec des $n \in \mathbb{N}$ bien choisis pour que cela tende vers un nombre fini). On obtient ainsi une équation ;
  - tout développer et identifier les coefficients. On obtient ainsi un système linéaire en les coefficients qui faut résoudre.

Exemple 8.29. Considérons la fraction rationnelle

$$F = \frac{2X^4}{X^4 + 2X^3 + 2X^2 + 2X + 1} \in \mathbb{R}(X).$$

Cette fraction rationnelle est écrite sous forme irréductible et

$$X^4 + 2X^3 + 2X^2 + 2X + 1 = (X^2+1)(X+1)^2$$

Tout d'abord, on remarque que

$$F = 2 - \frac{4X^3 + 4X^2 + 4X + 2}{X^4 + 2X^3 + 2X^2 + 2X + 1}$$

Il existe $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ tels que

$$F = 2 + \frac{\alpha}{X+1} + \frac{\beta}{(X+1)^2} + \frac{\gamma X + \delta}{X^2+1}$$

Calculons β :

$$\beta = (X+1)^2 F(-1) = \frac{2(-1)^4}{(-1)^2+1} = 1$$

Calculons γ et δ. Pour cela, on fait la décomposition ($\lambda \in \mathbb{C}$) :

$$\frac{\gamma X + \delta}{X^2+1} = \frac{\lambda}{X-i} + \frac{\overline{\lambda}}{X+i}$$

Alors

$$\lambda = [(X-i)F](i) = \frac{2i^4}{(1+i)^2 2i} = -\frac{1}{2}$$

et donc

$$\frac{\gamma X + \delta}{X^2+1} = \frac{-1}{2(X-i)} - \frac{1}{2(X+i)} = \frac{-X}{X^2+1}$$

i.e. $\gamma = -1$ et $\delta = 0$ Pour trouver α, on va calculer $\lim\limits_{x\to\infty} x(F(x)-2)$ (qui existe et est finie pour des questions de degré) :

$$\lim_{x\to\infty} x(F(x)-2) = \lim_{x\to\infty} -x\frac{4x^3 + 4x^2 + 4x + 2}{x^4 + 2x^3 + 2x^2 + 2x + 1} = -4$$

et

$$\lim_{x\to\infty} x(F(x)-2) = \lim_{x\to\infty} \frac{\alpha x}{x+1} + \frac{\beta x}{(x+1)^2} + \frac{\gamma x^2 + \delta x}{x^2+1} = \alpha + \gamma = \alpha - 1$$

On en déduit que $\alpha = -3$. Ainsi

$$F = 2 + \frac{-3}{X+1} + \frac{1}{(X+1)^2} + \frac{-X}{X^2+1}$$

8.2.3 Intégration

8.2.3.1 Primitives de $f_{n,a} : x \mapsto \frac{1}{(x-a)^n}$, $n \in \mathbb{N}^*$

On se fixe un intervalle I inclus dans $]-\infty, a[$ ou $]a, +\infty[$.

— Si $n = 1$ alors les primitives de $f_{1,a}$ sur I sont $x \in I \mapsto \ln|x-a| + C, \quad C \in \mathbb{R}$

— Si $n \neq 1$ alors les primitives de $f_{n,a}$ sont $x \in I \mapsto \frac{1}{(1-n)(x-a)^{n-1}} + C, \quad C \in \mathbb{R}$

8.2.3.2 Primitives de $x \mapsto \frac{\alpha x+\beta}{(x^2+bx+c)^n}$ avec $b^2 - 4c < 0$ et $n \in \mathbb{N}^*$

Tout d'abord, on peut faire la décomposition suivante (pour $x \in \mathbb{R}$) :

$$\frac{\alpha x + \beta}{(x^2+bx+c)^n} = \frac{\alpha}{2}\frac{2x+b}{(x^2+bx+c)^n} + \left(\beta - \frac{\alpha b}{2}\right)\frac{1}{(x^2+bx+c)^n}$$

En considérant $u : x \mapsto x^2 + bx + c$, le premier terme se réécrit de la façon suivante :

$$\frac{\alpha}{2}\frac{2x+b}{(x^2+bx+c)^n} = \frac{\alpha}{2}\frac{u'(x)}{u(x)^n}$$

Ainsi la primitive de $x \mapsto \frac{\alpha}{2}\frac{2x+b}{(x^2+bx+c)^n}$ est

— $x \mapsto \frac{\alpha}{2}\ln(x^2+bx+c)$ si $n=1$;
— $x \mapsto \frac{\alpha}{2}\frac{1}{(1-n)(x^2+bx+c)^{n-1}}$

Pour calculer une primitive de $x \mapsto \frac{1}{(x^2+bx+c)^n}$, on peut remarquer que

$$\begin{aligned} x^2+bx+c &= \left(x+\frac{b}{2}\right)^2+\frac{4c-b^2}{4} \\ &= \frac{4c-b^2}{4}\left(\left(\frac{2x}{\sqrt{4c-b^2}}+\frac{b}{\sqrt{4c-b^2}}\right)^2+1\right) \end{aligned}$$

Alors grâce au changement de variable $u = \frac{2x}{\sqrt{4c-b^2}}+\frac{b}{\sqrt{4c-b^2}}$, on obtient pour tout $\alpha < \beta$,

$$\begin{aligned} \int_\alpha^\beta \frac{dx}{(x^2+bx+c)^n} &= \int_{\frac{2\alpha+b}{\sqrt{4c-b^2}}}^{\frac{2\beta+b}{\sqrt{4c-b^2}}} \frac{4}{(4c-b^2)(u^2+1)}\frac{\left(\sqrt{4c-b^2}\right)du}{2} \\ &= \int_{\frac{2\alpha}{\sqrt{4c-b^2}}}^{\frac{2\beta}{\sqrt{4c-b^2}}} \frac{2}{\sqrt{4c-b^2}(u^2+1)}du \end{aligned}$$

Il nous reste plus qu'à trouver une primitive de $x \in \mathbb{R} \mapsto \frac{1}{(x^2+1)^n} \in \mathbb{R}$, $n \in \mathbb{N}^*$. Notons I_n une telle primitive.
On sait que $I_1 = \text{Arctan}(x)+C$, $C \in \mathbb{R}$.
On remarque tout d'abord que

$$I_n = \int \frac{1+x^2}{(1+x^2)^n}dx - \int \frac{x^2}{(1+x^2)^n}dx = I_{n-1} - \int \frac{x^2}{(1+x^2)^n}dx$$

Ensuite, en faisant une intégration par parties sur le deuxième terme (avec $u : x \mapsto x/2$ et $v : x \mapsto \frac{1}{(1-n)(1+x^2)^{n-1}}$), on obtient

$$\int \frac{x^2}{(1+x^2)^n}dx = \frac{x}{2(1-n)(1+x^2)^{n-1}} - \frac{1}{2(1-n)}\int \frac{dx}{(1+x^2)^{n-1}} = \frac{x}{2(1-n)(1+x^2)^{n-1}} - \frac{1}{2(1-n)}I_{n-1}$$

En conclusion, on a :

$$I_n = -\frac{x}{2(1-n)(1+x^2)^{n-1}} + \frac{3-2n}{2(1-n)}I_{n-1}$$

Par exemple,

$$I_2 = \frac{-x}{-2(1+x^2)} + \frac{-1}{-2}I_1 = \frac{x}{2(1+x^2)} + \frac{1}{2}\text{Arctan}(x)+C$$