Polynômes

Dans toute la suite, $\mathbb{K}$ désigne le corps des réels, le corps des complexes ou un sous corps de $\mathbb{C}$.

1. $(\mathbb{K}[X], +, \cdot)$

1.1. Définitions.

Définition (Définition d'un polynôme)**.** On appelle polynôme formel à coefficients dans $\mathbb{K}$ (ou polynôme à une indéterminée X) toute suite infinie d'éléments de $\mathbb{K}$ notée $(a_0, a_1, \ldots, a_n, \ldots)$, avec $\forall i \in \mathbb{N}\ a_i \in \mathbb{K}$, telle qu'à partir d'un certain rang tous les éléments de la suite sont nuls.

On notera $P = (a_0, a_1, \ldots, a_n, \ldots)$. Les a_i sont les coefficients de P et a_0 est appelé terme constant.

On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$.

Polynôme nul. C'est le polynôme tel que $\forall i \in \mathbb{N}$, $a_i = 0$ et on le note $0_{\mathbb{K}[X]}$.

Définition (degré et valuation)**.** Soit $P = (a_0, a_1, \ldots, a_n, \ldots) \in \mathbb{K}[X]$ un polynôme non nul.

Le degré de P est le plus grand indice $n \in \mathbb{N}$ tel que $a_n \neq 0$ et pour tout $k > n$ on a $a_k = 0$. On le note $\deg(P)$.

La valuation de P est le plus petit indice i tel que $a_i \neq 0$ et si il existe $k \in \mathbb{N}$ avec $k < i$ alors $a_k = 0$. On le note $\mathrm{val}(P)$.

Propriété. Si $P = (a_0, a_1, \ldots, a_n, \ldots) \in \mathbb{K}[X]$ un polynôme non nul, alors :
- $\forall k > \deg P$ on a $a_k = 0$
- si $\mathrm{val}\, P \geq 1$ alors $\forall 0 \leq k < \mathrm{val}\, P$ on a $a_k = 0$
- $\mathrm{val}\, P \leq \deg P$
- $\mathrm{val}\, P = \deg P \Leftrightarrow P = (0, \ldots, 0, a_n(\neq 0), 0, \ldots, 0, \ldots)$. Dans ce cas P est appelé monôme.

Égalité de deux polynômes. Les deux polynômes $P = (a_0, a_1, \ldots, a_n, \ldots)$ et $Q = (b_0, b_1, \ldots, b_n, \ldots)$ sont égaux (on écrit $P = Q$) si et seulement si $a_i = b_i$ pour tout $i \in \mathbb{N}$.

1.2. Opérations sur les polynômes – structure de $\mathbb{K}[X]$.

Dans la suite, $P = (a_0, a_1, \ldots, a_n, \ldots)$ et $Q = (b_0, b_1, \ldots, b_n, \ldots)$.

Somme de P et Q. Le polynôme somme de P et Q, noté $P + Q$ est égal à $(a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, \ldots)$. $P + Q$ est un polynôme car pour tout $k > \max(\deg P, \deg Q)$ on a $a_k + b_k = 0$.

Cette addition est une loi de composition interne qui procure à $\mathbb{K}[X]$ une structure de groupe abélien, $(\mathbb{K}[X], +)$. L'élément neutre pour cette loi est le polynôme nul $0_{\mathbb{K}[X]}$ et le symétrique de P pour cette addition est le polynôme noté $-P$ défini par $-P = (-a_0, -a_1, \ldots, -a_n, \ldots)$.

Multiplication interne de P et Q. On pose $P \times Q = PQ = (c_0, c_1, \ldots, c_n, \ldots)$ défini par

$$\forall k \in \mathbb{N}, \quad c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

PQ est un polynôme car si $k > \deg P + \deg Q$ alors $c_k = 0$. Il suffit de remarquer que si $i \in \{0, \ldots, k\}$ (avec $k > \deg P + \deg Q$) alors $i \leq \deg P \Rightarrow k - i \geq k - \deg P > \deg Q \Rightarrow b_{k-i} = 0$ et $i > \deg P \Rightarrow a_i = 0$, ce qui donne dans tous les cas $a_i b_{k-i} = 0$, d'où $c_k = 0$.

On démontre que si P, Q et R sont des polynômes alors $PQ = QP$, $(PQ)R = P(QR)$ et $(P + Q)R = PR + QR$. De plus la relation (à vérifier) $(1, 0, \ldots, 0, \ldots)P = P(1, 0, \ldots, 0, \ldots) = P$ nous montre que $(1, 0, \ldots, 0, \ldots)$ est l'élément neutre pour la multiplication interne.

Conclusion. $(\mathbb{K}[X], +, \cdot)$ est un anneau commutatif unitaire.

Proposition. Si P et Q sont deux polynômes non nuls alors $\deg(PQ) = \deg P + \deg Q$.

Preuve. On sait déjà que si $k \geq \deg P + \deg Q + 1$ alors $c_k = 0$. Posons $n = \deg P$, $m = \deg Q$ et montrons que $c_{n+m} = a_n b_m$. D'après la définition $c_{n+m} = \sum_{k=0}^{n+m} a_k b_{n+m-k}$. Or d'après la définition du degré on a :
- $k < \deg P \Rightarrow n + m - k > m \Rightarrow b_{n+m-k} = 0$

– $k > \deg P \Rightarrow a_k = 0$

– $k = \deg P \Rightarrow a_k b_{n+m-k} = a_n b_m$, ce qui donne le résultat. Ainsi $c_{n+m} = a_n b_m \neq 0$ (car $a_n \neq 0$ et $b_m \neq 0$), d'où $\deg(PQ) = \deg P + \deg Q$.

Conséquence. $(\mathbb{K}[X], +, \cdot)$ est un anneau commutatif intègre unitaire.

Multiplication par un scalaire. Si $\lambda \in \mathbb{K}$ on définit le polynôme $\lambda P = (\lambda a_0, \lambda a_1, \ldots, \lambda a_n, \ldots)$.

1.3. **Notation définitive.** Posons $X = (0, 1, 0, \ldots, 0, \ldots)$. On obtient par calcul que $X^2 = (0, 0, 1, \ldots, 0, \ldots)$, $X^3 = (0, 0, 0, 1, \ldots, 0, \ldots)$, etc. Identifions les constantes $\alpha \in \mathbb{K}$ avec le polynôme $(\alpha, 0, 0, \ldots, 0, \ldots)$ (on peut remarquer que cette identification est compatible avec la multiplication interne et externe, i.e. $\alpha P = (\alpha, 0, 0, \ldots, 0, \ldots)P$). La structure d'anneau de $(\mathbb{K}[X], +, \cdot)$ permet alors d'écrire le polynôme $P = (a_0, a_1, \ldots, a_n, \ldots)$ sous la forme et en posant $n = \deg P$

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n + (\text{ termes nuls}) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n = \sum_{k=0}^{n} a_k X^k.$$

Nous adopterons désormais cette écriture pour les polynômes.

Les polynômes de degré o s'appellent les constantes.

Définition. Soit $P = a_n X^n + \cdots + a_1 X + a_0$ un polynôme de degré n (i.e. $a_n \neq 0$). Alors a_n s'appelle le coefficient dominant de P et $a_n X^n$ s'appelle le monôme de plus haut degré de P. Si $a_n = 1$ on dit que le polynôme est unitaire.

2. Les deux divisions de polynômes dans $\mathbb{K}[X]$

2.1. Divisibilité dans $\mathbb{K}[X]$.

Définition. Soient deux polynômes non nuls A et B. On dit que B divise A, ou A est multiple de B s'il existe $Q \in \mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\}$ tel que $A = BQ$. On écrit aussi que $B|A$.

Propriété. $\forall A \in \mathbb{K}[X]$ avec $A \neq 0$ on a $A|A$.
$\forall A, B, C, D \in \mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\}$:
Si $A|B$ et $B|C$ alors $A|C$.
Si $A|B$ et $A|C$ alors $A|(B + C)$.
Si $A|B$ et $C|D$ alors $AC|BD$.
Si I désigne l'ensemble des multiples de B, i.e. $I = B\mathbb{K}[X] = \mathbb{K}[X]B = \{BQ\,;\, Q \in \mathbb{K}[X]\}$ alors I vérifie les deux propriétés,
(1) $\forall P \in \mathbb{K}[X], \forall Q \in I, PQ \in I$
(2) $\forall Q_1, Q_2 \in I, Q_1 - Q_2 \in I$.

2.2. Division euclidienne.

Théorème. Soient deux polynômes non nuls A et B. Il existe un unique couple (Q, R) de polynômes de $\mathbb{K}[X]$ tel que $A = BQ + R$ et ($\deg R < \deg B$ ou bien $R = 0_{\mathbb{K}[X]}$). Déterminer ce couple (Q, R) c'est effectuer la division euclidienne du polynôme A par le polynôme B.

Preuve. Montrons tout d'abord l'existence d'un tel couple. Si $\deg A < \deg B$ alors le couple $(0_{\mathbb{K}[X]}, A)$ convient.

Si $\deg A \geq \deg B$, posons $n = \deg A$ et $m = \deg B$. Les polynômes A et B s'écrivent alors

$$A = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \qquad \text{avec } a_n \neq 0,$$

$$B = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0 \qquad \text{avec } b_m \neq 0.$$

Comme $n \geq m$, posons $Q_1 = \frac{a_n}{b_m} X^{n-m}$. Ainsi le polynôme R_1 définie par $R_1 = A - BQ_1$ est de degré au plus $n - 1$. Deux cas sont alors possibles.

1er cas : $\deg R_1 < \deg B$. Alors $A = BQ_1 + R_1$ et le couple (Q_1, R_1) convient.

2ème cas : $\deg R_1 \geq \deg B$. On continue le procédé en considérant R_1 et B et en posant

$$Q_2 = \frac{\text{coefficient de plus haut degré de } R_1}{b_m} X^{\deg R_1 - m}.$$

Le polynôme R_2 défini par $R_2 = R_1 - BQ_2$ est de degré strictement plus petit que $\deg R_1$. De la même façon que précédemment ou bien $\deg R_2 < \deg B$ et alors $(Q_1 + Q_2, R_2)$ convient, ou bien on continue le procédé. En itérant on obtient ainsi :

$$\begin{array}{ccc} R_1 = A - BQ_1 & \text{avec} & \deg R_1 < \deg A; \\ R_2 = R_1 - BQ_2 & \text{avec} & \deg R_2 < \deg R_1; \\ \vdots & & \vdots \\ R_k = R_{k-1} - BQ_k & \text{avec} & \deg R_k < \deg R_{k-1}. \end{array}$$

On construit une suite finie de polynômes R_i, dont les degrés sont décroissants d'au moins une unité à chaque étape. Au bout d'un nombre fini d'étapes on obtient $k \in \mathbb{N}$ tel que ($\deg R_k < \deg B$ ou bien $R_k = 0_{\mathbb{K}[X]}$) et $\deg R_{k-1} \geq \deg B$. D'où $A = B(Q_1 + Q_2 + \cdots + Q_k) + R_k$ et $\deg R_k < \deg B$.
Montrons l'unicité d'un tel couple. Soient $Q, R, S, T \in \mathbb{K}[X]$ tels que $A = BQ + R$, $A = BS + T$, $\deg R < \deg B$ et $\deg T < \deg B$. Si $R = T$ alors $B(Q - S) = 0$ et comme $\mathbb{K}[X]$ est un anneau intègre et $B \neq 0$ on en déduit que $Q = S$. Supposons que $R \neq T$ et montrons que l'on aboutit à une contradiction. En effet si $R - T \neq 0$ alors $B(Q - S) \neq 0$, d'où $\deg(B(Q - S)) = \deg B + \deg(Q - S) \geq \deg B$. Or nous avons $\deg(T - R) \leq \max(\deg T, \deg R) < \deg B$, d'où la contradiction puisque $T - R = B(Q - S)$.

Exemple : Soient $A = 3X^5 + 4X^2 + 1$ et $B = X^2 + 2X + 3$.

$$\begin{array}{rrrrrr|l}
 & 3X^5 & & +4X^2 & & +1 & X^2+2X+3 \\
\hline
- & 3X^5 & +6X^4 & +9X^3 & & & 3X^3-6X^2+3X+16 \\
\hline
 & & -6X^4 & -9X^3 & +4X^2 & +1 & \\
 & - & -6X^4 & -12X^3 & -18X^2 & & \\
\hline
 & & & 3X^3 & +22X^2 & +1 & \\
 & & - & 3X^3 & +6X^2 & +9X & \\
\hline
 & & & & 16X^2 & -9X+1 & \\
 & & & - & 16X^2 & +32X+48 & \\
\hline
 & & & & & -41X-47 &
\end{array}$$

Donc $Q = 3X^3 - 6X^2 + 3X + 16$ et $R = -41X - 47$.

2.3. Division suivant les puissances croissantes de X à l'ordre k, $k \in \mathbb{N}$.

Théorème. Soient deux polynômes non nuls A et B tels que $\operatorname{val} B = 0$ (i.e. le coefficient "constant" de B est non nul) et k un élément de $\mathbb{N}$. Il existe un unique couple (Q, R) d'éléments de $\mathbb{K}[X]$ tel que $A = BQ + X^{k+1}R$ avec $Q = 0$ ou $\deg Q \leq k$. Déterminer le couple (Q, R) c'est effectuer la division de A par B suivant les puissances croissantes de X à l'ordre k.

Preuve. Montrons tout d'abord l'existence. Posons $i = \operatorname{val} A$, $n = \deg A$ et $m = \deg B$. Les polynômes A et B s'écrivent alors

$$A = a_i X^i + a_{i+1}X^{i+1} + \cdots + a_n X^n \qquad \text{avec } a_n \neq 0, \quad a_i \neq 0$$

$$B = b_0 + b_1 X^1 + \cdots + b_m X^m \qquad \text{avec } b_m \neq 0, \quad b_0 \neq 0 (\operatorname{val} B = 0).$$

Distinguons 2 cas.
1er cas : $\operatorname{val} A > k$. Posons $R_0 = a_i X^{i-(k+1)} + \cdots + a_n X^{n-(k+1)}$. On a $A = X^{k+1}R_0$ et le couple $(0, R_0)$ convient.
2ème cas : $\operatorname{val} A \leq k$. Posons $Q_1 = \frac{a_i}{b_0} X^i$ et $R_1 = A - BQ_1$. Il est facile de vérifier que $\operatorname{val} R_1 > \operatorname{val} A$ et que $\deg Q_1 = \operatorname{val} A \leq k$.
Si $\operatorname{val} R_1 > k$ alors R_1 s'écrit $R_1 = X^{k+1}S_1$, avec $S_1 \in \mathbb{K}[X]$, ce qui donne $A = BQ_1 + X^{k+1}S_1$ et le couple (Q_1, S_1) convient.
Si $\operatorname{val} R_1 \leq k$ posons $Q_2 = \frac{\text{terme de plus bas degré de } R_1}{b_0}$ et $R_2 = R_1 - BQ_2$. On a $\deg Q_2 = \operatorname{val} R_1$ et $\operatorname{val} R_2 > \operatorname{val} R_1$.

Dans le cas où $\operatorname{val} R_2 > k$ on obtient $R_2 = X^{k+1}S_2$ avec $S_2 \in \mathbb{K}[X]$, d'où $A = B(Q_1 + Q_2) + X^{k+1}S_2$ et le couple $(Q_1 + Q_2, S_2)$ convient. Sinon on continue le procédé... Ainsi de suite on construit

$$\begin{array}{ccccc} BQ_1 = R_1 & \text{avec} & \deg Q_1 = \operatorname{val} A, & \operatorname{val} R_1 > \operatorname{val} A; \\ R_1 - BQ_2 = R_2 & \text{avec} & \deg Q_2 = \operatorname{val} R_1, & \operatorname{val} R_2 > \operatorname{val} R_1; \\ \vdots & & \vdots & \vdots \\ R_{k-1} - BQ_k = R_k & \text{avec} & \deg Q_k = \operatorname{val} R_{k-1}, & \operatorname{val} R_k > \operatorname{val} R_{k-1}. \end{array}$$

tels que la valuation de R_i croît au moins d'une unité à chaque étape. Au bout d'un nombre fini d'opérations on aura $\operatorname{val} R_{k-1} \leq k$, $\operatorname{val} R_k > k$ et $A = B(Q_1 + Q_2 + \cdots + Q_k) + R_k$. Comme chaque Q_i est un monôme de degré au plus k, $Q = Q_1 + Q_2 + \cdots + Q_k$ est de degré au plus k. Comme $\operatorname{val} R_k \geq k+1$, on a $R_k = X^{k+1}R$ avec $R \in \mathbb{K}[X]$. Ainsi le couple (Q, R) convient.
Montrons l'unicité de ce couple. Supposons que $A = BQ + X^{k+1}S$, $A = BS + K^{k+1}T$ avec $\deg Q \leq k$ et $\deg S \leq k$. Alors $B(Q-S) = X^{k+1}(R-T)$. Si $R = T$ on obtient que $B(Q-S) = 0$, d'où $Q = S$. Si $R \neq T$ alors $B(Q-S) \neq 0$ et $\operatorname{val}(B(Q-S)) = \operatorname{val} B + \operatorname{val}(Q-S) \leq \operatorname{val} B + \deg(Q-S) \leq k$; ce qui conduit à une contradiction puisque $X^{k+1}(R-T) \neq 0$ entraîne que $\operatorname{val}(X^{k+1}(R-T)) = \operatorname{val} X^{k+1} + \operatorname{val}(R-T) \geq k+1$. Finalement on obtient que $R = T$ et $Q = S$.

3. PGCD

Théorème. Soient A et B deux polynômes non nuls de $\mathbb{K}[X]$. Considérons le sous–ensemble $I = \{AU + BV\,;\, U \in \mathbb{K}[X],\ V \in \mathbb{K}[X]\}$. Le sous-ensemble I de $\mathbb{K}[X]$ est non vide et vérifie :

(1) $\forall P \in \mathbb{K}[X], \forall Q \in I, PQ \in I$,

(2) $\forall Q_1, Q_2 \in I, Q_1 - Q_2 \in I$. De plus, il existe un unique polynôme unitaire $D \in I$ tel que $I = D\mathbb{K}[X] = \{DQ\,;\, Q \in \mathbb{K}[X]\}$. I est alors l'ensemble des multiples de D. D divise A et B et est appelé le plus grand commun diviseur de A et B et noté $\operatorname{pgcd}(A, B)$.

Preuve. Comme A et B sont non nuls il est clair que I n'est pas réduit à $\{0\}$. On démontre facilement que I vérifie les propriétés (1) et (2). Posons $\mathcal{A} = \{\deg R\,;\, R \in I \text{ et } R \neq 0\}$. $\mathcal{A}$ est une partie non vide de $\mathbb{N}$ et admet donc un plus petit élément noté α. Soit $P \in I$ tel que $\deg P = \alpha$ (avec $P \neq 0$) et tel que P soit unitaire (on remarque ici que l'on peut toujours "rendre" P unitaire avec (1) car $\forall \lambda \in \mathbb{K}\ \lambda P \in I$ et il suffit alors de choisir $\lambda = 1/a_\alpha$ avec a_α le coefficient du terme de plus haut degré de P).

Montrons que $\forall R \in I$ avec $R \neq 0$ alors P divise R. En effet effectuons la division euclidienne de R par P. Soit (Q, S) le couple d'éléments de $\mathbb{K}[X]$ tel que $R = QP + S$ et $\deg S < \deg P$. Comme R et P sont éléments de I on déduit de (1) et (2) que $R - QP \in I$ et ainsi $S \in I$. Comme $\deg S < \deg P$ la définition du degré de P entraîne que $S = 0$. Ainsi on a $R = QP$ et P divise R.

On en déduit alors que I est inclus dans l'ensemble des multiples de P, et avec (1) et (2) il est clair que $\forall R \in \mathbb{K}[X]$ on a $RP \in I$. Donc $I = P\mathbb{K}[X]$ et l'existence de D est démontrée.

Montrons l'unicité de D. S'il existe un deuxième polynôme unitaire D' tel que $I = D'\mathbb{K}[X]$, on obtient que D divise D' ($D' \in D\mathbb{K}[X]$) et que D' divise D ($D \in D'\mathbb{K}[X]$). Ainsi $D = \lambda D'$ avec $\lambda \in \mathbb{R}$ et comme D et D' sont tous deux unitaires l'étude du coefficient de plus haut degré nous donne $\lambda = 1$ c'est à dire $D = D'$.

Propriété. Tout diviseur commun à A et B divise D et est de degré plus petit (ou égal) que $\deg D$.

Une conséquence immédiate du théorème précédent est l'identité de Bezout.
Identité de Bezout. Il existe U_0, V_0 éléments de $\mathbb{K}[X]$ tels que $D = AU_0 + BV_0$.

Algorithme d'Euclide. Soient A et B deux polynômes non nuls tels que $\deg A \geq \deg B$.

Effectuons la division euclidienne de A par B. Soient Q_1 et R_1 tels que $A = BQ_1 + R_1$ et $\deg R_1 < \deg B$.
1er cas : $R_1 = 0$. On en déduit alors que B divise A et ainsi $\operatorname{pgcd}(A, B) = \lambda B$ avec $\lambda \in \mathbb{K}^*$ tel que λB soit unitaire.
2ème cas : $R_1 \neq 0$. Comme $A - BQ_1 = R_1$, on en déduit que $\operatorname{pgcd}(A, B)$ divise R_1 d'où $\operatorname{pgcd}(A, B)$ divise B et R_1. De la même façon $\operatorname{pgcd}(B, R_1)$ divise $BQ_1 + R_1 = A$, d'où $\operatorname{pgcd}(B, R_1)$ divise B et A. Les propriétés du pgcd entraînent que $\operatorname{pgcd}(A, B) = \operatorname{pgcd}(B, R_1)$. On continue alors le procédé en effectuant la division

euclidienne de B par R_1 : soient Q_2 et R_2 tels que $B = R_1Q_2 + R_2$ et $\deg R_2 < \deg R_1$. Si $R_2 = 0$ on obtient $\text{pgcd}(B, R_1) = \lambda R_1$ (avec $\lambda \in \mathbb{K}^*$ tel que λR_1 unitaire) sinon $\text{pgcd}(B, R_1) = \text{pgcd}(R_1, R_2)$ et on continue…

On construit ainsi de suite

$$\begin{array}{ccc} A = BQ_1 + R_1 & \text{avec} & \deg R_1 < \deg B \text{ et } \text{pgcd}(A,B) = \text{pgcd}(B,R_1); \\ B = R_1Q_2 + R_2 & \text{avec} & \deg R_2 < \deg R_1 \text{ et } \text{pgcd}(B,R_1) = \text{pgcd}(R_1,R_2); \\ \vdots & & \vdots \quad \vdots \\ R_{k-1} = R_kQ_{k+1} + R_{k+1} & \text{avec} & \deg R_{k+1} < \deg R_k \text{ et } \text{pgcd}(R_{k-1},R_k) = \text{pgcd}(R_k,R_{k+1}). \end{array}$$

La suite des polynômes R_k est une suite dont le degré de chaque terme diminue d'au moins une unité à chaque étape. Au bout d'un nombre fini de divisions il existe k tel que $R_{k+1} = 0$ et $R_k \neq 0$. La construction nous donne alors $\text{pgcd}(A, B) = \text{pgcd}(B, R_1) = \cdots = \text{pgcd}(R_{k-1}, R_k) = \lambda R_k$ avec $\lambda \in \mathbb{K}^*$ tel que λR_k unitaire.

Remarque. Si le dernier reste non nul R_k est de degré zéro, i.e. R_k est une constante, on obtient $\text{pgcd}(A, B) = 1$.

Exemple Soient $A = 2X^5 + 2X^4 + X^3 + 1$ et $B = 3X^4 + X^3 - 3X - 1$. Successivement on calcule

$$\begin{aligned} A &= \Big(\frac{2}{3}X + \frac{4}{9}\Big)B + \frac{5}{9}X^3 + 2X^2 + 2X + \frac{13}{9} \\ B &= \Big(\frac{27}{5}X - \frac{441}{25}\Big)\Big(\frac{5}{9}X^3 + 2X^2 + 2X + \frac{13}{9}\Big) + \frac{612}{5}(X^2 + X + 1) \\ \frac{5}{9}X^3 + 2X^2 + 2X + \frac{13}{9} &= \Big(\frac{5}{9}X + \frac{13}{9}\Big)(X^2 + X + 1) + 0 \end{aligned}$$

Donc $\text{pgcd}(A, B) = X^2 + X + 1$.

4. Polynômes premiers entre eux

Définition. On dit que A et B éléments non nuls de $\mathbb{K}[X]$ sont premiers entre eux si $\text{pgcd}(A, B) = 1$.

Théorème. Soient A, B et C des éléments non nuls de $\mathbb{K}[X]$. Si A divise BC et si A est premier avec B alors A divise C.

Théorème (Théorème de Bezout)**.** Soient deux polynômes non nuls A et B. Pour que A et B soient premiers entre eux il faut et il suffit qu'il existe $U \in \mathbb{K}[X]$ et $V \in \mathbb{K}[X]$ tels que $AU + BV = 1$.

Preuve du théorème. Commençons par montrer (indépendamment des hypothèses) que $\text{pgcd}(BC, AC) = \lambda C \,\text{pgcd}(B, A)$ où $\lambda \in \mathbb{K}^*$ est tel que λC soit unitaire. Il est clair que tout diviseur de $\lambda C \,\text{pgcd}(B, A)$ divise BC et AC, donc $\lambda C \,\text{pgcd}(B, A)$ divise $\text{pgcd}(BC, AC)$. Inversement, d'après l'identité de Bezout, soient U et V tels que $\text{pgcd}(B, A) = AU + BV$. On a alors $\text{pgcd}(B, A)C = (AC)U + (BC)V$ et donc tout diviseur commun à AC et BC divise $\text{pgcd}(B, A)C$. Finalement les diviseurs communs à AC et BC sont les diviseurs de $\text{pgcd}(B, A)C$ et comme $\lambda C \,\text{pgcd}(B, A)$ est un polynôme unitaire on en déduit que $\text{pgcd}(BC, AC) = \lambda C \,\text{pgcd}(B, A)$.

Supposons que A divise BC et que A est premier avec B. On obtient alors aisément que A divise $\text{pgcd}(BC, AC)$. Or on a $\text{pgcd}(BC, AC) = \lambda C \,\text{pgcd}(A, B) = \lambda C$. On en conclut que A divise C.

Preuve du théorème de Bezout. Supposons tout d'abord que A et B sont premiers entre eux. D'après l'identité de Bezout, il existe U et V éléments non nuls de $\mathbb{K}[X]$ tels que $AU + BV = \text{pgcd}(A, B) = 1$. Réciproquement supposons qu'il existe U et V tels que $AU + BV = 1$. Si D est un diviseur commun à A et B, alors D est un diviseur commun à AU et BV, d'où D divise $AU + BV = 1$. Ainsi tout diviseur commun à A et B est une constante et $\text{pgcd}(A, B) = 1$.

5. Polynômes premiers ou irréductibles

Définition. Un polynôme P est dit irréductible (ou premier) si $\deg P \geq 1$ et si les seuls diviseurs de P sont les polynômes constants et les polynômes de la forme λP avec $\lambda \in \mathbb{K}^*$.

Théorème (Lemme d'Euclide)**.** Soit P un polynôme unitaire et irréductible. Si P divise le produit AB alors il divise l'un des facteurs.

Preuve. Supposons que P ne divise pas A. P étant irréductible, P et A sont premiers entre eux. Comme P divise AB, le théorème de Gauss entraîne que P divise B.

Corollaire. Soient A, B et P trois polynômes unitaires et irréductibles. Si P divise le produit AB alors P est égal à l'un des facteurs.

Théorème. Tout polynôme unitaire non irréductible peut s'écrire de manière unique (à l'ordre près) sous forme d'un produit de polynômes unitaires et irréductibles.

Preuve. Soit $P \in \mathbb{K}[X]$ unitaire et non irréductible. Comme P n'est pas irréductible soient P_1 et Q_1 deux polynômes unitaires tels que $P = P_1Q_1$ avec $P_1 \neq P$, $Q_1 \neq P$. Si P_1 et Q_1 sont irréductibles la décomposition est terminée. Dans le cas contraire si P_1 ou Q_1 (ou les deux) sont non irréductibles on recommence. On a $\deg P_1 < \deg P$ et $\deg Q_1 < \deg P$. On écrit (par exemple) $P_1 = P_2P_3 \dots$ A chaque nouvelle étape le degré des polynômes écrits est majoré par $\deg P$, minoré par 1 et décroît d'au moins 1. Au bout d'un nombre fini d'opérations on aura $P = R_1R_2 \cdots R_s$ avec R_i unitaire et irréductible pour tout $1 \leq i \leq s$.

Montrons l'unicité. Supposons que $P = R_1R_2 \cdots R_s = Q_1Q_2 \cdots Q_k$ avec R_i unitaire et irréductible ($1 \leq i \leq s$), Q_i unitaire et irréductible ($1 \leq i \leq k$). D'après le lemme d'Euclide R_1 divise au moins l'un des facteurs irréductibles Q_i. Quitte à renuméroter les polynômes Q_i on peut supposer que R_1 divise Q_1. Puisque Q_1 est irréductible et R_1 non constant, il existe $\lambda \in \mathbb{K}^*$ tels que $R_1 = \lambda Q_1$. Les polynômes R_1 et Q_1 étant unitaires on en déduit que $R_1 = Q_1$. Par récurrence on démontre que $k = s$ et, à une renumérotation près des polynômes Q_i, que $Q_i = R_i$ pour tout $1 \leq i \leq s$.

Application. Soit $P \in \mathbb{K}[X]^*$ avec $n = \deg P \geq 1$. Le polynôme P s'écrit

$$P = a_nX^n + a_{n-1}X^{n-1} \cdots + a_1X_1 + a_0 = a_n\Big(X^n + \frac{a_{n-1}}{a_n}X^{n-1} + \cdots + \frac{a_1}{a_n}X + \frac{a_0}{a_n}\Big) \quad (\text{car } a_n \neq 0)$$

Le polynôme $X^n + \frac{a_{n-1}}{a_n}X^{n-1} + \cdots + \frac{a_1}{a_n}X + \frac{a_0}{a_n}$ étant unitaire, le théorème de décomposition en facteurs unitaires et irréductibles entraîne que $P = a_nR_1 \cdots R_s$ avec R_i unitaire irréductible ($1 \leq i \leq s$).

Remarque. Si P est un polynôme unitaire non irréductible on démontre grâce au théorème précédent que P s'écrit sous la forme $P = R_1^{\alpha_1} \cdots R_k^{\alpha_k}$ avec $R_1, \dots, R_k$ polynômes unitaires et irréductibles deux à deux distincts et $\alpha_1 \dots, \alpha_k$ éléments de $\mathbb{N}^*$ (on a juste regroupé les facteurs irréductibles égaux).

Polynômes de degré 1**.** Tous les polynômes de degré 1 sont irréductibles. En effet si P est un polynôme de degré 1 et que $P = RQ$ avec $R \in \mathbb{K}[X]^*$ et $Q \in \mathbb{K}[X]^*$, on a $1 = \deg P = \deg Q + \deg R$, donc ou bien Q est de degré 0 (Q est une constante), ou bien Q est de degré 1 et dans ce cas R est une constante, ce qui donne $P = \lambda Q$. Les diviseurs de P sont donc bien les constantes ou de la forme λP.

Si $a, b \in \mathbb{K}$ et $a \neq b$ alors les polynômes $(X - a)$ et $(X - b)$ sont premiers entre eux. En effet il suffit de remarquer que $\frac{1}{b-a}(X - a) + \frac{1}{a-b}(X - b) = 1$ et d'appliquer le théorème de Bezout.

6. Racines d'un polynôme

Fonction polynôme. À tout polynôme $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ on associe la fonction polynôme f_P définie de $\mathbb{K}$ dans $\mathbb{K}$ par $f_P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ (la structure de corps de $\mathbb{K}$ justifie l'existence l'expression) pour tout $x \in \mathbb{K}$. Dans la suite on notera P pour f_P.

Définition. Soit P un polynôme non nul de $\mathbb{K}[X]$ et a un élément de $\mathbb{K}$. On dit que a est zéro de P (ou est racine de P) si la fonction polynôme associée à P s'annule en a, i.e. $P(a) = 0$.

Théorème. Soit $P \in \mathbb{K}[X]^*$ et $a \in \mathbb{K}$. Le polynôme P admet a comme zéro si et seulement si P est divisible par $(X - a)$.

Preuve. Si P est divisible par $X - a$ alors il existe $Q \in \mathbb{K}[X]$ tel que $P = Q \cdot (X - a)$, ce qui entraîne $P(a) = 0$. Réciproquement supposons que a est racine de P. Effectuons la division euclidienne de P par $(X - a)$: soient (Q, R) éléments de $\mathbb{K}[X]$ tels que $P = Q \cdot (X - a) + R$ et $\deg R < 1$. Le polynôme R est ou bien nulle ou bien un polynôme constant, λ avec $\lambda \in \mathbb{K}^*$. Comme a est racine de P on obtient que $R(a) = \lambda = 0$ et ainsi $R = 0$ et P est divisible par $(X - a)$.

Ordre de multiplicité d'une racine. Soit P un polynôme non nul de $\mathbb{K}[X]$ et a un zéro de P. Si $P = (X-a)\cdot Q_1$ avec $Q_1(a) \neq 0$ on dit que a est une racine simple ou d'ordre 1 de P. Si $P = (X-a)^2 \cdot Q_2$ avec $Q_2(a) \neq 0$, a est racine double ou d'ordre 2 de P ... Si $P = (X-a)^k \cdot Q_k$ avec $k \in \mathbb{N}^*$, $k > 1$ et $Q_k(a) \neq 0$, a est racine d'ordre (ou de multiplicité) k de P.

Théorème. Soit P un polynôme non nul de $\mathbb{K}[X]$ admettant les racines distinctes $a_1, a_2, \ldots, a_k$, ces racines admettant pour ordre de multiplicité $m_1, m_2, \ldots, m_k$ ($\forall i \in \{1,\ldots,k\}\ m_i \in \mathbb{N}^*$). Alors

$$P = (X-a_1)^{m_1}(X-a_2)^{m_2}\cdots(X-a_k)^{m_k}T$$

avec $T \in \mathbb{K}[X]^*$ et pour tout $i \in \{1,\ldots,k\}$, $T(a_i) \neq 0$.

Preuve. (Par récurrence) Le résultat est vrai pour une seule racine de multiplicité m.

Supposons le résultat vrai pour $k-1$ racines distinctes de multiplicité $m_1, m_2, \ldots, m_{k-1}$. Donc P s'écrit

$$P = (X-a_1)^{m_1}(X-a_2)^{m_2}\cdots(X-a_{k-1})^{m_{k-1}}T$$

avec $T \in \mathbb{K}[X]^*$ et pour tout $i \in \{1,\ldots,k-1\}$ $T(a_i) \neq 0$. D'autre part P admet a_k comme racine de multiplicité m_k, ce qui donne $P = (X-a_k)^{m_k}S$ avec $S \in \mathbb{K}[X]^*$ et $S(a_k) \neq 0$. On a donc

$$(X-a_k)^{m_k}S = (X-a_1)^{m_1}(X-a_2)^{m_2}\cdots(X-a_{k-1})^{m_{k-1}}T. \tag{1}$$

Les polynômes $(X-a_1), (X-a_2), \ldots, (X-a_k)$ sont des polynômes premiers et sont premiers entre eux deux à deux puisque les a_i sont distincts. Ainsi $(X-a_k)$ est premier avec $(X-a_i)$ pour tout $i \in \{1,\ldots,k-1\}$, d'où $(X-a_k)^{m_k}$ est premier avec $(X-a_i)^{m_i}$ pour tout $i \in \{1,\ldots,k-1\}$. Finalement $(X-a_k)^{m_k}$ est premier avec $\prod_{i=1}^{k-1}(X-a_i)^{m_i}$. L'égalité (1) et le théorème de Gauss impliquent alors que $(X-a_k)^{m_k}$ divise T. Donc $T = (X-a_k)^{m_k}U$ avec $U \in \mathbb{K}[X]^*$. On conclut que $P = (X-a_1)^{m_1}(X-a_2)^{m_2}\cdots(X-a_k)^{m_k}U$ avec $U \in \mathbb{K}[X]^*$. Pour tout $i \in \{1,\ldots,k-1\}$, $T(a_i) \neq 0$ entraîne que $U(a_i) \neq 0$. De plus on a $S = \left[\prod_{i=1}^{k-1}(X-a_i)^{m_i}\right]U$, ce qui donne $S(a_k) = \left[\prod_{i=1}^{k-1}(a_k-a_i)^{m_i}\right]U(a_k)$ et ainsi $S(a_k) \neq 0$ entraîne que $U(a_k) \neq 0$.

Corollaire. Un polynôme de degré n ($n \in \mathbb{N}^*$) admet au plus n racines.

7. Polynômes à coefficients complexes

Nous admettrons le résultat suivant,

Théorème (Théorème de d'Alembert–Gauss)**.** Tout polynôme dans $\mathbb{C}[X]$ de degré plus grand que 1 admet au moins une racine dans $\mathbb{C}$.

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

Théorème. Soit $P \in \mathbb{C}[X]^*$ de degré n avec $n \geq 1$. Il existe $a_1, \ldots, a_n \in \mathbb{C}$ et $\lambda \in \mathbb{C}^*$ tel que λ est le coefficient dominant de P et

$$P = \lambda(X-a_1)\cdots(X-a_n).$$

Preuve. Si P est de degré 1 alors le problème est résolu. Si $n \geq 2$, soit λ le coefficient du terme de plus haut degré de P ($\frac{1}{\lambda}P$ est alors unitaire). En utilisant le théorème de décomposition en facteurs irréductibles, soient $R_1, \ldots, R_s$ polynômes unitaires et irréductibles de $\mathbb{C}[X]$ tels que $P = \lambda R_1 \cdots R_s$. Pour tout $i \in \{1,\ldots,s\}$, le polynôme R_i étant irréductibles (dans $\mathbb{C}[X]$), soit $a_i \in \mathbb{C}$ tel que $R_i = X - a_i$. On obtient donc que $P = \lambda(X-a_1)\cdots(X-a_s)$. Il est clair que $\deg\big((X-a_1)\cdots(X-a_s)\big) = s$, d'où $s = n$.

Dans le théorème précédent on obtient donc que tout polynôme de $\mathbb{C}[X]$ possède n racines distinctes ou non (i.e. comptées avec leur ordre de multiplicité). Si P est un polynôme de $\mathbb{C}[X]$ de degré n avec $n \geq 1$ (en distinguant les racines) on obtient qu'il existe $a_1, \ldots, a_p \in \mathbb{C}$ deux à deux distincts, $m_1, \ldots, m_p \in \mathbb{N}^*$ tels que

$$P = \lambda(X-a_1)^{m_1}\cdots(X-a_p)^{m_p} \quad \text{où } \lambda \text{ est le coefficient dominant de } P$$

et $m_1 + m_2 + \cdots + m_p = n$.

8. Polynômes à coefficients réels

Commençons par remarquer que dans $\mathbb{R}[X]$, l'ensemble des polynômes irréductibles n'est pas réduit aux seuls polynômes de degré 1. En effet considérons le polynôme X^2+1 (dans $\mathbb{R}[X]$). Si X^2+1 est non irréductible dans $\mathbb{R}[X]$, il est alors produit de deux polynômes réels de degré 1 et ainsi il admet deux racines réelles ce qui est faux puisque $x^2+1 \geq 1$ pour tout $x \in \mathbb{R}$.

Pour déterminer précisément les polynômes réels irréductibles nous allons utiliser les résultats précédents sur les polynômes complexes puisque tout polynôme réel peut être considéré comme polynôme complexe.

Proposition. Soit $P \in \mathbb{R}[X]^*$. Alors pour tout $z \in \mathbb{C}$, $P\big(\overline{z}\big) = \overline{P(z)}$ (ici $P(\cdot)$ désigne ici la fonction polynôme P considéré comme élément de $\mathbb{C}[X]$).

Preuve. Soit $P = \sum_{k=0}^{n} a_k X^k$ avec $n = \deg P$ (i.e. $a_n \neq 0$) et $a_i \in \mathbb{R}$ pour tout $i \in \{0,\dots,n\}$ et soit $z \in \mathbb{C}$. Comme $a_k \in \mathbb{R}$ (pour tout $k \in \{0,\dots,n\}$), on a $a_k(\overline{z})^k = a_k\overline{z^k} = \overline{\left(a_k z^k\right)}$. Donc $P\big(\overline{z}\big) = \sum_{k=0}^{n} a_k(\overline{z})^k = \sum_{k=0}^{n} \overline{\left(a_k z^k\right)} = \overline{P(z)}$.

Corollaire. Soit $P \in \mathbb{R}[X]$ de degré plus grand ou égal à 1. Si dans $\mathbb{C}[X]$, P admet la racine non réelle α de multiplicité k alors P admet la racine non réelle $\overline{\alpha}$ de multiplicité k.

Théorème. Dans $\mathbb{R}[X]$, les polynômes unitaires et irréductibles sont les polynômes de degré 1 (i.e. $X-a$ avec $a \in \mathbb{R}$) et les polynômes de degré 2 du type $X^2+\alpha X+\beta$ avec $(\alpha,\beta) \in \mathbb{R}^2$ tel que $\alpha^2-4\beta<0$.

Preuve. Le polynôme $X^2+\alpha X+\beta$ avec $(\alpha,\beta) \in \mathbb{R}^2$) est irréductible dans $\mathbb{R}[X]$ si et seulement si $\alpha^2-4\beta<0$ (ce résultat vient du fait que $X^2+\alpha X+\beta$ admet au moins une racine réelle si et seulement si $\alpha^2-4\beta \geq 0$). Montrons maintenant que tout polynôme réel P, de degré plus grand que 3 est non irréductible dans $\mathbb{R}[X]$. D'après le théorème de d'Alembert–Gauss, P admet au moins une racine complexe, noté α. Si α n'est pas réelle, alors $\overline{\alpha}$ est racine de P (P est élément de $\mathbb{R}[X]$). Donc $P = (X-\alpha)(X-\overline{\alpha})\cdot Q = (X^2-(\alpha+\overline{\alpha})X+\alpha\overline{\alpha})\cdot Q$ avec $Q \in \mathbb{C}[X]$. Le polynôme $X^2-(\alpha+\overline{\alpha})X+\alpha\overline{\alpha}$ est à coefficients réels puisque $\alpha+\overline{\alpha} = 2\Re(\alpha) \in \mathbb{R}$ et $\alpha\overline{\alpha} = |\alpha|^2 \in \mathbb{R}$. En prenant soin de distinguer les cas $|\alpha|^2=0$ et $|\alpha|^2 \neq 0$, on démontre (exercice) en étudiant les coefficients (a priori complexes) du polynôme Q que ceux-ci sont en fait des réels. Ainsi si la racine α n'est pas réelle, P est le produit de deux polynômes à coefficients réels et n'est donc pas irréductible dans $\mathbb{R}[X]$.

9. Polynôme dérivé

Définition. Soit P un polynôme de $\mathbb{K}[X]$ de degré n avec $n \geq 1$. P s'écrit alors $P = \sum_{k=0}^{n} a_k X^k$ avec $a_n \neq 0$. On appelle polynôme dérivé de P, que l'on note P', le polynôme $\sum_{k=1}^{n} k a_k X^{k-1}$. Si P est le polynôme nul ou un polynôme constant, par définition le polynôme dérivé est $0_{\mathbb{K}[X]}$.

Propriété. Pour tout $\lambda \in \mathbb{K}$, pour tout P, Q éléments de $\mathbb{K}[X]$ on a : $(P+Q)' = P'+Q'$, $(\lambda P)' = \lambda P'$ et $(P\cdot Q)' = P'Q+PQ'$.

Dérivée successive Notons D l'application de $\mathbb{K}[X]$ dans $\mathbb{K}[X]$ qui à tout polynôme P de $\mathbb{K}[X]$ fait correspondre le polynôme dérivé P' de $\mathbb{K}[X]$. Notons encore $\mathrm{D}^1 = \mathrm{D}$, $\mathrm{D}\circ\mathrm{D} = \mathrm{D}^2$ …et pour tout $k \geq 2$, $\mathrm{D}^k = \mathrm{D}\circ\mathrm{D}^{k-1}$. Pour tout P éléments de $\mathbb{K}[X]$ on définit $\mathrm{D}^k(P) = P^{(k)}$ qui est le polynôme dérivé k–ième de P.

Soit le monôme normalisé X^n avec $n \geq 1$. On a $\mathrm{D}(X^n) = nX^{n-1}$, $\mathrm{D}^2(X^n) = n(n-1)X^{n-2}$. Pour tout $k<n$, on démontre (par récurrence) que $\mathrm{D}^k(X^n) = n(n-1)\cdots(n-k+2)(n-k+1)X^{n-k}$. Si $k=n$ on obtient $\mathrm{D}^n(X^n) = n!$ et si $k>n$ on a $\mathrm{D}^k(X^n)=0$. Pour $k \leq n$ on écrit aussi que $\mathrm{D}^k(X^n) = \frac{n!}{(n-k)!}X^{n-k}$.

Avec les propriétés de la dérivation, si le polynôme $P = \sum_{i=0}^{n} a_i X^i$, on établit que les dérivées successives de P sont données par :

si $k \leq n$ alors $\mathrm{D}^k(P) = P^{(k)} = \sum_{i=k}^{n} i(i-1)\cdots(i-k+1)X^{i-k}a_i$ (ce qui donne pour $k = n$, $P^{(n)} = a_n n!$) ;
si $k > n$ alors $\mathrm{D}^k(P) = P^{(k)} = 0$

Formule de Leibniz. Pour tout P, Q éléments de $\mathbb{K}[X]$ et pour tout $n \in \mathbb{N}^*$:

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

Formule de Taylor pour un polynôme. Soit P un polynôme de $\mathbb{K}[X]$ tel que $\deg P = n$. Soit a un élément quelconque de $\mathbb{K}$. On appelle formule de Taylor appliquée à P en a l'égalité

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

où $P^{(k)}(a)$ désigne la valeur prise par la fonction polynôme associée au polynôme dérivé k–ième au point a.

Pour $a = 0$ c'est la formule de Mac–Laurin. Avec l'expression des dérivées successives du polynôme $P = \sum_{k=0}^{n} a_k X^k$ on démontre que $P^{(k)}(0) = k!a_k$, d'où l'égalité quand $a = 0$. Dans le cas général, posons $Q = P \circ (X + a)$. Par récurrence on prouve que pour tout $k \leq \deg P$, $Q^{(k)} = P^{(k)} \circ (X + a)$. Comme $\deg Q = \deg P = n$, en appliquant la formule de Mac–Laurin au polynôme Q on obtient

$$Q = \sum_{k=0}^{n} \frac{Q^{(k)}(0)}{k!}X^k = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}X^k.$$

Ajoutons que $Q \circ (X - a) = \big(P \circ (X + a)\big) \circ (X - a) = P \circ (X) = P$ et on obtient le résultat.

Racine multiple et polynômes dérivés.

Soit P un polynôme de $\mathbb{K}[X]$ admettant a comme racine de multiplicité k avec $k > 1$. Alors P' admet a comme racine de multiplicité $k - 1$. En effet le polynôme P s'écrit $P = (X - a)^k Q$ avec $Q \in \mathbb{K}[X]$ et $Q(a) \neq 0$. Dérivons P : $P' = k(X - a)^{k-1}Q + (X - a)^k Q' = (X - a)^{k-1}\big(kQ + (X - a)Q'\big)$ et on a $\big(kQ+(X-a)Q'\big)(a) = kQ(a) \neq 0$, ce qui prouve que a est racine de P' de multiplicité $k-1$. Réciproquement on peut prouver que si a est racine de P et de P', k étant l'ordre de multiplicité de a racine de P' alors $k+1$ est l'ordre de multiplicité de a racine de P.

Théorème. Soit P un polynôme non nul de $\mathbb{K}[X]$. P admet a comme racine de multiplicité k ($k \in \mathbb{N}^*$) si et seulement si les polynôme $P, P', \ldots, P^{(k-1)}$ admettent a comme racine et $P^{(k)}$ n'admet pas a comme racine.

Preuve. Si P admet a comme racine d'ordre k alors : P' admet a comme racine d'ordre $k - 1$, P'' admet a comme racine d'ordre $k - 2$, …, $P^{(k-1)}$ admet a comme racine d'ordre 1. De plus $P^{(k)}$ ne peut admettre a comme racine car sinon a serait racine d'ordre au moins $k + 1$ de P. Réciproquement, supposons que a est racine de $P, P', \ldots, P^{(k-1)}$ et ne l'est pas de $P^{(k)}$. Appliquons la formule de Taylor à P en a (on pose $n = \deg P$) :

$$P = \sum_{i=0}^{n} \frac{P^{(i)}(a)}{i!}(X - a)^i.$$

Comme $P^{(i)}(a) = 0$ pour tout $i \in \{0, \ldots, (k-1)\}$, P se factorise sous la forme $P = (X - a)^k T$ avec

$$T = \frac{1}{k!}P^{(k)}(a) + \frac{(X-a)}{(k+1)!}P^{(k+1)}(a) + \cdots + \frac{(X-a)^{n-k}}{n!}P^{(n)}(a).$$

On a bien $T \in \mathbb{K}[X]^*$ et $T(a) = \frac{1}{k!}P^{(k)}(a) \neq 0$. Nous avons donc démontré que a est racine de multiplicité k du polynôme P.

1. Fractions rationnelles

Définition. Une fraction rationnelle est une expression $\dfrac{P}{Q}$ où P et Q sont deux polynômes de $\mathbb{K}[X]$ avec $Q \neq 0$.

Dans la pratique on identifie toujours une fraction rationnelle à sa forme irréductible. Soient P et Q deux éléments non nuls de $\mathbb{K}[X]$ et soit $D = \text{pgcd}(P, Q)$. On a alors $P = P_1 D$, $Q = Q_1 D$ (et $\text{pgcd}(P_1, Q_1) = 1$) et on identifie la fraction rationnelle $\dfrac{P}{Q}$ avec la fraction rationnelle $\dfrac{P_1}{Q_1}$ qui est une forme irréductible de $\dfrac{P}{Q}$.

On note par $F_{\mathbb{K}}[X]$ l'ensemble des fractions rationnelles $\frac{P}{Q}$ tels que $P \in \mathbb{K}[X]$, $Q \in \mathbb{K}[X]^*$.

Définition. Soit $\dfrac{P}{Q}$ une fraction rationnelle telle que $\text{pgcd}(P, Q) = 1$.

1) Les racines de P sont appelées les zéros (ou les racines) de la fraction $\frac{P}{Q}$. Si a est racine d'ordre h de P, on dit que a est zéro d'ordre h de la fraction rationnelle $\frac{P}{Q}$.

2) Les racines de Q sont appelées les pôles de la fraction $\frac{P}{Q}$. Si a est racines d'ordre k de Q, on dit que a est un pôle d'ordre k de la fraction rationnelle $\frac{P}{Q}$.

L'ensemble des fractions rationnelles muni de l'addition ($\frac{P_1}{Q_1} + \frac{P_2}{Q_2} = \frac{P_1Q_2+P_2Q_1}{Q_1Q_2}$), de la multiplication ($\frac{P_1}{Q_1} \cdot \frac{P_2}{Q_2} = \frac{P_1P_2}{Q_1Q_2}$) possède une structure de corps commutatif.

Fonction rationnelle associée. Soit $\dfrac{P}{Q}$ une fraction rationnelle avec $\text{pgcd}(P, Q) = 1$. On lui associe alors la fonction rationnelle définie par $\dfrac{P(t)}{Q(t)}$ pour $t \in \mathbb{K}$ tel que $Q(t) \neq 0$.

1.1. Décomposition des fractions rationnelles à coefficients complexes.

Théorème. Soit $\dfrac{P}{Q}$ une fraction rationnelle irréductible à coefficients complexes (i.e. $P \in \mathbb{C}[X]$ et $Q \in \mathbb{C}[X]^*$ et $\text{pgcd}(P, Q) = 1$). Soient $a_1, \ldots, a_p$ les racines complexes distinctes de Q, de multiplicité $m_1, \ldots, m_p$ (m_i élément de $\mathbb{N}^*$ est l'ordre de la racine a_i). Le polynôme Q s'écrit donc

$$Q = \lambda(X - a_1)^{m_1} \cdots (X - a_p)^{m_p}$$

avec λ le coefficients dominant de Q. Alors il existe une décomposition unique de la fraction rationnelle $\frac{P}{Q}$ sous la forme

$$\begin{aligned}\frac{P}{Q} = T &+ \frac{\lambda_{m_1}}{(X-a_1)^{m_1}} + \frac{\lambda_{m_1-1}}{(X-a_1)^{m_1-1}} + \cdots + \frac{\lambda_1}{(X-a_1)} \\ &+ \frac{\alpha_{m_2}}{(X-a_2)^{m_2}} + \frac{\alpha_{m_2-1}}{(X-a_2)^{m_2-1}} + \cdots + \frac{\alpha_1}{(X-a_2)} \\ &\vdots \\ &+ \frac{\mu_{m_p}}{(X-a_p)^{m_p}} + \frac{\mu_{m_p-1}}{(X-a_p)^{m_p-1}} + \cdots + \frac{\mu_1}{(X-a_p)},\end{aligned}$$

où $T \in \mathbb{C}[X]$ et les coefficients $\lambda_{m_1}, \ldots, \lambda_1$, $\alpha_{m_2}, \ldots, \alpha_1$, etc, $\mu_{m_p}, \ldots, \mu_{m_1}$ sont éléments de $\mathbb{C}$. On dit que la décomposition ci–dessus est la décomposition en éléments simples de $\frac{P}{Q}$ dans $\mathbb{C}[X]$. T est la partie entière de la décomposition et les termes $\frac{\lambda_{m_1}}{(X-a_1)^{m_1}}, \ldots, \frac{\lambda_1}{(X-a_1)}, \ldots$ sont appelés éléments simples.

Calcul des éléments simples dans $\mathbb{C}[X]$.

1) T est déterminé en effectuant la division euclidienne de P par Q. Soit le couple (R, S) de $\mathbb{C}[X]$ tel que $P = SQ + R$ avec $\deg R < \deg Q$. On a alors $\frac{P}{Q} = S + \frac{R}{Q}$ et on pose $T = S$. Remarquons que $T = 0$ dès que $\deg P < \deg Q$. Une fois T déterminé, il reste à décomposer la fraction rationnelle $\frac{R}{Q}$.

On suppose désormais que $\deg P < \deg Q$ ce qui entraîne $T = 0$. Considérons a un pôle d'ordre n de $\frac{P}{Q}$. Le but est de déterminer les éléments simples de la décomposition relatifs au pôle a. Le polynôme Q s'écrit $Q = (X-a)^n C$ avec $C \in \mathbb{C}[X]$ et $C(a) \neq 0$. Admettons (ce résultat se démontre grâce au théorème précédent en utilisant l'existence et l'unicité de la décomposition en éléments simples de $\frac{P}{Q}$) que

$$\frac{P}{Q} = \frac{P}{(X-a)^n C} = \frac{\lambda_n}{(X-a)^n} + \frac{\lambda_{n-1}}{(X-a)^{n-1}} \cdots + \frac{\lambda_2}{(X-a)^2} + \frac{\lambda_1}{(X-a)^1} + \frac{A}{C} \tag{2}$$

avec $A \in \mathbb{C}[X]$ tel que $\deg A < \deg C$ et tel que les coefficients $\lambda_1, \ldots, \lambda_n$ sont les coefficients que l'on cherche.

Posons $Y = X - a$, i.e. $X = Y + a$, ce qui entraîne $P(X) = P(Y+a)$ et $Q(X) = Y^n C(Y+a)$. Ainsi $P(Y+a)$ et $C(Y+a)$ sont deux polynômes en Y (Y est l'indéterminée). Effectuons la division suivant les puissances croissantes de Y du polynôme $P(Y+a)$ par $C(Y+a)$ jusqu'à l'ordre $n-1$:

$$P(Y+a) = \left(\mu_0 + \mu_1 Y + \cdots + \mu_{n-1} Y^{m-1}\right) C(Y+a) + Y^n R(Y).$$

Donc

$$\frac{P(Y+a)}{Q(Y+a)} = \frac{P(Y+a)}{Y^n C(Y+a)} = \frac{\mu_0}{Y^n} + \frac{\mu_1}{Y^{n-1}} + \cdots + \frac{\mu_{n-1}}{Y} + \frac{R(Y)}{C(Y+a)}$$

ce qui donne par rapport à l'indéterminée X

$$\frac{P(X)}{Q(X)} = \frac{\mu_0}{(X-a)^n} + \frac{\mu_1}{(X-a)^{n-1}} + \cdots + \frac{\mu_{n-1}}{(X-a)} + \frac{R(X-a)}{C(X)}$$

et ainsi les coefficients relatifs au pôle a sont déterminés, il reste à continuer l'étude des pôles autres que a.

La remarque suivante est importante pour déterminer λ_n.

Remarque. Dans l'égalité (2) multiplions la fraction rationnelle par $(X-a)^n$, on obtient

$$\frac{P}{C} = \lambda_n + (X-a)\lambda_{n-1} + \cdots + (X-a)^{n-1}\lambda_1 + (X-a)^n \frac{A}{C}.$$

Évaluons chacun des termes pour $X = a$ (ce qui est possible puisque $C(a) \neq 0$) ; on obtient $\frac{P(a)}{C(a)} = \lambda_n$. Dans la pratique on écrit

$$\frac{P}{Q}(X-a)^n \Big]_{X=a} = \frac{P(a)}{C(a)} = \lambda_n.$$

Remarque. Il existe plusieurs techniques qui permettent d'accélérer le calcul des coefficients. La méthode qui « marche » de façon sûre est celle des coefficients indéterminés, c'est aussi la plus longue, la plus calculatoire. Parmi les techniques usuelles, citons la dérivation, la parité de la fraction rationnelle, les limites en l'infini, le calcul dans $F_{\mathbb{C}}[X]$ pour donner le résultat dans $F_{\mathbb{R}}[X]$,…et autre cas particulier.

Remarque. Si a est un pôle d'ordre 1, i.e. $n = 1$, on a

$$\frac{P}{Q}(X-a) \Big]_{X=a} = \frac{P(a)}{C(a)} = \lambda_1.$$

Sans avoir à factoriser Q par $(X-a)$ on peut néanmoins donner la valeur de $C(a)$. En effet, $Q = (X-a)C$, d'où (par dérivation) $Q' = (X-a)C' + C$, ce qui donne (fonctions polynômes associées évaluées en a) $Q'(a) = C(a)$.

Exemple. Soit la fraction $\dfrac{1}{X^4-1}$. Il n'y a pas de partie entière puisque $\deg 1 = 0 < 4$. Posons $Q = X^4 - 1$. Les pôles sont les racines quatrièmes de l'unité, soit 1, i, -1 et $-i$: $Q = (X-1)(X-i)(X+1)(X+i)$. Donc il existe un unique quadruplet $(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ d'éléments de $\mathbb{C}$ tel que

$$\frac{1}{X^4-1} = \frac{\lambda_1}{X-1} + \frac{\lambda_2}{X-i} + \frac{\lambda_3}{X+1} + \frac{\lambda_4}{X+i}.$$

On a $Q' = 4X^3$, ce qui donne (en utilisant la remarque précédente) $\lambda_1 = \dfrac{1}{Q'(1)} = 1/4$, $\lambda_2 = \dfrac{1}{Q'(i)} = \dfrac{1}{4i^3} = \dfrac{i}{4}$, $\lambda_3 = \dfrac{1}{Q'(-1)} = \dfrac{-1}{4}$ et $\lambda_4 = \dfrac{1}{Q'(-i)} = \dfrac{1}{-4i^3} = \dfrac{-i}{4}$.

Exemple. Soit la fraction $\dfrac{4}{(X^2+1)^2}$. La partie entière est nulle et clairement on a $(X^2+1)^2 = (X-i)^2(X+i)^2$. Il existe donc λ_1, λ_2, μ_1 et μ_2 éléments de $\mathbb{C}$ tels que

$$\frac{4}{(X^2+1)^2} = \frac{\lambda_2}{(X-i)^2} + \frac{\lambda_1}{X-i} + \frac{\mu_2}{(X+i)^2} + \frac{\mu_1}{X+i}$$

Si X est changé en $-X$, la fraction rationnelle est invariante ($(-X)^2$) ce qui donne une information supplémentaire :

$$\frac{4}{(X^2+1)^2} = \frac{\lambda_2}{(-X-i)^2} + \frac{\lambda_1}{-X-i} + \frac{\mu_2}{(-X+i)^2} + \frac{\mu_1}{-X+i}$$

soit

$$\frac{4}{(X^2+1)^2} = \frac{\lambda_2}{(X+i)^2} + \frac{-\lambda_1}{X+i} + \frac{\mu_2}{(X-i)^2} + \frac{-\mu_1}{X-i}$$

et l'unicité de la décomposition en éléments simples permet d'obtenir que $\lambda_2 = \mu_2$ et $\mu_1 = -\lambda_1$ et réduit le nombre d'inconnus à 2.

Posons $Y = X - i$ et utilisons la technique de la division suivant les puissances croissantes pour déterminer μ_2 et μ_1.

$$\frac{4}{(X-i)^2(X+i)^2} = \frac{4}{(Y+2i)^2Y^2} = \frac{4}{(-4+4iY+Y^2)Y^2}.$$

On effectue la division suivant les puissances croissantes de Y à l'ordre 1 de 4 par $(-4+4iY+Y^2) : 4 = (-4+4i+Y^2)(-1-iY) + iY^3$. Donc $\lambda_2 = -1$ et $\lambda_1 = -i$. Finalement

$$\frac{4}{(X^2+1)^2} = \frac{-1}{(X-i)^2} + \frac{-i}{X-i} + \frac{-1}{(X+i)^2} + \frac{i}{X+i}.$$

On peut procéder autrement une fois établi que $\lambda_2 = \mu_2$ et $\mu_1 = -\lambda_1$. Déterminons d'abord λ_2 avec l'une des remarques précédentes :

$$\left.\frac{4(X-i)^2}{(X^2+i)^2(X-i)^2}\right]_{X=i} = -1 = \lambda_2.$$

Pour déterminer λ_1, on peut alors évaluer la fraction rationnelle en $X = 0$. On obtient l'équation $4 = \frac{-1}{i^2} + \frac{\lambda_1}{-i} + \frac{-1}{(-i)^2} + \frac{-\lambda_1}{i}$, d'où $\lambda_1 = -i$.

1.2. **Décomposition des fractions rationnelles à coefficients réels.**

Théorème. Soit $\frac{P}{Q}$ une fraction rationnelle à coefficients réels (i.e. $P \in \mathbb{R}[X]$ et $Q \in \mathbb{R}[X]^*$) avec $\operatorname{pgcd}(P,Q) = 1$. Dans $\mathbb{R}[X]$, le polynôme Q se décompose sous la forme

$$Q(X) = \lambda(X-a_1)^{m_1}\cdots(X-a_r]^{m_r}\left[(X-p_1)^2+q_1^2\right]^{n_1}\cdots\left[(X-p_s)^2+q_s^2\right],$$

où : $\forall i \in \{1,\dots,r\}$ $a_i \in \mathbb{R}$ est racine de Q de multiplicité m_i et les a_i sont distincts ;
$\forall j \in \{1,\dots,s\}$, $p_j \in \mathbb{R}$, $q_j \in \mathbb{R}^*$, le polynôme $(X-p_j)^2+q_j^2$ est irréductible dans $\mathbb{R}[X]$ et $(p_j,q_j) \neq (p_k,q_k)$ si $j \neq k$ ($(X-p_j)^2+q_j^2$ admet deux racines complexes conjuguées qui sont $p_j \pm iq_j$).

La fraction rationnelle $\frac{P}{Q}$ admet alors l'unique décomposition en éléments simples de la forme

$$\begin{aligned}\frac{P}{Q} = T &+ \frac{\lambda_{m_1}}{(X-a_1)^{m_1}} + \frac{\lambda_{m_1-1}}{(X-a_1)^{m_1-1}} + \cdots + \frac{\lambda_1}{(X-a_1)} \\ &+ \frac{\alpha_{m_2}}{(X-a_2)^{m_2}} + \frac{\alpha_{m_2-1}}{(X-a_2)^{m_2-1}} + \cdots + \frac{\alpha_1}{(X-a_2)} \\ &\vdots \\ &+ \frac{\mu_{m_r}}{(X-a_r)^{m_r}} + \frac{\mu_{m_r-1}}{(X-a_r)^{m_r-1}} + \cdots + \frac{\mu_1}{(X-a_r)} \\ &+ \frac{M_{n_1}X+N_{n_1}}{[(X-p_1)^2+q_1^2]^{n_1}} + \cdots + \frac{M_1X+N_1}{[(X-p_1)^2+q_1^2]} \\ &\vdots \\ &+ \frac{L_{n_s}X+O_{n_s}}{[(X-p_s)^2+q_s^2]^{n_s}} + \cdots + \frac{L_1X+O_1}{[(X-p_s)^2+q_s^2]}\end{aligned}$$

où $T \in \mathbb{C}[X]$ et les coefficients $\lambda_{m_1}, \ldots, \lambda_1, \alpha_{m_2}, \ldots, \alpha_1$, etc, $\mu_{m_p}, \ldots, \mu_{m_1}, M_{n_1}, \ldots, M_1, N_{n_1}, \ldots, N_1, \ldots, L_{n_s}, \ldots, L_1$ et $O_{n_s}, \ldots, O_1$ sont éléments de $\mathbb{R}$. On dit que la décomposition ci–dessus est la décomposition en éléments simples de $\frac{P}{Q}$ dans $\mathbb{R}[X]$. T est la partie entière de la décomposition. Les éléments simples du type $\frac{\lambda}{(X-a)^k}$ sont appelés éléments simples de 1ère espèce. Les éléments simples du type $\frac{MX+N}{[(x-p)^2+q^2]^k}$ sont appelés éléments simples de 2ème espèce.

Calcul des éléments simples dans $\mathbb{R}[X]$.

1) Pour les éléments simples de 1ère espèce ainsi que pour la partie entière on conserve les mêmes techniques que dans le cas complexe.

2) Pour les éléments simples de 2ème espèce.

On suppose dans la suite que $\deg P < \deg Q$ (ainsi T la partie entière est nulle).

– 1er Cas : $Q = [(X-p)^2+q^2)]^n$ avec $n \in \mathbb{N}^*$. Le théorème entraîne l'existence (et l'unicité) de la décomposition

$$\frac{P}{Q} = \frac{\mu_n X+\nu_n}{[(X-p)^2+q^2]^n} + \frac{\mu_{n-1}X+\nu_{n-1}}{[(X-p)^2+q^2]^{n-1}} \cdots + \frac{\mu_1 X+\nu_1}{[(X-p)^2+q^2]}$$

On divise P euclidiennement par $(X-p)^2+q^2$, soit $P = [(X-p)^2+q^2)]Q_1 + R_1$ avec $\deg R_1 < 2$. On continue avec Q_1 ; $Q_1 = [(X-p)^2+q^2)]Q_2 + R_2$ avec $\deg R_2 < 2$, etc, jusqu'à obtenir $Q_{k-1} = [(X-p)^2+q^2)]Q_k + R_k$ avec $\deg R_k < 2$ et $\deg Q_k < 2$. En "remontant" la suite des divisions euclidiennes successives on obtient que $P = S_k[(X-p)^2+q^2)]^k + S_{k-1}[(X-p)^2+q^2)]^{k-1} + \cdots S_1[(X-p)^2+q^2)] + S_0$ où S_j est de degré strictement plus petit que 2.

Exemple. Soit $f = \frac{X^5+2}{(X^2+X+1)^3}$. On a $\deg(X^5+2) = 5 < 6 = \deg((X^2+X+1)^3)$, et la partie entière de la décomposition en éléments simples est nulle. On vérifie que X^2+X+1 est bien un polynôme irréductible dans $\mathbb{R}[X]$ (par exemple son discriminant est strictement négatif). Donc il existe 6 réels μ_3, μ_2, μ_1, λ_3, λ_2 et λ_1 tels que

$$\frac{X^5+2}{(X^2+X+1)^3} = \frac{\mu_3 X+\nu_3}{(X^2+X+1)^3} + \frac{\mu_2 X+\nu_2}{(X^2+X+1)^2} + \frac{\mu_1 X+\nu_1}{(X^2+X+1)}.$$

Divisions euclidiennes successives : $X^5+2 = (X^2+X+1)(X^3-X^2+1) + (-X+1)$, $X^3-X^2+1 = (X^2+X+1)(X-2)+(X+3)$. Donc $X^5+2 = (X^2+X+1)\big((X^2+X+1)(X-2)+(X+3)\big)+(-X+1)$, soit

$$\frac{X^5+2}{(X^2+X+1)^3} = \frac{-X+1}{(X^2+X+1)^3} + \frac{X+3}{(X^2+X+1)^2} + \frac{X-2}{X^2+X+1}.$$

– 2ème Cas : $Q = [(X-p)^2+q^2)]^n C$ avec $n \in \mathbb{N}^*$ et $C \in \mathbb{R}[X]$ tel que $C(p+iq) \neq 0$ (ce qui entraîne $\text{pgcd}([(X-p)^2+q^2)], C) = 1$. On démontre (grâce au théorème de décomposition en éléments simples) que

$$\frac{P}{Q} = \frac{\mu_n X + \nu_n}{[(X-p)^2+q^2]^n} + \frac{\mu_{n-1}X+\nu_{n-1}}{[(X-p)^2+q^2]^{n-1}} \cdots + \frac{\mu_1 X + \nu_1}{[(X-p)^2+q^2]} + \frac{K}{C} \tag{3}$$

avec $K \in \mathbb{R}[X]^*$ et $\mu_1, \ldots, \mu_n, \nu_1, \ldots, \nu_n$ sont les coefficients cherchés.

Multiplions (3) par $[(X-p)^2+q^2)]^n$;

$$\frac{P}{Q}[(X-p)^2+q^2)]^n = \frac{P}{C} = \mu_n X + \nu_n + [(X-p)^2+q^2)]\frac{D}{C}$$

avec $D \in \mathbb{R}[X]$. Évaluons cette égalité pour $X = p+iq$:

$$\frac{P}{Q}[(X-p)^2+q^2)]^n\Big]_{X=p+iq} = \frac{P(p+iq)}{C(p+iq)} = \mu_n(p+iq)+\nu_n.$$

Comme μ_n et ν_n sont des réels, en identifiant partie réelle et partie imaginaire on trouve μ_n et ν_n.

Si $n = 1$, c'est terminé.

Si $n > 1$ on calcule

$$\frac{P}{Q} - \frac{\mu_n X + \nu_n}{[(X-p)^2+q^2]^n} = \frac{P-(\mu_n X+\nu_n)C}{[(X-p)^2+q^2]^n C}.$$

Remarquons que μ_n et ν_n sont tels que $P-(\mu_n X+\nu_n)C$ évalué en $X = p+iq$ est nul, ce qui entraîne que $P-(\mu_n X+\nu_n)C$ (polynôme réel) est nécessairement multiple de $[(X-p)^2+q^2]$. Ainsi

$$\frac{P}{Q} - \frac{\mu_n X + \nu_n}{[(X-p)^2+q^2]^n} = \frac{A}{[(X-p)^2+q^2]^{n-1}C} = \frac{\mu_{n-1}X+\nu_{n-1}}{[(X-p)^2+q^2]^{n-1}} \cdots + \frac{\mu_1 X + \nu_1}{[(X-p)^2+q^2]} + \frac{K}{C}$$

et on continue les calculs …

Exemple. Soit $f = \dfrac{X+1}{(X^2+1)^2(X^2+X+1)^2}$. On vérifie que les polynômes X, X^2+X+1 et X^2+1 sont premiers entre eux et que X^2+X+1 et X^2+1 sont irréductibles dans $\mathbb{R}[X]$. Donc la décomposition en éléments simples s'écrit

$$f = \frac{\lambda_2 X+\mu_2}{(X^2+1)^2} + \frac{\lambda_1 X+\mu_1}{(X^2+1)} + \frac{\gamma_2 X+\nu_2}{(X^2+X+1)^2} + \frac{\gamma_1 X+\nu_1}{(X^2+X+1)}$$

avec $\lambda_2, \lambda_1, \mu_2, \mu_1, \gamma_2, \gamma_1, \nu_2, \nu_1$ réels.

$$f(X^2+1)^2\big]_{X=i} = \frac{X+1}{(X^2+X+1)^2}\Big]_{X=i} = \frac{i+1}{i^2} = i-1 = \lambda_2 i + \mu_2$$

Donc $\lambda_2 = -1$ et $\mu_2 = -1$.

$$f + \frac{X+1}{((X^2+X+1)^2} = \frac{X+1+(X+1)(X^2+X+1)^2}{(X^2+1)^2(X^2+X+1)^2} = \frac{X^5+3X^4+5X^3+5X^2+4X+1}{(X^2+1)^2(X^2+X+1)^2}$$
$$= \frac{(X^2+1)(X^3+3X^2+4X+2)}{(X^2+1)^2(X^2+X+1)^2} = \frac{X^3+3X^2+4X+2}{(X^2+1)(X^2+X+1)^2} = g$$

On a

$$g = \frac{\lambda_1 X+\mu_1}{(X^2+1)} + \frac{\gamma_2 X+\nu_2}{(X^2+X+1)^2} + \frac{\gamma_1 X+\nu_1}{(X^2+X+1)},$$

d'où

$$g(X^2+1)\big]_{X=i} = \frac{-i-3+4i+2}{i^2} = -3i+1 = \lambda_1 i + \mu_1$$

soit $\lambda_1 = -3$ et $\mu_1 = 1$. On continue avec

$$\begin{aligned} g + \frac{3X-1}{X^2+1} &= \frac{X^3+3X^2+4X+2+(3X-1)(X^2+X+1)^2}{(X^2+1)(X^2+X+1)^2} \\ &= \frac{3X^5+5X^4+8X^3+6X^2+5X+1}{(X^2+1)(X^2+X+1)^2} = \frac{(X^2+1)(3X^3+5X^2+5X+1)}{(X^2+1)(X^2+X+1)^2} \\ &= \frac{3X^3+5X^2+5X+1}{(X^2+X+1)^2} \end{aligned}$$

Division euclidienne : $3X^3+5X^2+5X+1 = (3X+2)(X^2+X+1)-1$. Donc on obtient $\gamma_2 = 0$, $\nu_2 = -1$, $\gamma_1 = 3$ et $\nu_1 = 2$.

Autre méthode (après avoir obtenu λ_2, μ_2, λ_1 et μ_1)

Si $j = \exp\left(\frac{2i\pi}{3}\right)$ (j racine de X^2+X+1)

$$f(X^2+X+1)^2\big]_{X=j} = \frac{j+1}{(j^2+1)^2} = j^2 + j = -1 = \gamma_2 j + \nu_2,$$

d'où $\nu_2 = -1$ et $\gamma_2 = 0$.

Valeur particulière $X = 0$; on obtient $1 = \mu_2 + \mu_1 + \nu_2 + \nu_1 = -1 + 1 - 1 + \nu_1$, soit $\nu_1 = 2$.

Utilisation de la limite en $+\infty$: $\lim_{x\to+\infty}(xf(x)) = 0 = \lambda_1 + \gamma_1$. Donc $\gamma_1 = -\lambda_1 = 3$

Exemple. On peut aussi d'abord décomposer une fraction rationnelle réelle dans $\mathbb{C}[X]$ pour obtenir la décomposition dans $\mathbb{R}$. Soit $f = \dfrac{1}{(X^2+X+1)(X^2-X+1)}$. Avec $j = \exp\left(\frac{2i\pi}{3}\right)$, on a $X^2+X+1 = (X-j)(X-j^2)$ et $X^2-X+1 = (X+j)(X+j^2)$. Dans $\mathbb{C}$, f se décompose sous la forme

$$f = \frac{\lambda}{X-j} + \frac{\mu}{X-j^2} + \frac{\alpha}{X+j} + \frac{\beta}{X+j^2}.$$

Nous avons donc uniquement des pôles d'ordre 1. Après calculs on trouve que

$$f = \frac{1}{6}\left(\frac{1-j}{X-j} + \frac{1-j^2}{X-j^2} + \frac{j-1}{X+j} + \frac{j^2-1}{X+j^2}\right)$$

Pour obtenir la décomposition dans $\mathbb{R}[X]$ on additionne les éléments simples de pôles conjugués ($\overline{j} = j^2$ et $\overline{-j} = -j^2$).

$$f = \frac{1}{6}\left(\frac{(1-j)(X-j^2)+(1-j^2)(X-j)}{X^2+X+1} + \frac{(j-1)(X+j^2)+(j^2-1)(X+j)}{X^2-X+1}\right)$$

soit

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

Remarque (Applications)**.** L'une des applications de la décomposition en éléments simples d'une fraction rationnelle est le calcul de primitive. Calculons la primitive de la fonction

$$\frac{1}{(x^2+x+1)(x^2-x+1)}.$$

D'après l'exemple précédent on écrit

$$\begin{aligned}\frac{1}{(x^2+x+1)(x^2-x+1)} &= \frac{x+1}{2(x^2+x+1)} + \frac{-x+1}{2(x^2-x+1)} \\ &= \frac{x+\frac{1}{2}}{2(x^2+x+1)} + \frac{1}{4\big((x+\frac{1}{2})^2+\frac{3}{4}\big)} + \frac{-x+\frac{1}{2}}{2(x^2-x+1)} + \frac{1}{4\big((x-\frac{1}{2})^2+\frac{3}{4}\big)} \\ &= \frac{1}{4}\times\frac{2x+1}{x^2+x+1} + \frac{1}{3}\times\frac{1}{\Big(\frac{2x+1}{\sqrt{3}}\Big)^2+1} + \frac{-1}{4}\times\frac{2x-1}{x^2-x+1} + \frac{1}{3}\times\frac{1}{\Big(\frac{2x-1}{\sqrt{3}}\Big)^2+1}\end{aligned}$$

D'où, en intégrant et à une erreur de calcul près, la primitive est

$$\frac{1}{4}\times\ln(x^2+x+1) + \frac{1}{3}\times\frac{\sqrt{3}}{2}\arctan\Big(\frac{2x+1}{\sqrt{3}}\Big) - \frac{1}{4}\times\ln(x^2-x+1) + \frac{1}{3}\times\frac{\sqrt{3}}{2}\arctan\Big(\frac{2x-1}{\sqrt{3}}\Big).$$