Chapitre 16
POLYNÔMES ET FRACTIONS

Mohamed TARQI

Table des matières

• • • • • • • • • • • •

Dans ce chapitre $\mathbb{K}$ est un corps commutatif. Dans la plupart des cas usuels $\mathbb{K}$ sera le corps des nombres réels ou le corps des nombres complexes.

1 Notion de polynômes

1.1 Définition des polynômes

Définition 1.1 *On appelle polynôme à une indéterminée, à coefficients dans $\mathbb{K}$, toute suite P d'éléments a_i de $\mathbb{K}$, soit $(a_0, a_1, ..., a_n, ...)$, tous nuls à partir d'un certain rang. Les éléments a_i de $\mathbb{K}$ sont les coefficients du polynôme P.*

Donc un polynôme à une indéterminée est une application de $\mathbb{N}$ dans $\mathbb{K}$ dont seul un nombre fini des valeurs sont non nulles.
Soit $P = (a_0, a_1, ..., a_i, ...)$ et $Q = (b_0, b_1, ..., b_i, ...)$ deux polynômes à coefficients dans $\mathbb{K}$. Alors

$$P = Q \Longrightarrow a_i = b_i, \forall i \in \mathbb{N}$$

Sur l'ensemble, que l'on désigne pour l'instant par $\mathscr{P}$, de tous les polynômes à coefficients dans $\mathbb{K}$, nous définissons deux opérations internes, addition et multiplication par les formules suivantes : Si $P = (a_i)$ et $Q = (b_i)$ alors

$$(1) \qquad P + Q = (a_i + b_i)$$

et

$$(2) \qquad PQ = (c_i)$$

avec $c_i = a_0 b_i + a_1 b_{k-1} + ... + a_i b_0 = \sum\limits_{j+k=i} a_j b_k$.

On a le résultat suivant :

Théorème 1.1 **$\mathscr{P}$ muni de l'addition (1) et de la multiplication (2) a une structure d'anneau commutatif, dont le sous-anneau décrit par $(a, 0, 0, ...)$, $(a \in \mathbb{K})$ est isomorphe à $\mathbb{K}$.**

Démonstration : • $(\mathscr{P}, +)$ est un groupe abélien est un sous-groupe de $(\mathbb{K}^{\mathbb{N}}, +)$. L'opposé de $P = (a_0, a_1, ..., a_i, ...)$ est $-P = (-a_0, -a_1, ..., -a_i, ...)$, il existe un polynôme zéro : $O = (0, 0, 0, ...)$.
• $\mathbb{K}$ étant un corps commutatif, la multiplication (2) est donc commutative, l'élément neutre est $e = (1, 0, 0, ...)$, on a bien, en effet, pour tout polynôme P :

$$Pe = eP = P$$

D'autre part, la multiplication est distributive. Montrons que la multiplication est associative, soient

$$P = (a_i),\ Q = (b_i) \text{ et } R = (c_i)$$

Posons

$$S = PQ = (p_i),\ T = QR = (q_i)$$

$$U = (PQ)R = (r_i),\ V = P(QR) = (s_i)$$

Il faut vérifier donc que $r_i = s_i$ pour tout $i \in \mathbb{N}$.
Nous aurons

$$\begin{aligned} r_n &= \sum_{h+k=n} p_h c_k = \sum_{h+k=n} (\sum_{i+j=h} a_i b_j) c_k \\ &= \sum_{h+k=n} (\sum_{i+j=h} a_i b_j c_k) = \sum_{i+j+k=n} a_i b_j c_k \end{aligned}$$

de même , on a :

$$\begin{aligned} s_n &= \sum_{i+l=n} a_i q_l = \sum_{i+l=n} a_i (\sum_{j+k=l} b_j c_k) \\ &= \sum_{i+l=n} (\sum_{j+k=l} a_i b_j c_k) = \sum_{i+j+k=n} a_i b_j c_k \end{aligned}$$

donc $U = V$ ou encore $(PQ)R = P(QR)$.
L'ensemble $(\mathscr{P}, +, .)$ est donc un anneau commutatif.
• Soit $\mathscr{P}_0 = \{P = (a, 0, 0, ...)/a \in \mathbb{K}\}$, l'application :

$$\begin{array}{rcl} \varphi : \mathbb{K} & \longrightarrow & \mathscr{P}_0 \\ a & \longrightarrow & (a, 0, 0, ...) \end{array}$$

est visiblement bijective, de plus $\forall a, b \in \mathbb{K}$

$$\varphi(a)+\varphi(b)=(a,0,\ldots)+(b,0,\ldots)=(a+b,0,\ldots)=\varphi(a+b)$$

et

$$\varphi(a)\varphi(b)=(a,0,\ldots)(b,0,\ldots)=(ab,0,\ldots)=\varphi(ab)$$

□

1.2 Notion d'indéterminé. Notation $\mathbb{K}[X]$

Considérons les polynômes suivants e_k, $k\in\mathbb{N}$, définis par :

$$e_k=(\delta_{k0},\delta_{k1},\ldots,\delta_{ki},\ldots)=\underbrace{(0,\ldots,1,\ldots)}_{k^{ème}\text{psition}}$$

où

$$\delta_{ik}=\begin{cases}1 & \text{si} \quad k=i\\ 0 & \text{si} \quad k\neq i\end{cases} \qquad \text{(le symbole de KRONECKER)}$$

Pour tout polynôme P de $\mathscr{P}$, nous aurons :

$$P=(a_0,a_1,\ldots,a_i,\ldots)=\sum_k a_k e_k \quad \text{(somme finie)}$$

donc

$$P=\sum_k a_k e_k=0\Longleftrightarrow \forall k\in\mathbb{N},\ a_k=0$$

et si $P=\sum\limits_k a_k e_k$ et $Q=\sum\limits_k b_k e_k$ sont deux polynômes de $\mathscr{P}$ alors

$$P=Q\Longleftrightarrow a_k=b_k,\ \forall k\in\mathbb{N}.$$

Calculons $e_p e_q$:

$$a_p e_q=\sum_k a_k e_k$$

avec $a_k=\sum\limits_{i+j=k}\delta_{pi}\delta_{qj}$ le seul cas où $\delta_{pi}\delta_{qj}\neq 0$ est celui où $(i,j)=(p,q)$ d'où :

$$a_p e_q=e_{p+q}.$$

Désignons par X le polynôme e_1, donc $\forall k\in\mathbb{N}^*$, $e_k=X^k=\underbrace{X\ldots X}_{k\ \text{fois}}=(0,\ldots,1,\ldots)$, d'autre part $e_0=1$, d'où le théorème :

Théorème 1.2 **X désignant le polynôme $(0,1,0,\ldots)$**

1. **Pour tout $n\in\mathbb{N}$ la relation $(k\in\mathbb{N})$**

$$a_0+a_1X+\ldots+a_nX^n=0\Longrightarrow a_k=0,\quad \forall k\in\mathbb{N}$$

2. **Tout polynôme P de $\mathscr{P}$ s'écrit d'une manière unique**

$$P=a_0+a_1X+\ldots+a_nX^n$$

avec $a_0,a_1,\ldots,a_n\in\mathbb{K}$ et $a_n\neq 0$

Notation : L'anneau $\mathscr{P}$ est engendré par $\mathbb{K} \cup X$, nous le noterons $\mathbb{K}[X]$. On voit immédiatement que les anneaux $\mathbb{K}[X]$ et $\mathbb{K}[Y]$ sont isomorphes. Nous dirons que X est une indéterminée, nous dirons aussi que tout polynôme de $\mathbb{K}[X]$ est un polynôme en X à coefficients dans $\mathbb{K}$.
Soit l'opération externe de $\mathbb{K} \times \mathbb{K}[X]$ définie par $(\lambda, P) \longrightarrow \lambda P$, avec

$$\forall \lambda \in \mathbb{K}, \forall P = a_0 + a_1 X + \ldots + a_n X^n \in \mathbb{K}[X], \ \ \lambda P = \lambda a_0 + \lambda a_1 X + \ldots + \lambda a_n X^n$$

on a :

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

d'où le résultat suivant :

Proposition 1.1 **L'ensemble $\mathbb{K}[X]$ muni des opérations suivantes :**

$$(p, Q) \longrightarrow P + Q \text{ et } (\lambda, P) \longrightarrow \lambda P$$

a une structure d'espace vectoriel sur $\mathbb{K}$.
Muni de plus de la multiplication

$$(P, Q) \longrightarrow PQ$$

a une structure d'algèbre commutative associative et unitaire sur $\mathbb{K}$.

1.3 Degré d'un polynôme à une indéterminée

Définition 1.2 *On appelle degré du polynôme $P = \sum_k a_k X^k$ de $\mathbb{K}[X]$, que l'on note deg$P$, le plus grand entier n tel que $a_n \neq 0$.*

Il résulte de la définition que le polynôme zéro n'a pas de degré, on pose par convention $\deg 0 = -\infty$.
Les polynômes $a_k X^k$ $(a_k \neq 0)$ sont appelés monômes de degré k.
Les polynômes de degré 0, sont appelés les polynômes constants, ce sont les éléments non nuls de $\mathbb{K}$ (par identification).
Si $\deg P = n$, le monôme $a_n X^n$ s'appelle le monôme dominant de P et a_n le coefficient dominant de P ; si $a_n = 1$ on dit que P est un polynôme unitaire.

Proposition 1.2 **P et Q étant deux polynômes non nuls de $\mathbb{K}[X]$.**

1. **Si deg$P$ $\neq$deg$Q$ on a $P+Q \neq 0$ et deg$(P+Q) = \sup($deg$P$,deg$Q)$ et si deg$P$=deg$Q$ et si $P+Q \neq 0$ on a deg$(P+Q) \leq \sup($deg$P$,deg$Q)$.**
2. **Si $P \neq 0$ et $Q \neq 0$, deg(PQ) =deg$P$+deg$Q$.**

Démonstration : Soient P et Q deux polynômes non nuls posons :

$$P = a_0 + a_1 X + \ldots + a_n X^n, (a_n \neq 0)$$

$$Q = b_0 + b_1 X + \ldots + b_m X^m, (b_m \neq 0)$$

Si $n \neq m$, alors $P+Q \neq 0$ et $\deg(P+Q) = \sup(n, m)$
Si $n = m$ et si $P+Q \neq 0$ on a $\deg(P+Q) \leq \sup(n, m)$ (on aurait l'égalité si, et seulement si, $a_n + b_m \neq 0$).
Considérons maintenant le polynôme produit :

$$PQ = c_0 + c_1 X + \ldots + c_p X^p$$

la formule $c_i = a_0 b_i + a_1 b_{k-1} + \ldots + a_i b_0 = \sum_{j+k=i} a_j b_k$ montre que :

$$p > n + m \Longrightarrow c_p = 0, \ c_{n+m} = a_n b_m \neq 0$$

donc $\deg(PQ)$ =deg$P$+deg$Q$. □

Corollaire 1.1 **L'ensemble des polynômes de $\mathbb{K}[X]$ de degré inférieure ou égale à n est un sous-espace vectoriel de $\mathbb{K}[X]$, on le note $\mathbb{K}_n[X]$.**

Démonstration : C'est immédiate. □

Corollaire 1.2 **L'anneau $(\mathbb{K}[X],+,.)$ est intègre.**

Démonstration : En effet si P et Q sont polynômes tels que $P \neq 0$ et $Q \neq 0$, alors deg(PQ) =deg$Q$+deg$Q \neq -\infty$, donc $PQ \neq 0$. □

Corollaire 1.3 **Les éléments inversibles de l'anneau $(\mathbb{K}[X],+,.)$ sont les éléments inversibles de $\mathbb{K}$, c'est-à-dire $\mathbb{K}^*$.**

Démonstration : Soient P et Q deux polynômes tels que $PQ = 1$, alors deg$P$+deg$Q = 0$, donc deg$P$ =deg$Q$=0 ce qui implique que P et Q sont des polynômes constans et inversibles, donc P et Q sont dans $\mathbb{K}^*$. □

1.4 Fonction polynôme d'une variable

Soient $P = a_0 + a_1X + ... + a_nX^n$ un élément de $\mathbb{K}[X]$ et $x \in \mathbb{K}$, à tout élément (x,P) nous pouvons faire correspondre l'élément $a_0 + a_1x + ... + a_nx^n$, que nous noterons $\widetilde{P}(x)$.

Définition 1.3 *À tout polynôme $P = a_0 + a_1X + ... + a_nX^n$ de $\mathbb{K}[X]$, on fait correspondre une application $\widetilde{P}$ de $\mathbb{K}$ dans $\mathbb{K}$ définie par :*

$$\forall x \in \mathbb{K},\ \widetilde{P}(x) = a_0 + a_1x + ... + a_nx^n$$

appelée fonction polynôme associée au polynôme P, on note leur ensemble $\mathscr{P}(\mathbb{K},\mathbb{K})$ qui a évidement une structure d'anneau.

On a le théorème suivant :

Proposition 1.3 **L'application $P \longrightarrow \widetilde{P}$ de $\mathbb{K}[X]$ dans $\mathscr{P}(\mathbb{K},\mathbb{K})$ est un morphisme d'anneaux surjective.**

Démonstration : $\forall P,Q \in \mathbb{K}[X]$ on a :

$$(P+Q)(X) = P(X) + Q(X) \text{ et } PQ(X) = P(X)Q(X)$$

donc

$$\forall x \in \mathbb{K},\ \widetilde{P+Q}(x) = \widetilde{P}(x) + \widetilde{Q}(x) \text{ et } \widetilde{PQ}(x) = \widetilde{P}(x)\widetilde{Q}(x)$$

L'application est surjective par construction. □

2 Dérivation dans $\mathbb{K}[X]$. Formule de TAYLOR

2.1 Dérivation dans $\mathbb{K}[X]$

Définition 2.1 *Soit $P = \sum_{k=0}^{k=n} a_kX^k$ un polynôme , on appelle polynôme dérivé de P que l'on note $DP = P'$, le polynôme définie par :*

$$P' = \sum_{k=1}^{k=n} ka_kX^{k-1}$$

On note $P^{(0)} = P$, $P^{(1)} = P'$, $P^{(2)} = P'' = (P')'$ et pour tout $k \in \mathbb{N}^*$, $P^{(k)} = (P^{(k-1)})'$.
Si $n = 0$, $P^0 = 0$.

Proposition 2.1

1. **Pour tout polynôme P de $\mathbb{K}[X]$,**

$$degP' = \begin{cases} deg(P-1) & \text{si} \quad degP \geq 1 \\ -\infty & \text{si} \quad degP \leq 0 \end{cases}$$

2. **Pour tout polynôme P de $\mathbb{K}[X]$, $degP \leq n \Longleftrightarrow P^{(n+1)} = 0$.**

Proposition 2.2 **P et Q étant des polynômes à coefficients dans $\mathbb{K}$ et λ un réel :**

1. **$(P+Q)' = P' + Q'$, $(\lambda P)' = \lambda P'$ et $(PQ)' = P'Q + PQ'$**
2. **L'application $D : P \longrightarrow P'$ est un endomorphisme de l'espace vectoriel $\mathbb{K}[X]$.**

2.2 Formule de TAYLOR

Théorème 2.1 **Pour tout polynôme P de $\mathbb{K}[X]$ de degré n et pour tout $a \in \mathbb{K}$:**

$$P(X) = P(a) + (X-a)P'(a) + \ldots + \frac{(X-a)^{n-1}}{(n-1)!}P^{(n-1)}(a) + \frac{(X-a)^n}{(n)!}P^{(n)}(a)$$

Démonstration : Soit l'application :

$$\varphi : P \longrightarrow P(a) + (X-a)P'(a) + \ldots + \frac{(X-a)^{n-1}}{(n-1)!}P^{(n-1)}(a) + \frac{(X-a)^n}{(n)!}P^{(n)}(a)$$

Il est clair que φ est linéaire, pour montrer que $\varphi(P) = P$, il suffit de vérifier que $\varphi(X^i) = X^i$ pour tout entier $0 \leq i \leq n$, puisque chaque polynôme est une combinaison linéaire de ces derniers.
$\forall i \in \mathbb{N}$, on a :

$$\begin{aligned}
\varphi(X^i) &= \sum_{p=0}^{i} \frac{(X^i)^{(p)}(a)}{p!}(X-a)^p \\
&= \sum_{p=0}^{i} \frac{A_i^p a^{i-p}}{p!}(X-a)^p \\
&= \sum_{p=0}^{i} C_i^p a^{i-p}(X-a)^p = X^i
\end{aligned}$$

d'où le résultat. □

3 Divisibilité dans l'anneau $\mathbb{K}[X]$

3.1 Division euclidienne des polynômes

Théorème 3.1 **A et B étant deux polynômes de $\mathbb{K}[X]$, $B \neq 0$, alors il existe un couple unique $(Q,R) \in \mathbb{K}[X] \times \mathbb{K}[X]$ tel que**

$$A = BQ + R \text{ et } (R = 0 \text{ ou } degR < degB)$$

Q et R sont appelés respectivement quotient et reste de la division euclidienne de A par B.

Démonstration : Soient A et B deux polynômes non nuls. Supposons par exemple A non divisible par B, donc $\forall P \in \mathbb{K}[X]$, $A - BQ \neq 0$.
Soit la partie de $\mathbb{N}$, définie par :

$$E = \{n \in \mathbb{N}/n = deg(A - BP),\ \ P \in \mathbb{K}[X]\}$$

E est une partie de $\mathbb{N}$ non vide de $\mathbb{N}$ ($A \nmid B$), soit $l = \min E$ et Q l'un des polynômes tel que $\deg(A - BQ) = l$, posons

$$A = a_n X^n + \ldots + a_1 X + a_0,\ \ (a_n \neq 0), B = b_m X^m + \ldots + b_1 X + b_0,\ \ (b_m \neq 0)$$

et

$$A - BQ = c_l X^l + \ldots + c_1 X + c_0,\ \ (c_l \neq 0)$$

Montrons que : $l < m$, supposons $l \geq m$, le polynôme

$$P = Q + \frac{c_l}{b_m} X^{l-m}$$

est tel que

$$A - BP = (c_{l-1} - \tfrac{c_l}{b_m} b_{m-1})X^{l-1} + \ldots + c'_0$$

donc $B - AP$ ne serait pas de degré minimum.
Montrons que Q est unique, supposons en effet qu'il existe des polynômes Q et Q' distincts, tels que

$$deg(A - BQ) < degB \text{ et } deg(A - BQ') < degB$$

donc

$$Q \neq Q' \text{ et } deg[(A - BQ) - (A - BQ')] = deg[B(Q - Q')] < degB$$

ce qui impossible, d'où le résultat on posant $R = A - BQ$. □

Définition 3.1 *Soient P, A des polynômes de $\mathbb{K}[X]$, on dit que A divise P et on note $A|P$ si, et seulement si, il existe $Q \in \mathbb{K}[X]$ tel que $P = AQ$. On dit aussi que P est un multiple de A. On note, pour tout polynôme P, $\mathcal{D}(P)$ l'ensemble des diviseurs de P.*

Remarques :

1. $\forall A \in \mathbb{K}[X]$, $A/0$.
2. $\forall P \in \mathbb{K}[X]$, $0/P \Longleftrightarrow P = 0$
3. La relation $A|B$ est une relation binaire sur $\mathbb{K}[X]$, qui est reflexive et transitive, mais elle n'est pas antisymétrique. En effet si $A|B$ et $B|A$ alors il existe D et D' deux polynômes tels que $A = BD$ et $B = AD'$, donc $A = ADD'$ ou encore $A(DD' - 1) = 0$, d'où :

   $$\begin{cases} A|B \\ B|A \end{cases} \Longleftrightarrow \exists \lambda \in \mathbb{K}^* : B = \lambda A$$

   Dans ce cas, A et B sont dits associés.
4. Soit D un diviseur commun de A et B, il existe donc A' et B' des polynômes tel que $A = A'D$ et $B = B'D$.
   De la division euclidienne de A' par B' ($B' \neq 0$), on déduit :

   $$A' = B'Q' + R' \qquad \text{et} \qquad (R' = 0 \text{ ou deg} R' < \text{deg} B'$$

   donc

   $$A'D = B'DQ' + R'D \qquad \text{et} \qquad \text{deg } R'D < \text{deg } B'D = \text{deg} B$$

   d'où $R = A - BQ = (A' - B'Q')D = R'D$, donc D divise aussi R.

3.2 Divisibilité dans $\mathbb{K}[X]$

3.2.1 Notion d'idéal

Définition 3.2 *Soient $(A, +, \times)$ un anneau commutatif et I une partie de A. On dit que I est un idéal de A si, et seulement si,*

1. *$(I, +)$ est sous-groupe de $(A, +)$.*
2. *$\forall x \in A$, $\forall y \in I$, $xy \in I$.*

Proposition 3.1 **Soit $(A, +, .)$ un anneau commutatif. Soient I et J deux idéaux de A. Alors $I + J = \{i + j / i \in I,\ \ j \in J\}$ est un idéal de A, c'est l'idéal engendré par $I \cup J$. De même $I \cap J$ est un idéal de A.**

Démonstration :

1. $I + J$ est une partie non vide $(0 \in I + J)$. Soient $x = i + j$ et $x' = i' + j'$ deux éléments de $I + J$, alors $x - x' = (i - i') + (j - j') \in I + J$.
   Soit $a \in A$ et $x = i + j \in I + J$. Alors $a(i + j) = ai + aj \in I + J$.
   Donc la somme de deux idéaux est un idéal.
2. Il est clair que $I \cap J$ est un sous-groupe de $(A, +)$, de plus si $x \in I \cap J$ et $a \in A$ alors $ax \in I \cap J$.

□

Généralisation : Ce résultat peut être généralisé à une famille finie $I_1, I_2, ..., I_n$ de idéaux de $(A, +, .)$: $I_1 + I_2 + ... + I_n = \{i_1 + i_2 + ... + i_n / I_j \in I_j\}$ est l'idéal engendré par $\bigcup_{j=1}^{n} I_j$. De même $\bigcap_{j=1}^{n} I_j$ est un idéal de A.

Remarque : Soit $P \in \mathbb{K}[X]$, alors $(P) = \{PQ/Q \in \mathbb{K}[X]\}$ est un idéal de $\mathbb{K}[X]$. On va montrer que ce sont les seuls idéaux de $\mathbb{K}[X]$.

Proposition 3.2 **Soit I un idéal de $\mathbb{K}[X]$ non nul, alors il existe un polynôme P_0 non nul unitaire, unique de degré minimal tel que $I = \{P_0 Q/Q \in \mathbb{K}[X]\}$. On note $I = (P_0) = \mathbb{K}[X]P_0$.**

Démonstration : Soit $I \neq \{0\}$ un idéal de l'anneau $\mathbb{K}[X]$, il existe dans I des polynômes non nuls, l'ensemble de leurs degrés admet un plus petit élément n, soit $P_0 \in I$ de degré n, quitte à diviser par son coefficient de monôme de haut degré on peut supposer P_0 unitaire.
Soit $P \in I$, effectuons la division euclidienne de P par P_0

$$P = QP_0 + R, (R = 0 \text{ ou } \deg R < \deg P_0)$$

or $R = P - QP_0$ appartient à I donc, P_0 étant de degré minimum dans I, il est impossible que $\deg R < \deg P_0$), donc $R = 0$ et $P = QP_0$, donc $I = (P_0)$. □

Remarque : Si $I \neq \{0\}$ tel que $I = (P) = (Q)$, alors il existe des polynômes A et B tels que $P = AQ$ et $Q = BP$, donc $P = ABP$, alors il existe $\lambda \neq 0$ tel que $Q = \lambda P$.

3.2.2 Plus grand commun diviseur de deux polynômes

Définition 3.3 *Soient A et B deux polynômes . Alors il existe un unique polynôme unitaire D tel que $\mathbb{K}[X]A + \mathbb{K}[X]B = \mathbb{K}[X]D$.*
On dit que D est le pgcd de A et de B. On le note $D = pgcd(A,B)$ ou $D = A \wedge B$.

Remarques :

1. D'après la définition il existe des polynômes U et V tels que $A \wedge B = UA + VB$ et tout élément de la forme $PA + QB$ $(P,Q \in \mathbb{K}[X])$ est un multiple de $A \wedge B$.
2. Les polynômes A et B sont premiers entre eux si, et seulement si, $A \wedge B = 1$.

D'après la définition et les propriétés précédentes on déduit facilement le théorème suivant :

Théorème 3.2 **Étant donné deux polynômes A et B, les propriétés suivantes sont équivalentes :**

1. **A et B sont premiers entre eux.**
2. **il existe des polynômes U et V tels que**

$$AU + BV = 1 \qquad \text{(égalité de BEZOUT)}$$

3. **pour tout polynôme R, il existe des polynômes P et Q tels que $AP + BQ = R$.**

Remarque : Les couples (U,V) et (P,Q) ne sont pas uniques (cf. TD).

Théorème 3.3 **Ètant donnés trois polynômes A,B et C, on a :**

$$(A \wedge B = 1 \text{ et } A|BC \Longrightarrow A|C) \text{ (Théorème de GAUSS)}$$

Démonstration : Supposons $A \wedge B = 1$ et $A|BC$. D'après l'identité de BEZOUT, il existe deux polynômes U et V tels que $AU + BV = 1$, ce qui implique $ACU + BCV = C$. On alors $A|ACU + BCV = C$. □
On peut préciser l'égalité de BEZOUT pour deux polynômes A et B premiers entre eux.Alors il existe deux polynômes U et V tels que $1 = UA + VB$. Effectuons la division euclidienne de U par B et de V par A :

$$U = BU_1 + U_0, \text{ avec } U_0 = 0 \text{ ou } \deg U_0 < \deg B$$

$$V = AV_1 + V_0, \text{ avec } V_0 = 0 \text{ ou } \deg V_0 < \deg A$$

d'où

$$PU_0 + BV_0 + AB(U_1 + V_1) = 1 \quad (1)$$

si U_0 (resp. V_0) est nul, B divise U donc $1 = AU + BV$ et $\deg B = 0$ (resp. $\deg A = 0$), nous supposerons A et B de degré strictement positif, donc U_0 et V_0 sont non nuls.
Nous avons alors $\deg(AU_0+BV_0) < \deg(A+\deg B)$, donc si $U_1+V_1 \neq 0$, l'égalité (1) est impossible car $\deg[AB(U_1+V_1)]$ serait strictement supérieure à $\deg A+\deg B$. Donc $U_1 + V_1 = 0$.
Montrons que le couple (U_0, V_0) est unique ; soit deux couples (U_0, V_0) et (U_2, V_2) vérifiant

$$\deg U_0 < \deg B \text{ et } \deg V_0 < \deg A$$

$$\deg U_2 < \deg B \text{ et } \deg V_2 < \deg A$$

donc

$$PU_0 + BV_0 = PU_2 + BV_2 = 1 \Longrightarrow A(U_0 - U_2) = B(V_2 - V_0)$$

A étant premier avec B donc divise $V_2 - V_0$ d'après le théorème de GAUSS. Or $\deg A > \deg(V_2 - V_0)$, donc $V_2 - V_0 = 0$ et $U_2 = U_0$ d'où le résultat suivant :

Proposition 3.3 **A et B étant deux polynômes premiers entre eux, de degré non nul il existe un couple unique (U_0, V_0) de polynômes vérifiant :**

$$AU_0 + BV_0 = 1, \ (\deg U_0 < \deg B, \ \deg V_0 < \deg A).$$

3.2.3 Algorithme d'EUCLIDE pour la recherche du $A \wedge B$

Proposition 3.4 **Soit R le reste de la division euclidienne de A par B (A et B des polynômes non nuls). Alors $pgcd(A,B) = pgcd(B,R)$**

Démonstration : En effet soit D un diviseur commun de A et B, alors D divise aussi R, de même si D divise R et B il divise B, donc $A \wedge B = B \wedge D$. □
Soient A et B deux polynômes non nuls. Effectuons les divisions euclidiennes (on supposera $b > 0$)

$$A = BQ_0 + R_0 \quad \text{et} \quad \deg R_0 < \deg B$$

$$B = R_0Q_1 + R_1 \quad \text{et} \quad \deg R_1 < \deg R_0$$

$$R_0 = R_1Q_2 + R_2 \quad \text{et} \quad \deg R_2 < \deg R_1$$

$$.$$

$$.$$

$$R_{n-1} = R_nQ_{n+1} + R_{n+1} \quad \text{et} \quad \deg R_{n+1} < \deg R_n$$

On forme ainsi une suite $degB > degR_1 > degR_2 > degR_3 > ... > degR_{n-1} > degR_n > ... \geq 0$ strictement décroissante d'entiers, on arrive forcément à un premier reste $R_{n+1} = 0$. D'après le théorème

$$pgcd(A,B) = pgcd(B,R_1) = ... = pgcd(R_{n-1},R_n) = R_n$$

Ainsi $R \wedge B$ est le dernier reste non nul dans cette succession de divisions.

Exemple : Soient $A = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ et $B = X^3 + X^2 + X + 1$ de $\mathbb{R}[X]$. $A \wedge B = X^2 + 1$.

3.2.4 Plus grand commun diviseur d'une famille finie d'éléments de $\mathbb{K}[X]$

Théorème et définition 3.1 **Étant donné une famille finie de polynômes non nuls $P_1, P_2, ..., P_n$. Alors il existe un unique polynôme D unitaire tel que**

$$\mathbb{K}[X]P_1 + \mathbb{K}[X]P_2 + ... + \mathbb{K}[X]P_2 = \mathbb{K}[X]D.$$

On dit que D est le pgcd de $P_1, P_2, ..., P_n$. On le note $D = pgcd(D_1, D_2, ..., D_n)$ ou $D = P_1 \wedge P_2 \wedge ... \wedge P_n$.

Démonstration : En effet, $I = \mathbb{K}[X]P_1 + \mathbb{K}[X]P_2 + \ldots + \mathbb{K}[X]P_n$ est un idéal de $(\mathbb{K}[X], +, .)$, donc il existe un unique polynôme unitaire D tel que $I = \mathbb{K}[X]D$. □

D'après la définition ci-dessus et la définition 2.3, on déduit le théorème suivant :

Théorème 3.4 **Étant donné des polynômes non nuls $P_1, P_2, \ldots, P_n$, les propriétés suivantes sont équivalentes :**

1. **$P_1, P_2, \ldots, P_n$ sont premiers entre eux dans leur ensemble.**
2. **il existe des polynômes $U_1, U_2, \ldots, U_n$ tels que**

$$P_1U_1 + P_2U_2 + \ldots + P_nU_n = 1 \qquad \text{(égalité de Bezout)}$$

3. **pour tout polynôme R, il existe des polynôme $Q_1, Q_2, \ldots, Q_n$ tels que $P_1Q_1 + P_2Q_2 + \ldots + P_nQ_n = R$.**

3.2.5 Plus petit commun multiple de deux ou plusieurs polynômes

Théorème et définition 3.2 **Soient A, B deux polynômes de $\mathbb{K}[X]$. Il existe un unique polynôme M unitaire de degré minimal tel que $\mathbb{K}[X]A \cap \mathbb{K}[X]B = \mathbb{K}[X]M$. Le polynôme M s'appelle le plus petit commun multiple de A et de B. On le note $M = ppcm(A, B)$, ou $M = A \vee B$.**

Démonstration : En effet, $\mathbb{K}[X]A \cap \mathbb{K}[X]B$ est un idéal de $(\mathbb{K}[X], +, .)$, donc de la forme $\mathbb{K}[X]M$. □

Remarque : Soient A et B deux polynômes et $M = A \vee B$. D'une part M est un multiple de A et de B. D'autre part tout multiple de A et de B est un multiple de M. Donc M est le polynôme de plus bas degré multiple commun de A et de B, ces propriétés caractérisent entièrement le polynôme $M = A \vee B$.

Corollaire 3.1 **Si A et B sont deux polynômes premiers entre eux, alors $A \vee B$ et AB sont associés.**

Démonstration : Il est clair que les multiples de AB sont des multiples communs de A et de B.
Réciproquement, supposons $A|P$ et $B|P$; il existe un polynôme tel que $P = QB$. Comme A divise P et qu'il est premier avec B, on en déduit que A divise Q (d'après Gauss), soit donc le polynôme R tel que $Q = AR$, ce qui implique $P = ABR$.
Les multiples communs de A et B sont donc les multiples de AB. □

Corollaire 3.2 **Si A et B sont deux polynômes , alors les polynômes**

$$AB \text{ et } (A \wedge B)(A \vee B)$$

sont associés.

Démonstration : Le résultat étant évidente si $AB = 0$, supposons A et B non nuls et unitaires quitte à les diviser par leurs coefficients dominants.
Soient $D = A \wedge B$ et A_1, B_1 tels que $A = DA_1$, $B = DB_1$ et $A_1 \wedge B_1 = 1$. Comme A_1 et B_1 sont premiers entre eux, on a $A_1 \vee B_1 = A_1B_1$. Alors

$$A \vee B = D(A_1 \vee B_1) = DA_1B_1$$

et par conséquent $(A \wedge B)(A \vee B) = AB$. □

De manière analogue, on peut généraliser la notion de $ppcm$ à une famille finie de polynômes : on a le résultat suivant :

Théorème et définition 3.3 **Étant donné des polynômes $P_1, P_2, \ldots, P_n$ non nuls, il existe un unique polynôme M unitaire dans tel que**

$$\mathbb{K}[X]P_1 \cap \mathbb{K}[X]P_2 \cap \ldots \cap \mathbb{K}[X]P_n = \mathbb{K}[X]M$$

L'entier M s'appelle le plus petit commun multiple de $P_1, P_2, \ldots, P_n$. On le note $M = ppcm(P_1, P_2, \ldots, P_n)$, ou $M = P_1 \vee P_2 \vee \ldots \vee P_n$.

4 Racines d'un polynôme de $\mathbb{K}[X]$

4.1 Racines

Définition 4.1 *Soit P un polynôme à coefficients dans $\mathbb{K}$ et $a \in \mathbb{K}$, on dit que a est une racine de P si, et seulement si, $P(a) = 0$.*

Exemples :

1. $\sqrt{2}$ est une racine de $X^2 - 2$ dans $\mathbf{R}[X]$.
2. i est une racine de $X^2 + 1$ dans $\mathbf{C}[X]$.

Théorème 4.1 **$\alpha \in \mathbb{K}$ est racine de P si, et seulement si, P est divisible par $X - \alpha$.**

Démonstration : La division euclidienne de P par $X - a$ donne :

$$P(X) = (X - a)Q(X) + R(X) \ (R = 0 \text{ ou } degR = 0)$$

donc $R \in \mathbb{K}$ et $P(a) = R(X)$ et par conséquent $P(a) = 0$ si, et seulement si, $R(X) = 0$, d'où le résultat. □

Exemple : Soit $P = X^{2n} - 2X + 1, n \in \mathbb{N}^*$. On a $P(1) = 0$, donc $X - 1$ divise P

Exercice : Calculer le polynôme Q, le quotient de la division de $P = X^{2n} - 2X + 1$ par $X - 1$.

Définition 4.2 *Deux polynômes A et B sont premiers entre eux s'ils n'ont pour diviseurs communs que les polynômes de degré 0.*

Remarquons que tout polynôme P divisant 0 ($0P = 0$), donc deux polynômes sont premiers sont non nuls.

Définition 4.3 *Les polynômes $P_1, P_2, ..., P_n$ sont premiers entre eux dans leur ensemble s'ils n'ont pour diviseurs communs que les polynômes de degré 0.*

4.2 Factorisation d'un polynôme ($\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$)

4.2.1 L'ordre de multiplicité d'une racine

Théorème et définition 4.1 **Soit $P \in \Bbbk[\mathbf{X}]$, $\alpha \in \Bbbk$ et $k \in \mathbf{N}^*$. Les assertions suivantes sont équivalentes :**

1. **Il existe un polynôme Q tel que $P = (X - \alpha)^k Q(X)$ et $Q(\alpha) \neq 0$**
2. **$(X - \alpha)^k$ divise P et $(X - \alpha)^{k+1}$ ne divise pas P.**

Dans ce cas où les assertions sont vraies, on dit que α est une racine d'ordre k ou k est l'ordre de multiplicité de la racine α.

Démonstration : 1) $\Longrightarrow$ 2) Il existe un polynôme S tel que :

$$Q = (X - \alpha)S + Q(\alpha)$$

donc

$$Q(X - \alpha)^k = (X - \alpha)^{k+1} S + Q(\alpha)(X - \alpha)^k$$

et

$$\begin{aligned} P &= (X - \alpha)^{k+1} S + Q(\alpha)(X - \alpha)^k \\ &= (X - \alpha)^k [(X - \alpha)S + Q(\alpha)] \end{aligned}$$

il est clair que $(X - \alpha)^{k+1}$ ne divise pas P.

2) $\Longrightarrow$ 1) Soit Q tel que $P = (X - \alpha)^k Q$. Puisque $(X - \alpha)^{k+1}$ ne divise pas P, $X - \alpha$ ne divise pas Q, donc $Q(\alpha) \neq 0$. □

Exemples : • $P = aX^2 + bX + c \quad (a,b,c \in \mathbf{C},\ a \neq 0)$. P admet une racine double (d'ordre 2) si et seulement si $b^2 - 4ac = 0$.
• Les racines de $X^2 + X + 1$ sont toutes simples, c'est-à-dire d'ordre 1.
• $P = X^3 + X^2 - 5X + 3$. La racine 1 est d'ordre 2 et la racine -3 est simple.

Proposition 4.1 **Soit $P \in \mathbb{k}[\mathbb{X}]$, $\alpha \in \mathbb{k}$ et $k \in \mathbb{N}^*$. Pour que α soit une racine de P, d'ordre k, il faut et il suffit que :**

$$P(\alpha) = P'(\alpha) = \dots = P^{(k-1)}(\alpha) = 0 \quad et \quad P^{(k)}(\alpha) \neq 0$$

Démonstration : Soit P un polynôme de degré n. D'après la formule de TAYLOR :

$$\begin{aligned} P(X) &= P(\alpha) + (X-\alpha)\frac{P'(\alpha)}{1!} + \dots + (X-\alpha)^k \frac{P^{(k)}(\alpha)}{k!} + \dots + (X-\alpha)^n \frac{P^{(n)}(\alpha)}{n!} \\ &= (X-\alpha)^k [\frac{P^{(k)}(\alpha)}{k!} + \dots + (X-\alpha)^{n-k} \frac{P^{(n)}(\alpha)}{n!}] + [P(\alpha) + (X-\alpha)\frac{P'(\alpha)}{1!} + \dots \\ &\quad + (X-\alpha)^{k-1} \frac{P^{(k-1)}(\alpha)}{(k-1)!}] \\ &= (X-\alpha)^k Q(X) + R(X) \end{aligned}$$

avec

$$Q(X) = [\frac{P^{(k)}(\alpha)}{k!} + \dots + (X-\alpha)^{n-k} \frac{P^{(n)}(\alpha)}{n!}]$$

et

$$R(X) = [P(\alpha) + (X-\alpha)\frac{P'(\alpha)}{1!} + \dots + (X-\alpha)^{k-1} \frac{P^{(k-1)}(\alpha)}{(k-1)!}]$$

donc $(X-\alpha)^k$ divise P et $(X-\alpha)^{k+1}$ ne divise pas P si et seulement si $R = 0$ et $Q(\alpha) \neq 0$ c'est-à-dire si et seulement si $P(\alpha) = P'(\alpha) = \dots = P^{(k-1)}(\alpha) = 0$ et $P^{(k)}(\alpha) \neq 0$ □

Exemple : Soit $P = X^4 - 5X^3 + 6X^2 + 4X - 8$. $P(2) = P'(2) = P''(2) = 0$ et $P^{(3)}(2) \neq 0$, donc 2 est une racine d'ordre 3.
EXERCICE : Trouver la relation entre p et q de $\mathbb{C}$ pour que le polynôme $X^3 + pX + q$ ait une racine double α. Quelle est alors cette racine double ?
On en déduit facilement le corollaire suivant :

Exemple : Soit $P = X^4 - 5X^3 + 6X^2 + 4X - 8$. $P(2) = P'(2) = P''(2) = 0$ et $P^{(3)}(2) \neq 0$, donc 2 est une racine d'ordre 3.
EXERCICE : Trouver la relation entre p et q de $\mathbb{C}$ pour que le polynôme $X^3 + pX + q$ ait une racine double α. Quelle est alors cette racine double ?
On en déduit facilement le corollaire suivant :

Corollaire 4.1 **Tout polynôme à coefficients dans $\mathbb{k}$, de degré n, admet au plus n racines.**

Proposition 4.2 **Soient P et Q deux polynômes de $\mathbb{k}[\mathbf{X}]$, de degrés n, s'ils prennent les mêmes valeurs en $n+1$ points ; deux à deux distincts de $\mathbb{k}$ alors $P = Q$.**

Démonstration : On pose $R = P - Q$. R est un polynôme de degré au plus n et admet $n+1$ racines distinctes, donc R ne peut être que le polynôme nul. □

Corollaire 4.2 **Si $\mathbb{K}$ est infini, l'application $P \longrightarrow \widetilde{P'}$ est isomorphisme d'anneau de $K[X]$ dans $\mathscr{F}(\mathbb{K}, \mathbb{K})$.**

Démonstration : On sait que l'application est morphisme surjective, montrons qu'elle est injective. En effet $\widetilde{P} = 0$, alors $\forall x \in \mathbb{K},\ P(x) = 0$
Donc le polynôme admet une infinité de racines, donc $P = 0$. □

4.2.2 Factorisation d'un polynôme é coefficients complexe

Théorème 4.2 **(Théorème de D'ALEMBERT-GAUSS[1]) (admis) Tout polynôme, à coefficients complexes, admis une racine dans $\mathbb{C}$, on dit que le corps $\mathbb{C}$ est algébriquement clos.**

Proposition 4.3 *(Décomposition dans $\mathbb{C}[X]$)* **Soit $P \in \mathbb{C}[\mathbb{X}]$ de degré n, $n \in \mathbb{N}^*$. Alors il existe des scalaires $\alpha_0, \alpha_1, ..., \alpha_r$ distincts, des entiers $k_0, k_1, ..., k_r$ et $a \in \mathbb{C}^*$ tels que :**

$$P = a(X-\alpha_0)^{k_0}(X-\alpha_1)^{k_1}...(X-\alpha_r)^{k_r}.$$

Démonstration : Soit $P = aX + b$ un polynôme de degré 1, alors $P = a(X-\alpha)$, avec $\alpha = \frac{-b}{a}$, donc la propriété est vrai pour les polynômes de degré 1.
Supposons maintenant le résultat vrai pour tous les polynômes de degrés $1, 2, ..., n$ et montrons le pour les polynômes de degré $n+1$. Soit P un polynôme de degré $n+1$, d'après le théorème de **D'ALEMBERT**, P admet une racine α_0 d'ordre k_0, donc il existe un polynôme Q tel que :

$$P = (x-\alpha_0)^{k_0}Q, \ \ \deg Q \leq n$$

d'après l'hypothése de recurrence, il existe des scalaires $\alpha_1, \alpha_2, ..., \alpha_r$ et des entiers $k_1, k_2, .., k_r$ tels que :

$$Q = a(X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2}...(X-\alpha_r)^{k_r}$$

donc

$$P = a(X-\alpha_0)^{k_0}(X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2}...(X-\alpha_r)^{k_r}$$

d'où le résultat. □

Remarque : On a :

$$\deg P = k_0 + k_1 + k_2 + ... + k_r = n$$

4.2.3 Factorisation d'un polynôme à coefficients réels

Lemme 4.1 **Soit P un polynôme à coefficients réels, si z est une racine de P, alors $\bar{z}$ est aussi une racine de P.**

Démonstration : Soit $P = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ à coefficients réels.
On a, $\forall z \in \mathbf{C}$:

$$\begin{aligned} P(z) = 0 &\iff \overline{P(z)} = 0 \\ &\iff \overline{a_n z^n + a_{n-1}z^{n-1} + ... + a_1 z + a_0} = 0 \\ &\iff a_n \overline{z}^n + a_{n-1}\overline{z}^{n-1} + ... + a_1 \overline{z} + a_0 \\ &\iff P(\overline{z}) = 0 \end{aligned}$$

□

Remarque : z et $\overline{z}$ ont le même ordre de multiplicité.

Théorème 4.3 **(Décomposition dans $\mathbb{R}[\mathbb{X}]$) Tout polynôme à coefficients r2els, de degré n, $n \in \mathbf{N}^*$ se décompose d'une manière unique sous la forme :**

$$P = a\prod_{i=1}^{i=r}(x-\alpha_i)^{k_i}\prod_{j=1}^{j=p}(x^2+\beta_j x+\gamma_j)^{l_j}, \ \ a \in \mathbb{R}$$

avec les α_i les racines réelles distinctes de P, les β_j, γ_j des réels tels que $\beta_j^2 - 4\gamma_j < 0$, et les k_i, l_j des entiers

1. Jean le Rond d'Alembert (1717-1783), philosophe, écrivain et mathématicien français.

Démonstration : Soit $P \in \mathbb{R}[X]$, P se décompose, dans $\mathbb{C}[X]$, d'une manière unique sous la forme :

$$P = a\prod_{i=1}^{i=r}(x-\alpha_i)^{k_i}\prod_{j=1}^{j=p}(x-a_j)^{l_j}\prod_{j=1}^{j=p}(x-\bar{a}_j)^{l_j}$$

(les α_i désignent les racines réelles de P et $a_j, \bar{a}_j$ les racines complexes de P)

$$\begin{aligned} P &= a\prod_{i=1}^{i=r}(x-\alpha_i)^{k_i}\prod_{j=1}^{j=p}(x^2-2Re(a_j)x+|a_j|^2)^{l_j} \\ &= a\prod_{i=1}^{i=r}(x-\alpha_i)^{k_i}\prod_{j=1}^{j=p}(x^2+\beta_j x+\gamma_j)^{l_j} \end{aligned}$$

avec

$$\forall j = 1,2,\dots,p \qquad \beta j = 2Re(a_j),\ \gamma_j = |a_j|^2,\ \beta_j^2 - 4\gamma_j < 0$$ □

Remarques :

1. On peut avoir $r = 0$ ou $p = 0$.
2. $\deg P = k_1 + k_2 + \dots + k_r + 2(l_1 + l_2 + \dots + l_p) = n$

Exemples : Pour tout entier naturel non nul p, on a :

1. $X^{2p} - 1 = (X-1)(X+1)\prod_{k=0}^{p-1}(X^2 - 2\cos\frac{k\pi}{p}X + 1)$.
2. $X^{2p+1} - 1 = (X-1)\prod_{k=0}^{p-1}(X^2 - 2\cos\frac{2k\pi}{2p+1}X + 1)$.

4.3 Relations entre les coefficients et les racines dans un polynôme

Soit $P = a_nX^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$ un polynôme de $\mathbb{K}[X]$, avec $a_n \neq 0$. Supposons que P s'écrit sous la forme :

$$\begin{aligned} P &= a_n(X-x_1)(X-x_2)\dots(X-x_n) \\ &= a_n(X^n - \sigma_1X^{n-1} + \sigma_2X^{n-2} + \dots + (-1)^p\sigma_pX^{n-p} + \dots + (-1)^n\sigma) \end{aligned}$$

avec

$$\sigma_p = \sum_{i_1<i_2<\dots<i_p} x_{i_1}x_{i_2}\dots x_{i_p}$$

en particulier :

$$\begin{aligned} \sigma_1 &= \sum_{i=1}^{n} x_i = x_1 + x_2 + \dots + x_n \\ \sigma_2 &= \sum_{i<j} x_ix_j = x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n \\ \sigma_n &= \prod_{i=1}^{n} x_i = x_1x_2\dots x_n \end{aligned}$$

Définition 4.4 *Les σ_i sont appelées fonctions symétriques élémentaires des racines du polynôme P.*

Les fonctions symétriques élémentaires des racines du polynôme P s'expriment en fonction des coefficients du polynôme :

$$\sigma_1 = -\frac{a_{n-1}}{a_n}, \sigma_2 = \frac{a_{n-2}}{a_n}, \dots, \sigma_p = (-1)^p\frac{a_{n-p}}{a_n}, \dots, \sigma_n = (-1)^n\frac{a_0}{a_n}$$

Cas particuliers : Relations entre les coefficients et les racines dans les polynômes de degrés 2 et 3.

a.Polynôme de degrés 2 : Soit $P = aX^2 + bX + c$ un polynôme de degré 2 ($a \neq 0$). x_1 et x_2 ces deux racines.
On pose $s = x_1 + x_2$ et $p = x_1x_2$.
On a d'autre part :

$$\begin{aligned} P &= a(X - x_1)(X - x_2) \\ &= aX^2 - a(x_1 + x_2)X + ax_1x_2 \\ &= aX^2 - asX + ap \end{aligned}$$

D'où : $s = \frac{-b}{a}$ et $p = \frac{c}{a}$.

Application : Résoudre dans $\mathbb{R}^2$, les systèmes d'équations :

$$(1)\begin{cases} \frac{1}{x} + \frac{1}{y} = 5 \\ 6xy = 1 \end{cases} \qquad (2)\begin{cases} xy^2 + yx^2 = 17710 \\ xy = 385 \end{cases} \qquad (3)\begin{cases} x^2 + y^2 = 10 \\ x + y - xy = 5 \end{cases}$$

b.Polynômes de degrés 3 : Soit $P = aX^3 + bX^2 + cX + d$ un polynôme de degré 3 ($a \neq 0$). x_1,x_2, x_2 ces trois racines, distinctes ou non.
Posons :

$$\begin{aligned} s &= x_1 + x_2 + x_3 \\ p &= x_1x_2 + x_1x_3 + x_2x_3 \\ q &= x_1x_2x_3 \end{aligned}$$

$$\begin{aligned} P &= a(X - x_1)(X - x_2)(X - x_2) \\ &= aX^3 - a(x_1 + x_2 + x_3)X^2 + a(x_1x_2 + x_1x_3 + x_2x_3)X - a(x_1x_2x_3) \\ &= aX^3 + bX^2 + cX + d \end{aligned}$$

donc

$$s = \frac{-b}{a}, \quad p = \frac{c}{a}, \quad q = \frac{-d}{a}$$

Application : Résoudre donc $\mathbf{C}^3$, le système suivant :

$$\begin{cases} x + y + z = 0 \\ xy + xz + yz = 0 \\ xyz = 1 \end{cases}$$

x, y, z sont les racines de l'équation : $t^3 - 1 = 0$, d'où :

$$S = \{(1, j, \bar{j}), (1, \bar{j}, j), (j, \bar{j}, 1), (\bar{j}, j, 1), (j, 1, \bar{j}), (\bar{j}, 1, j)\}$$

avec

$$j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}.$$

Exercice résolu :

1. Résoudre dans $\mathbb{R}$ l'équation : $\cos 3x = \frac{1}{2}$
   En exprimant $\cos 3x$ en fonction de $X = \cos x$, en déduire que les nombres

   $$X_1 = \cos\frac{\pi}{9}, \quad X_2 = \cos\frac{7\pi}{9}, \quad X_3 = \cos\frac{13\pi}{9}$$

   sont des solutions de l'équation : $8X^3 - 6X - 1 = 0$ et que, pour tout X réel, on a :

   $$(3)\ 8X^3 - 6X - 1 = 8(X - X_1)(X - X_2)(X - X_3)$$

2. Al'aide de l'égalité (3) et en développant le deuxième membre, déduire les valeurs numériques de :

   $$A = \cos\frac{\pi}{9} + \cos\frac{7\pi}{9} + \cos\frac{13\pi}{9}$$
   $$B = \cos\frac{\pi}{9}\cos\frac{7\pi}{9} + \cos\frac{7\pi}{9}\cos\frac{13\pi}{9} + \cos\frac{13\pi}{9}\cos\frac{\pi}{9}$$
   $$C = \cos\frac{\pi}{9}\cos\frac{7\pi}{9}\cos\frac{13\pi}{9}$$

Solution :

1. $\cos 3x = \frac{1}{2} \Longleftrightarrow 3x = \pm\frac{\pi}{3} + 2k\pi, k \in \mathbf{Z} \Longleftrightarrow x = \pm\frac{\pi}{9} + \frac{2\pi}{3}k, k \in \mathbf{Z}$

$$\begin{aligned} \cos 3x &= \cos 2x \cos x - \sin 2x \sin x \\ &= (2\cos^2 x - 1)\cos x - 2\sin^2 x \cos x \\ &= (2\cos^2 x - 1)\cos x - 2(1-\cos^2 x)\cos x \\ &= 4\cos^3 x - \cos x \end{aligned}$$

Posons $X = \cos x$

$$(\forall x \in \mathbb{R}),\ \cos 3x = \frac{1}{2} \Longleftrightarrow 4\cos^3 x - \cos x = \frac{1}{2} \Longleftrightarrow 8X^3 - 6X - 1 = 0$$

donc x est une racine de (1) si et seulement si X est une racine de (2)
d'où les racines de (2)

$$X_1 = \cos\frac{\pi}{9}\ (k=0),\ \ X_2 = \cos\frac{7\pi}{9}\ (k=1),\ \ X_3 = \cos\frac{13\pi}{9}\ (k=2)$$

ceci entraîne :

$$(3)\quad 8X^3 - 6X - 1 = 8(X - X_1)(X - X_2)(X - X_3)$$

2. Par identification des coefficients dans l'égalité (3) on trouve :

$$A = 0,\ \ B = -\frac{3}{4}\ \text{ et }\ C = \frac{1}{8}.$$

5 Décomposition d'un polynôme

5.1 Polynômes irréductibles dans $\mathbb{K}[X]$

Définition 5.1 *Un polynôme P de $\mathbb{K}[X]$ est dit scindé sur $\mathbb{K}$ si, et seulement si, s'il existe $\lambda \in \mathbb{K}^*$, $n \in \mathbb{N}$, $a_1, a_2, ..., a_n \in \mathbb{K}$ tels que*

$$P = \lambda \prod_{i=1}^{n} (X - a_i)$$

D'après le théorème de D'ALEMBERT-GAUSS, on a :

Proposition 5.1 **Tout polynôme à coefficients dans $\mathbb{C}$ est scindé.**

ℝm Ce résultat est faux dans $\mathbb{R}[X]$, par exemple le polynôme $X^2 + 1$ n'est pas scindé sur $\mathbb{R}$. Cependant, tout polynôme à coefficients réels est aussi à coefficients complexes et par suite scindé dans $\mathbb{C}$.

Définition 5.2 *P est un polynôme irréductible de $\mathbb{K}[X]$ s'il n'est pas inversible (c'est-à-dire $degP > 0$) et s'il n'est pas divisible que par λ et λP. (λ élément quelconque de $\mathbb{K}^*$).*

ℝms

1. Le polynôme zéro étant divisible par n'importe quel polynôme : un polynôme irréductible est donc toujours non nul.
2. Un polynôme du 1^{er} degré est toujours irréductible.

Exemples :

1. $X^2 - 2$ et $X^2 + 1$ sont irréductibles dans $\mathbb{Q}[X]$, sont réductibles respectivement dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$.
2. Les polynômes irréductibles de $\mathbb{C}$ sont les polynômes de degré 1, les polynômes irréductibles de $\mathbb{R}$ sont les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant est strictement négatif.

ℝm Tout polynôme ayant une racine dans $\mathbb{K}$ n'est pas irréductible ; la réciproque est fausse : le polynôme $(X^2+1)^2$ est réductible sur $\mathbb{R}$ et n'admet pas de racines dans $\mathbb{R}$.

5.2 Décomposition d'un polynôme en facteurs irréductibles

Théorème 5.1 **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 : Soit P un polynôme non constant de degré inférieure ou égal à n. Démontrons le résultat par récurrence sur n.
Le résultat est évidente pour les polynômes de degrés 1 : sont de la forme $aX+b$, donc sont irréductibles.
Supposons le résultat est vrai pour tout les polynômes de degrés n. Soit P un polynôme de degré $n+1$.

1. Si P est irréductible, alors c'est le produit d'un seul polynôme irréductible.
2. Sinon, il existe deux polynômes tels $P=QR$, les polynômes Q et R sont de degrés strictement inférieure à $n+1$, donc on peut appliquer l'hypothèse de récurrence à Q et R, ce qui permet d'obtenir une décomposition de P en produit des polynômes irréductibles, en mettant en facteur les coefficients dominants de chaque polynôme irréductible.

Montrons qu'une telle décomposition est unique, soit

$$P = uP_1P_2...P_n = vQ_1Q_2...Q_m$$

avec les P_i et les Q_i des polynômes irréductibles et unitaires, le coefficient dominant de P étant unique, donc $u=v$. P_1 divise l'un des facteurs de $Q_1Q_2...Q_m$, soit par exemple Q_1(pou simplifier), mais Q_1 est irréductibles donc $P_1=Q_1$, on simplifie donc par P_1 ; en réitérant ce raisonnement un nombre fini de fois on arrive à épuiser tous les facteurs de l'un des membres, d'où : $R_1,R_2,...,R_l$ étant les facteurs irréductibles restants :

$$R_1R_2...R_l = 1$$

ceci est impossible car les R_i sont de degrés supérieurs ou égaux à 1, donc en épuise en même temps les facteurs de deux membres.
En regroupant les facteurs égaux dans la décomposition précédente on obtient le résultats souhaité :

Exemple : La décomposition du polynôme X^6-1 en facteurs irréductibles dans $\mathbb{R}[X]$ est

$$X^6-1=(X^3-1)(X^3+1)=(X-1)(X^2+X+1)(X+1)(X^2-X+1)$$

Application 1. Les diviseurs d'un polynôme P ayant la décomposition $P=uP_1^{k_1}P_2^{k_2}...P_n^{k_m}$ sont tous de la forme :

$$D = vP_1^{h_1}P_2^{h_2}...P_m^{h_m} \qquad v\in\mathbb{K}^* \quad 0\le h_i\le k_i$$

Application 2. Désignons par $P_1,P_2,...,P_n$ l'ensemble des facteurs irréductibles unitaires deux à deux distincts de P et de Q, on peut écrire :

$$P = uP_1^{k_1}P_2^{k_2}...P_n^{k_n},\ k_i\ge 0$$

$$Q = vP_1^{l_1}P_2^{l_2}...P_n^{l_n},\ l_i\ge 0$$

On obtient :

$$P\wedge Q = \prod_{i=1}^{i=n} P_i^{\min(k_i,l_i)}$$

et

$$P\vee Q = \prod_{i=1}^{i=n} P_i^{\max(k_i,l_i)}$$

Dans ce chapitre $\mathbb{K}$ est un corps commutatif. Dans la plupart des cas usuels $\mathbb{K}$ sera le corps des nombres réels ou le corps des nombres complexes. On rappelle que l'anneau $\mathbb{K}[X]$ est un anneau intègre.

6 Fractions rationnelles et fonctions rationnelles

6.1 Corps des fractions d'un anneau (Rappel)

Soit A un anneau, cherchons un corps $\mathbb{K}$ tel que A soit un sous-anneau de $\mathbb{K}$. D'autre part A, sous-anneau de $\mathbb{K}$, devra être dépourvu de diviseurs de zéro. Nous allons voir une construction générale qui permet de construire un corps à partir d'un anneau.
Soit $(A,+,\times)$ un anneau intègre. Sur l'ensemble $A\times A^*$, on définit une relation par :

$$\forall((a,b),(a',b'))\in A\times A^*,\ (a,b)\mathscr{R}(a',b') \Longleftrightarrow a\times b' = a'\times b$$

On vérifie que $\mathscr{R}$ est une relation d'équivalence sur $A \times A^*$. On note $\mathbb{K}$ l'ensemble des classes d'équivalences de cette relation. Un élément $k \in \mathbb{K}$ est donc la classe d'un couple $(a,b) \in A \times A^*$, et on note cette classe

$$k = \frac{a}{b}$$

Sur l'ensemble $\mathbb{K}$, on définit deux lois notées $(+)$ et $(\times)$. Soient $k = cl(a,b)$ et $k' = cl(a',b') \in \mathbb{K}$ deux classes d'équivalences de représentants (a,b) et (a',b). On note :

$$k + k' = cl(a \times b' + b \times a', b \times b') \text{ tel que } \frac{a}{b} + \frac{a'}{b'} = \frac{a \times b' + b \times a'}{b \times b'}$$

$$k \times k' = cl(a \times a', b \times b') \text{ tel que } \frac{a}{b} \times \frac{a'}{b'} = \frac{a \times a'}{b \times b'}$$

et on vérifie que ces classes sont indépendantes des représentants $(a,b) \in k$ et $(a',b') \in k'$ choisis.
On montre aussi que $(\mathbb{K},+,\times)$ est un corps commutatif, appelé corps des fractions de l'anneau $(A,+,\times)$. De plus en peut prolonger l'anneau A dans le corps $\mathbb{K}$, à l'aide de l'injection :

$$\begin{array}{rrcl} \phi : & A & \longrightarrow & \mathbb{K} \\ & a & \longrightarrow & cl(a,1) \end{array}$$

Théorème 6.1 **Soient $(A,+,\times)$ un anneau intègre. Il existe un corps $(\mathbb{K},+,\times)$ unique à un isomorphisme près, tel que A est un sous-anneau de K et tel que**

$$\mathbb{K} = \{ab^{-1} \ / \ a,b \in A, \ \ b \neq 0\}$$

On dit que $\mathbb{K}$ est le corps des fractions de la'anneau intègre A.

Exemple : Le corps $(\mathbb{Q},+,\times)$ c'est le corps de fractions de l'anneau intègre $(\mathbb{Z},+,\times)$.

6.2 Corps des fractions rationnelles

Définition 6.1 *On appelle fraction rationnelle à une indéterminée X tout élément du corps des fractions de l'anneau intègre $\mathbb{K}[X]$. Ce corps est noté $\mathbb{K}(X)$.*

Soit F une fraction rationnelle, en fait F est une classe d'équivalence, soient (U,V) et (U',V') deux représentants de F, (U,U',V,V' des polynômes avec $V \neq 0, V' \neq 0$), nous aurons

$$\frac{U}{V} = \frac{U'}{V'} \Longleftrightarrow UV' = U'V$$

Donc c'est par abus de notations que nous écrivons : $F = \frac{U}{V}$.
Tout polynôme P peut être considéré comme le représentant d'un élément de $\mathbb{K}(X)$, il suffit de poser $P = \frac{P}{1}$ et nous avons déjà vu que $\mathbb{K}$ peut être considéré comme partie de $\mathbb{K}[X]$, donc

$$\mathbb{K} \subset \mathbb{K}[X] \subset \mathbb{K}(X)$$

Les coefficients de U et V sont encore appelés coefficients de F.
Si U et V sont premiers entre eux, nous dirons que la fraction $\frac{U}{V}$ est irréductible.

Proposition 6.1 **Tout fraction rationnelle de $\mathbb{K}(X)$ admet pour représentant une fraction irréductible à dénominateur unitaire et ceci d'une manière unique.**

Démonstration : Soient (U,V) et (U',V') deux représentants irréductibles de F (U,U',V,V' des polynômes avec $V \neq 0, V' \neq 0$ et V et V' unitaires). la relation

$$UV' = U'V$$

entraîne U divise U' et V divise V' (théorème de GAUSS), il existe donc $\lambda \in \mathbb{K}^*$ tel que $V' = \lambda V$ et $\lambda = 1$, donc $U' = U$ et $V' = V$. $\square$

6.3 Fonction rationnelle d'une variable

Soit F une fraction rationnelle et x un élément de $\mathbb{K}$, s'il existe un représentant de F, soit $\frac{U_1}{V_1}$, vérifiant $V_1(x) \neq 0$: On dit que x est substituable dans F. Si $\frac{U_2}{V_2}$ est un autre représentant de F tel que $V_2(x) \neq 0$, on aura :

$$\frac{U_2(x)}{V_2(x)} = \frac{U_1(x)}{V_1(x)}$$

cette valeur commune sera appelée valeur de F en x, substituable dans F, on la note $F(x)$
$\mathbb{R}$m Si x est substituable dans F, n'entraîne pas que pour tout représentant $\frac{U}{V}$ de f, on ait $V(x) \neq 0$; par exemple 1 est substituable dans $F = \frac{U}{V}$ avec $U = \frac{1}{2}(X^2 - 1)X$ et $V = -X - 2X + 3$, car

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

alors que $V(1) = 0$.

Définition 6.2 *Soit F une fraction rationnelle non nulle de forme irréductible $\frac{U}{V}$.*

1. *On appelle racine de F toute racine de U.*
2. *On appelle pôle de F toute racine de V.*
3. *Si a est une racine (resp.pole)de F, l'ordre de multiplicité de a est l'ordre de multiplicité de a en tant que racine de U (resp. V).*

Soient F et G deux fractions rationnelles données, désignons par S_F et S_G l'ensemble des valeurs de $\mathbb{K}$ substituables respectivement dans F et G, on aura :

$$(1) \quad \forall x \in S_F \ (\lambda F)(x) = \lambda F(x) \ \forall \lambda \in \mathbb{K}.$$

$$(2) \quad \forall x \in S_F \cap S_G \ (F+G)(x) = F(x) + G(x) \text{ et } (FG)(x) = F(x)G(x).$$

Donc pour x fixé, les formules (2) montrent que l'ensemble des fractions pour lesquelles x est substituable est sous-anneau A_x de $\mathbb{K}(X)$.
De plus si x est substituable dans $F = \frac{U}{V}$ $(V(x) \neq 0)$, vérifie $F(x) \neq 0$, alors $U(x) \neq 0$ et $\frac{U(x)}{V(x)}$ a pour inverse $\frac{V(x)}{U(x)}$ on voit donc que

$$(3) \quad (x \in S_F, F(x) \neq 0) \Longrightarrow \frac{1}{F}(x) = \frac{1}{F(x)}$$

on voit facilement que si F décrit A_x, $F(x)$ décrit un corps.
A toute fraction rationnelle F on peut associer une application $\widetilde{F}$ de S_F dans $\mathbb{K}$ définie par :

$$(\forall x \in S_F) \ \ \widetilde{F}(x) = F(x)$$

$\widetilde{F}$ est appelée fonction rationnelle associé à F, elle est définie sur S_F.
Les relations (1) (2) et (3) montrent que

$$(4) \quad \forall x \in S_F \ (\widetilde{\lambda F})(x) = \lambda \widetilde{F}(x) \ \forall \lambda \in \mathbb{K}.$$

$$(5) \quad \forall x \in S_F \cap S_G \ (\widetilde{F+G})(x) = \widetilde{F}(x) + \widetilde{G}(x) \text{ et } (\widetilde{FG})(x) = \widetilde{F}(x)\widetilde{G}(x).$$

Enfin si $F \neq 0$ et si S'_F est la partie de S_F telle que $F(x) \neq 0$

$$(6) \quad (x \in S'_F) \Longrightarrow \widetilde{\frac{1}{F}}(x) = \frac{1}{\widetilde{F}(x)}$$

Théorème 6.2 **Si $\mathbb{K}$ est infini l'application $F \longrightarrow \widetilde{F}$ est bijective.**

Démonstration : Soit $\frac{U}{V}$ un représentant de F,

$$[(x \in S_F), \ \ \widetilde{F}(x) = \frac{U(x)}{V(x)} = 0] \Longrightarrow [U(x) = 0 \text{ et } V(x) \neq 0]$$

or V a un nombre fini de racines, donc quel que soit le degré n de U, il y aura dans S_F une infinité de valeurs de x, donc au moins $n+1$, telle que $U(x) = 0$, c'est-à-dire $U = 0$ et par conséquent $F = 0$.
Supposons maintenant que

$$(\forall x \in S_F \cap S_G), \ \ \widetilde{F}(x) = \widetilde{G}(x)$$

d'après ce qui précède $F - G = 0$, ce qui preuve le théorème. □

7 Décomposition en éléments simples

7.1 Degré d'une fraction. partie entière

Soit F un élément non nul de $\mathbb{K}(X)$, si $\frac{U}{V}$ et $\frac{U'}{V'}$ sont deux représentants de F, la relation $UV' = U'V$ entraîne :

$$\deg U - \deg V = \deg U' - \deg V' = d$$

Définition 7.1 *Si F est une fraction rationnelle, la quantité $degU - degV \in \mathbb{Z} \cup \{\infty\}$ ne dépend pas du représentant (U,V) choisi pour la fraction F. On l'appelle degré de F et on le note $\deg F$.*

Lemme 7.1 **Pour tout élément F de $\mathbb{K}(X)$, on a d'une manière unique :**

$$(1) \quad F = P + G$$

P étant un polynôme de $\mathbb{K}[X]$, appelé partie entière de F et G un élément de $\mathbb{K}(X)$, nul ou de degré strictement négatif.

Démonstration : Soit (U,V) un représentant de F, effectuons la division euclidienne de U par V :

$$U = PV + R \qquad R = 0 \quad \text{ou} \quad degR < degV$$

d'où

$$F = \frac{U}{V} = P + \frac{R}{V} \ \ [P \in \mathbb{K}[X] \ \text{ et } \ (R = 0 \ \text{ ou } \ degR < degV]$$

Montrons qu'une telle decomposition est unique, supposons

$$F = P + G = P' + G'$$

avec $(P,P') \in \mathbb{K}[X]^2$, $(G,G') \in \mathbb{K}(X)^2$, $degG < 0$ et $degG' < 0$.
Alors $P - P'$ est un polynôme , et comme il est égal à $G' - G$, son degré est strictement négatif, donc $P' - P = 0$ c'est-à-dire $P' = P$ et par suite $G' = G$. □

ℝms

1. Si $degF < 0$: $P = 0$ et $G = F$.
2. Si $F \in \mathbb{K}[X]$: $P = F$ et $G = O$.

Exemple : La partie entière de la fraction $\frac{X^4 - X^3 + 1}{X^3 + 1}$ est $X + 1$ et la partie fractionnelle est $\frac{-X}{X^3+1}$.

Proposition 7.1 **Si F est une fraction rationnelle admettant a pour pôle d'ordre n, il existe un unique n-uplet de scalaires $(\mu_i)_{1 \le i \le n}$ et une unique fraction F_0 n'admettant pas a pour pôle tel que :**

$$F = \sum_{i=1}^{n} \frac{\mu_i}{(X-a)^i} + F_0$$

La quantité :

$$\sum_{i=1}^{n} \frac{\mu_i}{(X-a)^i}$$

s'appelle la partie polaire de F relative au pôle a.

Démonstration : **L'existence :** Soit $F = \frac{U}{(X-a)^n V_1}$ avec V_1 un polynôme unitaire tel que $V_1(a) \neq 0$. Les polynômes $(X-a)^n$ et V_1 sont premiers entre eux, donc d'après l'égalité de Bezout, il existe deux polynômes P et Q tels que

$$V_1 P + (X-a)^n Q = 1.$$

On a alors :

$$P = \frac{UP}{(X-a)^n} + \frac{UQ}{V_1}$$

La formule de Taylor permet d'écrire :

$$(PU)(X) = \sum_{k=0}^{+\infty} \alpha_k (X-a)^k$$

ce qui entraîne

$$\frac{UP}{(X-a)^n} = \sum_{i=0}^{n-1} \frac{\alpha_i}{(X-a)^{n-i}} + R$$

où R est un polynôme . Alors

$$F = \sum_{i=0}^{n-1} \frac{\alpha_i}{(X-a)^{n-i}} + R + \frac{UQ}{V_1}$$

et la fraction rationnelle $R + \frac{QV}{V_1}$ n'admet pas a pour pôle.

L'unicité : Supposons qu'il existe deux n-uplets distincts $(\mu_i)_{1\leq i\leq n}$ et $(\lambda_i)_{1\leq i\leq n}$ et deux fractions F_1 et F_2 n'admettant pas a pour pôle tels que

$$F = \sum_{i=1}^{n} \frac{\mu_i}{(X-a)^i} + F_1 = \sum_{i=1}^{n} \frac{\lambda_i}{(X-a)^i} + F_2$$

Soit $p = \max\{k \in [1,n]/\mu_k \neq \lambda_k\}$, donc $\forall k \in [k+1,n]$, $\mu_k = \lambda_k$, alors :

$$\sum_{i=1}^{p} \frac{\mu_i}{(X-a)^i} + F_1 = \sum_{i=1}^{p} \frac{\lambda_i}{(X-a)^i} + F_2$$

ce qui donne en multipliant par $(X-a)^p$:

$$\mu_p + \sum_{i=1}^{p-1} \mu_i (X-a)^{p-i} + (X-a)^p F_1 = \lambda_p + \sum_{i=1}^{p-1} \lambda_i (X-a)^{p-i} + (X-a)^p F_2$$

En substituant a à X dans cette égalité de fractions ($F_1(a) \neq 0$ et $F_2(a) \neq 0$), on obtient $\mu_p = \lambda_p$ ce qui est absurde. □

Soit F une fraction rationnelle admettant a pour pôle.

1. Si a est un pôle d'ordre 1 (pôle simple), on peut écrire $F = \frac{U}{(X-a)V_1}$ où V_1 est un polynôme n'admettant pas a pour racine. Donc il existe μ tel que :

$$(1)\ \ F = \frac{\mu}{X-a} + F_0$$

où la fraction F_0 n'admettant pas a pour pôle.

$$(1) \Longleftrightarrow \frac{U}{V_1} = \mu + (X-a)F_0$$

ce qui donne $\mu = \frac{U(a)}{V_1(a)}$. Mais $V' = (X-a)V_1' + V_1$ entraîne $V'(a) = V_1(a)$. La partie polaire relative au pole a est donc :

$$\frac{\mu}{(X-a)} \text{ avec } \mu = \frac{U(a)}{V_1(a)} = \frac{P(a)}{V'(a)}$$

2. Si a est un pôle d'ordre deux, on peut écrire $F = \frac{U}{(X-a)^2 V_1}$ où V_1 est un polynôme n'admettant pas a pour racine. Donc il existe μ_1 et μ_2 tels que :

$$(1)\ \ F = \frac{\mu_1}{X-a} + \frac{\mu_2}{(X-a)^2} + F_0$$

où F_0 est une fraction n'admettant pas a pour pôle.

$$(1) \Longleftrightarrow \frac{U}{V_1} = \mu_1(X-a) + \mu_2 + (X-a)^2 F_0$$

ce qui donne $\mu_2 = \frac{U(a)}{V_1(a)}$.
Pour trouver μ_1, on retranche $\frac{\mu_2}{(X-a)^2}$ pour obtenir une fraction dont a n'est pas un pôle, ou est pôle simple ce qui ramène au cas précédent.

3. Si a est un pôle d'ordre n ($n > 2$), on peut écrire $F = \frac{U}{(X-a)^n V_1}$ où V_1 est un polynôme n'admettant pas a pour racine. De la même manière on obtient $\mu_n = \frac{U(a)}{V_1(a)}$.
Comme $V = (X-a)^n V_1$, alors on a $V_1(a) = \frac{V^{(n)(a)}}{n!}$.

7.2 Décomposition en éléments simples dans $\mathbb{C}[X]$

Théorème 7.1 **Étant donnée une fraction rationnelle F dans $\mathbb{C}[X]$ dont les pôles sont $a_1, a_2, ..., a_n$ distinctes deux à deux et d'ordres de multiplicité respectifs $r_1, r_2, ..., r_n$, il existe un unique polynôme $P \in \mathbb{C}[X]$ et unique famille de scalaires $(\mu_{i,j})_{1\leq i\leq n, 1\leq j\leq r_i}$ tels que :**

$$F = P + \sum_{i=1}^{n} \left(\sum_{j=1}^{r_i} \frac{\mu_{i,j}}{(X-a_i)^j}\right).$$

Cette décomposition s'appelle la décomposition en éléments simples dans $\mathbb{C}(X)$ de la fraction F.

Démonstration :

1. **Existence :** Soit $\{a_1, a_2, ..., a_n\}$ l'ensemble des pôles de F, en retranchant de F la partie polaire associée à l'un de ses pôles a_i, on obtient une fraction rationnelle dont les pôles sont les autres pôles de F, avec le même ordre de multiplicité que dans F.
Donc en retranchant toutes les parties polaires associées à chacun des pôles, on obtient une fraction de la forme irréductible $\frac{P}{Q}$ qui n'admet pas pôle, c'est-à-dire le polynôme Q, qui est à coefficient dans $\mathbb{C}$, n'admet pas racine, ce qui montre qu'il est constant.
On a ainsi montré l'existence de la décomposition demandée de F.

2. **Unicité :** Supposons $F = P + \sum_{i=1}^{n}(\sum_{j=1}^{r_i} \frac{\mu_{i,j}}{(X-a_i)^j})$, alors P est la partie entière de F car $F - P$ est une somme de fractions de degrés strictement négatifs.
Pour chaque $1 \le k \le n$, on peut écrire :
$$F = \sum_{j=1}^{r_k} \frac{\mu_{k,j}}{(X-a_k)^j} + F_k.$$
où F_k est une fraction n'admet pas a_k pour pôle.
Donc $\sum_{j=1}^{r_k} \frac{\mu_{k,j}}{(X-a_k)^j}$ est la partie polaire de F associée au pôle a_k, ce qui entraîne l'unicité de $\mu_{k,1}, \mu_{k,2}, ..., \mu_{k,r_k}$.

□

7.3 Exemples d'applications

1. $F = \dfrac{X^3 - 2X^2 + 2}{X^2 - 3X + 2}$
La division euclidienne de $X^3 - 2X^2 + 2$ par $X^2 - 3X + 2$ entraîne :
$$F = X + 1 + F_1 \text{ avec } F_1 = \frac{X}{(X-1)(X-2)}.$$
F_1 c'est une fraction irréductible de degré négatif, donc sa partie entière est nulle et d'après le théorème, F_1 s'écrit sous la forme :
$$F_1 = \frac{\alpha}{X-1} + \frac{\beta}{X-2}$$
En multipliant les deux membres par $X - 1$, on obtient
$$(X-1)F_1(X) = \frac{X}{X-2} = \alpha + \frac{\beta(X-1)}{X-2)}$$
et en égalent les valeurs au point 1 des fractions obtenues, on obtient $\alpha = -1$.
De même , en multipliant par $(X-2)$, on obtient : $\beta = 2$.
D'où
$$F = X + 1 + \frac{-1}{X-1} + \frac{2}{X-2}$$

2. $F = \frac{X^4+1}{X(X^2-1)^2}$.
C'est une fraction irréductible, de degré négatif, donc sa partie entière est nulle. Elle est impaire, admet 0 pour pôle simple, 1 et -1 pour pôles doubles, donc F s'écrit sous la forme :
$$F = \frac{\alpha_1}{X} + \frac{\alpha_2}{(X-1)^2} + \frac{\alpha_3}{X-1} + \frac{\alpha_4}{(X+1)^2} + \frac{\alpha_5}{X+1}$$
et par parité, on obtient :
$$-F = -\frac{\alpha_1}{X} + \frac{\alpha_2}{(X+1)^2} - \frac{\alpha_3}{X+1} + \frac{\alpha_4}{(X-1)^2} - \frac{\alpha_5}{X-1}$$
L'unicité de le décomposition entraîne : $\alpha_4 = -\alpha_2$ et $\alpha_5 = \alpha_3$.
En multipliant les deux membres par X, et en égalent les valeurs au point 0 des fractions obtenues, on obtient $\alpha_1 = 1$.
De même , en multipliant par $(X-1)^2$), et en égalent les valeurs au point 1 des fractions obtenues, on obtient : $\alpha_2 = \frac{1}{2}$.
Enfin, $\lim_{x \longrightarrow +\infty} xF(x) = 1$ implique $1 = \alpha_1 + \alpha_3 + \alpha_5$; d'où $\alpha_3 = 0$ et
$$F = \frac{1}{X} + \frac{1}{2(X-1)^2} - \frac{1}{2(X+1)^2}.$$

3. $F = \frac{1}{X^n - 1}$.
   F admet pour pôles simples les n racines $n^{ième}$ de l'unité $w_k = e^{\frac{2k\pi i}{n}}$, $(1 \leq k \leq n-1)$, donc la décomposition s'écrit :
$$\frac{1}{X^n - 1} = \sum_{k=0}^{n-1} \frac{\alpha_k}{X - w_k}$$
   Les w_k étant simples, donc
$$\alpha_k = \frac{P(w_k)}{Q'(w_k)} = \frac{1}{n(w_k)^{n-1}} = \frac{w_k}{n} \text{ avec } P = 1 \text{ et } Q = X^n - 1$$
   car $(w_k)^n = 1$, d'où :
$$\frac{1}{X^n - 1} = \frac{1}{n} \sum_{k=0}^{n-1} \frac{w_k}{X - w_k}$$
4. Soit $P = a_0(X - x_1)(X - x_2)...(X - x_n)$ un polynôme de $\mathbb{C}[X]$ à racines simples. Alors il existe des scalaires (α_k) tels que :
$$\frac{P'}{P} = \sum_{k=1}^{n} \frac{\alpha_k}{X - x_k}$$
   en multipliant par $X - x_i$, on obtient :
$$(X - x_i)\frac{P'}{P} = \alpha_i + \sum_{k=1, k\neq i}^{n} \frac{\alpha_k(X - x_i)}{X - x_k}$$
   D'autre part
$$\lim_{x \longrightarrow x_i} (x - x_i)\frac{P'(x)}{P(x)} = \lim_{x \longrightarrow x_i} \frac{P'(x)}{\frac{P(x) - P(x_i)}{x - x_i}} = 1$$
   donc $\alpha_i = 1$ et par conséquent :
$$\frac{P'}{P} = \sum_{k=1}^{n} \frac{1}{X - x_k}.$$

Exercice : : Soit P un polynôme dont les racines sont $x_1, x_2, ..., x_n$ d'ordres de multiplicité respectifs $r_1, r_2, ..., r_n$, c'est-à-dire un polynôme de la forme :
$$P = \lambda \prod_{k=1}^{n} (X - x_i)^r_k \text{ avec } \lambda \in \mathbb{C}^*$$
Déterminer la décomposition de $\frac{P'}{P}$.

• • • • • • • • • • •