Cours de MOMI

Licence I Math-Info

Chapitre VIII: Polynômes

Dans tout ce chapitre $\mathbb{K}$ désigne $\mathbb{C}$, $\mathbb{R}$ ou $\mathbb{Q}$.

1 - L'anneau des polynômes

Définition. Un polynôme à coefficients dans $\mathbb{K}$ est une suite d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang.

On munit l'ensemble des polyômes de trois opérations:

- **L'addition:**

$$(a_0, a_1, a_2, \ldots)+(b_0, b_1, b_2, \ldots) \overset{\text{déf.}}{=} (a_0+b_0, a_1+b_1, a_2+b_2, \ldots)$$

- **Le produit:**

$$(a_0, a_1, a_2, \ldots)x(b_0, b_1, b_2, \ldots) \overset{\text{déf.}}{=} (c_0, c_1, c_2, \ldots),$$

où pour tout $n \in \mathbb{N}$, on a $c_n = \sum_{k=0}^{n} a_k b_{n-k}$.

- **Le produit par un scalaire:** Pour tout $\lambda \in \mathbb{K}$:

$$\lambda x(a_0, a_1, a_2, \ldots) \overset{\text{déf.}}{=} (\lambda a_0, \lambda a_1, \lambda a_2, \ldots).$$

On vérifie facilement que ces trois opérations donnent bien des polynômes (c'est-à-dire, des suites s'annulant à partir d'un certain rang) et vérifient les propriétés suivantes quelque soit les polynômes P, Q et R:

- $P+(0,0,0,\cdots)=P,\quad P+Q=Q+P,\quad P+(Q+R)=(P+Q)+R,$
- $(a_0,a_1,a_2,\cdots)+(-a_0,-a_1,-a_2,\cdots)=(0,0,0,\cdots)$
- $PxQ=QxP,\quad Px(QxR)=(PxQ)xR,$
- $Px(1,0,0,\cdots)=P,$
- $Px(Q+R)=PxQ+PxR.$

Avec toutes ces propriétés vérifiées, on dit alors que l'ensemble des polynômes à coefficients dans $\mathbb{K}$ est un *anneau commutatif.*

2 - Représentation usuelle des polynômes

(1) Le polynôme $(a_0,0,0,\cdots)$ s'identifie au scalaire a_0, on le note tout simplement a_0. Donc, on voit $\mathbb{K}$ comme une partie de l'ensemble des polynômes à coefficients dans $\mathbb{K}$. Ainsi, les opérations qu'on vient de définir sur les polynômes étendent celles de $\mathbb{K}$.

(2) Le polynôme $(0,1,0,0,\cdots)$ se note **X**, et on l'appelle l'indéterminée **X**. Ce polynôme est crucial pour travailler sur les polynômes. En effet, avec l'opération de multiplication des polynômes, on vérifie:

$(0,1,0,\cdots)^2 = (0,0,1,0,\cdots)$, $(0,1,0\cdots)^3 = (0,0,0,1,\cdots)$, etc

On note:

- $(0,0,1,0\cdots)$ par X^2,
- $(0,0,0,1,0\cdots)$ par X^3,
- etc

Maintenant, on a pour tout polynôme

$$(a_0,a_1,a_2,\cdots,a_d,0,0,\cdots) = a_0x(1,0,0\cdots)+a_1x(0,1,0,\cdots)+ a_2x(0,0,1,0,\cdots)+\cdots+a_dx(0,0,\cdots,1,0,\cdots)$$

1 à la (d+1)-ème place

Notations. (1) On note le polynôme $(a_0, a_1, \cdots, a_d, 0 \cdots)$ par $a_0 + a_1X + a_2X^2 + \cdots + a_dX^d$.

(2) L'ensemble des polynômes à coefficients dans $\mathbb{K}$ se note $\mathbb{K}[X]$.

3 - Degré d'un polynôme

Définitions. *(1) Soit $P = a_0 + a_1X + \cdots + a_dX^d$ un polynôme non nul tel que a_d soit le dernier terme non nul de la suite $(a_0, a_1, \cdots, a_d, 0, 0, \cdots)$. L'entier d s'appelle le degré de P et se note* $\deg P$.

Le degré du polynôme nul (c-à-d la suite $(0, 0, 0, \cdots)$) est $-\infty$. Avec la convention que $-\infty + d = -\infty$ et $-\infty < d$ pour tout $d \in \mathbb{N}$.

(2) On appelle polynôme constant tout polynôme de degré 0 (autrement dit, un polynôme de la forme a_0 pour $a_0 \in \mathbb{K}$).

(3) Un monôme est un polynôme de la forme a_dX^d.

Définitions. *(1) Soit $P = a_0 + a_1X + \cdots + a_dX^d$ un polynôme non nul de degré d.*

(1) Les éléments $a_0, a_1, \cdots, a_d$ de $\mathbb{K}$ s'appellent les coefficients de P.

(2) Le coefficient a_0 (resp. a_d) s'appelle le coefficient constant de P (resp. le coefficient dominant de P).

(3) On dit que le polynôme P est unitaire si $a_d = 1$.

La proposition suivante donne les degrés de la somme et du produit de deux polynômes:

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

$$\deg(P+Q) \leq \mathrm{Max}\{\deg P, \deg Q\} \quad \textit{et} \quad \deg(PxQ) = \deg P + \deg Q.$$

Si de plus, $\deg P \neq \deg Q$, alors
$\deg(P+Q) = \mathrm{Max}\{\deg P, \deg Q\}$.

Preuve. Posons $P = a_0 + a_1X + \cdots + a_mX^m$ et $Q = b_0 + b_1X + \cdots + b_nX^n$ (avec $m = \deg P$ et $n = \deg Q$). Sans perdre de généralités, on peut supposer $m \leq n$. Alors, la somme s'écrit:

$$P+Q = (a_0+b_0)+(a_1+b_1)X+\cdots+(a_m+b_m)X^m + b_{m+1}X^{m+1}+\cdots+b_nX^n.$$

On voit bien que $\deg(P+Q) \leq n = \mathrm{Max}\{m,n\}$, et $\deg(P+Q) = n$ si $m \neq n$. On a aussi:

$$PxQ = (\text{monômes de degré } < m+n) + a_m b_n X^{m+n}.$$

Ainsi, $\deg(PxQ) = m+n$ puisque $a_m b_n \neq 0$. □

Remarque. *Lorsque* $\deg P = \deg Q$, *on peut avoir* $\deg(P+Q) < \mathrm{Max}\{P,Q\}$. *Par exemple, pour* $P = 1+2X-3X^2$ *et* $Q = 2+X+3X^2$, *on a bien* $P+Q = 3+3X$ *qui est de degré* $1 < 2 = \mathrm{Max}\{2,2\}$.

Définition. *Soit* $P \in \mathbb{K}[X]$ *un polynôme non nul de coefficient dominant* $a \in \mathbb{K}$. *Le normalisé de* P *est le polynôme* $a^{-1}P$. *C'est un polynôme unitaire!*

Exemple. Le normalisé du polynôme $P = 2-X+2X^3+4X^5$ est le polynôme $\frac{1}{2}-\frac{1}{4}X+\frac{1}{2}X^3+X^5$.

Exemple. Soient $P = -1 + X + 2X^2$ et $Q = 3X - X^2 + X^3$.On a:

$$P + Q = -1 + 4X + X^2 + X^3.$$

$$P \times Q = -3X + 4X^2 + 4X^3 - X^4 + 2X^5.$$

Définition. *Un polynôme $P \in \mathbb{K}[X]$ est dit inversible s'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $PxQ = 1$.*

Proposition. *Les seuls polynômes inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls, c.-à-d., les éléments de $\mathbb{K}$ non nuls.*

Preuve. Soit $P \in \mathbb{K}[X]$ un polynôme inversible. Alors, il existe $Q \in \mathbb{K}[X]$ tel que $PxQ = 1$. Il est clair que P et Q ne sont pas nuls. En prenant le degré, on obtient $\deg(PxQ) = \deg P + \deg Q = \deg 1 = 0$. Comme $\deg P$ et $\deg Q$ sont des entiers naturels, alors $\deg P = \deg Q = 0$. Par conséquent, P est un polynôme constant non nul. □

Notation. On note $\mathbb{K}[X]^*$ l'ensemble des polynômes non nuls.

4 - Arithmétique des polynômes

Dans ce paragraphe, on va établir l'analogue de plusieurs résultats vus dans le chapitre "Arithmétique dans $\mathbb{Z}$".

Définition. *Soit $A, B \in \mathbb{K}[X]$ deux polynômes avec $A \neq 0$. On dit que A divise B s'il existe un polynôme $C \in \mathbb{K}[X]$ tel que:* $B = AxC$.

Notation. Lorsque A divise B, on écrit $A \mid B$. Dans le cas contraire, on écrit $A \nmid B$

Langage. Lorsque A divise B, on dit aussi que B est un multiple de A; ou A est un diviseur de B; ou B est divisible par A.

Remarque. La divisibilité dépend de l'ensemble considéré. Par exemple, 2 ne divise pas 3 en tant qu'éléments de $\mathbb{Z}$, par contre 2 divise 3 en tant que polynômes de $\mathbb{R}[X]$ car $3 = 2 \times \frac{3}{2}$ et $\frac{3}{2} \in \mathbb{R}[X]$.

On donne un résultat liant le degré à la divisibilité:

Proposition. *On a les affirmations suivantes:*

(1) Soient $A, B \in \mathbb{K}[X]^*$. Si A divise B, alors $\deg A \leq \deg B$.

(2) Soient $A, B \in \mathbb{K}[X]$ avec $A \neq 0$. Si A divise B et $\deg B < \deg A$, *alors $B = 0$.*

Preuve. À faire en exercice. □

Corollaire. *Soit $A, B \in \mathbb{K}[X]$ deux polynômes tels que $A \mid B$ et $B \mid A$. Alors, il existe $\lambda \in \mathbb{K}$ tel que $B = \lambda A$. Si de plus, A et B sont unitaires, alors $A = B$.*

Preuve. On peut supposer que A et B sont non nuls. Puisque A divise B, il existe $C \in \mathbb{K}[X]$ tel que $B = AxC$. En particulier, $\deg A \leq \deg B = \deg A + \deg C$. De même, $\deg B \leq \deg A$ car B divise A. Ainsi, $\deg B = \deg A$ et $\deg C = 0$, ce qui signifie que C est un polynôme constant. Donc, $C = \lambda \in \mathbb{K}$.

Si de plus A et B sont unitaires, alors en comparant les coefficients dominants dans l'égalité $B = \lambda A$, on déduit que $\lambda = 1$, c-à-d, $A = B$. □

Proposition (Division Euclidienne polynomiale)

Soit $A, B \in \mathbb{K}[X]$ deux polynômes avec $A \neq 0$. Alors, il existe deux polynômes uniques Q et R tels que:

$$\begin{cases} B = AxQ + R \\ \deg R < \deg A. \end{cases}$$

Preuve. Posons $A = a_0 + a_1X + \cdots + a_mX^m$ et $B = b_0 + b_1X + \cdots + b_nX^n$. Tout d'abord prenons le cas $B = 0$. On a alors $B = Ax0 + B$. Comme $\deg B = -\infty < \deg A$ car A n'est pas nul, on prend $Q = 0$ et $R = B$.

Pour la suite, on suppose $B \neq 0$. On procède par récurrence sur $\deg B$ (second principe).

• **Initialisation:** Supposons $\deg B = 0$, c-à-d, $B = b_0 \in \mathbb{K} \setminus \{0\}$.
– Si $\deg A \geq 1$, alors on écrit $B = Ax0 + b_0$. On a bien $\deg b_0 = 0 < \deg A$ et donc on prend $Q = 0$ et $R = b_0$.
– Si $\deg A = 0$, alors $A = a_0 \in \mathbb{K} \setminus \{0\}$. On a alors $B = Ax\frac{b_0}{a_0} + 0$. On prend $Q = \frac{b_0}{a_0}$ et $R = 0$ car $\deg 0 = -\infty < \deg A = 0$.
• **Hérédité:** On suppose que pour tout polynôme C de degré $< n$, il existe Q, R deux polynômes tels que $C = AxQ + R$ avec $\deg R < \deg A$.

Montrons le résultat pour B qui est de degré n. Si $\deg A > n$, alors on prend $B = Ax0 + B$. On prend $Q = 0$ et $R = B$ car $\deg B = n < \deg A$. Supposons $\deg A \leq n$.

On introduit le polynôme

$$C = B - \frac{b_n}{a_m} X^{n-m} A.$$

On remarque que $\deg C < \deg B$. Par hypothèse de récurrence, il existe Q et R deux polynômes tels que: $C = AxQ + R$ et $\deg R < \deg A$. Ainsi, on obtient

$$B = \left(Q + \frac{b_n}{a_m} X^{n-m} \right) \times A + R.$$

Unicité de Q et R: Supposons qu'il existe Q' et R' tels que $B = AxQ + R = AxQ' + R'$ avec $\deg R < \deg A$ et $\deg R' < \deg A$. Alors, on obtient $A \times (Q - Q') = R' - R$ et donc A divise $R' - R$. Or $\deg(R' - R) \leq \mathrm{Max}\{\deg R, \deg R'\} < \deg A$. Par la proposition précédente, on déduit que $R' - R = 0$ et donc $Q - Q' = 0$. □

Définition. *Avec les mêmes notations que dans la proposition précédente (division Euclidienne polynomiale), on dit que:*

- *B est le dividende de la division Euclidienne de B par A.*
- *A est le diviseur de la division Euclidienne de B par A.*
- *Q est le quotient de la division Euclidienne de B par A.*
- *R est le reste de la division Euclidienne de B par A.*

Exemple. Effectuer la division Euclidienne de $B = X^4 - 2X^2 + X - 1$ par $A = X^2 - X + 1$.

$$
\begin{array}{rrrrr|lll}
X^4 & & -2X^2 & +X & -1 & X^2 & -X & +1 \\
\cline{6-8}
X^4 & -X^3 & +X^2 & & & X^2 & +X & -2 \\
\cline{1-5}
 & X^3 & -3X^2 & +X & -1 & & & \\
 & X^3 & -X^2 & +X & & & & \\
\cline{2-5}
 & & -2X^2 & & -1 & & & \\
 & & -2X^2 & 2X & -2 & & & \\
\cline{3-5}
 & & & -2X & +1 & & &
\end{array}
$$

Ainsi, le quotient est $X^2 + X - 2$ et le reste est $-2X + 1$. □

La division Euclidienne est reliée à la notion de divisibilité:

Lemme. *Soient $A, B \in \mathbb{K}[X]$ deux polynômes avec $A \neq 0$. Alors, A divise B équivaut à dire que le reste de la division Euclidienne de B par A est nul.*

Preuve. Par la division Euclidienne de B par A, il existe $Q, R \in \mathbb{K}[X]$ tels que: $B = AxQ + R$ et $\deg R < \deg A$.

– Supposons A divise B. Alors, il existe $C \in \mathbb{K}[X]$ tel que $B = AxC$. Ainsi, $Ax(C - Q) = R$, ce qui signifie que A divise R. Comme $\deg R < \deg A$, on déduit que $R = 0$.

– Réciproquement, supposons $R = 0$. Alors, $B = AxQ$, ce qui signifie que A divise B. □

Définition. *Soient $A, B \in \mathbb{K}[X]$. On dit qu'un polynôme* **unitaire** *D est le plus grand diviseur commun à A et B s'il vérifie les deux conditions:*

- *$D \mid A$ et $D \mid B$.*
- *Si $C \in \mathbb{K}[X]$ tel que $C \mid A$ et $C \mid B$, alors $C \mid D$.*

Notation. Le polynôme D de la définition précédente se note $\mathrm{pgcd}(A, B)$.

Remarque. Comme pour les entiers, $\mathrm{pgcd}(0, 0)$ n'existe pas; et lorsque A est non nul, le $\mathrm{pgcd}(A, 0)$ est égal au normalisé de A. □

On montre que le polynôme D de la définition précédente est unique. Reste à montrer son existence. C'est l'objet de la proposition suivante:

Proposition. *Soient $A, B \in \mathbb{K}[X]^*$. Alors:*
(1) Le $\mathrm{pgcd}(A, B)$ existe.
(2) Il existe $U, V \in \mathbb{K}[X]$ tels que: $\mathrm{pgcd}(A, B) = AU + BV$.

Preuve. L'idée de la preuve est la même que celle utilisée dans le cas des entiers. On considère l'ensemble $M = \{AP + BQ \mid P, Q \in \mathbb{K}[X]\}$. Cet ensemble est stable par l'addition et la multiplication par des polynômes. De plus M n'est pas réduit au polynôme nul (car $A = Ax1 + Bx0 \in M$). Soit D un polynôme de M non nul de degré minimal (ce polynôme existe par le lemme du plus petit élément). Quitte à normaliser D, on peut supposer que D est unitaire.

Affirmation. $D = \mathrm{pgcd}(A, B)$ et il existe $U, V \in \mathbb{K}[X]$ tels que $D = AU + BV$.

En effet, l'existence de $U, V \in \mathbb{K}[X]$ tels que $D = AU + BV$ se déduit du fait que $D \in M$. Reste à montrer que D vérifie les conditions du pgcd.

– Si $C \in \mathbb{K}[X]$ divise A et B, alors C divise $AU + BV = D$.

– Montrons que D divise A. Par la division Euclidienne de A par D, il existe $Q, R \in \mathbb{K}[X]$ tels que: $A = DxQ + R$ et $\deg R < \deg D$.

Puisque $A, D \in M$, alors $A - DxQ = R \in M$. Puisque $\deg R < \deg Q$, on a nécessairement $R = 0$ car sinon D ne serait pas de degré minimal parmi les éléments non nuls de M. De la même façon, on montre que D divise B. □

Définition. *Deux polynômes $A, B \in \mathbb{K}[X]$ sont dits premiers entre eux si $\operatorname{pgcd}(A, B) = 1$.*

De la proposition précédente, on déduit les corollaires suivants:

Corollaire (Bézout). *Soient $A, B \in \mathbb{K}[X]$. On a $\operatorname{pgcd}(A, B) = 1$ si et seulement si il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$.*

Corollaire (Gauss). *Soient $A, B, C \in \mathbb{K}[X]$. Si $A \mid BxC$ et $\operatorname{pgcd}(A, B) = 1$, alors $A \mid C$.*

6 - Calcul du PGCD

On donne un lemme:

Lemme. *Soient $A, B \in \mathbb{K}[X]$ deux polynômes non nuls. On a:*

- *Si A divise B, alors $\mathrm{pgcd}(A, B)$ est le normalisé de A.*
- *Si $B = A \times Q + R$ pour certains $Q, R \in \mathbb{K}[X]$, alors $\mathrm{pgcd}(A, B) = \mathrm{pgcd}(A, R)$.*

(Q et R ne sont pas nécessairement le quotient et le reste de la division Euclidienne de B par A.)

Preuve. On reprend les mêmes arguments que dans le cas des entiers relatifs. □

Conclusion. On calcule le pgcd de deux poylnômes $A, B \in \mathbb{K}[X]$ non nuls en appliquant le lemme précédent. Explicitement, supposons que $\deg A \leq \deg B$. Si A divise B, alors $\mathrm{pgcd}(A, B)$ est le normalisé de A. Sinon, on effectue les divisions Euclidienne successives (en commençant par celle de B par A) jusqu'à avoir un reste nul. Le $\mathrm{pgcd}(A, B)$ est alors le normalisé du dernier reste non nul.

6 - Racines de polynômes

6.1 - Fonction polynomiale

Définition. *À tout polynôme* $P = a_0 + a_1X + \cdots + a_mX^m$, *on associe la fonction*

$$\begin{array}{rccc} \widetilde{P}: & \mathbb{K} & \longrightarrow & \mathbb{K} \\ & x & \mapsto & a_0 + a_1x + \cdots + a_mx^m \end{array}$$

qu'on appelle la fonction polynomiale associée au polynôme P.

Très important. Il ne faut pas confondre un polynôme et sa fonction polynomiale. Il y a des situations (hors du cas $\mathbb{K} = \mathbb{C}$, $\mathbb{R}$ ou $\mathbb{Q}$) où la fonction polynomiale est nulle alors que le polynôme n'est pas nul!

Remarque. Si $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$, alors on a:

$$\widetilde{P+Q} = \widetilde{P} + \widetilde{Q},$$

$$\widetilde{\lambda P} = \lambda \widetilde{P},$$

$$\widetilde{PxQ} = \widetilde{P}x\widetilde{Q}.$$

Notation. Pour tout $x_0 \in \mathbb{K}$, l'image de x_0 par $\widetilde{P}$, c-à-d, $\widetilde{P}(x_0)$ s'appelle la valeur P en x_0. On la note tout simplement $P(x_0)$.

Définition. *Un scalaire $r \in \mathbb{K}$ est dit une racine d'un polynôme $P \in \mathbb{K}[X]$ si $P(r) = 0$.*

Le résultat suivant donne une interprétation de l'évaluation d'un polynôme en un scalaire:

Proposition. *Soient $P \in \mathbb{K}[X]$ et $r \in \mathbb{K}$. Alors, $P(r)$ est le reste de la division Euclidienne de P par $X - r$.*

Preuve. Par la division Euclidienne de P par $X - r$, il existe $Q, R \in \mathbb{K}[X]$ tels que: $P = (X - r)Q + R$ et $\deg R < \deg(X - r) = 1$. Donc, $\deg R = 0$ ou $-\infty$. Cela veut dire que R est une constante. En prenant la fonction polynomiale, on a:

$$\widetilde{P} = (x - r)\widetilde{Q} + R.$$

En évaluant en r, on déduit que $P(r) = R$. □

Corollaire. *Soient $P \in \mathbb{K}[X]$ et $r \in \mathbb{K}$. Alors, r est une racine de P si et seulement si $X - r$ divise P.*

Preuve. On sait que $P(r)$ est le reste de la division Euclidienne de P par $X - r$. Ainsi, $P(r) = 0$ (c'est-à-dire, r est une racine de P) si et seulement si $X - r$ divise P. □

Remarques. (1) Soient $r_1, r_2 \in \mathbb{K}$ distincts. Alors, les polynômes $X - r_1$ et $X - r_2$ sont premiers entre eux (on vérifie facilement que leur pgcd est le polynôme constant 1).

(2) Si R_1 et R_2 sont des polynômes premiers entre eux divisant un polynôme P, alors $R_1 \times R_2$ divise P (on utilise le théorème de Gauss).

Corollaire. *Soient $P \in \mathbb{K}[X]$ et $r_1, \cdots, r_n \in \mathbb{K}$ des scalaires deux à deux distincts. Si $r_1, \cdots, r_n$ sont des racines de P, alors le polynôme $(X - r_1) \times \cdots \times (X - r_n)$ divise P.*

Preuve. Puisque $r_1, \cdots, r_n$ sont des racines de P, alors les polynômes $X - r_1, \cdots, X - r_n$ divisent P (Corollaire précédent). Par la remarque précédente, $(X - r_1) \times \cdots \times (X - r_n)$ divise P. □

Corollaire. *Soit $P \in \mathbb{K}[X]$ de degré n. Si P admet un nombre de racines $\geq n + 1$, alors P est le polynôme nul.*

Preuve. Soit $P \in \mathbb{K}[X]$ un polynôme de degré n, et $r_1, \cdots, r_d$ des racines de P deux à deux distinctes avec $d \geq n+1$. Par le corollaire précédent, le polynôme $(X - r_1) \times \cdots \times (X - r_d)$ divise P. Comme $(X - r_1) \times \cdots \times (X - r_d)$ est de degré $d \geq n+1 > \deg P$, on déduit que $P = 0$. □

Corollaire. *Le polynôme nul est le seul polynôme qui admet une infinité de racines.*

7 - Polynôme dérivé - Formule de Taylor

Définition. *Soit $P = a_0 + a_1 X + \cdots + a_d X^d \in \mathbb{K}[X]$ un polynôme de degré d. Le polynôme dérivé de P, noté P' ou $P^{(1)}$, est le polynôme donné par:*

$$a_1 + 2a_2 X + \cdots + (d-1)a_{d-1} X^{d-2} + d a_d X^{d-1}.$$

Par itération, on définit le polynôme $P^{(n)} = (P^{(n-1)})'$ pour tout entier $n \geq 1$, avec la convention $P^{(0)} = P$.

Notons que $\deg P' = \deg P - 1$ lorsque $\deg P \geq 1$.

Remarques. (1) Pour un polynôme $P \in \mathbb{K}[X]$, la fonction polynomiale associée au polynôme dérivé P' n'est autre que la dérivée de la fonction polynomiale associée à P.

(2) La dérivée polynomiale vérifie les propriétés habituelles de la dérivée:

$$(P+Q)' = P' + Q', \quad (\lambda P)' = \lambda P', \quad (P \times Q)' = P' \times Q + P \times Q'$$

pour tous polynômes $P, Q \in \mathbb{K}[X]$ et tout $\lambda \in \mathbb{K}$.

(3) Un polynôme a pour dérivée nulle si et seulement si il est constant.

On donne la formule de Taylor pour les polynômes:

Théorème.(Formule de Taylor) *Soient $P \in \mathbb{K}[X]$ un polynôme de degré d et $x_0 \in \mathbb{K}$. Alors, on a:*

$$P(X) = P(x_0) + P'(x_0)(X - x_0) + \frac{P^{(2)}(x_0)}{2!}(X - x_0)^2 + \cdots + \frac{P^{(d)}(x_0)}{d!}(X - x_0)^d.$$

Donc, P est déterminé par son évaluation en x_0 et ses $(d+1)$ premières dérivées.

Preuve. Posons $P = c_0 + c_1X + c_2X^2 + \cdots + c_dX^d$. On procède par récurrence sur le degré d de P (premier principe).

– **Initialisation:** Supposons $d = 0$. Alors, $P(X) = c_0$ est un polynôme constant. Dans ce cas, la formule de Taylor revient à montrer $P(X) = P(x_0)$, ce qui est vrai.

– **Hérédité:** Supposons que la formule soit vraie pour les polynômes de degré $d-1$ et montrons la pour les polynômes de degré d. On applique l'hypothèse de récurrence au polynôme dérivé P' de P, on obtient.

$$\begin{aligned} c_1 + 2c_2X + \cdots + (d-1)c_{d-1}X^{d-2} + dc_dX^{d-1} &= P'(x_0) + (P')'(x_0)(X-x_0) + \cdots + \frac{(P')^{(d-1)}(x_0)}{(d-1)!}(X-x_0)^{d-} \\ &= P'(x_0) + P^{(2)}(x_0)(X-x_0) + \cdots + \frac{P^{(d)}(x_0)}{(d-1)!}(X-x_0)^{d-1} \end{aligned}$$

Ce qu'on écrit aussi:

$$P'(X) = \left(P'(x_0)(X-x_0) + \frac{P^{(2)}(x_0)}{2!}(X-x_0)^2 + \cdots + \frac{P^{(d)}(x_0)}{d!}(X-x_0)^d\right)'.$$

Ainsi, $P(X) = \alpha + P'(x_0)(X-x_0) + \frac{P^{(2)}(x_0)}{2!}(X-x_0)^2 + \cdots + \frac{P^{(d)}(x_0)}{d!}(X-x_0)^d$, où α est une constante à déterminer. En évaluant en x_0, on déduit que $\alpha = P(x_0)$. □

Définition. *Un scalaire $r \in \mathbb{K}$ est dit une racine (ou un zéro) de multiplicité e d'un polynôme $P \in \mathbb{K}[X]$ si $(X-r)^e$ divise P et $(X-r)^{e+1}$ ne divise pas P.*

Langage. Une racine de multiplicité 1, 2 et 3 est respectivement dite une racine simple, double et triple. Une racine de multiplicité ≥ 2 est dite une racine multiple.

On obtient la caractérisation suivante de la multiplicité des racines:

Proposition. *Soit $P \in \mathbb{K}[X]$. Un scalaire $r \in \mathbb{K}$ est une racine de P de multiplicité $e \geq 1$ si et seulement si r est racine de P, P', $P^{(2)}, \cdots, P^{(e-1)}$, et r n'est pas une racine de $P^{(e)}$*
Autrement dit: $P(r) = P'(r) = \cdots = P^{(e-1)}(r) = 0$ et $P^{(e)}(r) \neq 0$.

Preuve. On utilise la formule de Taylor (à faire en exercice). □

8 - Décomposition en irréductibles dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$

Définition. *Un polynôme $P \in \mathbb{K}[X]$ est dit irréductible s'il est de degré ≥ 1 et ses seuls diviseurs sont:*
– les polynômes constants.
– les polynômes de la forme λP pour $\lambda \in \mathbb{K}$.

Remarques. (1) Un polynôme $P \in \mathbb{K}[X]$ de degré ≥ 1 n'est pas irréductible s'il existe $Q \in \mathbb{K}[X]$ tel que: Q divise P et $1 \leq \deg Q < \deg P$.

(2) Tout polynôme de $\mathbb{K}[X]$ de degré 1 est irréductible.

(3) La notion d'irréductibilité d'un polynôme dépend si on est sur $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ (donner un exemple d'un polynôme irréductible dans $\mathbb{R}[X]$ qui ne l'est pas dans $\mathbb{C}[X]$).

8.1 - Décomposition en irréductibles dans $\mathbb{C}[X]$

On admet le théorème suivant dû à d'Alembert:

Théorème. *Tout polynôme de $\mathbb{C}[X]$ non constant admet au moins une racine dans $\mathbb{C}$.*

Corollaire. *Les polynômes de $\mathbb{C}[X]$ irréductibles sont les polynômes de degré 1, c'est-à-dire, ceux de la forme $aX + b$ avec $a, b \in \mathbb{C}$ et $a \neq 0$.*

Preuve. On sait que les polynômes de degré 1 sont irréductibles. Soit $P \in \mathbb{C}[X]$ irréductible. Supposons que $\deg P > 1$. Par le théorème de d'Alembert, il existe $r \in \mathbb{C}$ racine de P. Ainsi, $X - r$ divise P. Comme $1 \leq \deg(X - r) < \deg P$, alors P n'est pas irréductible, une contradiction. □

Corollaire. *Tout polynôme $P \in \mathbb{C}[X]$ non constant se décompose en produit d'irréductibles comme suit:*

$$P(X) = c(X - r_1)^{e_1} \times \cdots \times (X - r_n)^{e_n},$$

où $c \in \mathbb{C}$ est le coefficient dominant de P, et $r_1, \cdots, r_n$ sont les racines de P de multiplicité respective $e_1, \cdots, e_n$. Cette décomposition est unique à une permutation des facteurs irréductibles près.

Preuve. Soit $P \in \mathbb{C}[X]$ non constant. On procède par récurrence sur $\deg P$ (premier principe). Si $\deg P = 1$, alors $P = aX + b$ avec $a, b \in \mathbb{C}$ et $a \neq 0$. On a $P = a(X + \frac{b}{a})$ et on prend $r_1 = -\frac{b}{a}$, $e_1 = 1$ et $c = a$. Supposons que le corollaire soit vrai pour tout polynôme de degré $\deg P - 1$. D'après le théorème de d'Alembert, il existe $r_1 \in \mathbb{C}$ une racine de P. Alors, $X - r_1$ divise P. Par conséquent, il existe $Q \in \mathbb{C}[X]$ tel que $P = (X - r_1)Q$. Puisque $\deg Q = \deg P - 1$, on applique l'hypoyhèse de récurrence à Q pour conclure. □

8.2 - Décomposition en irréductibles dans $\mathbb{R}[X]$

Contrairement au cas de $\mathbb{C}[X]$, il y a plus d'irréductibles dans $\mathbb{R}[X]$:

Proposition. *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les suivants:*

- *Les polynômes de degré 1: $aX + b$ avec $a, b \in \mathbb{R}$ et $a \neq 0$.*
- *Les polynômes de la forme $aX^2 + bX + c$ avec $a, b, c \in \mathbb{R}$, $a \neq 0$ et $b^2 - 4ac < 0$. Autrement dit, les polynômes de degré 2 sans racine réelle.*

Preuve. On sait que tout polynôme de degré 1 est irréductible. Soit un polynôme $aX^2 + bX + c \in \mathbb{R}[X]$ avec $a \neq 0$ et $b^2 - 4ac < 0$. Supposons que ce polynôme ne soit pas irréductible dans $\mathbb{R}[X]$, alors il est divisible par un polynôme $Q \in \mathbb{R}[X]$ vérifiant $1 \leq \deg Q < \deg(aX^2 + bX + c) = 2$. Ainsi, $\deg Q = 1$. En écrivant $Q = uX + v$, on voit bien que Q admet $\frac{-v}{u}$ pour racine, en particulier l'équation $ax^2 + bx + c = 0$ admet $\frac{-v}{u}$ pour solution et donc $b^2 - 4ac \geq 0$, ce qui n'est pas possible.

Plus généralement, soit $P \in \mathbb{R}[X]$ irréductible de degré ≥ 2. Donc, P n'admet pas de racine réelle. Par le théorème de d'Alembert, il existe $z \in \mathbb{C}[X]$ une racine de P. Comme $\overline{P(z)} = P(\overline{z}) = 0$ (car P est à coefficients réels), alors $\overline{z}$ est une racine de P. Puisque $z \neq \overline{z}$, les polynômes $X - z$ et $X - \overline{z}$ sont premiers entre eux en tant que polynômes de $\mathbb{C}[X]$. Puisque ces deux polynômes divisent P, alors $(X - z)(X - \overline{z})$ divise P. Soit $Q \in \mathbb{C}[X]$ tel que

$$P = (X - z)(X - \overline{z})Q.$$

Or $(X - z)(X - \overline{z}) = X^2 - 2\mathrm{Re}(z)X + |z|^2 \in \mathbb{R}[X]$ implique que $Q \in \mathbb{R}[X]$.

Puisque P est irréductible, on a alors $\deg Q = 0$, c'est -à-dire, $Q \in \mathbb{R}$. De plus, le fait que $z, \overline{z}$ ne sont pas réels, on a $(2\mathrm{Re}(z))^2 - 4|z|^2 < 0$. □

Théorème. *Soit $P \in \mathbb{R}[X]$ un polynôme non constant. Alors, P admet une décomposition en irréductibles comme suit:*

$$P = c(X-r_1)^{e_1} \times \cdots \times (X-r_n)^{e_n} \times (X^2+a_{n+1}X+b_{n+1})^{e_{n+1}} \times \cdots \times (X^2+a_{n+m}X+b_{n+m})^{e_{n+m}},$$

telle que

- *c est le coefficient dominant de P.*
- *les r_i sont les racines de P de multiplicité $e_i \geq 1$ pour tout $1 \leq i \leq n$.*
- *les polynômes $X^2 + a_{n+j}X + b_{n+j}$ sont sans racines réelles, c'est-à-dire, $a_{n+j}^2 - 4b_{n+j} < 0$ pour tout $1 \leq j \leq m$.*

De plus, cette décomposition est unique à une permutation près des facteurs.

9 - Factorisation du polynôme $X^n - z$

Soit $z \in \mathbb{C}$ un nombre complexe. On sait par le théorème de d'Alembert que le polynôme $P = X^n - z$ s'écrit comme produit de polynômes unitaires de degré 1. Factoriser ce polynôme revient à trouver les solutions de l'équation $X^n = z$. Lorsque $z = 0$, l'unique solution de cette équation est 0. On suppose donc $z \neq 0$ et on prend son écriture exponentielle: $z = |z|e^{i\theta}$, où $\theta = \arg(z)$. On a:

Proposition. *L'équation $X^n = z$ admet n solutions distinctes $r_1, \cdots, r_n$ données par:*

$$r_k = \sqrt[n]{|z|}e^{i(\frac{\theta}{n} + \frac{2k\pi}{n})} \quad \textit{pour} \quad k = 0, 1, \cdots, n-1.$$

Ainsi, le polynôme $X^n - z$ se factorise dans $\mathbb{C}[X]$ comme suit:

$$X^n - z = (X - r_1) \times \cdots \times (X - r_n).$$

Preuve. Soit $r \in \mathbb{C}$ une solution de l'équation $X^n = z$. Soit $\rho = |r|$ et $\varphi = \arg(r)$. Alors, $r = \rho e^{i\varphi}$. Puisque $r^n = z$, on obtient par la formule de Moivre $\rho^n e^{in\varphi} = |z|e^{i\theta}$.

Par conséquent, on déduit $\rho^n = |z|$ et $n\varphi = \theta + 2k\pi$ pour un certain $k \in \mathbb{Z}$. Ce qui implique:

$$\begin{cases} \rho = \sqrt[n]{|z|} \\ \varphi = \frac{\theta}{n} + \frac{2k\pi}{n}. \end{cases}$$

Comme l'argument est pris à un multiple de 2π près, on peut supposer $0 \leq k \leq n-1$. □

Exemples. (1) Les solutions de l'équation $X^n = 1$ s'appellent les racines n-ième de l'unité. On les exprime sous la forme (en prenant $z = 1 = e^{i0}$):

$$r_k = e^{i\frac{2k\pi}{n}} \quad \text{pour} \quad k = 0, 1, \cdots, n-1.$$

Pour $n = 3$, les racines troisièmes de l'unité sont:

- $r_0 = 1$.
- $r_1 = e^{\frac{2i\pi}{3}}$.
- $r_2 = e^{\frac{4i\pi}{3}}$.

Ainsi, $X^3 - 1$ se factorise en irréductibles comme suit:

- Dans $\mathbb{C}[X]$: $X^3 - 1 = (X - 1)(X - e^{\frac{2i\pi}{3}})(X - e^{\frac{4i\pi}{3}})$.
- Dans $\mathbb{R}[X]$: Comme $r_2 = \overline{r_1}$, on obtient $(X - r_1)(X - r_2) = X^2 - 2\mathrm{Re}(r_1) + r_1 \times r_2 = X^2 + X + 1$. Donc, $X^3 - 1 = (X - 1)(X^2 + X + 1)$.

(2) Les racines carrées de $2i$ sont les solutions de l'équation: $X^2 = 2i$. En posant $2i = 2e^{\frac{i\pi}{2}}$, on déduit les deux racines carrées données par la formule de la proposition précédente:

- $r_0 = \sqrt{2}e^{\frac{i\pi}{4}} = 1 + i$.
- $r_1 = \sqrt{2}e^{\frac{5i\pi}{4}} = -1 - i$.

10 - Les fonctions symétriques élémentaires

Le but de ce paragraphe est de donner le lien entre les racines et les coefficients d'un polynôme. Pour cela, on introduit la définition:

Définition. *Soient $r_1, \cdots, r_d \in \mathbb{K}$. On définit les d fonctions symétriques élémentaires associées à ces scalaires par:*

$$\begin{aligned}
\sigma_1(r_1, \cdots, r_d) &= \sum_{1 \leq i \leq d} r_i = r_1 + \cdots + r_d. \\
\sigma_2(r_1, \cdots, r_d) &= \sum_{1 \leq i < j \leq d} r_i r_j. \\
&\vdots \\
\sigma_k(r_1, \cdots, r_d) &= \sum_{1 \leq i_1 < \cdots < i_k \leq d} r_{i_1} \cdots r_{i_k}. \\
&\vdots \\
\sigma_d(r_1, \cdots, r_d) &= \prod_{i=1}^{d} r_i = r_1 r_2 \cdots r_d.
\end{aligned}$$

Remarque. Ces expressions ne changent pas si on change l'ordre des scalaires $r_1, \cdots, r_d$. Ceci justifie le terme "symétrique".

Par exemple pour $d = 2$, posons $s = \sigma_1(r_1, r_2) = r_1 + r_2$ et $p = \sigma_2(r_1, r_2) = r_1 r_2$. Alors, on obtient que r_1 et r_2 sont les racines du polynôme $P := X^2 - sX + p$. Par conséquent, les coefficients s et p du polynôme P sont donnés en fonction de ses racines.

Plus généralement, on a le résultat suivant:

Proposition. *Soient $r_1, \cdots, r_d \in \mathbb{K}$. Les coefficients du polynôme*

$$(X - r_1) \cdots (X - r_d) = X^d + c_{d-1} X^{d-1} + \cdots + c_0$$

sont donnés en fonction des fonctions symétriques élémentaires associées aux scalaires $r_1, \cdots, r_d$ comme suit:

$$\forall\, 1 \leq k \leq d, \quad c_{d-k} = (-1)^k \sigma_k(r_1, \cdots, r_d).$$

Proposition. (Formule du binôme de Newton)
Soient $a, b \in \mathbb{C}$ et $n \in \mathbb{N}$. Alors, on a

$$(a+b)^n = \sum_{p=0}^{n} C_n^p a^p . b^{n-p}.$$

Preuve. On procède par récurrence sur n.

Pour $n \in \mathbb{N}$, soit $P(n)$ la propriété:

$$\forall\, a, b \in \mathbb{C} \quad (a+b)^n = \sum_{p=0}^{n} C_n^p a^p . b^{n-p}.$$

Soient $a, b \in \mathbb{C}$.

• (Initialisation) $(a+b)^0 = 1$ et $\sum_{p=0}^{0} C_0^p a^p . b^{0-p} = C_0^0 a^0 . b^0 = 1$. Donc, $P(0)$ est vraie.

• (Hérédité) Soit $n \in \mathbb{N}$ tel que $P(n)$ soit vraie. Montrons que $P(n+1)$ est vraie.

$$
\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b)\left(\sum_{p=0}^{n} C_n^p a^p . b^{n-p}\right) \quad (\text{car } P(n) \text{ vraie}) \\
&= \left(\sum_{p=0}^{n} C_n^p a^{p+1} . b^{n-p}\right) + \left(\sum_{p=0}^{n} C_n^p a^p . b^{n+1-p}\right) \\
&= \left(\sum_{q=1}^{n+1} C_n^{q-1} a^q . b^{n+1-q}\right) + \left(\sum_{q=0}^{n} C_n^q a^q . b^{n+1-q}\right) \\
&= \left(\sum_{q=1}^{n} (C_n^{q-1} + C_n^q) a^q . b^{n+1-q}\right) + C_n^n a^{n+1} b^0 + C_n^0 a^0 b^{n+1} \\
&= \left(\sum_{q=1}^{n} C_{n+1}^q a^q . b^{n+1-q}\right) + C_{n+1}^{n+1} a^{n+1} b^0 + C_{n+1}^0 a^0 b^{n+1} \\
&= \sum_{q=0}^{n+1} C_{n+1}^q a^q b^{n+1-q}.
\end{aligned}
$$

Ainsi, $P(n+1)$ est vraie.

Conclusion: Par le premier principe de récurrence $P(n)$ est vraie pour tout $n \in \mathbb{N}$, c'est-à-dire, on a:

$$\forall\, a, b \in \mathbb{C},\ \forall\, n \in \mathbb{N} \quad (a+b)^n = \sum_{p=0}^{n} C_n^p a^p . b^{n-p}.$$

□

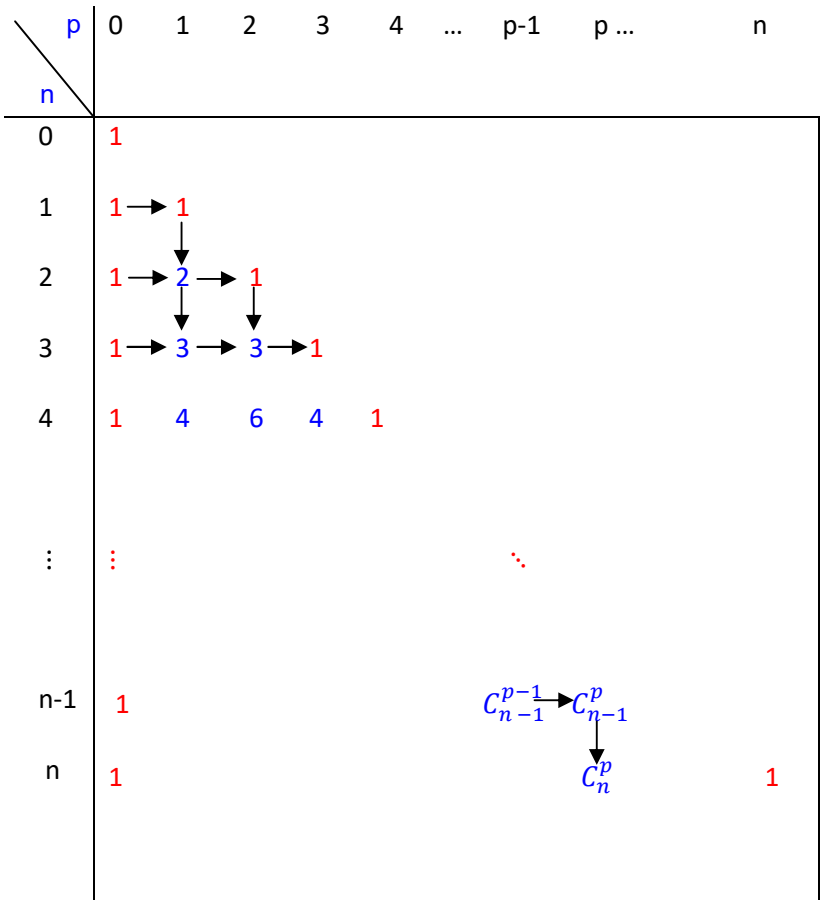
Triangle de Pascal.

On utilise le triangle de Pascal pour calculer les coefficients binomiaux C_n^p pour $p \leq n$.

Dans le triangle (voir ci-dessous), le coefficient C_n^p est placé à la ligne n et la colonne p.

On calcule ces coefficients en se basant sur la formule $C_n^p = C_{n-1}^p + C_{n-1}^{p-1}$ pour tout $1 \leq p \leq n-1$.

Cette formule s'interprète dans le triangle comme suit: *Le coefficient C_n^p de la ligne n et la colonne p s'obtient en ajoutant le coefficient C_{n-1}^{p-1} de la ligne $n-1$ et la colonne $p-1$ au coefficient C_{n-1}^p de la ligne $n-1$ et la colonne p.*



$$(a+b)^0 = 1$$

$$(a+b)^1 = 1.a + 1.b$$

$$(a+b)^2 = 1a^2 + 2ab + 1.b^2$$

$$(a+b)^3 = 1.a^3 + 3a^2b + 3ab^2 + 1.b^3$$