Polynômes à une indéterminée

« Toutes les équations d'algèbre reçoivent autant de solutions que la dénomination de la plus haute quantité le démontre. »
Inventions nouvelles en l'algèbre, Albert Girard (1595 - 1632)

Les polynômes font partie des premiers objets apparus dans l'histoire des mathématiques. On les trouve dès l'époque babylonienne par la description de méthodes de résolution des équations de degré 2.
Les résolutions des équations de degré supérieur ont beaucoup occupé les scientifiques de la Renaissance : Cardan, Tartaglia, Ferraro. Elles ont fait l'objet de nombreux « défis » dans lesquels les mathématiciens se mesuraient l'un à l'autre et démontraient leur agilité.
C'est au XIX^{e} siècle qu'Abel puis Galois mettent fin à la course aux résolutions d'équations polynomiales en démontrant que les équations de degré 5 et plus ne sont en général pas résolubles par radicaux. Les outils qu'ils introduisent pour leur démonstration ouvrent de nouvelles perspectives aux mathématiques et donnent une impulsion déterminante à l'algèbre.
Les polynômes ont la spécificité de constituer un pont naturel entre l'analyse et l'algèbre, selon qu'ils sont vus comme applications, ou comme objets algébriques. La démonstration par Gauss du théorème de d'Alembert-Gauss en est un exemple éloquent (et hors programme).

Notation : Dans tout le chapitre, $\mathbf{K}$ désigne le corps $\mathbf{R}$ ou $\mathbf{C}$.

1 L'anneau $\mathbf{K}[X]$

A Définition

Nous allons commencer par définir de façon algébrique les polynômes. La définition est un peu déroutante, mais permet de rendre certains résultats complètement triviaux.

Définition 1.1 *(Polynôme formel)*

On appelle **polynôme** sur $\mathbf{K}$ toute suite de $\mathbf{K}^{\mathbf{N}}$ stationnaire à 0.

Exemple

La suite $(0, 1, 5, 2, 9, 0, 0, 3, 0, 0, 0, ...)$ est un polynôme sur $\mathbf{R}$.

Théorème 1.2 *(Identification)*

Deux polynômes sont égaux si et seulement si leurs coefficients sont égaux deux à deux.

Preuve

Découle directement de la définition d'une suite. Si on avait utilisé une définition d'un polynôme à partir des fonctions polynomiales, un tel résultat reste accessible, mais s'obtient beaucoup plus difficilement. ■

Notation *(Indéterminée X)*

Soit P un polynôme sur $\mathbf{K}$ défini par la suite $(a_n) \in \mathbf{K}^{\mathbf{N}}$ stationnaire à 0.
On note alors

$$P = \sum_{k=0}^{+\infty} a_k X^k.$$

Lorsque le coefficient a_k est nul, en général on n'écrit pas le terme $a_k X^k$.

On note $\mathbf{K}[X]$ l'ensemble des polynômes d'indéterminée X sur $\mathbf{K}$.

Explications

Il faut comprendre que ce n'est qu'une **notation** :

1. X est l'indéterminée. Ce n'est pas un nombre, ni une variable.
2. La puissance de X désigne la place du coefficient dans la suite. À ce stade, il n'y a aucun rapport avec les puissances entières.
3. Malgré la notation, la somme *formelle* n'est pas infinie car à partir d'un certain rang, tous les termes de la suite sont nuls.

Exemple

Le polynôme $(0,1,5,2,9,0,0,3,0,0,0,...)$ s'écrit également

$$P = X + 5X^2 + 2X^3 + 9X^4 + 3X^7.$$

Remarque : On veille à toujours écrire les coefficients par rang croissant ou décroissant de la puissance de X.

Définition 1.3 *(Polynômes particuliers)*

On appelle **polynôme nul**, le polynôme $P = 0$.
On appelle **polynôme unité**, le polynôme $P = 1$.
On appelle **monôme**, un polynôme dont un seul coefficient est non nul.
Un polynôme est **pair**, si tous ses coefficients d'indice impair sont nuls.
Un polynôme est **impair**, si tous ses coefficients d'indice pair sont nuls.

Exemple

$P = 2X^5$ est un monôme.
$P = 1 - 3X^2 + 2X^8$ est un polynôme pair.

Définition 1.4 *(Degré d'un polynôme)*

On appelle **degré du polynôme**, l'indice de son dernier coefficient non nul.
On note $\deg(P)$ ou $\partial^o P$ le degré de P.
Par convention $\deg(0) = -\infty$.

Le **coefficient dominant** d'un polynôme (non nul) est son dernier coefficient non nul.
Un **polynôme unitaire** est un polynôme de coefficient dominant égal à 1.
Un **polynôme constant** est un polynôme nul ou de degré 0.

Exemple

Le degré de $-3X^5 - X^2 + 7$ est 5, son coefficient dominant est -3.
$X^4 + X^3 - X - 9$ est un polynôme unitaire.

Si on sait que $\deg P \leqslant n$, alors on peut écrire $P = \sum_{k=0}^{n} a_k X^k$.

⚠ $\deg P = 0 \not\Rightarrow P = 0$.

Notation

Pour $n \in \mathbf{N}$, on note $\mathbf{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n.

⚠ Si $P \in \mathbf{K}_n[X]$, alors on n'a pas nécessairement $\deg P = n$, mais plutôt $\deg P \leqslant n$.

B Opérations sur les polynômes

Définition 1.5 *(Sommes et produits avec les polynômes)*

Soient $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$ deux polynômes de $\mathbf{K}[X]$. Soit $\lambda \in \mathbf{K}$.

On définit la **somme** de P et Q par $P + Q = \sum_{k=0}^{+\infty} (a_k + b_k) X^k$.

On définit le **produit** de P par le scalaire λ par $\lambda P = \sum_{k=0}^{+\infty} (\lambda a_k) X^k$.

On définit le **produit** de P par Q par $PQ = \sum_{k=0}^{+\infty} c_k X^k$ avec $c_k = \sum_{i=0}^{k} a_i b_{k-i}$.

Exemple

Si $P = 1 + 2X - 3X^4$, $Q = 3X + X^3 + X^4 - X^5$ et $\lambda = 2$ alors :

$$P + Q = 1 + 5X + X^3 - 2X^4 - X^5.$$
$$\lambda P = 2 + 4X - 6X^4.$$
$$PQ = (1 + 2X - 3X^4)(3X + X^3 + X^4 - X^5)$$
$$= 3X + 6X^2 + X^3 + 3X^4 - 8X^5 - 2X^6 - 3X^7 - 3X^8 + 3X^9.$$

Explications

Pour la somme et pour le produit avec un scalaire, ces opérations coïncident avec les opérations naturelles sur les suites. Par contre, pour le produit entre deux polynômes, le produit naturel entre suites consisterait simplement à multiplier entre eux les coefficients de même rang ce qui n'est pas le choix réalisé ici.
En effet, la règle définie pour le produit est celle qui utilise la distributivité par rapport au « + » dans laquelle l'exposant de l'indéterminée est identifié à une puissance. Ce choix est indispensable pour pouvoir ensuite établir un lien intéressant entre les polynômes et les fonctions polynomiales comme nous le ferons plus loin.
Construction du coefficient c_k.
Le coefficient noté c_k correspond à tous les produits de termes qui interviennent dans le monôme X^k. Si on « *choisit* » $a_i X^i$ dans le premier polynôme, alors il faut le multiplier par un monôme de degré X^{k-i} pour obtenir un monôme de degré X^k. On a donc le terme $a_i b_{k-i}$. Il faut ajouter tous les produits ainsi obtenus à partir des différents coefficients de P. On trouve $c_k = \sum_{i=0}^{n} a_i b_{k-i}$.
Ce coefficient peut aussi être interprété à partir d'une somme double.

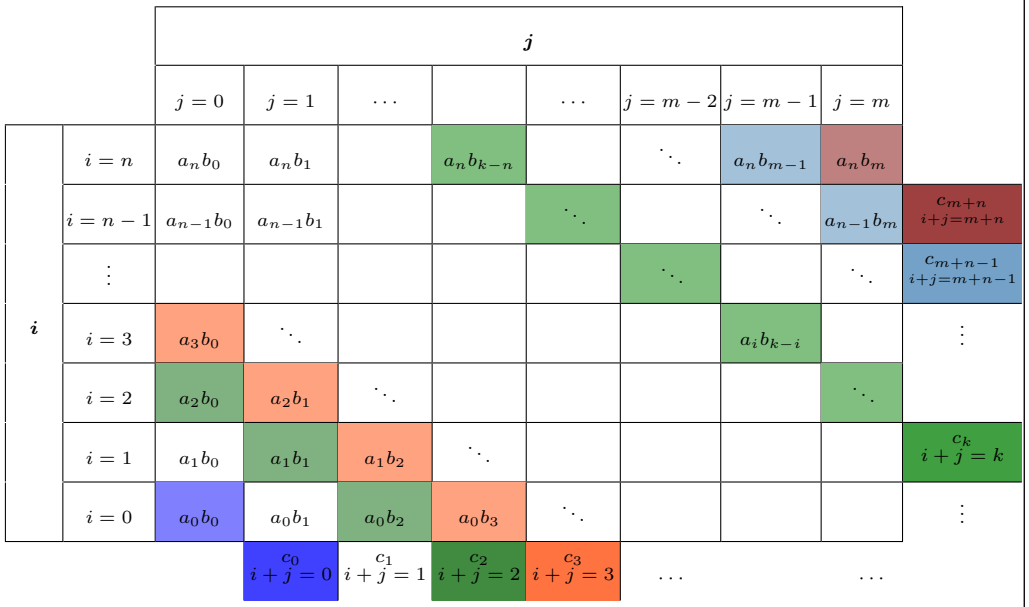
Pour $\deg P = n$ et $\deg Q = m$, on trouve en effet :

$$P\,Q = \left(\sum_{i=0}^{n} a_i X^i\right)\left(\sum_{j=0}^{m} b_j X^j\right) = \sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j X^{i+j} = \sum_{k=0}^{n+m}\sum_{i+j=k} a_i b_j X^{i+j}$$
$$= \sum_{k=0}^{n+m}\sum_{i=0}^{k} a_i b_{k-i} X^k$$
$$= \sum_{k=0}^{n+m} c_k X^k.$$

On a noté $a_i = 0$ pour $i \geqslant n$ et $a_j = 0$ pour $j \geqslant m$.

Nous avons déjà vu plusieurs façons de calculer une somme double au moment du chapitre sur sommes et produit. La multiplication polynomiale nous en donne une dernière : **les sommes de Cauchy**.

Au lieu de sommer en ligne ou en colonne, on somme en diagonale. Sur chaque diagonale, la somme $i + j$ est constante : on obtient un monôme. Le polynôme produit est la somme de tous ces monômes.



Méthode *(Calcul pratique du produit de deux polynômes)*

Pour faire le produit de deux polynômes (ou plus), il est souvent malhabile de faire un développement « classique » tel que vous le faites depuis le collège.

Il est préférable de faire directement le calcul des c_k : choisir les termes dans chaque parenthèse, pour que, multipliés entre eux, ils donnent le bon degré k.

Nous avons déjà utilisé ces méthodes de *calcul rapide* lors de la linéarisation/délinéarisation en trigonométrie.

Définition 1.6 *(Puissance k-ième d'un polynôme)*

On définit par récurrence la puissance k-ième d'un polynôme P avec

- $P^0 = 1$,
- $\forall k \geqslant 0,\quad P^{k+1} = P \times P^k = P^k \times P$.

Preuve

On montre aisément par récurrence que l'on a bien $P^k \times P = P \times P^k$. ■

Définition 1.7 *(Composée de deux polynômes)*

Soient $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$ deux polynômes de $\mathbf{K}[X]$. On définit la composée de Q par P avec

$$P \circ Q = \sum_{k=0}^{+\infty} a_k Q^k = \sum_{k=0}^{+\infty} a_k \left(\sum_{i=0}^{+\infty} b_i X^i\right)^k.$$

Exemple

Soient $P = 3X^2 + 7X - 1$ et $Q = X^2 + 1$. Calculer $P \circ Q$.

Solution :

$P \circ Q = 3\left(X^2+1\right)^2 + 7\left(X^2+1\right) - 1 = 3X^4 + 13X^2 + 15$.

Théorème 1.8 *(Stabilité des polynômes)*

$\mathbf{K}[X]$ est stable par somme, par produit avec un scalaire, par produit entre polynômes et par composition.

C'est-à-dire que la somme de deux polynômes est un polynôme,
le produit de deux polynômes est un polynôme,
le produit d'un polynôme par un scalaire est un polynôme,
la composée de deux polynômes est un polynôme.

Preuve

La preuve consiste à montrer que les sommes correspondant au résultat sont bien finies (la suite doit être stationnaire à 0, sinon ce n'est pas un polynôme). C'est trivial pour la somme ou le produit avec un scalaire.

Pour le produit de deux polynômes, on fera cette preuve avec les degrés un peu plus loin.

Pour la composition, cela découle du produit. ■

Théorème 1.9 *(Structure d'anneau)*

- L'opération somme « + » sur les polynômes est :
  - *interne :* la somme de deux polynômes est un polynôme.
  - *associative.* $\forall (P, Q_1, Q_2) \in (\mathbf{K}[X])^3$, $(P+Q_1)+Q_2 = P+(Q_1+Q_2)$.
  - *admet un élément neutre :* $0 \in \mathbf{K}[X]$ tel que $\forall P \in \mathbf{K}[X]$, $P+0=0+P=P$.
  - *tout polynôme admet un opposé :* $\forall P \in \mathbf{K}[X]$, $-P \in \mathbf{K}[X]$ avec $P+(-P)=(-P)+P=0$.
  - *commutative :* $\forall (P, Q) \in (\mathbf{K}[X])^2$, $P+Q=Q+P$.

  $\to (\mathbf{K}[X], +)$ est un groupe commutatif (ou abélien).
- L'opération produit« × » sur les polynômes est :
  - *interne :* le produit de deux polynômes est un polynôme.
  - *associative.* $\forall (P, Q_1, Q_2) \in (\mathbf{K}[X])^3$, $(P\times Q_1)\times Q_2 = P\times(Q_1\times Q_2)$.
  - *admet un élément unité :* $1 \in \mathbf{K}[X]$ tel que $\forall P \in \mathbf{K}[X]$, $P\times 1 = 1\times P = P$.
  - *distributive par rapport à « + » :* $\forall (P, Q_1, Q_2) \in (\mathbf{K}[X])^3$, $P\times(Q_1+Q_2) = P\times Q_1 + P\times Q_2$.
  - *commutative :* $\forall (P, Q) \in (\mathbf{K}[X])^2$, $P\times Q = Q\times P$.

  $\to (\mathbf{K}[X], +, \times)$ est un anneau commutatif.

Remarque : Les différentes structures (groupes, anneaux, corps) seront revues dans un chapitre spécifique.
Nous verrons également que la structure de $\mathbf{K}[X]$ est plus riche que cela, c'est un espace vectoriel et même une algèbre.

Preuve
Les vérifications sont immédiates. ■

Propriété 1.10 *(Formule du binôme de Newton)*

La formule du binôme de Newton est valable sur $\mathbf{K}[X]$:
Soient $(P, Q) \in (\mathbf{K}[X])^2$ et $n \in \mathbf{N}$.

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

Preuve
Cela provient du fait que le produit entre polynômes est commutatif. C'est alors exactement la même preuve que sur $\mathbf{K}$. ■

Nous verrons en exercice que cela, joint avec le principe d'identification, permet d'obtenir facilement des identités sur les coefficients binomiaux.

Propriété 1.11 *(Égalité de Bernoulli)*

La formule de Bernoulli est valable sur $\mathbf{K}[X]$:
Soient $(P, Q) \in (\mathbf{K}[X])^2$ et $n \in \mathbf{N}$.

$$P^{n+1} - Q^{n+1} = (P-Q)\sum_{k=0}^{n} P^k Q^{n-k}.$$

Preuve
Comme sur $\mathbf{K}$ car le produit entre polynômes commute. ■

C Degrés

Propriété 1.12

Soient P et Q, deux polynômes de $\mathbf{K}[X]$,

$$\begin{aligned} \deg(P+Q) &\leqslant \max(\deg P, \deg Q), \\ \deg(PQ) &= \deg P + \deg Q, \\ \deg(P\circ Q) &= \deg P \times \deg Q \qquad \text{pour } Q \text{ non constant.} \end{aligned}$$

Et $\deg(P+Q) < \max(\deg P, \deg Q)$ si, et seulement si P et Q sont de même degré avec coefficients dominants opposés.

Remarque : Lorsqu'un, ou les deux polynômes sont nuls, les relations pour la somme et le produit restent valables en prenant $\deg 0 = -\infty$ et en appliquant les règles de calcul sur $\overline{\mathbf{R}}$.

Preuve
Trivial pour la somme, c'est donné par la formule du cours.
Pour le produit, si P ou Q est nul, le résultat est immédiat.
Si P et Q sont tous deux non nuls, on démontre le résultat en deux étapes (on obtient l'égalité par une double inégalité).
On note $\deg P = n$ et $\deg Q = m$.
Étapes de la preuve.

1. On montre que $\deg(PQ) \leqslant m+n$, c'est-à-dire que tous les coefficients d'indice supérieur sont nuls.
2. On montre que $\deg(PQ) \geqslant m+n$, c'est-à-dire que le coefficient d'indice $m+n$ est non nul.

Rédaction.

1. On commence par montrer $\deg(PQ) \leqslant m+n$ en vérifiant que pour tout $k \geqslant m+n+1$, $c_k = 0$.

On suppose donc $k \geqslant m+n+1$, alors

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{n} a_i b_{k-i} \qquad \text{car } a_i = 0 \text{ pour } i \geqslant n+1$$
$$= \sum_{i=k-m}^{n} a_i b_{k-i} \qquad \text{car } b_{k-i} = 0 \text{ pour } k-i > m \iff i < k-m.$$

Or $k \geqslant m+n+1$, donc $k-m \geqslant n+1 > n$ donc la somme est vide.
Donc pour $k \geqslant m+n+1$, $c_k = 0$. Donc $\deg(PQ) \leqslant m+n$

2. On montre ensuite que $c_{m+n} \neq 0$.
D'après le raisonnement précédent, pour $k = m+n$, on a

$$c_{k=m+n} = \sum_{i=k-m}^{n} a_i b_{k-i} \qquad \text{car } b_{k-i} = 0 \text{ pour } k-i > m \iff i < k-m$$
$$= \sum_{i=n}^{n} a_i b_{m+n-i} \qquad \text{on remplace } k \text{ par } m+n$$
$$= a_n b_m.$$

Or $a_n \neq 0$ car $\deg P = n$ et $b_m \neq 0$ car $\deg Q = m$, donc $c_{m+n} = a_n b_m \neq 0$.
Donc $\deg(PQ) \geqslant m+n$.

3. Conclusion : par double inégalité, $\deg(PQ) = m+n$.

• Pour la composition.
D'après le cas du produit que l'on vient de prouver, on sait par récurrence immédiate que $\deg Q^k = k \deg Q$.
Ainsi, pour $P = \sum_{k=0}^{n} a_k X^k$,

$$\deg P \circ Q = \max\left(k \deg Q,\ a_k \neq 0\right).$$

Car les degrés sont distincts (Q non constant), donc $\deg PQ = n \deg Q$. ■

Théorème 1.13

$P \times Q = 0 \Rightarrow P = 0$ ou $Q = 0$.
On dit que l'anneau $\mathbf{K}[X]$ est *intègre*.

Corollaire 1.14

On peut simplifier par des polynômes non nuls dans les équations.

Preuve

Voici un exemple qui montre que raisonner avec les degrés peut s'avérer très efficace :
Par contraposée, si $P \neq 0$ et $Q \neq 0$, alors $\deg P \in \mathbf{N}$ et $\deg Q \in \mathbf{N}$,
ainsi $\deg PQ = \deg P + \deg Q \in \mathbf{N}$, donc $PQ \neq 0$.
Faire la preuve du corollaire en exercice. ■

Exemple

Soient P, Q et R trois polynômes de $\mathbf{K}[X]$.
Si $PR = PQ$ avec $P \neq 0$, alors $R = Q$.

Théorème 1.15

Les seuls polynômes inversibles de $\mathbf{K}[X]$ sont les constantes non nulles : $\lambda.1_{\mathbf{K}[X]}$, pour $\lambda \in \mathbf{K}^*$.

Explications

Cela veut dire qu'il est hors de question de diviser par un polynôme (ou de mettre à la racine carrée, ou ...).
Les seules opérations que nous ayons définies sur les polynômes sont :

- addition (et soustraction) entre polynômes
- multiplication par une constante,
- multiplication entre polynômes.
- puissances entières de polynômes et compositions entre polynômes.

Et **c'est tout !**

Preuve

Analyse :
P est inversible si et seulement s'il existe un polynôme Q tel que $PQ = 1$.
En particulier P et Q sont non nuls.
Si on suppose P inversible et Q son inverse, alors

$$\deg P + \deg Q = \deg PQ = \deg 1_{\mathbf{K}[X]} = 0.$$

Or $\deg P \in \mathbf{N}$ et $\deg Q \in \mathbf{N}$ (car ils sont non nuls), donc la seule solution est $\deg P = \deg Q = 0$.
Donc P est une constante non nulle.
Synthèse :
Réciproquement, si P est une constante non nulle λ, alors si on pose $Q = \frac{1}{\lambda}$, c'est aussi un polynôme et $PQ = 1$. Donc P est inversible.
Conclusion : P est inversible si et seulement si c'est une constante non nulle. Son inverse est alors l'inverse de cette constante dans $\mathbf{K}$. ■

Remarque : De même que l'on a défini le degré, on pourrait définir la *valuation* d'un polynôme qui correspond à l'indice de son premier coefficient non nul. On obtiendrait alors des propriétés très similaires à celles du degré et on poserait $\text{val}(0) = +\infty$.

D Dérivation formelle

Définition 1.16 *(Polynôme dérivé)*

Soit $P = a_0 + a_1X + a_2X^2 + \cdots + a_{n-1}X^{n-1} + a_nX^n$ un polynôme de $\mathbf{K}[X]$.
On définit le **polynôme dérivé**, P' par

$$P' = a_1 + 2a_2X + \cdots + (n-1)a_{n-1}X^{n-2} + na_nX^{n-1}.$$

Avec les notations des suites :
Si $P = (a_0, a_1, a_2, \cdots, a_{n-1}, a_n, 0, \cdots)$,
alors $P' = (a_1, 2a_2, \cdots, (n-1)a_{n-1}, na_n, 0, 0, \cdots)$.

On définit par récurrence la dérivée n-ième de P par

- $P^{(0)} = P$,
- $\forall n \in \mathbf{N}$, $P^{(n+1)} = (P')^{(n)} = \left(P^{(n)}\right)'$.

Par abus de notation, je m'autoriserai à écrire $0 \times X^{-1} = 0$ étant entendu que l'objet X^{-1} n'existe pas.
Ainsi, cette convention personnelle consiste à tolérer son écriture à condition de le multiplier par 0, et définit un tel objet comme étant le polynôme nul.
Cette petite convention simplifiera les écritures des preuves avec les dérivées.

Remarque : Pour le moment, c'est une dérivation formelle qui n'a aucun lien avec la dérivation d'une fonction. On rappelle que X n'est pas une variable, mais une indéterminée.
⚠ On met l'ordre de dérivation entre parenthèses pour ne pas confondre avec la puissance du polynôme.

Preuve

Il faut montrer la dernière égalité pour la dérivée n-ième sur les polynômes :

$$(P')^{(n)} = \left(P^{(n)}\right)'.$$

On le démontre par récurrence sur $n \in \mathbf{N}$.
Pour $n = 0$, le résultat est trivial.
On le suppose vérifié à un rang $n \in \mathbf{N}$ fixé.
Alors $(P')^{(n+1)} = \left((P')^{(n)}\right)' = \left(P^{(n+1)}\right)'$. ■

Propriété 1.17 *(Propriétés de la dérivation)*

Soient P et Q deux polynômes de $\mathbf{K}[X]$ et $n \in \mathbf{N}$,

1. *(linéarité)* $(\lambda P + Q)^{(n)} = \lambda P^{(n)} + Q^{(n)}$.
2. - si $n \leqslant \deg P$, alors $\deg\left(P^{(n)}\right) = \deg P - n$,
   - si $n > \deg(P)$, alors $P^{(n)} = 0$.

Propriété 1.18 *(Formule de Leibniz)*

Si $(P, Q) \in (\mathbf{K}[X])^2$, alors

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

Pour $n \in \mathbf{N}$, $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)}Q^{(n-k)} = \sum_{k=0}^{n} \binom{n}{k} P^{(n-k)}Q^{(k)}$.

Preuve

Pour $n = 0$, l'égalité est évidente.
Pour $n = 1$: on pose $P = \sum_{k=0}^{+\infty} a_kX^k$ et $Q = \sum_{p=0}^{+\infty} b_pX^p$.

$$PQ = \sum_{k=0}^{+\infty} a_kX^k \sum_{p=0}^{+\infty} b_pX^p = \sum_{k=0}^{+\infty}\sum_{p=0}^{+\infty} a_kb_pX^kX^p.$$

$$\begin{aligned}
(PQ)' &= \sum_{i=0}^{+\infty}\sum_{j=0}^{+\infty} a_ib_j(X^iX^j)' \text{par linéarité} \\
&= \sum_{i=0}^{+\infty}\sum_{j=0}^{+\infty} (i+j)a_ib_jX^{i+j-1} \\
&= \sum_{i=0}^{+\infty}\sum_{j=0}^{+\infty} \Big((ia_iX^{i-1})(b_jX^j) + (a_iX^i)(jb_jX^{j-1})\Big) \\
&= \sum_{i=0}^{+\infty}\sum_{j=0}^{+\infty} (ia_iX^{i-1})(b_jX^j) + \sum_{i=0}^{+\infty}\sum_{j=0}^{+\infty} (a_iX^i)(jb_jX^{j-1}) \\
&= \sum_{i=0}^{+\infty} (ia_iX^{i-1})Q + P\sum_{j=0}^{+\infty} (jb_jX^{j-1}) \\
&= P'Q + PQ'.
\end{aligned}$$

On généralise pour $n \geqslant 1$ par récurrence en écrivant $(PQ)^{(n+1)} = ((PQ)')^{(n)}$ (à faire en exercice). ■

Remarque : En algèbre, un opérateur de dérivation est une application additive (entre des ensembles munis des bonnes structures) qui vérifie l'identité de Leibniz. La dérivation vue jusqu'à présent en est un cas particulier.

Propriété 1.19 *(Dérivée d'une composée)*

Si $(P, Q) \in (\mathbf{K}[X])^2$, alors

$$(P \circ Q)' = Q' \times P' \circ Q.$$

Preuve

Commençons par le montrer par récurrence sur $n \in \mathbf{N}$ pour $P = X^n$.
Pour $n = 0$, on trouve $P \circ Q = 1$, donc $(P \circ Q)' = 0 = Q' \times P' \circ Q$ (car $P' = 0$).

On suppose le résultat vrai à un rang $n \in \mathbf{N}$ fixé.
On pose $P = X^{n+1}$, alors $(P \circ Q)' = \left(Q^{n+1}\right)' = (Q \times Q^n)' = Q' \times Q^n + Q \times (Q^n)' = Q' \times Q^n + Q \times n \times Q'Q^{n-1} = (n+1)Q' \times Q^n$.
Ce qui démontre le résultat.
Pour généraliser à un polynôme P quelconque, il suffit d'utiliser la linéarité. ■

2 Arithmétique sur $\mathbf{K}[X]$

A Division euclidienne

Théorème 2.1 *(Division euclidienne)*

Soient A, B deux polynômes sur $\mathbf{K}$ avec B non nul.
Il existe un unique couple $(Q, R) \in (\mathbf{K}[X])^2$ tel que

- $A = BQ + R$.
- $\deg R < \deg B$.

Preuve

unicité : Si $A = BQ + R$ et $A = BQ' + R'$, avec $\deg R < \deg B$ et $\deg R' < \deg B$.
$B(Q - Q') = R' - R$ donc par égalité des degrés on a nécessairement $\deg(Q - Q') = -\infty$ (sinon le degré du membre de gauche serait strictement supérieur à celui du membre de droite). Donc $Q = Q'$ et $R = R'$.
existence : par récurrence *forte* sur le degré de A.

- *Initialisation :* si $\deg B > \deg A$, on prend $Q = 0$ et $R = A$.
- *Hérédité :* On suppose le résultat vrai au rang n et on considère A de degré $n+1$, avec $n + 1 \geqslant \deg B = p$.
  On écrit $A = a_{n+1}X^{n+1} + a_nX^n + \cdots + a_1X + a_0$ avec $a_{n+1} \neq 0$ et $B = b_pX^p + b_{p-1}X^{p-1} + \cdots + b_1X + b_0$ avec $b_p \neq 0$.
  Alors $A = \frac{a_{n+1}}{b_p}X^{n+1-p}B + A_1$.
  On voit immédiatement que $\deg A_1 \leqslant n$, donc on peut lui appliquer l'hypothèse de récurrence : $A_1 = BQ_1 + R$ avec $\deg R < \deg Q$.
  D'où, $A = BQ + R$ avec $Q = \frac{a_{n+1}}{b_p}X^{n+1-p} + Q_1$.

■

Explications

L'existence de la division euclidienne dans $\mathbf{K}[X]$ permet de définir une arithmétique très proche de celle de $\mathbf{Z}$, avec PGCD, PPCM (non uniques), polynômes premiers entre eux... Quelle joie !
On dit que $\mathbf{K}[X]$ est un anneau euclidien.

Exemple *(Méthode)*

Faire la division euclidienne de $A = 3X^5 + 4X^2 + 1$ par $B = X^2 + 2X + 3$ en utilisant la méthode déployée dans la preuve.

Solution :

On pose la division euclidienne comme au primaire pour les entiers. On écrit alors

$$3X^5 + 4X^2 + 1 \;\big|\; X^2 + 2X + 3$$

On s'intéresse aux coefficients dominants et on voit qu'il faut multiplier X^2 par $3X^3$ pour obtenir $3X^5$.
On obtient alors :

$$\begin{array}{rrrrr|l}
3X^5 & & & +4X^2 & +1 & X^2+2X+3 \\
\cline{6-6}
-(3X^5 & +6X^4 & +9X^3) & & & 3X^3 \\
\cline{1-3}
 & -6X^4 & -9X^3 & +4X^2 & +1 &
\end{array}$$

On continue ainsi : à l'étape suivant, on rajoute $-6X^2$ au quotient pour annuler le terme $-6X^4$ ... et ainsi de suite.

$$\begin{array}{rrrrrrr|l}
3X^5 & & & +4X^2 & & +1 & X^2+2X+3 \\
\cline{7-7}
-(3X^5 & +6X^4 & +9X^3) & & & & 3X^3-6X^2+3X+16 \\
\cline{1-3}
 & -6X^4 & -9X^3 & +4X^2 & & +1 & \\
 & -(-6X^4 & -12X^3 & -18X^2) & & & \\
\cline{2-4}
 & & 3X^3 & +22X^2 & & +1 & \\
 & & -(3X^3 & +6X^2 & +9X) & & \\
\cline{3-5}
 & & & 16X^2 & -9X & +1 & \\
 & & & -(16X^2 & +32X & +48) & \\
\cline{4-6}
 & & & & -41X & -47 &
\end{array}$$

On trouve alors

$$3X^5 + 4X^2 + 1 = \left(X^2 + 2X + 3\right)\left(3X^3 - 6X^2t + 3X + 16\right) - 41X - 47.$$

B Divisibilité

Dès lors qu'on possède la division euclidienne et la relation de divisibilité, on peut construire une arithmétique sur $\mathbf{K}[X]$ à l'instar de ce qui a été fait sur $\mathbf{Z}$.
On va donc faire un gigantesque « copier-coller » à partir du cours d'arithmétique sur $\mathbf{Z}$.
Les preuves sont très similaires au cas entier et il est donc conseillé au lecteur de les rédiger par lui-même en révision du chapitre d'arithmétique sur $\mathbf{Z}$.

Définition 2.2 *(Divisibilité)*

Pour $(A, B) \in (\mathbf{K}[X])^2$, on dit que B **divise** A s'il existe $Q \in \mathbf{K}[X]$ tel que $A = BQ$.
On le note $B|A$.
On dit que aussi que A est **un multiple de** B.

Remarque : B divise A si, et seulement si le reste de la division euclidienne de A par B est nul.

Définition 2.3 *(Polynômes associés)*

Deux polynômes P et Q sont **associés** sur $\mathbf{K}$ si, et seulement s'il existe $\lambda \in \mathbf{K}^*$ tel que $P = \lambda Q$.

Propriété 2.4

$P|Q$ et $Q|P$ si, et seulement si P et Q sont associés.

Preuve

Si $Q = 0$, alors $P = 0$ car $Q|P$ et les polynômes sont bien associés.
Sinon, comme $P|Q$ alors $\deg Q \geqslant \deg P$ (relation sur les degrés pour le produit), et par symétrie, comme $Q|P$, alors $\deg P \geqslant \deg Q$.
Donc P et Q sont de même degré. L'égalité $P = AQ$ donne donc que $\deg A = 0$, c'est-à-dire $A \in \mathbf{K}$: les polynômes sont associés. ■

Propriété 2.5

La relation de divisibilité est réflexive et transitive sur $\mathbf{K}[X]$.
C'est une relation d'ordre (partielle) sur l'ensemble des polynômes *unitaires* ou nuls de $\mathbf{K}[X]$.

Preuve

Réflexivité : immédiat car $P = 1 \times P$.
Transitivité : pas plus dur : si $P|Q$ et $Q|R$ alors il existe des polynômes A et B tels que $Q = AP$ et $R = BQ$, donc $R = ABP$, avec $AB \in \mathbf{K}[X]$. Ainsi $P|R$.
Si on ne considère que les polynômes unitaires ou nuls, la relation est aussi transitive d'après la propriété précédente (les polynômes sont associés, mais le coefficient multiplicateur est nécessairement 1 par égalité des coefficients dominants). ■

Propriété 2.6 *(Propriété de la divisibilité)*

- Si $P|Q_1$ et $P|Q_2$, alors pour tous polynômes U et V, $P|UQ_1 + VQ_2$.
- Si $P_1|Q_1$ et $P_2|Q_2$ alors $P_1P_2|Q_1Q_2$.
- Si $P|Q$ et $n \in \mathbf{N}$, alors $P^n|Q^n$.

Preuve

Immédiat : à faire en exercice. ■

C Algorithme d'Euclide

Définition 2.7 *(Diviseur commun)*

Soient $A_1, A_2, \cdots, A_n$ sont n polynômes non tous nuls.
D est un **diviseur commun** à $A_1, A_2, \cdots, A_n$ s'il divise tous les A_k pour $k \in [\![1, n]\!]$.

Définition 2.8 *(Plus grand diviseur commun)*

Soient A et B deux polynômes non tous les deux nuls.
Un **plus grand diviseur commun** à A et B est un diviseur commun à A et B de degré maximal.
On dit alors que c'est un PGCD de A et B.

⚠ Il y a plusieurs PGCD (contrairement à l'arithmétique dans $\mathbf{Z}$). C'est la raison pour laquelle, on parle d'*un* plus grand diviseur commun et non *du* plus grand diviseur commun.
On va voir que les plus grands diviseurs communs sont associés entre eux.

Preuve

$E = \{\deg D,\ D \in \mathbf{K}[X] \setminus \{0\}$ tel que $D|A,\ D|B\}$ est une partie non vide majorée de $\mathbf{N}$.
En effet, 1 est un diviseur non nul commun à A et B, donc $0 \in E$, et tout diviseur commun à A et B est de degré inférieur[1] à $\max(\deg A, \deg B)$.
Donc E admet un plus grand élément, ce qui prouve l'existence de plus grands diviseurs communs aux $P_1, \cdots, P_n$ au sens de la définition.
Nous verrons plus loin que nous pouvons dire beaucoup plus sur ces diviseurs, mais ce sera plus facile après l'algorithme d'Euclide. ■

Propriété 2.9

Soient A, B deux polynômes non tous les deux nuls, et Q et R dans $\mathbf{K}[X]$ tels que $A = BQ + R$. Alors

Les diviseurs de A et B sont les mêmes que ceux de B et R.

En particulier

A et B ont les mêmes PGCD que B et R.

Preuve

Si $D|A$ et $D|B$ alors $D|A - BQ = R$, donc $D|B$ et $D|R$.
Réciproquement si $D|B$ et $D|R$ alors $D|BQ + R = A$, donc $D|A$ et $D|R$. ■

1. Si A et B sont non nuls, il est inférieurs à chacun de leurs degrés, le fait de considérer le maximum évite de traiter à part le cas où l'un des deux polynômes est nul.

Théorème 2.10 *(Algorithme d'Euclide)*

Soit $(A, B) \in (\mathbf{K}[X] \setminus \{0\})^2$, on note $R_{-1} = A$ et $R_0 = B$, et on définit la suite $(R_n)_{n\in\mathbf{N}}$ par :
$\forall n \in \mathbf{N}$,

- si $R_n \neq 0$, alors R_{n+1} est le reste de la division euclidienne de R_{n-1} par R_n.
- si $R_n = 0$, alors $R_{n+1} = 0$.

La suite est stationnaire à 0.

Ainsi, il existe un rang $n_0 \geqslant 1$ tel que $R_{n_0-1} \neq 0$ et $R_{n_0} = 0$.
On a alors R_{n_0-1} qui est *un* plus grand diviseur commun à A et B.

Preuve

C'est le même raisonnement que pour $\mathbf{Z}$ en observant la décroissance des degrés.
D'après la propriété, on montre par récurrence sur $k \in [\![0, n_0]\!]$ que les diviseurs communs à A et B sont les mêmes que les diviseurs communs à R_{k-1} et R_k (tant que $R_{k-1} \neq 0$, c'est-à-dire $k \leqslant n_0$, sinon R_k n'est plus défini à partir d'une division euclidienne et la propriété précédente ne s'applique plus).
On obtient donc au rang n_0 que A et B ont les mêmes diviseurs que R_{n_0-1} et R_{n_0}.
Or $R_{n_0} = 0$ est divisible par tous les polynômes, donc les diviseurs communs cherchés sont exactement les diviseurs de R_{n_0-1}.
En particulier R_{n_0-1} est un PGCD de A et B. ■

Remarque : On voit que si $\deg A < \deg B$, alors la première étape consiste à échanger A et B.

D PGCD

Théorème 2.11 *(PGCD)*

Soient A et B deux polynômes non tous nuls.

- Tous les plus grands diviseurs communs à A et B sont associés entre eux.
- Il existe un unique diviseur commun **unitaire** que l'on note $A \wedge B$.
- D est un plus grand diviseur commun à A et B si, et seulement si D est un diviseur commun à A et B et si tout diviseur commun à A et B divise également D.
  (les plus grands diviseurs communs sont donc des éléments maximaux pour la relation de divisibilité).

Par convention, $0 \wedge 0 = 0$.

Preuve

- On observe trivialement que si D est un plus grand diviseur commun alors tous les polynômes qui lui sont associés sont aussi plus grands diviseurs communs.
  Réciproquement, si A est un diviseur de degré maximal, nous avons vu, lors de l'algorithme d'Euclide, que $A|R_{n_0-1}$ et qu'il est de même degré.
  Donc A est associé à R_{n_0-1}, ce qui montre bien que tous les plus grands diviseurs sont associés entre eux, et qu'il en existe un unique unitaire.
- Avec l'algorithme d'Euclide, on montre de même que tout diviseur commun à A, B est diviseur de R_{n_0-1}, donc diviseur du PGCD.

■

Propriété 2.12

Soit $(A, B) \in (\mathbf{K}[X])^2$.
Si $A = BQ + R$ avec $(Q, R) \in \mathbf{K}[X] \times \mathbf{K}[X] \setminus \{0\}$, alors $A \wedge B = B \wedge R$.

Théorème 2.13 *(Relation de Bézout)*

Soient A et B deux polynômes non tous les deux nuls,

$$\exists (U, V) \in (\mathbf{K}[X])^2, \ AU + BV = A \wedge B.$$

Preuve

Grâce à l'algorithme d'Euclide étendu comme en arithmétique sur $\mathbf{Z}$. ■

⚠ Les polynômes U et V ne sont pas définis de façon unique.

Définition 2.14 *(Polynômes premiers entre eux)*

Deux polynômes A et B non tous les deux nuls sont dits **premiers entre eux**, si

$$A \wedge B = 1.$$

Propriété 2.15

Deux polynômes sont premiers entre eux si leurs seuls diviseurs communs sont les constantes non nulles.

Exemple

$(X - \alpha)$ est premier avec $X - \beta$ si, et seulement si $\alpha \neq \beta$.
Solution :
Si $\alpha = \beta$, alors $(X - \alpha)$ est un divisieur commun non constant, donc ils ne sont pas premiers entre eux.
Si $\alpha \neq \beta$, alors on note D un diviseur commun à $X - \alpha$ et $X - \beta$.
On peut donc écrire $(X - \alpha) = DQ_1$.
Si par l'absurde D non constant, alors $\deg Q_1 = 0$ donc $X - \alpha$ et D sont associés.
De la même manière $X - \beta$ et D sont aussi associés. On peut donc écrire $D = \lambda(X - \alpha) = \mu(X - \beta)$ avec $(\lambda, \mu) \in \mathbf{K}^2$. Mais par identification des coefficients, la seule solution est alors $\mu = \lambda = 0$. Donc $(X - \alpha) \wedge (X - \beta) = 1$.

Théorème 2.16 *(Théorème de Bézout)*

Soient A et B deux polynômes non tous les deux nuls,

$$A \wedge B = 1 \iff \exists (U, V) \in (\mathbf{K}[X])^2,\ AU + BV = 1.$$

Définition 2.17

Soient $P_1, P_2, \cdots, P_n$, n polynômes non nuls.

- $P_1, P_2, \cdots, P_n$ sont premiers entre eux **deux à deux** si
$$\forall (i, j) \in [\![1, n]\!]^2,\ i \neq j \Rightarrow P_i \wedge P_j = 1.$$
- $P_1, P_2, \cdots, P_n$ sont premiers entre eux **dans leur ensemble** si leurs seuls diviseurs communs sont les constantes non nulles.

Définition 2.18 *(PGCD d'une famille de polynômes)*

Soient $(A_1, A_2, \cdots, A_n)$, n polynômes non tous nuls.

1. Tout diviseur commun à $A_1, \cdots, A_n$ de degré maximal est appelé **plus grand diviseur commun.**
Il existe un plus grand diviseur commun unitaire appelé le PGCD et noté $A_1 \wedge A_2 \wedge \cdots \wedge A_n$.
2. L'ensemble des plus grands diviseurs communs est l'ensemble des polynômes associés au PGCD.
3. D est un plus grand diviseur commun à $A_1, \cdots, A_n$ si, et seulement si
   - D est un diviseur commun à $A_1, \cdots, A_n$.
   - Tout diviseur commun à $A_1, \cdots, A_n$ est également diviseur de D.

Remarque : Des polynômes sont premiers entre eux *dans leur ensemble* si, et seulement si leur PGCD est égal à 1.

Preuve

On utilise la preuve dite « *plus algébrique* » dans le cours d'arithmétique sur $\mathbf{Z}$. L'approche est moins naturelle, mais plus simple à conduire. Elle part de la relation de Bézout au lieu de la voir comme conséquence.
On note

$$\begin{aligned} E &= A_1\mathbf{K}[X] + A_2\mathbf{K}[X] + \cdots + A_n\mathbf{K}[X] \\ &= \{A_1U_1 + A_2U_2 + \cdots + A_nU_n,\ (U_1, U_2, \cdots, U_n) \in (\mathbf{K}[X])^n\}. \end{aligned}$$

E est non vide et $\{\deg P,\ P \in E \setminus \{0\}\}$ est une partie non vide de $\mathbf{N}$ qui admet donc un plus petit élément.
Soit $D \in E$ de degré égal à ce minimum, que l'on peut choisir unitaire.

- Montrons que D est un diviseur commun à tous les éléments de E.
Soit $i \in [\![1, n]\!]$, on peut alors réaliser la division euclidienne $A_i = DQ_i + R_i$ avec $\deg R_i < \deg D$.
Mais en utilisant la définition de E, on voit immédiatement que $R_i \in E$.
Par minimalité du degré de D, on a donc $R_i = 0$, donc D divise A_i.
Donc D est un diviseur commun à $A_1, \cdots, A_n$.
- Montrons que tout diviseur commun est diviseur de D.
C'est évident, car si $P|A_1$, $P|A_2$, $\cdots$, $P|A_n$ alors pour tous polynômes $U_1, U_2, \cdots, U_n$, $P|A_1U_1 + A_2U_2 + \cdots + A_nU_n$.
Donc P divise tous les éléments de E, donc $P|D$.
Ceci montre en particulier que D est un diviseur commun de degré maximal (la divisibilité donne l'inégalité des degrés).
Il est évident que si D est un plus grand diviseur commun, alors tous les polynômes qui lui sont associés, le sont aussi. Il existe donc un plus grand diviseur commun unitaire.
- *Unicité du* PGCD *:* Si D_1 et D_2 convenaient, alors on vient de voir que $D_1|D_2$ et $D_2|D_1$ par symétrie des rôles, donc D_1 et D_2 associés.
Or comme ils sont supposés unitaires, ils sont égaux.

■

Propriété 2.19 *(Relation de Bézout)*

Soient $(A_1, A_2, \cdots, A_n)$, n polynômes non tous nuls.
Il existe $(U_1, U_2, \cdots., U_n) \in (\mathbf{K}[X])^n$ tel que

$$\sum_{k=1}^{n} A_kU_k = A_1 \wedge \cdots \wedge A_n.$$

Preuve

Directement à partir de la preuve précédente. ■

E PPCM

Définition 2.20 *(PPCM)*

Soient $A_1, A_2, \cdots, A_n$, n polynômes.
M est un **multiple commun** à $A_1, A_2, \cdots, A_n$ s'il est multiple de tous les A_k pour $k \in [\![1, n]\!]$.

La preuve pour les plus petits communs multiples pour deux ou davantage de polynômes est strictement identique.
Aussi, pour ne pas surcharger inutilement ce cours, nous donnons directement le théorème et la preuve pour $n \geqslant 2$ polynômes.

Définition 2.21 *(PPCM d'une famille de polynômes)*

Soient $(A_1, A_2, \cdots, A_n)$, n polynômes

1. Tout multiple commun à $A_1, \cdots, A_n$ de degré entier minimal est appelé **plus petit multiple commun**
   (et s'il n'existe pas, le polynôme nul).
   Il existe un plus petit multiple commun unitaire ou nul appelé le PPCM et noté $A_1 \vee A_2 \vee \cdots \vee A_n$.
2. L'ensemble des plus petits multiples communs est l'ensemble des polynômes associés au PPCM.
3. M est un plus petit multiple commun à $A_1, \cdots, A_n$ si, et seulement si
   - M est un multiple commun à $A_1, \cdots, A_n$.
   - Tout multiple commun à $A_1, \cdots, A_n$ est également multiple de M.

Preuve

On suppose tous les A_i non nuls.
On considère l'ensemble $E = A_1\mathbf{K}[X] \cap A_2\mathbf{K}[X] \cap \cdots \cap A_n\mathbf{K}[X]$.
E désigne l'ensemble des multiples communs à $A_1, \cdots, A_n$.
E est non vide et non réduit à 0 (il contient le produit des A_i).
Soit M un polynôme de E de degré entier minimal (l'existence est immédiate).
Alors M est un multiple commun à $A_1, \cdots, A_n$. Tous ses polynômes associés sont aussi dans E, donc on peut choisir M unitaire.
Soit P un autre multiple commun. On effectue la division euclidienne $P = MQ + R$ avec $\deg R < \deg M$.
P et M étant multiples communs, R l'est aussi.
Mais par minimalité du degré de M, on a donc $R = 0$.
Donc P est multiple de M. ■

Propriété 2.22 *(Propriétés du PGCD et du PPCM)*

Si A et B sont deux polynômes non tous les deux nuls, alors

1. (commutativité)
$$A \wedge B = B \wedge A \quad \text{et} \quad A \vee B = B \vee A.$$
2. (insensible au produit par un facteur non nul) $\forall \lambda \in \mathbf{K}^*$,
$$(\lambda A) \wedge B = A \wedge B \quad \text{et} \quad (\lambda A) \vee B = A \vee B.$$

F Polynômes irréductibles

Définition 2.23

Un polynôme **non constant** est dit **irréductible** si ses seuls diviseurs sont ses polynômes associés et les constantes.

Remarque : Les polynômes constants ne sont pas irréductibles.
Nous verrons que l'irréductibilité d'un polynôme peut dépendre du corps $\mathbf{K}$ choisi.

Théorème 2.24 *(Lemme de Gauss)*

Soit $(A, B, C) \in (\mathbf{K}[X] \setminus \{0\})^3$.

$$\text{Si } A|BC \text{ et } A \wedge C = 1, \text{ alors } A|B.$$

Preuve

En utilisant Bézout comme dans $\mathbf{Z}$. ■

Théorème 2.25

Soit $(P_1, P_2, A) \in (\mathbf{K}[X] \setminus \{0\})^3$. Si $P_1|A$, $P_2|A$ et si $P_1 \wedge P_2 = 1$, alors $P_1P_2|A$.

Preuve

Avec Bézout $P_1U + P_2V = 1$, donc $P_1AU + P_2AV = A$.
Or, $P_1Q_1 = A$ et $P_2Q_2 = A$, donc en remplaçant on trouve

$$P_1P_2Q_2U + P_1P_2Q_1V = A.$$

ce qui donne le résultat voulu. ■

Théorème 2.26 *(Décomposition en produit d'irréductibles)*

Tout polynôme non nul de $\mathbf{K}[X]$ s'écrit de manière unique (à l'ordre près) comme produit d'irréductibles **unitaires** et d'une constante.

$$P = \lambda \prod_{i=0}^{k} Q_i$$

avec $\lambda \in \mathbf{K}^*$ et les Q_i sont des polynômes irréductibles unitaires.

Remarque : La caractère unitaire des polynômes permet d'avoir l'unicité.

Preuve

unicité : On suppose deux décompositions

$$\lambda_1 \prod_{i=0}^{k} Q_i = \lambda_2 \prod_{j=0}^{p} P_j.$$

On peut simplifier les Q_i et les P_j qui sont commun.

Soit Q_i dans la décomposition. Alors Q_i divise $\lambda_2 \prod_{j=0}^{p} P_j$.

Or, il est immédiat que pour tout $j \in [\![0, p]\!]$, $Q_i \wedge P_j = 1$ (s'ils avaient un diviseur commun de degré supérieur ou égal à 1, alors ce ne pourrait être que P_j car irréductible, et aussi Q_i car irréductible. C'est impossible car ils sont unitaires et différents).
Ainsi, par application successive du lemme de Gauss, $Q_i | \lambda_2$ ce qui est absurde.
Donc la décomposition est unique.
existence : On montre l'existence par récurrence (forte) sur le degré de P.
Pour $\deg P = 0$, le résultat est trivial.
On suppose le résultat vérifié pour $\deg P \leqslant n$.
Si $\deg P = n+1$.

- Soit P est irréductible et le théorème est vérifié.
- Soit P n'est pas irréductible et il existe Q_1 et Q_2 dans $\mathbf{K}[x]$ de degré supérieur à 1 tels que $P = Q_1 Q_2$.
  Alors $\deg Q_1 \leqslant n$ et $\deg Q_2 \leqslant n$ (d'après la formule du degré d'un produit).
  Donc Q_1 et Q_2 se décomposent comme produit d'irréductibles sur $\mathbf{K}[X]$.
  Donc P également.

■

Exemple

Donner la décomposition en produit d'irréductibles de $P = 2X^5 - 2X^4$.

3 Fonctions polynomiales

Définition 3.1

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbf{K}[X]$.
On appelle **application polynomiale** associée à P, l'application :

$$\widetilde{P} : \left\{ \begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{K} \\ x & \mapsto & \sum_{k=0}^{n} a_k x^k. \end{array} \right.$$

Remarque : Par abus de langage, on confond parfois polynôme et fonction polynomiale mais il faut comprendre la différence entre ces deux objets.

Propriété 3.2

Pour tous polynômes P et Q de $\mathbf{K}[X]$, et pour tout $\lambda \in \mathbf{K}$
$\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}$,
$\widetilde{\lambda P} = \lambda \widetilde{P}$,
$\widetilde{P \times Q} = \widetilde{P} \times \widetilde{Q}$,
$\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$,
$\widetilde{P'} = \widetilde{P}'$.

Remarque : dans la suite, on omettra généralement le signe « tilde » et on identifera P et $\widetilde{P}$: le contexte indiquera s'il s'agit du polynôme ou de la fonction polynomiale associée.
Un tel abus de notation sera mieux légitimé lors de l'expression du lien bijectif entre polynômes et fonctions polynomiales, plus loin dans ce chapitre.

4 Racines

A Racines et factorisation

Théorème 4.1 *(Formule de Taylor)*

Soit $P \in \mathbf{K}[X]$ et $\alpha \in \mathbf{K}$,

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

La somme est finie et s'arrête au coefficient égal au degré de P.

Remarque : α est quelconque, ce n'est pas nécessairement une racine de P.

Preuve

On procède par récurrence sur le degré du polynôme.
Pour P constant, la relation est immédiate.
On suppose la relation au rang $n \in \mathbf{N}$, et on la montre au rang $n+1$.
On considère donc P de degré $n+1$ et on pose $Q = P - \sum_{k=0}^{n+1} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k$.

$$Q' = P' - \sum_{k=1}^{n+1} \frac{P^k(\alpha)}{(k-1)!}(X-\alpha)^{k-1}.$$

Or $\deg P' = n$, donc on peut lui appliquer l'hypothèse de récurrence ce qui donne

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

Ainsi, on retrouve l'expression précédente et on a donc $Q' = 0$.
Donc Q est constant, et vaut $Q(\alpha) = P(\alpha) - P(\alpha) = 0$. Ceci montre la relation au rang $n+1$. ■

Propriété 4.2 *(Unicité de la décomposition)*

La décomposition pour la formule de Taylor est unique.
Si $\alpha \in \mathbf{K}$ et $P \in \mathbf{K}[X]$ tel que $P = \sum_{k=0}^{+\infty} a_k (X-\alpha)^k$, alors $\forall k \in \mathbf{N}$, $P^{(k)}(\alpha) = k! a_k$.

Preuve

On remarque que $P(X+\alpha) = \sum_{k=0}^{+\infty} a_k X^k$ et on utilise l'unicité de la décomposition sur la famille $(X^k)_{k \in \mathbf{N}}$ (principe d'identification). ■

Définition 4.3 *(Racine d'un polynôme)*

On dit que $\alpha \in \mathbf{K}$ est une **racine** de P si, et seulement si $\widetilde{P}(\alpha) = 0$.

Lemme 4.4

Pour $P \in \mathbf{K}[X]$ et $\alpha \in \mathbf{K}$,
le reste de la division euclidienne de P par $X - \alpha$ est $P(\alpha)$.

Preuve

On réalise la division euclidienne : $P = (X-\alpha)Q + R$ avec $\deg R < 1$, donc $R \in \mathbf{K}$.
En évaluant en α on trouve alors $R = P(\alpha)$. ■

Théorème 4.5 *(Lien entre racines et factorisation)*

α est une racine de P sur $\mathbf{K}$ si, et seulement si $X - \alpha$ divise P.

Preuve

(sens réciproque) si $(X-\alpha)$ divise P, alors $P = (X-\alpha)Q$.
Donc $\widetilde{P}(\alpha) = 0 \times \widetilde{Q}(\alpha) = 0$.
(sens direct) d'après le lemme. ■

Explications

Trouver les racines d'un polynôme sur $\mathbf{K}$ ou le factoriser revient au même. Si on trouve des racines évidentes d'un polynôme, cela donne une factorisation. Nous avons déjà utilisé cette méthode.

Exemple

Factoriser $P = X^4 - 2X^3 - 16X^2 + 2X + 15$.
Solution :
1 est racine évidente, donc on peut factoriser par $X - 1$:

$$P = (X-1)(X^3 - X^2 - 17X - 15)$$

-1 est racine évidente, donc on peut factoriser par $X + 1$:

$$P = (X-1)(X+1)(X^2 - 2X - 15).$$

On trouve ensuite deux racines -3 et 5 soit par essais, soit avec le calcul du discriminant Δ. Donc $P = (X-1)(X+1)(X+3)(X-5)$.

Définition 4.6 *(Multiplicité d'une racine)*

Si α est racine de P, alors sa **multiplicité** est égale au plus grand entier m tel que

$$P(\alpha) = P'(\alpha) = \ldots = P^{(m-1)}(\alpha) = 0.$$

Par abus, si $P(\alpha) \neq 0$, on dit que α est racine de multiplicité 0.

Remarque : m est le plus grand entier, ce qui suppose que $P^{(m)}(\alpha) \neq 0$.

Exemple

Pour un polynôme du second degré, on a une racine double α lorsque $\Delta = 0$.
Dans ce cas, on a bien $P(\alpha) = P'(\alpha) = 0$, et $P''(\alpha) \neq 0$.
En effet, la courbe est tangente à l'axe des abscisses en α. Elle s'annule donc en α et sa dérivée est nulle en ce point (minimum avec tangente horizontale).

Théorème 4.7 *(Racine multiple et factorisation)*

α est une racine de P de multiplicité m sur $\mathbf{K}$ si, et seulement si $(X-\alpha)^m$ divise P et $(X-\alpha)^{m+1}$ ne divise pas P.

Preuve

On applique la formule de Taylor à P en α et on l'interprète comme une division euclidienne :

$$\begin{aligned} P &= \sum_{k=0}^{+\infty} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k \\ &= \sum_{k=0}^{m-1} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k + \sum_{k=m}^{+\infty} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k \\ &= \underbrace{\sum_{k=0}^{m-1} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k}_{R_0} + (X-\alpha)^m \underbrace{\sum_{k=m}^{+\infty} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^{\overbrace{k-m}^{\geqslant 0}}}_{Q_0}. \end{aligned}$$

Et au rang m, on trouve aussi

$$P = \underbrace{\sum_{k=0}^{m} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k}_{R_1} + (X-\alpha)^{m+1} \underbrace{\sum_{k=m+1}^{+\infty} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^{\overbrace{k-m-1}^{\geqslant 0}}}_{Q_1}.$$

Par unicité de la division euclidienne, on voit que R_0 et R_1 sont respectivement les restes des divisions euclidiennes de P par $(X-\alpha)^m$ et par $(X-\alpha)^{m+1}$.
On peut alors écrire

$$\begin{aligned} \alpha \text{ racine de multiplicité } m &\iff \begin{cases} \forall k \in [\![0, m-1]\!],\ P^{(k)}(\alpha) = 0 \\ P^{(m)}(\alpha) \neq 0, \end{cases} \\ &\iff \begin{cases} R_0 = 0 \\ R_1 \neq 0, \end{cases} \\ &\iff \begin{cases} (X-\alpha)^m | P \\ (X-\alpha)^{m+1} \not| P \end{cases} \end{aligned}$$

La première équivalence (sens réciproque) provient de l'unicité de la décomposition en somme de Taylor énoncée au théorème 4.2.
La somme R_0 est nulle si, et seulement si $\forall k \in [\![0, m-1]\!]$, $P^{(k)}(\alpha) = 0$. ■

Exemple

0 est racine triple (de multiplicité 3) de $X^7 - 3X^5 + 2X^4 - X^3$.

Propriété 4.8

Soit $P \in \mathbf{K}[X]$, alors si $\alpha_1, \alpha_1, \cdots, \alpha_n$ sont n racines distinctes de P de multiplicités $m_1, m_2, \cdots, m_n$, alors

$$P \quad \text{divisible par} \quad (X-\alpha_1)^{m_1}(X-\alpha_2)^{m_2}\cdots(X-\alpha_n)^{m_n}.$$

Preuve

Par récurrence sur n.
Pour passer de n à $n+1$, on utilise le fait que $(X-\alpha_1)^{m_1}\cdots(X-\alpha_n)^{m_n}$ est premier avec $(X-\alpha_{n+1})^{m_{n+1}}$ et le théorème 2.25. ■

Corollaire 4.9

Le nombre de racines (comptées avec leur multiplicité) d'un polynôme non nul est inférieur ou égal à son degré.
Seul le polynôme nul admet une infinité de racines.

Explications

Ce théorème n'affirme pas qu'il existe autant de racines que le degré (c'est vrai sur $\mathbf{C}$ comme le donnera le théorème de d'Alembert-Gauss, mais en général faux sur $\mathbf{R}$).
Il donne simplement un majorant du nombre de racines.
Cependant, si on obtient autant de racines que le degré, cela permet d'affirmer, sans autres vérifications, qu'on les a toutes trouvées.

Exemple *(Rappel)*

Factoriser $X^n - 1$ sur $\mathbf{C}$.
Solution :
La factorisation revient à chercher les solutions de l'équation $x^n = 1$.
On retrouve les racines n-i èmes de l'unité :

$$\left\{ \mathrm{e}^{\frac{2ik\pi}{n}},\ k \in [\![0,\ n-1]\!] \right\}.$$

Ces racines sont deux à deux distinctes et il y en a autant que le degré, donc ce sont les seules.
Comme le coefficient dominant est 1, on obtient donc :

$$X^n - 1 = \sum_{k=0}^{n-1} \left(X - \mathrm{e}^{\frac{2ik\pi}{n}} \right).$$

Méthode *(Montrer qu'un polynôme est nul)*

Pour montrer qu'un polynôme est nul, on peut au choix :

1. montrer que tous ses coefficients sont nuls,
2. montrer qu'il admet une infinité de racines,
3. montrer qu'il admet plus de racines que son degré,
4. montrer que son degré ne peut être un nombre entier.

$\Rightarrow$ on raisonne souvent par l'absurde pour montrer qu'un polynôme est nul.

Exemple

Soient $\widetilde{P}$ et $\widetilde{Q}$ deux applications polynomiales.
S'il existe $x \in \mathbf{R}$ tel que $\widetilde{P}(x) = \widetilde{Q}(x)$, cela entraîne-t-il que $P = Q$?
S'il existe $a < b$ tels que $\forall x \in]a, b[,\ \widetilde{P}(x) = \widetilde{Q}(x)$, cela entraîne-t-il que $P = Q$?

Théorème 4.10 *(Lien bijectif entre les polynômes et les applications polynomiales)*

L'application

$$\phi \left\{ \begin{array}{ccc} \mathbf{K}[X] & \longrightarrow & \mathcal{P}(\mathbf{K}) \\ P & \mapsto & \widetilde{P} \end{array} \right.$$

réalise une **bijection** entre entre $\mathbf{K}[X]$ et l'ensemble des fonctions polynomiales sur $\mathbf{K}$.
Cette application est un morphisme pour les lois $+$, $\times$, $\cdot$, $\circ$ et pour l'opérateur de dérivation :

- $\phi(P+Q) = \phi(P) + \phi(Q)$,
- $\phi(P \times Q) = \phi(P) \times \phi(Q)$,
- $\phi(\lambda P) = \lambda \phi(P)$,
- $\phi(P \circ Q) = \phi(P) \circ \phi(Q)$,
- $\phi(P') = (\phi(P))'$.

Explications

C'est un THÉORÈME CLEF. C'est lui qui permet de faire le lien entre les polynômes et les applications polynomiales, c'est-à-dire entre l'algèbre et l'analyse.
Il justifie que l'on peut utiliser l'analyse pour démontrer des résultats d'algèbre et réciproquement.

Preuve

Surjectivité : trivial du fait de la définition de $\mathcal{P}(\mathbf{K})$.
Injectivité : la différence des deux polynômes antécédents a une infinité de racines. Donc elle est nulle. Donc chaque application polynomiale a un unique antécédent. ■

Propriété 4.11

Un polynôme est pair si, et seulement si sa fonction polynomiale est paire.
Un polynôme est impair si, et seulement si sa fonction polynomiale est impaire.

Preuve

Le sens direct est évident. Montrons le sens réciproque pour le cas pair.
Si on note $P = \sum_{k=0}^{+\infty} a_k X^k$ alors pour tout $x \in \mathbf{R}$ $P(x) = P(-x)$, ainsi $P(X) - P(-X)$ admet une infinité de racines donc est le polynôme nul.
On obtient donc $P(X) = P(-X)$ c'est-à-dire

$$\sum_{k=0}^{+\infty} a_k X^k = \sum_{k=0}^{n} (-1)^k a_k X^k.$$

Donc par identification :

$$\forall k \in 2\mathbf{N}+1,\ a_k = 0.$$

■

Exemple *(Algorithme de Horner)*

Soit $P = \sum_{k=0}^{n} a_k X^k$. Pour évaluer $P(x)$, on peut calculer simplement $P = \sum_{k=0}^{n} a_k x^k$, mais cela demande de calculer toutes les puissances de x et s'avère rarement optimal.
Horner a proposé une autre méthode qui s'appuie sur l'idée selon laquelle on peut calculer les puissances de x, non séparément, mais en s'utilisant à chaque fois de la puissance précédente.
Prenons un exemple :
Pour $3x^2 - 2x + 4$, on peut faire $3x - 2$, puis on multiplie par x et on ajoute 4, ce qui donne $(3x-2)\,x + 4$, ce qui est le résultat voulu.
Plus généralement pour P, on calcule

$$\begin{aligned} b_{n-1} &= a_n x + a_{n-1} \\ b_{n-2} &= b_{n-1} x + a_{n-2} \\ b_{n-3} &= b_{n-2} x + a_{n-3} \\ &\vdots \\ b_0 &= b_1 x + a_0 \end{aligned}$$

On a alors $b_0 = P(x)$.

B Théorème de d'Alembert-Gauss

Définition 4.12 *(Polynôme scindé)*

Un polynôme est **scindé** s'il peut s'écrire comme produit de polynômes unitaires de degré 1 et d'un coefficient constant.

$$P = \lambda \prod_{i=0}^{p} (X - \alpha_i)^{m_i}.$$

Remarque : Les polynômes constants sont scindés.

Théorème 4.13 *(d'Alembert-Gauss - Théorème fondamental de l'algèbre)*

Tout polynôme est scindé sur $\mathbf{C}$.

Autre formulation : Tout polynôme non constant admet au moins une racine sur $\mathbf{C}$.
Autre formulation : Les seuls polynômes irréductibles sur $\mathbf{C}$ sont les polynômes de degré 1.

Preuve

Admis - curieusement pour démontrer le théorème fondamental de l'algèbre, on a besoin de l'analyse. ■

⚠ C'est faux sur $\mathbf{R}[X]$, par exemple $X^2 + 1$ est irréductible sur $\mathbf{R}$, mais pas sur $\mathbf{C}$.

C Polynômes interpolateurs de Lagrange

Dans cette partie, il est important non seulement de connaître les résultats, mais de savoir les retrouver.

Notation *(Symbole de Krönecker)*

On définit le symbole de Krönecker par :

$$\forall (i,j) \in \mathbf{N}^2,\ \delta_{i,j} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon.} \end{cases}$$

Propriété 4.14 *(Polynômes interpolateurs de Lagrange)*

Soient $n \in \mathbf{N}$, $(x_1, x_2, \cdots, x_n) \in \mathbf{K}^n$ deux à deux **distincts**.
Pour tout $j \in [\![1, n]\!]$, il existe un unique polynôme $L_j \in \mathbf{K}_{n-1}[X]$ tel que

$$\forall i \in [\![1, n]\!],\ L_j(x_i) = \delta_{i,j}.$$

L_j est le j-ième **polynôme interpolateur de Lagrange.**

Preuve

Analyse : unicité.
Soit P un tel polynôme, alors, il admet $n-1$ racines : $\{x_i,\, i \neq j\}$.
Donc il est divisible par $\prod_{i\neq j}(X-x_i)$ (les x_i sont deux à deux distincts).
On peut donc écrire $P = Q\prod_{i\neq j}(X-x_i)$ avec $Q \in \mathbf{K}[X]$.
Mais $\deg P \leqslant n-1$, donc Q est une constante.
Or $P(x_j)=1$, donc cette constante est égale à $\frac{1}{\prod_{i\neq j} x_j - x_i}$.
Si le polynôme existe, alors il est défini de façon unique et son expression est

$$L_j = \prod_{i\neq j}\frac{X-x_i}{x_j-x_i}.$$

Synthèse : réciproquement, il est évident qu'un tel polynôme convient. ■

Propriété 4.15

Avec les notations précédentes :

$$\forall i \in [\![1,\, n]\!],\ L_j = \prod_{i\neq j}\frac{X-x_i}{x_j-x_i} \quad \text{et} \quad \sum_{j=1}^{n} L_j = 1.$$

Preuve

L'expression de L_j a été obtenue à la preuve précédente.
Si on note $P = \sum_{j=1}^{n} L_j - 1$, alors $\deg P \leqslant n-1$, et $\forall j \in [\![1,\, n]\!]$, $P(x_j)=0$.
Donc P admet au moins n racines distinctes, donc P est le polynôme nul. ■

Théorème 4.16

Soient $n \in \mathbf{N}$, $(x_1, x_2, \cdots, x_n) \in \mathbf{K}^n$ deux à deux distincts.
Soit $(y_1,\, y_2,\, \cdots,\, y_n) \in \mathbf{K}^n$.
Il existe un unique polynôme $P \in \mathbf{K}_{n-1}[X]$ tel que

$$\forall i \in [\![1,\, n]\!],\ P(x_i) = y_i.$$

Ce polynôme est donné par

$$P = \sum_{j=1}^{n} y_j L_j.$$

Preuve *(à savoir refaire)*

Unicité : Si on considère deux polynômes vérifiant les hypothèses : P et Q, alors $P-Q$ admet n racines distinctes (les x_i) et est de degré inférieur ou égal à $n-1$.
Donc c'est le polynôme nul, donc $P=Q$, d'où l'unicité.
Existence : On voit directement que l'expression donnée dans le théorème convient.
■

Propriété 4.17

Avec les notations précédentes, tout polynôme $P \in \mathbf{K}_{n-1}[X]$ se décompose de façon unique comme *combinaison linéaire* des L_j.

$$\forall P \in \mathbf{K}_{n-1}[X],\ \exists!(\alpha_1,\, \alpha_2,\, \cdots,\, \alpha_n) \in \mathbf{K}^n,\ P = \sum_{j=1}^{n}\alpha_j L_j.$$

Preuve

Unicité : On suppose que P s'écrit sous deux formes avec $(\alpha_1,\, \cdots,\, \alpha_n) \in \mathbf{K}^n$ et $(\beta_1,\, \cdots,\, \beta_n) \in \mathbf{K}^n$.
alors

$$\sum_{i=1}^{n}\alpha_i L_i = \sum_{i=1}^{n}\beta_i L_i.$$

En particulier, si on évalue en x_j on trouve $\alpha_j = \beta_j$.
Ceci étant pour tous les $j \in [\![1,\, n]\!]$, on a $\forall j \in [\![1,\, n]\!]$, $\alpha_j = \beta_j$, d'où l'unicité de l'écriture.
Existence : Si on note pour tout $j \in [\![1,\, n]\!]$, $y_j = P(x_i)$, alors le théorème précédent permet de trouver la forme qui convient :

$$P = \sum_{j=1}^{n} P(x_j) L_j.$$

■

On verra plus tard que l'on dit que les polynômes de Lagrange forment une *base* de $\mathbf{K}_{n-1}[X]$.

Théorème 4.18 *(Cas général)*

Soient $n \in \mathbf{N}$, $(x_1, x_2, \cdots, x_n) \in \mathbf{K}^n$ deux à deux distincts.
Soit $(y_1,\, y_2,\, \cdots,\, y_n) \in \mathbf{K}^n$.
Les polynômes $P \in \mathbf{K}[X]$ vérifiant $\forall i \in [\![1,\, n]\!]$, $P(x_i) = y_i$, sont exactement les polynômes

$$P = \sum_{j=1}^{n} y_j L_j + Q\prod_{j=1}^{n}(X-x_j),$$

pour Q décrivant $\mathbf{K}[X]$.

Preuve

Il est évident que les polynômes donnés conviennent. Montrons que ce sont les seuls.
Si on note P un tel polynôme, alors $P - \sum_{j=1}^{n} y_j L_j$ s'annule en tous les x_j, donc est divisible par $\prod_{j=1}^{n}(X-x_j)$ ce qui donne bien la forme voulue. ■

D Polynômes réels

Propriété 4.19

Soit $(A,\, B) \in \mathbf{R}[X]$ avec B non nul.
Le quotient et le reste de la division euclidienne de A par B est le même dans $\mathbf{C}[X]$ et dans $\mathbf{R}[X]$.

Preuve

Par unicité de la division euclidienne dans $\mathbf{C}$. ■

Propriété 4.20

Si $(A,\, B) \in \mathbf{R}[X]$, tous deux non nuls.
$A|B$ dans $\mathbf{R}[X]$ si, et seulement si $A|B$ dans $\mathbf{C}[X]$.

Preuve

Utiliser l'unicité de la division euclidienne. ■

Propriété 4.21

Le PGCD et le PPCM de deux polynômes réels sont les mêmes dans $\mathbf{R}[X]$ et dans $\mathbf{C}[X]$.

Preuve

D'après la propriété précédente. ■

Propriété 4.22

Les racines complexes d'un polynôme de $\mathbf{R}[X]$ sont conjuguées, et si α est racine de P, alors $\overline{\alpha}$ est aussi racine de P avec la *même multiplicité.*

Preuve

P est scindé sur $\mathbf{C}$:

$$P = \lambda \prod_{i=0}^{p} (X-\alpha_i)^{m_i}$$

Or, P est à coefficients réels, donc il est égal à son conjugué. Donc

$$\begin{aligned} P &= \overline{P} \\ &= \overline{\lambda \prod_{i=0}^{p} (X-\alpha_i)^{m_i}} \\ &= \overline{\lambda} \prod_{i=0}^{p} \overline{(X-\alpha_i)^{m_i}} \\ &= \overline{\lambda} \prod_{i=0}^{p} (X-\overline{\alpha_i})^{m_i} \end{aligned}$$

Donc

$$\lambda \prod_{i=0}^{p} (X-\alpha_i)^{m_i} = \overline{\lambda} \prod_{i=0}^{p} (X-\overline{\alpha_i})^{m_i}$$

Donc par unicité de la décomposition, pour chaque i, il existe j tel que $\alpha_i = \overline{\alpha_j}$. ■

Théorème 4.23 *(Irréductibles sur $\mathbf{R}$)*

Les polynômes irréductibles sur $\mathbf{R}$ sont

- les polynômes de degré 1,
- les polynômes de degré 2 à discriminant négatif.

Preuve

On décompose le polynôme sur $\mathbf{C}$.
On regroupe les racines complexes conjuguées : cela donne un produit de monômes (racines réelles) et de polynômes de degré 2 (racines complexes conjuguées). ■

Méthode

Pour décomposer un polynôme dans $\mathbf{R}[X]$, on peut déjà le décomposer dans $\mathbf{C}[X]$.

⚠ Ce n'est pas parce qu'un polynôme n'a pas de racines qu'il est irréductible.

Exemple

Par exemple $X^4+1 = (X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)$ (obtenu avec les racines nièmes de l'unité).

E Complément : relations coefficients-racines

Ce théorème n'est pas à apprendre par cœur. Vous devez le « voir » sur le polynôme.

Théorème 4.24 *(Relation coefficients-racines)*

Si P un polynôme **scindé** sur $\mathbf{K}$ et de degré $n \geqslant 1$:

$$P = \sum_{k=0}^{n} a_k X^k = a_n \prod_{i=1}^{n} (X-\alpha_i),$$

alors

$$\sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n} \qquad \text{et} \qquad \prod_{i=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}.$$

⚠ Le polynôme est supposé scindé.

Preuve

Il suffit de développer le polynôme scindé et de chercher le coefficient de X^0 et celui de X^{n-1}. ■

Exemple *(Cas des polynômes de degrés 2 et 3)*

Si $P=(X-\alpha)(X-\beta)$, alors $P=X^2-(\alpha+\beta)X+\alpha\beta$.
C'est-à-dire $a_1=-(\alpha+\beta)$ et $a_0=\alpha\beta$.
Si $P=(X-\alpha)(X-\beta)(X-\gamma)$, alors $P=X^3+(\alpha+\beta+\gamma)X^2+a_1X-\alpha\beta\gamma$. Le coefficient a_1 est égal à $\alpha\beta+\alpha\gamma+\beta\gamma$.

Explications

Vous remarquerez les valeurs des coefficients ne dépendent pas de l'ordre des racines (on peut intervertir α et γ par exemple). Heureusement.
De même que l'on a donné ici l'expression de a_1, on peut donner une forme générale du coefficient a_k en fonction des racines. On obtient une relation de type polynômiale, si ce n'est que chaque racine correspond à une indéterminée. Ce sont les polynômes à plusieurs variables. Ici, comme les indéterminées (ou variables) peuvent être interverties ont dit que les polynômes sont symétriques.

Méthode

Lorsque l'on connaît une racine d'un polynôme de degré 2, il est facile d'obtenir la seconde à partir des coefficients.