LES POLYNÔMES

Dans ce chapitre $\mathbb{K}$ *est un corps comme* $\mathbb{Q}$, $\mathbb{R}$ *ou* $\mathbb{C}$, $(a,b,\lambda)\in\mathbb{K}^3$ *et* $(k,m,n)\in\mathbb{N}^3$.

Opérations sur les polynômes

Définition de l'anneau des polynômes

• Un polynôme P de variable X à coefficients dans $\mathbb{K}$ est une combinaison linéaire de monômes X^k de degré $k\leq n$ où $(a_k)_{k=0}^n\in\mathbb{K}^{n+1}$:

$$P(X)=P=\sum_{k=0}^{n}a_kX^k=a_0X^0+a_1X^1+a_2X^2+\cdots+a_nX^n$$

Cette somme comporte nécessairement un nombre fini de monômes dont les coefficients ne sont pas nuls. Ainsi, par définition pour tout polynôme, il existe un tel indice n qui dépend de ce polynôme.

∗ Les monômes de coefficient nul ne sont généralement pas écrits. Les conventions $1X^n=X^n$, $X^1=X$ et $X^0=1$ simplifient l'écriture des polynômes et sont compatibles avec les règles de calcul ci-dessous.

◦ L'ensemble support du polynôme P est le sous-ensemble des indices des coefficients non nuls ; il est nécessairement fini :

$$\text{supp } P=\left\{k\in\mathbb{N}\;\middle/\;a_k\neq 0_{\mathbb{K}}\right\}\subset\mathbb{N}$$

∗ Le support est fini est équivalent à dire que le support est majoré :

$$\text{supp } P \text{ est fini} \iff \text{supp } P \text{ est majoré}$$

∗ Deux polynômes P et Q quelconques peuvent être représentés avec tous les deux des indices compris entre 0 et le même indice limite n, quitte à ajouter des monômes de la forme $0X^k$ à l'un des deux :

$$P=\sum_{k=0}^{n}a_kX^k\qquad Q=\sum_{k=0}^{n}b_kX^k$$

• Deux polynômes sont égaux si et seulement si les coefficients de chaque monôme X^k sont égaux. Ainsi avec les notations précédentes :

$$P=Q\iff(\forall\,k\in[\![0,n]\!]\quad a_k=b_k)$$

L'ensemble des polynômes à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$.

∗ Le polynôme nul $0_{\mathbb{K}[X]}$ est le polynôme dont tous les coefficients sont nuls ; ainsi supp $0_{\mathbb{K}[X]}=\emptyset$.

• La somme $P+Q$ est définie de la manière suivante :

$$P=\sum_{k=0}^{n}a_kX^k\qquad Q=\sum_{k=0}^{n}b_kX^k\qquad P+Q=\sum_{k=0}^{n}(a_k+b_k)X^k$$

Ces notations signifie supp $P\subset[\![0,n]\!]$ et supp $Q\subset[\![0,n]\!]$.

• Le produit de deux polynômes P et Q est défini ainsi ; ces quatre notations sont équivalentes :

$$\begin{aligned}
&P=\sum_{k=0}^{m}a_kX^k\qquad Q=\sum_{k=0}^{n}b_kX^k\\
&PQ\\
=\;&a_0b_0X^0+a_0b_1X^1+a_0b_2X^2+\cdots+a_0b_{n-1}X^{n-1}+a_0b_nX^n\\
&+a_1b_0X^1+a_1b_1X^2+a_1b_2X^3+\cdots+a_1b_{n-1}X^n+a_1b_nX^{n+1}\\
&+a_2b_0X^2+a_2b_1X^3+a_2b_2X^4+\cdots+a_2b_{n-1}X^{n+1}+a_2b_nX^{n+2}\\
&+\cdots\\
&+a_mb_0X^m+a_nb_1X^{m+1}+a_mb_2X^{m+2}+\cdots+a_mb_nX^{m+n}\\
=\;&a_mb_nX^{m+n}+(a_{m-1}b_n+a_mb_{n-1})X^{m+n-1}\\
&+(a_{m-2}b_n+a_{m-1}b_{n-1}+a_mb_{n-1})X^{m+n-2}+\cdots\\
&\cdots+(a_0b_2+a_1b_1+a_2b_0)X^2+(a_0b_1+a_1b_0)X+a_0b_0\\
=\;&\sum_{k=0}^{m+n}\Big(\sum_{\substack{0\leq i,j\\ i+j=k}}a_i\,b_j\Big)X^k=\sum_{k=0}^{m+n}c_kX^k\\
&\qquad\text{où } c_k=\sum_{\substack{0\leq i,j\\ i+j=k}}a_i\,b_j=\sum_{i=\max(0,k-n)}^{\min(m,k)}a_i\,b_{k-i}
\end{aligned}$$

Le première définition du produit correspond à la règle habituelle de distributivité dans les expressions algébriques et la deuxième regroupe les termes de même degré.

∗ Cette définition suppose uniquement ces inclusions, sans l'hypothèse $m=n$:

$$\text{supp } P\subset[\![0,m]\!]\qquad\text{supp } Q\subset[\![0,n]\!]$$

∗ Le produit d'un polynôme par une constante $\lambda\in\mathbb{K}$ correspond à

la fois au produit par le polynôme λX^0 et à un calcul coefficient par coefficient :

$$P = \sum_{k=0}^{n} a_k X^k \qquad \lambda P = (\lambda X^0)\, P = \sum_{k=0}^{n} (\lambda a_k) X^k$$

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

Le polynôme $-P = (-1)\, P$ est le polynôme opposé et vérifie $P - P = 0_{\mathbb{K}[X]}$

♦ Les opérations + et × sont des lois de composition internes. Les résultats de ces opérations sont bien des polynômes car les supports d'une somme et d'un produit vérifient ces inclusions et sont donc finis :

$$\text{supp}\,(P+Q) \subset \text{supp}\ P \cup \text{supp}\ Q \quad \text{supp}\,(PQ) \subset \text{supp}\ P + \text{supp}\ Q$$

∗ L'addition et la multiplication des polynômes sont donc des lois de composition interne qui reposent sur les règles du calcul algébrique :

$$aX^n + bX^n = (a+b)X^n \qquad aX^m \times bX^n = (ab)X^{m+n}$$

∗ Un polynôme constant est de la forme aX^0 ; les calculs sur les polynômes constants aX^0 de $\mathbb{K}[X]$ correspondent à ceux sur a dans $\mathbb{K}$, et ceci justifie donc la notation $X^0 = 1$.

■ L'addition des polynômes est associative et commutative ; le polynôme nul $0_{\mathbb{K}[X]}$ dont les coefficients sont tous nuls est l'élément neutre de l'addition. L'opposé d'un polynôme P, noté $-P$, est obtenu en prenant le polynôme dont tous les coefficients sont les opposés de ceux de P.
La multiplication des polynômes est commutative, associative et distributive par rapport à l'addition. L'élément unité pour le produit est le polynôme constant $1_{\mathbb{K}} X^0 = 1_{\mathbb{K}[X]} \neq 0_{\mathbb{K}[X]}$.
Ces propriétés vérifiées pour tout $(P, Q, R) \in \mathbb{K}[X]^3$ définissent la structure d'anneau de $\mathbb{K}[X]$:

$$P+Q = Q+P \qquad PQ = QP$$
$$P+(Q+R) = (P+Q)+R \qquad (PQ)R = P(QR)$$
$$P + 0_{\mathbb{K}[X]} = 0_{\mathbb{K}[X]} + P = P \qquad P \times 1_{\mathbb{K}[X]} = 1_{\mathbb{K}[X]} \times P = P$$
$$-P = (-1)P \qquad P + (-P) = P - P = -P + P = 0_{\mathbb{K}[X]}$$
$$P \times (Q+R) = PQ + PR \qquad (P+Q) \times R = PR + QR$$

Autres définitions

Puissance et composition de polynômes

• Par définition la puissance entière d'un polynôme est définie par récurrence à partir du produit avec la convention $P^0 = 1_{\mathbb{K}[X]} = 1X^0$ habituelle dans tout anneau :

$$P^0 = 1_{\mathbb{K}[X]} \qquad P^{m+1} = P^m\, P = P\, P^m \qquad \text{pour tout } m \in \mathbb{N}$$

• La composition de $P \in \mathbb{K}[X]$ par $Q \in \mathbb{K}[X]$ est le polynôme $Q \circ P$:

$$Q = \sum_{k=0}^{n} b_k X^k \in \mathbb{K}[X] \qquad Q \circ P = Q(P(X)) = \sum_{k=0}^{n} b_k P^k \in \mathbb{K}[X]$$

Application polynomiale

• L'application polynômiale f associée au polynôme P est définie par substitution d'une valeur à X :

$$P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X] \qquad \begin{array}{c} f : \mathbb{K} \longrightarrow \mathbb{K} \\ x \longmapsto P(x) = \displaystyle\sum_{k=0}^{n} a_k x^k \end{array}$$

Lorsque le corps $\mathbb{K}$ est $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, les fonctions polynômiales et les polynômes peuvent être identifiés : à toute application polynomiale est associé un et un seul polynôme, et réciproquement.

∗ Dans le cas où $\mathbb{K}$ est le corps $\mathbb{C}$ ou un sous-corps de $\mathbb{C}$ comme $\mathbb{R}$ ou $\mathbb{Q}$ les fonctions polynomiales et les polynômes peuvent être identifiés : à toute application polynomiale est associé un et un seul polynôme.
En revanche la connaissance des valeurs prises par une application polynomiale sur un corps fini $\mathbb{K}$ ne permet pas de déterminer un seul polynôme, par exemple d'autres polynômes que le polynôme nul sont à valeur constante égale à zéro pour tous les scalaires d'un corps fini

$\mathbb{K}$.

Polynômes constants

• Un polynôme de la forme aX^0 où $a \in \mathbb{K}$ est appelé polynôme constant.

∗ Aux notations près, les opérations sur les polynômes constants et sur les scalaires de $\mathbb{K}$ aboutissent aux mêmes résultats par l'intermédiaire de l'application injective j :

$$\begin{array}{lll} j : \mathbb{K} \longrightarrow \mathbb{K}[X] & j(0_{\mathbb{K}}) = 0_{\mathbb{K}[X]} & j(1_{\mathbb{K}}) = 1_{\mathbb{K}[X]} \\ a \longmapsto aX^0 & j(a+b) = j(a) + j(b) & j(ab) = j(a)\, j(b) \end{array}$$

Pour cette raison le monôme X^0 peut être sous-entendu dans l'écriture d'un polynôme, par exemple :

$$aX^2 + bX^1 + cX^0 = aX^2 + bX + c$$
$$X^n - X^0 = X^n - 1 \qquad \mathbb{K}X^0 = \mathbb{K}$$

∗ Ces propriétés caractérisent les polynômes constants :

$$P \in \mathbb{K} \Longleftrightarrow \deg P \leq 0 \qquad P \in \mathbb{K}^* \Longleftrightarrow \deg P = 0$$
$$P = 0 \Longleftrightarrow \deg P < 0$$

Polynômes à plusieurs variables

• Un polynôme $P(X)$ de $\mathbb{K}[X]$ est donc une somme finie de monômes en X ; sur le même principe un polynôme $Q(X, Y)$ à deux variables X et Y est une somme finie de termes en $a_{i,j}X^iY^j$, appelés monômes, où i et j sont des indices entiers positifs, et $a_{i,j} \in \mathbb{K}$ est un scalaire :

$$P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X] \qquad Q(X,Y) = \sum_{0 \leq i,j \leq n} a_{i,j} X^i Y^j \in \mathbb{K}[X,Y]$$

• La multiplication des monômes est définie ainsi, et la notion de degré distingue le degré selon les variables et le degré total :

$$X^m Y^n \, X^p Y^q = X^{m+p} Y^{n+q}$$
$$\deg_X(X^m Y^n) = m \qquad \deg_Y(X^m Y^n) = n \qquad \deg(X^m Y^n) = m + n$$

• L'ensemble $\mathbb{K}[X, Y]$ des polynômes à deux variables X et Y muni des opérations usuelles est une algèbre commutative unitaire car il a la structure d'un espace vectoriel et celle d'un anneau commutatif unitaire.

• Ces définitions et propriétés s'étendent aux polynômes ayant un nombre quelconque de variables, qui sont par définition constituées d'une somme finie de monômes.

Dérivée d'un polynôme

• Le polynôme dérivé P' d'un polynôme P est définie algébriquement, il coïncide avec la définition analytique des dérivées :

$$P = \sum_{k=0}^{n} a_k X^k \qquad P' = \sum_{k=1}^{n} k a_k \, X^{k-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} \, X^k$$
$$(X^0)' = 0 \qquad (X^k)' = kX^{k-1} \quad \text{pour } k > 0$$

∗ La dérivée diminue le degré et l'inégalité est stricte uniquement pour les polynômes de degré 0, c'est-à-dire constants et non nuls :

$$\deg P' \leq \deg P - 1 \qquad \deg P' < \deg P - 1 \Longleftrightarrow P \in \mathbb{K}^*$$

∗ La dérivée P' ne fait intervenir en aucune manière le terme constant a_0X^0 de P, d'où ces indices.
Un calcul de dérivée doit distinguer les cas $k = 0$ et $k \in \mathbb{N}^*$ dans la dérivation de X^k.
La formule générale appliquée à X^0 contredit le fait que la dérivée d'un polynôme est un polynôme car le résultat obtenu est la fraction rationnelle $0X^{-1} = 0/X$.

■ Les propriétés usuelles des dérivées des polynômes définies algébriquement sont similaires à celles des fonctions en analyse réelle :

$$\begin{array}{lll} (P+Q)' = P' + Q' & (\lambda P)' = \lambda \, P' & \\ (PQ)' = P'Q + P\,Q' & (P^m)' = mP^{m-1} & \text{si } m \in \mathbb{N}^* \\ Q \circ P = (Q' \circ P)P' & & \end{array}$$

◊ La linéarité de la dérivation des polynômes provient directement de la définition des sommes de polynômes ; il en est de même pour le produit par une constante.
La dérivée d'un produit repose sur la linéarité et ces égalités :

$$(X^{i+j})' = (i+j)X^{i+j-1} = iX^{i-1}X^j + jX^iX^{j-1} \quad \text{si } i \geq 1 \text{ et } j \geq 1$$

La démonstration de la dérivée d'une puissance se fait par récurrence à partir du produit, et celle de la composition par linéarité à partir de la puissance.

Toutes ces vérifications emploient uniquement des méthodes algébriques, sans faire intervenir des notions de limites et d'analyse.

◦ Les dérivées itérées d'un polynôme P sont définies par récurrence :

$$P^{(0)} = P \qquad P^{(1)} = P' \qquad P^{(m+1)} = (P^{(m)})' = (P')^{(m)}$$

∗ Les dérivées successives de X^n et leur valeur en 0 sont les suivantes :

$$(X^n)^{(m)} = \begin{cases} n(n-1)\cdots(n-m+1)X^{n-m} = \dfrac{n!}{(n-m)!}\,X^{n-m} & \\ & \text{si } m \leq n \\ n! & \text{si } m = n \\ 0 & \text{si } m > n \end{cases}$$

$$(X^n)^{(m)}{}_{/(0)} = \delta_{m,n}\, n! = \begin{cases} 0 & \text{si } m \neq n \\ n! & \text{si } m = n \end{cases} \quad \text{où } \delta_{m,n} = \begin{cases} 0 & \text{si } m \neq n \\ 1 & \text{si } m = n \end{cases}$$

★ Les coefficients a_k d'un polynôme P peuvent être obtenus à partir des dérivées successives de P en 0 :

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

En particulier le coefficient constant a_0 de P est $a_0 = P(0)$.

Degré d'un polynôme

• Le degré d'un polynôme est le plus grand des degrés des monômes dont les coefficients sont non nuls, avec cette convention pour le polynôme nul :

$$P = \sum_{k=0}^{n} a_k X^k \qquad\qquad \deg 0 = -\infty$$

$$\deg P = \max(\text{supp } P) = \max\left\{k \in \mathbb{N} \;\middle/\; a_k \neq 0\right\} \leq n$$

■ Les propriétés usuelles du degré des polynômes sont les suivantes :

$$\deg(PQ) = \deg P + \deg Q \qquad\qquad \deg X^n = n$$
$$\deg(P+Q) \leq \max(\deg P, \deg Q)$$
$$\deg P \neq \deg Q \Longrightarrow \deg(P+Q) = \max(\deg P, \deg Q)$$
$$\deg(Q \circ P) = \deg Q \, \deg P$$
$$\deg P' \leq \deg P - 1 \qquad \deg P \geq 1 \Longrightarrow \deg P' = \deg P - 1$$

◊ Si $\deg P = m$ et $\deg Q = n$ alors les coefficients a_m et b_n de P et Q sont non nuls, et le coefficient du monôme de plus haut degré X^{m+n} du produit PQ est $a_m b_n \neq 0$:

$$P = \sum_{k=0}^{m} a_k X^k \qquad Q = \sum_{k=0}^{n} b_k X^k \qquad a_m \neq 0 \qquad b_n \neq 0$$
$$PQ = a_m b_n X^{m+n} + \cdots + a_0 b_0 \qquad \deg(PQ) = m+n$$

Ces démonstrations traitent à part le cas du polynôme nul.

∗ Les conditions ci-dessous sont équivalentes :

$$P \text{ est un polynôme constant} \Longleftrightarrow \deg P \leq 0 \Longleftrightarrow P' = 0$$
$$P = 0 \Longleftrightarrow \deg P < 0 \Longleftrightarrow \deg P = -\infty$$

◦ La valuation d'un polynôme est le plus petit des degrés des monômes dont les coefficients sont non nuls :

$$P = \sum_{k=0}^{n} a_k X^k \qquad\qquad \text{val}\, 0 = +\infty$$

$$\text{val}\, P = \min(\text{supp } P) = \min\left\{k \in \mathbb{N} \;\middle/\; a_k \neq 0\right\}$$

□ Ce tableau récapitule les propriétés des valuations :

$$\text{val}(PQ) = \text{val}\, P + \text{val}\, Q \qquad\qquad \text{val}\, X^n = n$$
$$\text{val}(P+Q) \geq \min(\text{val}\, P, \text{val}\, Q)$$
$$\text{val}\, P \neq \text{val}\, Q \Longrightarrow \text{val}(P+Q) = \min(\text{val}\, P, \text{val}\, Q)$$
$$P \neq 0 \Longrightarrow \text{val}\, P \leq \deg P$$

◊ Les méthodes de démonstration sont similaires à celles employées pour justifier le formulaire sur les degrés.

∗ Tout polynôme P non nul peut donc s'écrire ainsi :

$$P = \sum_{k=\text{val}\, P}^{\deg P} a_k X^k \qquad a_{\deg P} \neq 0 \qquad a_{\text{val}\, P} \neq 0$$

◦ Un polynôme est unitaire si et seulement si son coefficient de plus haut degré est 1, $a_{\deg P} = 1$ avec les notations précédentes.

◦ Un monôme M est un polynôme de la forme λX^m avec $\lambda \neq 0$. L'égalité $\deg M = \text{val}\, M$ caractérise les monômes.

Division euclidienne de polynômes

■ La division euclidienne du polynôme A par le polynôme non nul B énonce qu'il existe un unique couple (Q,R) de polynômes appelés quotient et reste vérifiant ces deux conditions :

$$\exists!\,(Q,R)\in\mathbb{K}[X]^2 \quad A=BQ+R \ \mathsf{ET}\ \deg R<\deg B$$

◊ La méthode décrite ci-dessous, valable pour tout couple de polynômes (A,B) où $B\neq 0$, justifie l'existence du couple (Q,R).
Un argument sur les degrés prouve l'unicité :

$$\begin{cases} A=BQ_1+R_1=BQ_2+R_2 \\ \mathsf{ET}\ \deg R_1<\deg B\ \mathsf{ET}\ \deg R_2<\deg B \end{cases}$$
$$\Longrightarrow B(Q_2-Q_1)=R_1-R_2 \ \mathsf{ET}$$
$$\deg B(Q_2-Q_1)=\deg(R_1-R_2)\leq\max(\deg R_1,\deg R_2)<\deg B$$
$$\Longrightarrow \deg B+\deg(Q_2-Q_1)<\deg B$$
$$\Longrightarrow \deg(Q_2-Q_1)<0$$
$$\Longrightarrow Q_2-Q_1=0$$

En conclusion $Q_1=Q_2$ puis $R_1=A-BQ_1=A-BQ_2=R_2$.

∗ Ce résultat fonde l'arithmétique sur les polynômes comme la division euclidienne des entiers est à la base de l'arithmétique sur $\mathbb{Z}$.

∗ L'algorithme de la division euclidienne simplifie de proche en proche le terme de plus haut degré de A : il construit la suite finie $(A_k)_{k=0}^{\deg A-\deg B+1}$ définie par récurrence où α_k est le coefficient de $X^{\deg A-k}$ de A_k et $\beta\neq 0$ le coefficient de $X^{\deg B}$ de B ; le dernier terme de cette famille finie est le reste :

$$A_0=A \quad A_{k+1}=A_k-\frac{\alpha_k}{\beta}X^{\deg A-\deg B-k}B \qquad \deg A_k\leq\deg A-k$$

$$Q=\sum_{k=0}^{n}\frac{\alpha_k}{\beta}X^{\deg A-\deg B-k} \qquad R=A_{\deg A-\deg B+1}$$

À chaque étape $A=B\sum_{k=0}^{m}\frac{\alpha_k}{\beta}X^{\deg A-\deg B-k}+A_{m+1}$.

★ La présentation d'une division de polynômes est similaire à celle d'une division entière :

$$\begin{array}{rl|l}
A=A_0= & X^5+X^4+X^3+X^2+X+1 & B=X^3-1 \\
 & -(X^5\qquad\quad -X^2) & \hline \\
A_1= & \quad X^4+X^3+2X^2+X+1 & Q=X^2+X+1 \\
 & -(X^4\qquad\quad -X) & \\
 & \quad X^3+2X^2+2X+1 & \\
A_2= & -(X^3\qquad\quad -1) & \\
R=A_3= & \quad 2X^2+2X+2 &
\end{array}$$

Arithmétique des polynômes

Intégrité de l'anneau des polynômes

■ L'anneau $(\mathbb{K}[X],+,\times)$ est intègre, *i.e.* il vérifie cette proposition :

$$\forall\,(A,B)\in\mathbb{K}[X]^2 \quad AB=0\Longrightarrow A=0\ \mathsf{OU}\ B=0$$

□ Le produit PQ de deux polynômes P et Q non nuls est non nul.

◊ Un argument sur le degré le justifie :

$$\begin{aligned} P\neq 0\ \mathsf{ET}\ Q\neq 0 &\Longrightarrow \deg P\geq 0\ \mathsf{ET}\ \deg Q\geq 0 \\ &\Longrightarrow \deg(PQ)=\deg P+\deg Q\geq 0 \\ &\Longrightarrow PQ\neq 0 \end{aligned}$$

◊ La contraposée de l'implication énonce la propriété recherchée :
$P\neq 0\,\mathsf{ET}\,Q\neq 0\Longrightarrow PQ\neq 0 \qquad AB=0\Longrightarrow A=0\,\mathsf{OU}\,B=0$

□ Tout élément non nul de l'anneau intègre $\mathbb{K}[X]$ est régulier pour la multiplication :

$$\forall\,(A,B,C)\in\mathbb{K}[X]^3 \quad (AB=AC \ \ \mathsf{ET}\ \ A\neq 0)\Longrightarrow B=C$$

◊ La démonstration repose sur la définition précédente de l'anneau intègre appliquée à $AB-AC=A(B-C)$.

Polynômes inversibles

■ L'ensemble des polynômes inversibles est celui des polynômes de degré nul :

$$\mathbb{U}(\mathbb{K}[X])=\left\{P\in\mathbb{K}[X]\ /\ \exists\,Q\in\mathbb{K}[X] \quad PQ=1_{\mathbb{K}[X]}\right\}=\mathbb{K}^*X^0=\mathbb{K}^*$$

♦ L'étude de l'équation $PQ=1$ repose sur les degrés des polynômes produits à valeurs dans $\mathbb{N}\cup\{-\infty\}$ et aboutit à ces deux inclusions :

$$\begin{aligned} PQ=1 &\Longrightarrow \deg(PQ)=\deg P+\deg Q=0 \\ &\Longrightarrow \deg P=\deg Q=0 \\ &\Longrightarrow P\in\mathbb{K}^*=\mathbb{K}^*X^0 \qquad \mathbb{U}(\mathbb{K}[X])\subset\mathbb{K}^* \\ \lambda\in\mathbb{K}^* &\Longrightarrow (\lambda X^0)\times\frac{1}{\lambda}X^0=1 \\ &\Longrightarrow \lambda\in\mathbb{U}[\mathbb{K}[X]) \qquad\quad \mathbb{K}^*\subset\mathbb{U}(\mathbb{K}[X]) \end{aligned}$$

Divisibilité

• Le polynôme B divise le polynôme A si et seulement s'il existe $Q\in\mathbb{K}[X]$ vérifiant $A=QB$; cette proposition est notée $B|A$ et signifie que A est un multiple de B.
Lorsque $B\neq 0$ la proposition $B|A$ est équivalente au fait que le reste de la division de A par B est nul.

$$\begin{aligned} A\mid B &\Longleftrightarrow B\in A\,\mathbb{K}[X] \Longleftrightarrow B \text{ est un multiple de } A \\ &\Longleftrightarrow \exists\, Q\in\mathbb{K}[X] \quad B=QA \\ &\Longleftrightarrow \text{le reste de la division de } B \text{ par } A \text{ est nul,} \quad \text{pour } A\neq 0. \end{aligned}$$

La divisibilité d'un polynôme A par un polynôme B est à analogue à la divisibilité sur les entiers.

▪ Les propriétés élémentaires de la divisibilité des polynômes sont comparables à celle des entiers, en replaçant la multiplication par $\pm1\in\mathbb{U}(\mathbb{Z})$ par la multiplication par un scalaire non nul $\lambda\in\mathbb{K}^*=\mathbb{U}(\mathbb{K}[X])$:

$$1\mid A \qquad A\mid 0 \qquad A\mid A \qquad A\mid AB$$

$$A\mid B \Longleftrightarrow (\lambda A)\mid B \Longleftrightarrow A\mid(\lambda B)$$

$$A\mid B \;\mathsf{ET}\; B\mid C \Longrightarrow A\mid C \qquad A\mid B \;\mathsf{ET}\; A\mid C \Longrightarrow A\mid(B+C)$$

$$A\mid B \;\mathsf{ET}\; B\mid A \Longleftrightarrow \big(\exists\,\lambda\in\mathbb{K}^* \quad A=\lambda B\big) \qquad A\mid 1 \Longleftrightarrow A\in\mathbb{K}^*$$

$$A\mid B \Longleftrightarrow AC\mid BC \quad \text{lorsque } C\neq 0 \qquad A\mid B\Longrightarrow A\mid BC$$

∗ La divisibilité de polynômes est invariante par des multiplications par des constantes non nulles de $\mathbb{K}^*=\mathbb{U}(\mathbb{K}[X])$.
Cette propriété est analogue au fait que la divisibilité sur $\mathbb{Z}$ ne dépend pas du signe des entiers : une multiplication par un élément de $\mathbb{U}(\mathbb{Z})=\{+1,-1\}$.

Algorithme d'Euclide

Lemme d'Euclide

• Le polynôme $D\in\mathbb{K}[X]$ est un diviseur commun aux polynômes A et B si et seulement si D est un diviseur commun à D et à $R=A-BQ$ où $Q\in\mathbb{K}[X]$:

$$A=BQ+R \qquad R=A-BQ$$

$$\big(D\mid A\;\mathsf{ET}\;D\mid B\big)\Longleftrightarrow\big(D\mid B\;\mathsf{ET}\;D\mid R\big)$$

• Cette propriété est valable pour tous les polynômes A, B et Q de $\mathbb{K}[X]$, et s'applique le plus souvent lorsque Q et R sont le quotient et le reste de la division euclidienne de A par B.

Algorithme d'Euclide

• *L'algorithme d'Euclide* appliqué à A et à B consiste à construire, exactement comme pour les entiers, les suites $(A_k)_k$, $(B_k)_k$ et $(R_k)_k$ des restes successifs de divisions euclidiennes :
$A_0=A \qquad B_0=B$
pour tout $k\in\mathbb{N}$ tel que $B_k\neq 0$,
R_k est le reste de la division euclidienne de A_k par B_k
puis $A_{k+1}=B_k$ et $B_{k+1}=R_k \qquad \deg B_{k+1}=\deg R_k<\deg B_k$
$\operatorname{pgcd}(A,B)=A_p$ lorsque $B_p=0$.

Ces familles ne comportent qu'un nombre fini, noté p, de termes, car les degrés des polynômes B_k sont à valeurs entières, positives et strictement décroissants ; l'indice p est ainsi défini par $B_p=0$.
Le résultat de l'algorithme d'Euclide, noté $\operatorname{pgcd}(A,B)$, est en fait éventuellement multiplié par une constante non nul de façon à obtenir un polynôme unitaire :

$$A_p=B_{p-1}=R_{p-2} \quad B_p=R_{p-1}=0 \quad \operatorname{pgcd}(A,B)=\lambda A_p \quad \lambda\neq 0$$

• L'exemple suivant illustre l'algorithme d'Euclide d'un calcul de pgcd :

$$\begin{aligned} X^{16}-1 &= X^7(X^9+1)-X^7-1 \\ X^9+1 &= -X^2(-X^7-1)-X^2+1 \\ -X^7-1 &= (X^5+X^3+X)(-X^2+1)-X-1 \\ -X^2+1 &= (X-1)(-X-1)+0 \end{aligned} \qquad \operatorname{pgcd}(X^{16}-1,X^9+1)=X+1$$

Le dernier reste non nul de l'algorithme d'Euclide est $-X-1$, il

est multiplié par -1 pour représenter le pgcd sous la forme d'un polynôme unitaire.

Plus grand commun diviseur

• Le résultat $\text{pgcd}(A,B)$ de l'algorithme d'Euclide est un diviseur commun à A et à B de plus haut degré, d'où son nom :

$$\text{pgcd}(A,B) \mid A \qquad \text{pgcd}(A,B) \mid B$$
$$(D \mid A \,\mathsf{ET}\, D \mid B) \Longleftrightarrow D \mid \text{pgcd}(A,B)$$

• Ces propriétés sont directement issues, comme pour les entiers, du lemme d'Euclide.

• Les plus grands communs diviseurs d'entiers sont définis au signe près, c'est-à-dire à partir d'une multiplication par un élément inversible $\pm 1 \in \mathbb{U}(\mathbb{Z})$. De la même façon le pgcd de polynômes est défini à une constante multiplicative près de $\mathbb{K}^* = \mathbb{U}(\mathbb{K}[X])$.
La représentation sous la forme d'un polynôme unitaire du pgcd est donc unique et évite ainsi toute ambiguïté due à une multipliation par une constante.
Les polynômes unitaires de $\mathbb{K}[X]$ jouent le rôle des entiers positifs de $\mathbb{Z}$.

• Ces propriétés élémentaires du pgcd découlent de l'algorithme d'Euclide : par la définition du pgcd :

$$\text{pgcd}(A,1) = 1 \qquad \text{pgcd}(A,A) = A = \text{pgcd}(A,0)$$
$$\text{pgcd}(A,B) = \text{pgcd}(B,A) = \text{pgcd}(\lambda A,B) = \text{pgcd}(A,\lambda B)$$

• En toute rigueur $\text{pgcd}(A,A)$ est un polynôme unitaire de la forme λA.
La notation $\text{pgcd}(A,A) = A$ sous-entend la constante multiplicative λ, sur le même principe que les égalités de primitives ne sont valables qu'à une constante additive près.
Par ailleurs la propriété $\text{pgcd}(A,B) = \text{pgcd}(\lambda A,B)$ permet de réduire les calculs intermédiaires de l'algorithme d'Euclide de façon à simplifier les coefficients des polynômes intermédiaires.

• Par convention $\text{pgcd}(0,0) = 0$ même si tout polynôme divise 0, dans ce seul cas particulier le nom pgcd semble trompeur.

• Deux polynômes A et B vérifiant $\text{pgcd}(A,B) = 1$ sont dits premiers entre eux.

Propriété fondamentale du pgcd *et conséquences*

La propriété fondamentale du pgcd est celle-ci :

$$D \mid A \,\mathsf{ET}\, D \mid B \Longleftrightarrow D \mid \text{pgcd}(A,B)$$

• Ces deux propriétés découlent de la propriété fondamentale ci-dessus :

$$\text{pgcd}(CA,CB) = C\ \text{pgcd}(A,B) \qquad A = \text{pgcd}(A,B) \Longleftrightarrow A \mid B$$

• Ces propriétés sont justifiées de la même façon que celle sur les entiers.

• Le pgcd est associatif, d'où la définition de $\text{pgcd}(A,B,C)$:

$$\text{pgcd}(A,B,C) = \text{pgcd}(A,\text{pgcd}(B,C)) = \text{pgcd}(\text{pgcd}(A,B),C)$$

Théorèmes de Bezout et de Gauss

Équation de Bezout

• L'algorithme d'Euclide construit un couple-solution $(U,V) \in \mathbb{K}[X]^2$ à l'équation $AU+BV = \text{pgcd}(A,B)$ par substitutions successives des restes des divisions euclidiennes à partir de la dernière :

$$\exists\,(U,V) \in \mathbb{K}[X]^2 \quad \text{pgcd}(A,B) = AU + BV$$

• L'exemple ci-dessous reprend le calcul précédent du pgcd pour déterminer une solution de l'équation de Bezout :

$$\begin{aligned}
X+1 &= (-X^2+1)(X^5+X^3+1) + (X^7+1) \\
&= (X^9+1)(X^5+X^3+X) - (X^7+1)(X^7+X^5+X^3-1) \\
&= \quad (X^9+1)(X^5+X^3+X) \\
&\quad - (X^7(X^9+1) - X^{16}+1)(X^7+X^5+X^3-1) \\
&= \quad (X^{16}-1)(X^7+X^5+X^3-1) \\
&\quad - (X^9+1)(X^{14}+X^{12}+X^{10}-X^7-X^5-X^3-X)
\end{aligned}$$

Théorème de Bezout

• Le *Théorème de Bezout* énonce cette équivalence :

$$\text{pgcd}(A,B) = 1 \Longleftrightarrow \exists\,(U,V) \in \mathbb{K}[X]^2 \quad AU + BV = 1$$

• Plus précisément lorsque $\text{pgcd}(A,B) = 1$, l'ensemble $\mathcal{S}$ des solutions de l'équation de Bezout possède cette structure :

$$\exists!\,(U_0,V_0)\in\mathbb{K}[X]^2 \quad AU_0+BV_0=1 \,\mathsf{ET}\, \deg U_0<\deg B \,\mathsf{ET}\, \deg V_0<\deg A$$
$$\mathcal{S}=\left\{U_0+QB,V_0-QA)\ /\ Q\in\mathbb{K}[X]\right\}$$

Conséquences du théorème de Bezout

- Cette propriété est une conséquence du théorème de Bezout :
$$\text{pgcd}(A,B)=1 \,\mathsf{ET}\, \text{pgcd}(A,C)=1 \Longleftrightarrow \text{pgcd}(A,BC)=1$$
- Le produit des équations de Bezout associées à (A,B) et à (A,C) justifie ce résultat.
- Une récurrence prouve cette implication pour tout $(m,n)\in\mathbb{N}^2$:
$$\text{pgcd}(A,B)=1\Longrightarrow \text{pgcd}(A^m,B^n)=1$$
- Les polynômes du premier degré sont premiers entre eux dès que $a\neq b$:
$$\text{pgcd}(X-a,X-b)=1 \qquad \frac{1}{b-a}(X-a)+\frac{1}{a-b}(X-b)=1$$
$$\text{pgcd}((X-a)^m,(X-b)^n)=1$$

Théorème de Gauss

- Le *théorème de Gauss* sur les polynômes est formellement le même que celui sur les entiers :
$$\text{pgcd}(A,B)=1 \,\mathsf{ET}\, A\mid BC\Longrightarrow A\mid C$$
$$\text{pgcd}(A,B)=1 \,\mathsf{ET}\, A\mid C \,\mathsf{ET}\, B\mid C\Longrightarrow AB\mid C$$
- La démonstration est la même que pour les entiers.

Une analogie avec les entiers

- La démonstration de l'égalité suivante illustre le parallèle entre l'arithmétique sur les entiers et celle sur les polynômes
$$\text{pgcd}(X^m-1,X^n-1)=X^{\text{pgcd}(m,n)}-1 \qquad \text{pour tout } (m,n)\in\mathbb{N}^2$$
- Lorsque q et r sont le quotient de la division entière de m par n, ce produit remarquable énonce que le reste polynomial de la division de X^m-1 par X^n-1 est X^r-1 :

$$\begin{aligned} m&=qn+r & 0\leq r<n\\ X^m-1&=X^{qn+r}-1=(X^{qn}-1)X^r+X^r-1\\ &=((X^n)^q-1)X^r+X^r-1\\ &=(X^n-1)X^r\sum_{k=0}^{q-1}(X^q)^k+X^r-1\end{aligned}$$

De proche en proche le lemme d'Euclide appliqué d'une part aux entiers m et n et d'autre part aux polynômes X^m-1 et X^n-1 aboutit respectivement à $\text{pgcd}(m,n)$ et à $\text{pgcd}(X^m-1,X^n-1)$.
À chaque étape le reste de la division polynomial de X^m-1 par X^n-1 est X^r-1, d'où l'égalité demandée.

Plus petit commun multiple

- Le plus petit commun multiple strictement positif de A et B est, lorsque $AB\neq 0$, un polynôme multiple commun de A et de B de plus petit degré, par convention ce polynôme est multiplié par une constante non nulle pour être unitaire sans modifier ses propriétés de divisibilité :
$$\deg(\text{ppcm}(A,B))=\min\left\{\deg P\ /\ P\neq 0 \,\mathsf{ET}\, A\mid P \,\mathsf{ET}\, B\mid P\right\}$$
$$A\mid \text{ppcm}(A,B) \qquad B\mid \text{ppcm}(A,B)$$
$$\text{ppcm}(A,0)=\text{ppcm}(0,A)=\text{ppcm}(0,0)=0$$
- Ces propriétés découlent de la définition quand $\lambda\in\mathbb{K}^*$:
$$\text{ppcm}(A,\pm 1)=\text{ppcm}(A,A)=A$$
$$\text{ppcm}(A,B)=\text{ppcm}(B,A)=\text{ppcm}(\lambda A,B)=\text{ppcm}(A,\lambda B)$$
- Cette équivalence est la propriété fondamentale du ppcm :
$$A\mid P \,\mathsf{ET}\, B\mid P\Longleftrightarrow \text{ppcm}(A,B)\mid P$$
- Les conséquences sont les suivantes, et les éventuelles constantes multiplicatives ne sont pas représentées :
$$A\mid B\Longleftrightarrow \text{ppcm}(A,B)=B \qquad \text{ppcm}(CA,CB)=C\ \text{ppcm}(A,B)$$

point Cette égalité générale relie le pgcd et le ppcm :
$$\text{pgcd}(A,B)\ \text{ppcm}(A,B)=AB$$

- La démonstration se fait comme pour les entiers, par la conséquence du le théorème de Gauss lorsque les polynômes sont premiers entre eux : alors le théorème de Gauss prouve cette égalité :

$$\text{pgcd}(A,B)=1 \Longrightarrow AB|\,\text{ppcm}(A,B)$$

Par ailleurs $\text{ppcm}(A,B)$ divise A et B, donc $\text{ppcm}(A,B)=AB$, à une constante multiplicative près.
Une factorisation par $\text{pgcd}(A,B)$ termine la démonstration dans le cas général.

- Le ppcm est associatif, d'où cette définition de $\text{ppcm}(A,B,C)$:
  $\text{ppcm}(A,B,C)=\text{ppcm}(A,\text{ppcm}(B,C))=\text{ppcm}(\text{ppcm}(A,B),C)$

Racines et factorisation des polynômes

Dans ce paragraphe $\mathbb{K}$ est nécessairement un corps qui est un sous-ensemble de $\mathbb{C}$: généralement $\mathbb{C}$, $\mathbb{R}$ ou $\mathbb{Q}$.

Racines simples et multiples

□ La condition suivante caractérise le fait que le monôme X^m divise P :

$$P(0)=P'(0)=\cdots=P^{(m-1)}(0)=0$$

◊ Cette propriété provient du lien entre les coefficients d'un polynôme et les valeurs de ses dérivées successives en zéro. Le reste de la division de P par X^m est R :

$$P=\sum_{k=0}^{n}a_kX^k=\sum_{k=0}^{m-1}a_kX^k+X^m\sum_{k=m}^{n}a_kX^{k-m}$$

$$R=\sum_{k=0}^{m-1}a_kX^k \qquad a_k=\frac{P^{(k)}(0)}{k!}$$

$$X^m|P \Longleftrightarrow R=0 \Longleftrightarrow P(0)=P'(0)=\cdots=P^{(m-1)}(0)=0$$

■ La divisibilité de P par $(X-r)^m$ est équivalente à ces égalités qui définissent r comme racine d'ordre au moins m du polynôme supposé généralement non nul P :

$$P(r)=P'(r)=\cdots=P^{(m-1)}(r)=0$$

◊ La dérivation de polynômes composés justifient ces égalités :

$$\begin{aligned}Q(X)&=P(X+r) & P(X)&=Q(X-r)\\ Q'(X)&=P'(X+r) & P'(X)&=Q'(X-r)\\ Q''(X)&=P''(X+r) & P''(X)&=Q''(X-r)\\ Q^{(k)}(X)&=P^{(k)}(X+r) & P^{(k)}(X)&=Q^{(k)}(X-r)\end{aligned}$$

Les égalités suivantes en découlent :

$$\begin{aligned}Q(0)&=P(r) & Q'(0)&=P'(r)\\ Q''(0)&=P''(r) & Q^{(k)}(0)&=P^{(k)}(r)\end{aligned}$$

Les implications suivantes démontrent l'équivalence finale :

$$\begin{aligned}&P(X)=(X-r)^mB(X)\\ \Longrightarrow\;&Q(X)=(X-r+r)^mB(X+r)=X^mB(X+r)\\ \Longrightarrow\;&X^m|Q(X)\\ &Q(X)=X^m\,C(X)\\ \Longrightarrow\;&P(X)=Q(X-r)=(X-r)^mC(X-r)\\ \Longrightarrow\;&(X-r)^m|P(X)\\ &(X-r)^m\mid P(X)\\ \Longleftrightarrow\;&X^m\mid Q(X)\\ \Longleftrightarrow\;&Q(0)=Q'(0)=\cdots=Q^{(m-1)}(0)=0\\ \Longleftrightarrow\;&P(r)=P'(r)=\cdots=P^{(m-1)}(r)=0\end{aligned}$$

∗ Une racine multiple est une racine d'ordre $m\geq 2$.
Une racine simple est une racine d'ordre exactement un.
En particulier $X-r$ divise P si et seulement si r est une racine de P.

▶▶ Recherche de $n\in\mathbb{N}^*$ tel que $P_n=(X-1)^n-X^n+1\in\mathbb{C}[X]$ possède une racine double.

▷▷ Si P et P' possèdent une racine commune $r\in\mathbb{C}$ alors r vérifie cette première relation obtenue à partir de $P_n'(r)=0$:

$$P_n'=n(X-1)^{n-1}-nX^{n-1} \qquad (r-1)^{n-1}=r^{n-1}$$

Cette équation aboutit à $(r-1)/r$ est une racine $(n-1)$-ème de 1 lorsque $n>1$. Si $n=1$ alors le polynôme $P_1=X-1-X+1=0$ est nul.
Dans la suite $n\neq 1$ et $(r-1)^{n-1}=r^{n-1}$:

$$(r-1)^n = (r-1)(r-1)^{n-1} = (r-1)r^{n-1}$$
$$P_n(r) = (r-1)r^{n-1} - r^n + 1$$
$$= r^{n-1}(r-1-r) + 1 = -r^{n-1} + 1$$
$$\Big(\frac{r-1}{r}\Big)^{n-1} = 1 \qquad (r-1)^{n-1} = 1$$

Cette égalité énonce que r et $r-1$ sont des racines de 1 d'ordre $n-1$; ainsi $|r| = |r-1| = 1$ et r est de la forme $r = e^{\mathrm{i}\theta}$ où $\theta = 2k\pi/(n-1) \in]-\pi, \pi]$:

$$e^\theta - 1 = e^{\mathrm{i}\theta/2}(e^{\mathrm{i}\theta/2} - e^{-\mathrm{i}\theta/2}) = 2\mathrm{i}\,\sin\Big(\frac{\theta}{2}\Big)\,e^{\theta/2}$$
$$\big|e^{\mathrm{i}\theta} - 1\big| = \big|e^{\mathrm{i}\theta/2}(e^{\mathrm{i}\theta/2} - e^{-\mathrm{i}\theta/2})\big| = \Big|2\,\sin\Big(\frac{\theta}{2}\Big)\Big| = 1$$

Cette condition aboutit à $\sin(\theta/2) = \pm 1/2$ et ces quatre mesures de θ correspondent en fait aux deux nombres complexes $e^{\pm\mathrm{i}\pi/3}$:

$$\frac{\theta}{2} = \pm\frac{\pi}{6} \text{ OU } \frac{\theta}{2} = \pm\frac{5\pi}{6} \qquad \theta = \pm\frac{\pi}{3} \text{ OU } \theta = \pm\frac{5\pi}{3}$$

Par ailleurs $\theta = 2k\pi/(n-1)$ entraîne $(n-1) = \pm 6k$ et $n = 6k+1$. Ainsi il existe une éventuelle racine double lorsque $n \in 6\mathbb{N}+1$, et les seules racines possibles sont $e^{\pm\mathrm{i}\pi/3}$.

⋙ Réciproquement si n est de la forme $6m+1$ avec $m \in \mathbb{N}$ alors $P_n'(r) = P_n(r) = 0$ pour $r = e^{\pm\mathrm{i}\pi/3}$ pour ces raisons :

$$r - 1 = e^{\pm\mathrm{i}\pi/3} - 1 = e^{\pm\mathrm{i}\pi/6}(e^{\pm\mathrm{i}\pi/6} - e^{\mp\mathrm{i}\pi/6})$$
$$= 2\mathrm{i}\,\sin\Big(\pm\frac{\pi}{6}\Big)\,e^{\pm\mathrm{i}\pi/6}$$
$$(r-1)^{n-1} = (r-1)^{6m} = (2\mathrm{i}\,\sin\Big(\pm\frac{\pi}{6}\Big)\,e^{\pm\mathrm{i}\pi/6})^{6m}$$
$$= \mathrm{i}^{6m}(\pm 1)^{6m}e^{\pm\mathrm{i}m\pi} = (-1)^{3m}(-1)^m = 1$$
$$P_n'(r) = n(r-1)^{n-1} - nr^{n-1} = n - ne^{\pm 2\mathrm{i}m\pi} = 0$$
$$P_n(r) = (r-1)^n - r^n + 1 = (r-1)^{6m+1} - r^{6m+1} + 1$$
$$= (r-1)^{6m}(r-1) - r^{6m}r + 1 = r - 1 - r + 1 = 0$$

En conclusion P_n possède au moins une racine double si et seulement si $n \in 6\mathbb{N}+1$; dans ce cas les deux racines doubles sont les conjugués $e^{\pm\mathrm{i}\pi/3}$ et P_n est divisible par ce polynôme :

$$(X - e^{\mathrm{i}\pi/3})^2(X - e^{-\mathrm{i}\pi/3})^2 = (X^2 - X + 1)^2$$

Formule de Taylor sur les polynômes

• La dérivée algébrique des polynômes vérifient ces propositions similaires aux propriétés issues de l'analyse :

$$(PQ)' = P'Q + PQ' \qquad (Q \circ P)' = (Q(P(X)))' = (Q' \circ P) \times P'$$

• Les dérivées successives de X^n vérifient ces égalités :

$$(X^n)^{(p)} = \begin{cases} \dfrac{n!}{(n-p)!}X^{n-p} & \text{pour } p \le n \\ 0 & \text{pour } n < p \end{cases}$$

$$\frac{n!}{(n-p)!} = n(n-1)\cdots(n-p+1) \qquad (X^n)^{(n)} = n!\,X^0 = n!$$

• La valeur en 0 du monôme $(X^n)^{(p)}$ notée $(X^n)^{(p)}{}_{/(0)}$ la suivante :

$$(X^n)^{(p)}{}_{/(0)} = \delta_{n,p}\,n! \qquad \text{avec } \delta_{n,p} = \begin{cases} 1 & \text{si } n = p \\ 0 & \text{sinon} \end{cases}$$

• Par linéarité de la dérivation, tout polynôme P peut donc s'écrire de l'une et l'autre façon suivante dès que $n \ge \deg P$:

$$P = \sum_{k=0}^{\deg P} \frac{P^{(k)}(0)}{k!}X^k = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!}(X-r)^k \qquad \text{pour } n \ge \deg P$$

• La formule de Taylor sur les polynômes énonce cette égalité :

$$P = \sum_{k=0}^{\deg P} \frac{P^{(k)}(r)}{k!}(X-r)^k = \sum_{k=0}^{n} \frac{P^{(k)}(r)}{k!}(X-r)^k \quad \text{pour } n \ge \deg P$$

• La démonstration repose sur la formule précédente valable en 0 appliquée à $Q(X) = P(X+r)$ et à $P(X) = Q(X-r)$; les dérivées successives vérifient $Q^{(n)}(0) = P^{(n)}(r)$.

Racine et divisibilité

• Une racine $r \in \mathbb{K}$ du polynôme P est définie par l'une de ces propositions équivalentes :

$$X - r \mid P \iff \exists Q \in \mathbb{K}[X] \quad P = (X-r)Q$$
$$\iff \text{le reste de la division de } P \text{ par } X - r \text{ est nul}$$
$$\iff P(r) = 0$$

• Une racine $r \in \mathbb{K}$ du polynôme P d'ordre au moins $m \in \mathbb{N}^*$ est définie par l'une de ces propositions équivalentes fondées sur la formule de Taylor :

$$(X-r)^m \mid P \iff \exists\, Q \in \mathbb{K}[X] \quad P = (X-r)^m Q$$
$$\iff \text{le reste de la division de } P \text{ par } (X-r)^n \text{ est nul}$$
$$\iff P(r) = P'(r) = \cdots = P^{(m-1)}(r) = 0$$

• Une racine $r \in \mathbb{K}$ est exactement d'ordre m si et seulement si r est d'ordre au moins m et r n'est pas d'ordre $m+1$:

$$(X-r)^m \mid P \text{ ET } (X-r)^m \not| P$$
$$\iff P(r) = P'(r) = \cdots = P^{(m-1)}(r) = 0 \neq P^{(m)}(r)$$

• Un polynôme de degré inférieur ou égal à n ayant $n+1$ ou plus racines est la polynôme nul.
Un polynôme ayant une famille infinie de racines est le polynôme nul.

• Un polynôme P est scindé lorsqu'il possède une factorisation en produit de facteurs du premiers degré, à une constante multiplicative non nulle près :

$X^2 - 1 = (X-1)(X+1)$ est scindé dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$

$X^2 + 1 = (X-\mathrm{i})(X+\mathrm{i})$ est scindé dans $\mathbb{C}[X]$

$X^2 + 1$ n'est pas scindé dans $\mathbb{R}[X]$ car n'a pas de racines réelles

• Tout polynôme $P \neq 0$ de degré $n = \deg P$ qui possède n racines $(r_k)_{k=1}^n$ comptées avec leur ordre de multiplicité est scindé :

$$P = \lambda \prod_{k=1}^{n} (X - r_k) \qquad \lambda = 1 \text{ pour un polynôme unitaire}$$

Factorisation des polynômes à coefficients complexes

Théorème de d'Alembert-Gauss

■ Tout polynôme non nul P de $\mathbb{C}[X]$ se factorise de façon unique à l'ordre près de ses facteurs sous la forme suivante où $\lambda \in \mathbb{C}^*$ est le coefficient de plus haut degré de P, la famille $(r_k)_{k=1}^s \in \mathbb{C}^s$ définit les $s \in \mathbb{N}$ racines complexes de P supposées distinctes deux à deux, et $e_k \in \mathbb{N}^*$ est l'ordre de multiplicité de $r_k \in \mathbb{C}$ lorsque $k \in \{1 \cdots s\}$:

$$P = \lambda \prod_{k=1}^{s} (X - r_k)^{e_k} \qquad \text{ainsi} \sum_{k=1}^{s} e_k = \deg P$$

◊ Ce théorème, dit d'Alembert-Gauss, est admis. Les outils d'analyse

mis en œuvre dans sa démonstration ne font pas partie de ce cours sur les *méthodes de calcul*.

∗ Ce théorème occupe une place centrale en algèbre et en analyse.

∗ Tout polynôme $P \neq 0$ à coefficients complexes possède exactement $\deg P$ racines, comptées avec leur ordre de multiplicité.

∗ Le théorème de Gauss prouve que cette factorisation est unique à l'ordre près des racines.
Deux polyômes de $\mathbb{C}[X]$ sont sans facteur commun si et seulement s'ils n'ont pas de racines communes.

∗ Plus précisément il est possible de factoriser explicitement à l'aide de racines complexes tous les polynômes de degré 1 par un calcul direct, de degré 2 à partir des racines du discriminant, de degré 3 par les formules de Cardan ou de degré 4 avec les formules de Ferrari.
La théorie de Galois démontre en revanche que pour un polynôme quelconque de degré supérieur ou égal à 5, il n'existe généralement pas de formules explicites des racines sauf dans certains cas exceptionnels.
Un exemple particulièrement simple peut être obtenu à partir des racines complexes de l'unité ; les racines $\sqrt[6]{2}\exp(2\mathrm{i}k\pi/6)$ avec $k \in \{0 \cdots 5\}$ du polynôme $x^6 - 2$ s'expriment à l'aide de radicaux :

$$\pm\sqrt[6]{2} \quad \text{et} \quad \frac{\pm 1 \pm \mathrm{i}\sqrt{3}}{2}\sqrt[6]{2}.$$

∗ L'égalité du polynôme développé et du polynôme factorisé fournit des relations entre les racines. Ainsi les racines complexes u, v et w d'un polynôme du troisième degré vérifie ces relations :

$$(X-u)(X-v)(X-w) = X^3 + a_2X^2 + a_1X + a_0$$
$$= X^3 - (u+v+w)X^2 + (uv+vw+uw)X - uvw$$
$$\begin{cases} u+v+w = -a_2 \\ uv+vw+uw = a_1 \\ uvw = -a_0 \end{cases}$$

∗ La somme et le produit des racines de polynômes du second degré obéissent au même principe.
La méthode est la même pour les polynômes de degré supérieur.

▶ Détermination des complexes u, v et w vérifiant ces trois équa-

tions :

$$u+v+w=2 \qquad u^2+v^2+w^2=6 \qquad uvw=-2$$

⩥ La méthode consiste à rechercher le polynôme P de degré trois ayant ces trois racines u, v et w :

$$\left\{\begin{array}{r} u+v+w=2 \\ u^2+v^2+w^2=6 \\ uvw=-2 \end{array}\right. \qquad \begin{array}{l} 2(uv+vw+uw) \\ =(u+v+w)^2-(u^2+v^2+w^2)=-2 \end{array}$$

$$\begin{aligned} P(X) &= X^3-2X^2-X+2=(X-1)(X^2-X-2) \\ &= (X-1)(X+1)(X-2) \qquad \{u,v,w\}=\{-1,1,2\} \end{aligned}$$

La seule solution possible est celle-ci, la vérification que ces valeurs conviennent est immédiate.

Factorisation des polynômes à coefficients réels

■ Tout polynôme non nul P de $\mathbb{R}[X]$ se factorise de façon unique à l'ordre près des facteurs sous la forme suivante où $\lambda\in\mathbb{R}^*$ est le coefficient de plus haut degré de P, les $(r_k)_{k=1}^s\in\mathbb{R}^s$ sont les racines réelles de P supposées distinctes deux à deux, e_k est l'ordre de multiplicité de r_k pour $k\in\{1\cdots s\}$, les $t\in\mathbb{N}$ couples $(u_k,v_k)_{k=1}^t$ de $\mathbb{R}^2$ vérifiant $u_k^2-4v_k<0$ sont différents deux à deux, et $f_k\in\mathbb{N}^*$ est l'ordre de multiplicité de ces facteurs du second degré :

$$P=\lambda\prod_{k=1}^{s}(X-r_k)^{e_k}\prod_{k=1}^{t}(X^2+u_kX+v_k)^{f_k} \qquad u_k^2-4v_k<0$$

◊ Ce théorème, admis dans ce cours, est une conséquence du théorème de d'Alembert-Gauss.
Tout polynôme à coefficients dans $\mathbb{R}$ peut aussi être considéré comme un polynôme à coefficients dans $\mathbb{C}$.

∗ Le passage d'une factorisation à l'autre consiste à regrouper les racines complexes conjuguées des facteurs $X^2+u_kX+v_k$ de seconde espèce de discriminant négatif : $\Delta=u_k^2-4v_k<0$.

∗ Deux polynômes de $\mathbb{R}[X]$ peuvent avoir un facteur commun sans avoir de racines réelles communes :

$$\begin{aligned} X^4-1 &= (X-1)(X+1)(X^2+1) \\ &= (X-1)(X+1)(X-\mathrm{i})(X+\mathrm{i}) \\ X^4+2X^2+1 &= (X^2+1)^2=(X-\mathrm{i})^2(X+\mathrm{i})^2 \end{aligned}$$

∗ Tout polynôme $P\neq 0$ à coefficients réels se factorise en produit de polynômes du premier ou du deuxième degré et possède au maximum $\deg P$ racines réelles.

Autres propriétés des polynômes réels et complexes

∗ Tout polynôme $P\neq 0$ à coefficients complexes possède exactement $\deg P$ racines, comptées avec leur ordre de multiplicité.
Tout polynôme $P\neq 0$ à coefficients réels se factorise en produit de polynômes du premier ou du deuxième degré et possède au contraire au maximum $\deg P$ racines réelles.

∗ Tout polynôme réel ou complexe de degré inférieur ou égal à n ayant $n+1$ ou plus racines est la polynôme nul.
Tout polynôme ayant une famille infinie de racines est le polynôme nul.
Tout polynôme s'annulant sur un intervalle ni vide ni réduit à un point est le polynôme nul.

∗ Deux polyômes de $\mathbb{C}[X]$ sont sans facteur commun si et seulement s'ils n'ont pas de racines communes.
Deux polynômes de $\mathbb{R}[X]$ peuvent avoir un facteur commun sans avoir de racines réelles communes :

$$\begin{aligned} X^4-1 &= (X-1)(X+1)(X^2+1) \\ &= (X-1)(X+1)(X-\mathrm{i})(X+\mathrm{i}) \\ X^4+2X^2+1 &= (X^2+1)^2=(X-\mathrm{i})^2(X+\mathrm{i})^2 \end{aligned}$$

∗ La continuité et les limites en $\pm\infty$ prouvent que toute fonction polynomiale de degré impair possède au moins une racine réelle r, c'est-à-dire que r vérifie $P(r)=0$.

Exemples de factorisation

►⩥ Factorisations dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$ de X^4-1 et X^4+4 :

⩥ Cette factorisation repose sur des produits remarquables, deux méthodes sont possibles pour le second polynôme :

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

$$\begin{aligned}X^4+4&=(X^2-2\mathrm{i})(X^2+2\mathrm{i})\\&=(X^2-(\sqrt{2}e^{\mathrm{i}\pi/4})^2)(X^2-(\sqrt{2}e^{3\mathrm{i}\pi/4})^2)\\&=(X-\sqrt{2}e^{\frac{\mathrm{i}\pi}{4}})(X+\sqrt{2}e^{\frac{\mathrm{i}\pi}{4}})(X-\sqrt{2}e^{\frac{3\mathrm{i}\pi}{4}})(X+\sqrt{2}e^{\frac{3\mathrm{i}\pi}{4}})\\&=\big(X-(1+\mathrm{i})\big)\big(X-(-1-\mathrm{i})\big)\big(X-(-1+\mathrm{i})\big)\big(X-(1-\mathrm{i})\big)\\&=\Big(\big(X-(1+\mathrm{i})\big)\big(X-(1-\mathrm{i})\big)\Big)\Big(\big(X-(-1+\mathrm{i})\big)\big(X-(-1-\mathrm{i})\big)\Big)\\&=(X^2-2X+2)(X^2+2X+2)\end{aligned}$$

$$\begin{aligned}X^4+4&=(X^2+2)^2-4X^2=(X^2-2X+2)(X^2+2X+2)\\&=\big(X-(1+\mathrm{i})\big)\big(X-(1-\mathrm{i})\big)\big(X-(-1+\mathrm{i})\big)\big(X-(-1-\mathrm{i})\big)\end{aligned}$$

Le première méthode appliquée au second polynôme fournit d'abord quatre racines complexes qui regroupées par conjugaison aboutissent à la factorisation réelle.
La seconde méthode aboutit d'abord à la factorisation réelle avec un discriminent $\Delta=-4$ négatif dans les deux facteurs, avant d'en déduire la factorisation complexe.

▸▸ Les factorisations et les racines complexes des deux derniers polynômes se déduisent du premier :
$X^2-2\cos\theta\,X+1$ $\qquad$ $X^4-2\cos\theta\,X^2+1$ $\qquad$ $X^6-2\cos\theta\,X^3+1$

▹▹ Le discriminant $\Delta=4(\cos^\theta-1)=4\sin^2\theta$ du premier polynôme est de racine carrée $\pm\mathrm{i}\,\sin\theta$. Ses racines en coordonnées polaires sont donc $\cos\theta\pm\mathrm{i}\,\sin\theta=e^{\pm\mathrm{i}\theta}$.
Les racines des deux autres polynômes s'en déduisent par les changements de variables $Y=X^2$ et $Z=X^3$ et sont les racines carrées ou troisièmes de $e^{\pm\mathrm{i}\theta}$ immédiates à exprimer en coordonnées polaires :

$X^2-2\cos\theta\,X+1$ $\quad$ de racines $e^{\pm\mathrm{i}\theta}$

$X^4-2\cos\theta\,X^2+1$ $\quad$ de racines $\pm e^{\pm\mathrm{i}\theta/2}$

$X^6-2\cos\theta\,X^3+1$ $\quad$ de racines $e^{\pm\mathrm{i}(\theta+2k\pi)/3}$ avec $k\in\{0,1,2\}$

$$\begin{aligned}&X^2-2\cos\theta\,X+1=(X-e^{\mathrm{i}\theta})(X-e^{-\mathrm{i}\theta})\\&X^4-2\cos\theta\,X^2+1\\&=(X-e^{\mathrm{i}\theta/2})(X-e^{-\mathrm{i}\theta/2})(X+e^{\mathrm{i}\theta/2})(X+e^{-\mathrm{i}\theta/2})\\&=\Big(X^2-2\cos\Big(\frac{\theta}{2}\Big)X+1\Big)\Big(X^2+2\cos\Big(\frac{\theta}{2}\Big)X+1\Big)\end{aligned}$$

∗ Les n racines n-ème de l'unité sont les racines de X^n-1, d'où la

factorisation dans $\mathbb{C}[X]$:

$$z^n=1\Longleftrightarrow z=e^{2\mathrm{i}k\pi/n}\quad\text{avec } k\in\{0\cdots n-1\}$$

$$X^n-1=\prod_{k=0}^{n-1}\big(X-e^{\frac{2\mathrm{i}k\pi}{n}}\big)$$

∗ Les factorisations suivantes s'effectuent de la même façon :

$$X^n+1=\prod_{k=0}^{n-1}\big(X-e^{\frac{(2k+1)\mathrm{i}\pi}{n}}\big)\quad X^n-re^{\mathrm{i}\theta}=\prod_{k=0}^{n-1}\big(X-\sqrt[n]{r}\,e^{\frac{\mathrm{i}(\theta+2k\pi)}{n}}\big)$$

▸▸ Factorisations dans $\mathbb{R}[X]$ de $X^{2n}-1$ et de $X^{2n+1}+1$.

▹▹ Les racines réelles de $X^{2n}-1$ sont $1=e^{0\pi/(2n)}$ et $-1=e^{n\pi/(2n)}$. Les autres racines sont complexes, conjuguées et de module 1. La racine conjuguée de $e^{2\mathrm{i}k\pi/(2n)}$ est $e^{-2\mathrm{i}k\pi/(2n)}$ où $-n+1\leq-k\leq0$ dès que $0\leq k\leq n-1$.
Les factorisations réelles regroupent les racines conjuguées :

$$\begin{aligned}(X-e^{-\mathrm{i}\theta})(X-e^{\mathrm{i}\theta})&=X^2-2\cos\theta\,X+1\\X^{2n}-1&=\prod_{k=-n+1}^{n}\big(X-e^{\frac{2\mathrm{i}k\pi}{2n}}\big)\\&=(X-1)(X+1)\prod_{k=1}^{n-1}\Big(X^2-2\cos\Big(\frac{k\pi}{n}\Big)X+1\Big)\end{aligned}$$

La méthode est similaire pour le second polynôme où la seule racine réelle est $-1=e^{2\mathrm{i}(2n+1)\pi/(2n+1)}$; les racines conjuguées sont notées $e^{2\mathrm{i}(2k+1)\pi/(2n+1)}$ et $e^{-2\mathrm{i}(2n+1)\pi/(2n+1)}$ où $0\leq k<n$.

$$\begin{aligned}X^{2n+1}+1&=\prod_{k=-n}^{n}\big(X-e^{\frac{(2k+1)\mathrm{i}\pi}{2n+1}}\big)\\&=(X+1)\prod_{k=-n}^{-1}\big(X-e^{\frac{(2k+1)\mathrm{i}\pi}{2n+1}}\big)\prod_{k=0}^{n-1}\big(X-e^{\frac{(2k+1)\mathrm{i}\pi}{2n+1}}\big)\\&=(X+1)\prod_{k=0}^{n-1}\big(X-e^{-\frac{(2k+1)\mathrm{i}\pi}{2n+1}}\big)\prod_{k=0}^{n-1}\big(X-e^{\frac{(2k+1)\mathrm{i}\pi}{2n+1}}\big)\\&=(X-1)\prod_{k=0}^{n-1}\Big(X^2-2\cos\Big(\frac{(2k+1)\pi}{2n+1}\Big)X+1\Big)\end{aligned}$$

▸▸ Factorisation dans $\mathbb{R}[X]$ du polynôme X^4+X^2+1.

▹▹ Ce polynôme ne possède pas de racines réelles, car ses valeurs

sont supérieures à 1 ; sa factorisation comporte nécessairement deux polynômes réels du second degré :

$$X^4+X^2+1=(X^2+aX+b)(X^2+cX+d)$$
$$=X^4+(a+c)X^3+(b+ac+d)X^2+(ad+bc)X+bd$$

$$\begin{cases} a+c=0\\ b+ac+d=1\\ ad+bc=0\\ bd=1 \end{cases} \quad \begin{cases} c=-a \quad d=\dfrac{1}{b}\\ b-a^2+\dfrac{1}{b}=1\\ \dfrac{a}{b}-ab=0 \end{cases} \quad \begin{cases} c=-a \quad d=\dfrac{1}{b}\\ a\left(\dfrac{1}{b}-b\right)=0\\ b-a^2+\dfrac{1}{b}=1 \end{cases}$$

L'équation $a(1/b-b)=0$ aboutit à trois possibilités : $a=0$ ou $b=1$ ou $b=-1$ car $b=1/b$ est équivalent à $b^2-1=0$.
Le cas $a=0$ est impossible car l'équation $b-a^2+1/b=1$ devient $b^2-b+1=0$ qui a un discriminant $1-4<0$ et n'a donc pas de racines réelles.
Le cas $b=-1$ n'est pas possible car $b-a^2+1/b=1$ entraîne $-a^2-2=1$ qui n'a pas de solution réelle.
Ainsi $b=1$ est la seule possibilité et implique $2-a^2=1$, $a^2=1$, $a=\pm1$, $c=-a$ et $d=1$.
Les deux possibilités $a=1$ et $a=-1$ sont symétriques l'une de l'autre et intervertissent l'ordre des deux polynômes de la factorisation. La seule factorisation possible à l'ordre près des facteurs est donc la suivante :

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

Le théorème de factorisation justifie l'existence de cette factorisation, la seule possible. Il n'est donc pas nécessaire — sauf pour détecter des éventuelles erreurs de calculs — de vérifier effectivement le produit obtenu, même si ce raisonnement n'est pas constitué d'une suite d'équivalence.

⋗ Une autre méthode de factorisation de X^4+X^2+1. commence par un produit remarquable :

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

⋗ Il est aussi possible de rechercher les racines complexes j et $\overline{\mathrm{j}}$ de Y^2+Y+1 où $Y=X^2$, puis de calculer en coordonnées polaires leurs racines carrées ; $\mathrm{j}=e^{2\mathrm{i}\pi/3}$ a pour racines carrées $\pm e^{\mathrm{i}\pi/3}$, et $\overline{\mathrm{j}}$ a pour racines carrées $\pm e^{-\mathrm{i}\pi/3}$. La factorisation dans $\mathbb{R}[X]$ s'obtient

en regroupant les racines conjuguées :

$$X^4+X^2+1=Y^2+Y+1=(Y-\mathrm{j})(Y-\overline{\mathrm{j}})=(X^2-\mathrm{j})(X^2-\overline{\mathrm{j}})$$
$$=(X-e^{\mathrm{i}\pi/3})(X+e^{\mathrm{i}\pi/3})(X-e^{-\mathrm{i}\pi/3})(X+e^{\mathrm{i}\pi/3})$$
$$=(X-e^{\mathrm{i}\pi/3})(X-e^{-\mathrm{i}\pi/3})(X+e^{\mathrm{i}\pi/3})(X+e^{\mathrm{i}\pi/3})$$
$$=\left(X^2-2\cos\left(\frac{\pi}{3}\right)X+1\right)\left(X^2+2\cos\left(\frac{\pi}{3}\right)X+1\right)$$
$$=(X^2-X+1)(X^2+X+1)$$

∗ Ces différents exemples récapitulent les principales méthodes de factorisation des polynômes à coefficients réels ou complexes.

▶▶ Développer le produit suivant consiste à énumérer les deux choix possibles X et r_k pour les n facteurs. La formule développée comporte 2^n termes dont un de degré n et un de degré 0 :

$$\prod_{k=1}^{n}(X-r_k)=(X-r_1)(X-r_2)\cdots(X-r_n)$$
$$=X^n-\Big(\sum_{k=0}^{n}r_k\Big)X+\cdots+(-1)^n\prod r_k$$

En déduire la somme des carrés des racines du polynôme unitaire en fonction des coefficients de sa formule développée.

⋗ L'identification des formes développées et factorisées d'un polynôme P unitaire et scindé de degré $n>0$ aboutit à des relations entre ses coefficients et ses racines :

$$P(X)=\sum_{k=0}^{n}a_kX^k=\prod_{k=1}^{n}(X-r_k) \quad \text{avec } a_n=1 \quad \deg P=n$$

$$a_{n-1}=-\sum_{k=1}^{n}r_k \qquad a_{n-2}=\sum_{1\le i<j\le n}r_ir_j$$

$$a_{n-3}=\sum_{1\le i<j<k\le n}r_ir_jr_k \qquad a_0=(-1)^n\prod_{k=1}^{n}r_k$$

$$a_1=(-1)^{n-1}\sum_{k=1}^{n}\prod_{\substack{1\le i\le n\\ i\ne k}}r_i$$
$$=(-1)^{n-1}(r_2r_3\cdots r_n+r_1r_3\cdots r_n+\cdots+r_1r_2\cdots r_{n-1})$$

Ainsi la somme des carrés des racines du polynôme unitaire P est donc la suivante dès que $\deg P \geq 2$:

$$a_{n-1} = -\sum_{k=1}^{n} r_k \qquad a_{n-1}^2 = \Big(\sum_{k=1}^{n} r_k\Big)^2 = \sum_{k=1}^{n} r_k^2 + 2\sum_{1\leq i<j\leq n} r_i r_j$$

$$a_{n-2} = \sum_{1\leq i<j\leq n} r_i r_j \qquad \sum_{k=1}^{n} r_k^2 = a_{n-1}^2 - 2a_{n-2}$$

$*$ Des transformations algébriques permettent de déterminer de façon similaire cette somme des puissances troisièmes des racines, et celle des puissances d'ordre $m \in \mathbb{N}^*$.
La somme et le produit des deux racines d'un polynôme du second degré est un cas particulier de ces expressions :

$$P = X^2 + bX + c = (X - r_1)(X - r_2) = X^2 - (r_1 + r_2)X + r_1 r_2$$
$$b = -(r_1 + r_2) \qquad c = r_1 r_2$$

►> Déterminer les solutions complexes u, v et w de ce système consiste à rechercher un polynôme $X^3 + a_2X^2 + a_1X + a_0$ ayant ces trois racines, puis à déterminer ces racines qui sont évidentes sur cet exemple :

$$\begin{cases} u + v + z = 1 \\ uvw = -4 \\ \dfrac{1}{u} + \dfrac{1}{v} + \dfrac{1}{w} = 1 \end{cases}$$

$$1 = \frac{1}{u} + \frac{1}{v} + \frac{1}{w} = \frac{uv + vw + uw}{uvw} = \frac{uv + vw + uw}{-4}$$
$$(X - u)(X - v)(X - w)$$
$$= X^3 - (u+v+w)X^2 + (uv+vw+uw)X - uvw$$
$$X^3 - X^2 - 4X + 4 = (X - 1)(X^2 + 0X - 4)$$
$$= (X - 1)(X - 2)(X + 2)$$
$$\{u, v, w\} = \{-2, 1, 2\}$$

Application à la divisibilité et à l'arithmétique

Dans ce paragraphe les polynômes P et Q sont scindés et factorisés de la manière suivante où e_k ou f_k peuvent être éventuellement nuls.

$$P = \lambda \prod_{k=1}^{s} (X - r_k)^{e_k} \qquad Q = \mu \prod_{k=1}^{s} (X - r_k)^{f_k} \qquad \lambda \neq 0 \qquad \mu \neq 0$$

• De façon analogue aux nombres entiers, le polynôme P divise le polynôme Q si et seulement si les exposants de Q sont inférieurs à ceux de P :

$$P \mid Q \Longleftrightarrow \big(\forall\, k \in \{1 \cdots s\} \quad e_k \leq f_k\big)$$

• Le plus grand communs diviseur et le plus petit commun multiple de deux polynômes factorisés sont ceux-ci :

$$\operatorname{pgcd}(P, Q) = \prod_{k=1}^{s} (X - r_k)^{\min(e_k, f_k)}$$
$$\operatorname{ppcm}(P, Q) = \prod_{k=1}^{s} (X - r_k)^{\max(e_k, f_k)}$$

• La démonstration est comparable à celle de la propriété similaire sur les entiers ; le rôle des polynômes du premier degré $X - r$ est analogue à celui des nombres premiers dans $\mathbb{Z}$, et une multiplication par $\lambda \in \mathbb{K}^* = \mathbb{U}(\mathbb{K}[X]$ dans l'anneau des polynômes correspond à un produit par $\pm 1 \in \mathbb{U}(\mathbb{Z})$.

• Deux polynômes P et Q de $\mathbb{C}[X]$ sans racines complexes communes sont premier entre eux : $\operatorname{pgcd}(P, Q) = 1$.

• Sauf pour les polynômes déjà factorisés, l'algorithme d'Euclide est généralement plus efficace pour calculer le pgcd de deux polynômes car il évite la recherche des racines des polynômes.