Polynômes

Aperçu

D 1

- Un **polynôme** à coefficients dans $\mathbb{K}$ est une suite $P = (a_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang

$$P = (a_0, a_1, \dots, a_n, 0, 0, \dots, 0, \dots) \in \mathbb{K}^{\mathbb{N}}.$$

  On dit qu'une telle suite est de **support fini** ou qu'elle est **presque nulle**.
- a_k est un élément de $\mathbb{K}$ et s'appelle le **coefficient d'indice** k du polynôme P.
- On note $\mathbf{0} = (0, 0, 0, \dots, 0, \dots)$ le polynôme dont tous les coefficients sont nuls, on dit que $\mathbf{0}$ est le **polynôme nul**.

De la définition de l'égalité de deux applications (ici de $\mathbb{N}$ dans $\mathbb{K}$), il résulte que deux polynômes sont égaux si et seulement si ils ont mêmes coefficients.

Les sous-ensemble de $\mathbb{K}^{\mathbb{N}}$ formé des suites à support fini est noté $\mathbb{K}^{(\mathbb{N})}$. Toutefois, la définition formelle que nous venons de donner permet de définir rigoureusement la notion de polynômes mais elle est très lourde à manipuler. Nous allons donc adopter une notation plus pratique.

N

- Le polynôme $P = (a_0, a_1, \dots, a_n, 0, 0, \dots, 0, \dots)$ est noté
$$P(X) = \sum_{n \geq 0} a_n X^n.$$
On appellera respectivement **terme de degré** $\boldsymbol{n}$ et **coefficient de degré** $\boldsymbol{n}$ du polynôme P le **monôme** $a_n X^n \in \mathbb{K}[X]$ et le **coefficient** $a_n \in \mathbb{K}$.
- Un polynôme $\sum_{n \geq 0} a_n X^n$ tel que $a_n = 0$ pour $n \geq 1$ est appelé **polynôme constant** et identifié à l'élément a_0 de $\mathbb{K}$.
- On appelle **indéterminée** le polynôme
$$X = (0, 1, 0, 0, \dots) = (\delta_{1,n})_{n \in \mathbb{N}}.$$

L'ensemble des polynôme à coefficients dans $\mathbb{K}$ se note $\mathbb{K}[X]$.

E 2 La suite $(1, 0, 3, 0, \dots, 0, \dots)$ correspond à $1 + 3X^2$.

La notion d'égalité entre polynômes se déduit de l'égalité entre suites.

P 3 *Deux polynômes sont égaux si et seulement si leurs coefficients sont égaux.*

$$\sum_{n\geq 0} a_n X^n = \sum_{n\geq 0} b_n X^n \iff \forall n \in \mathbb{N}, a_n = b_n$$

$$\sum_{n\geq 0} a_n X^n = 0 \iff \forall n \in \mathbb{N}, a_n = 0.$$

X est une notation pour un objet particulier (un polynôme), *il ne s'agit ni d'une variable, ni d'une inconnue d'une équation*. L'avantage de cette notation est sa commodité d'emploi pour les opérations mais ne doit pas faire confondre une écriture telle que $aX + b = 0$ avec une équation en X. D'ailleurs,

$$aX + b = 0 \iff (a, b, 0, 0, \dots) = (0, 0, 0, 0, \dots) \iff a = 0 \text{ et } b = 0.$$

De même, dans aucun cas on pourra écrire une égalité $X = \lambda$ avec $\lambda \in \mathbb{K}$.

D 4 Soit $\lambda \in \mathbb{K}$ et soient P et Q deux polynômes à coefficients dans $\mathbb{K}$

$$P = \sum_{n \geq 0} a_n X^n \quad \text{et} \quad Q = \sum_{n \geq 0} b_n X^n.$$

- On appelle **somme des polynômes P et Q** le polynôme

$$P + Q = \sum_{n \geq 0} (a_n + b_n) X^n$$

- On appelle **produit des polynômes P et Q** le polynôme

$$P \times Q = \sum_{n \geq 0} c_n X^n \quad \text{avec} \quad c_n = \sum_{k=0}^{n} a_{n-k} b_k.$$

- On appelle **produit externe du polynôme P par le scalaire λ** le polynôme

$$\lambda \cdot P = \sum_{n \geq 0} \lambda a_n X^n.$$

T 5 *L'addition et la multiplications des polynômes sont des lois associatives, commutatives. De plus, la multiplication est distributive par rapport à l'addition.*

1. $\mathbb{K}[X]$ *muni de l'addition et de la multiplication des polynôme est un anneau commutatif.*
2. $\mathbb{K}[X]$ *muni de l'addition des polynôme et de la multiplication externe est un $\mathbb{K}$-espace vectoriel.*
3. $\mathbb{K}[X]$ *muni de ces trois opérations est une $\mathbb{K}$-algèbre.*

R

1. Lorsqu'aucune confusion est possible, on pourra omettre les symboles de multiplication: $PQ = P \times Q$, $\lambda P = \lambda \cdot P$.
2. La multiplication des polynômes admet pour élément neutre le polynôme $1 = 1X^0 + 0X^1 + \dots$.
3. Nous utiliserons la convention usuelle d'exponentiation: pour tout polynôme P, P^0 sera par convention le polynôme 1 ; pour tout $n \geq 1$, P^n désignera le polynôme $P \times \cdots \times P$ (n fois).
4. La formule du binôme de Newton, reste valide

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

ainsi que les autres identités remarquables comme

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

T 6 *Tout polynôme non nul de $\mathbb{K}[X]$ admet une unique écriture*

$$P(X) = \sum_{n=0}^{d} a_n X^n = a_0 + a_1 X + \cdots + a_d X^d, \quad \textit{avec} \quad a_d \neq 0.$$

Cela justifie, a posteriori, la notation $P = \sum_{n \geq 0} a_n X^n$.

D 7 Soit $P = \sum_{n \geq 0} a_n X^n \in \mathbb{K}[X]$.

- Lorsque $P \neq \mathbf{0}$, on appelle **degré** de P, et l'on note $\deg P$, le plus grand des entiers d tel que $a_d \neq 0$.
- Le **terme dominant** de P est $a_d X^d$ et son **coefficient dominant** est a_d. Ils ne sont définis que pour des polynômes non nuls.
- Le polynôme P est dit **unitaire** ou **normalisé** si son coefficient dominant est 1.
- Lorsque $P = \mathbf{0}$, le degré de P est égal par convention à $-\infty$.

Lorsqu'il sera question de degré de polynômes, nous conviendrons de prolonger à $\mathbb{N} \cup \{ -\infty \}$ la relation d'ordre et l'addition de $\mathbb{N}$ par les conventions suivantes, où $n \in \mathbb{N}$,

P 8

1. *Pour tous $P, Q \in \mathbb{K}[X]$,*

$$P \times Q = \mathbf{0} \implies P = \mathbf{0} \text{ ou } Q = \mathbf{0}.$$

   *On dit que $\mathbb{K}[X]$ est **intègre**.*
2. *L'ensemble des polynômes inversibles pour la multiplication est l'ensemble des polynômes constants non nuls.*
3. *On a les règles suivantes pour des polynômes P et Q non nuls:*

$$\text{terme dominant}(PQ) = \text{terme dominant}(P) \times \text{terme dominant}(Q)$$
$$\text{coefficient dominant}(PQ) = \text{coefficient dominant}(P) \times \text{coefficient dominant}(Q).$$

Démonstration. Soit P, Q deux polynômes non nuls. Écrivons $P(X) = a_0 + \cdots + a_d X^d$ et $Q(X) = b_0 + \cdots + b_e X^e$ avec $a_d \neq 0$ et $b_e \neq 0$. Alors, de la définition de la multiplication dans $\mathbb{K}[X]$, on tire

$$PQ(X) = a_0 b_0 + \cdots + a_d b_e X^{d+e} \quad \text{et} \quad a_d b_e \neq 0.$$

Le fait que $PQ \neq 0$ et les deux règles de s'en déduisent immédiatement.
Il est clair que si $P \in \mathbb{K} \setminus \{0\}$, P est inversible dans $\mathbb{K}$ donc dans $\mathbb{K}[X]$. Réciproquement, si $PQ = 1$, alors P et Q sont non nuls, et le polynôme $PQ = 1$ a pour terme dominant $1 = a_d b_e X^{d+e}$, d'où $a_d b_e = 1$ et $d + e = 0$, d'où $d = e = 0$. ∎

C 9 *Tout polynôme non nul est simplifiable, c'est-à-dire, pour* $P, A, B \in \mathbb{K}[X]$,

$$(P \times A = P \times B \text{ et } P \neq \mathbf{0}) \implies A = B.$$

T 10 *Pour tous* $P, Q \in \mathbb{K}[X]$,

1. $\deg(PQ) = \deg(P) + \deg(Q)$,
2. $\deg(P+Q) \leq \max\left(\deg(P), \deg(Q)\right)$,
3. $\deg(P+Q) < \max\left(\deg(P), \deg(Q)\right)$ *si, et seulement si*

$$\deg P = \deg Q \geq 0 \text{ et } cd(P) + cd(Q) = 0.$$

Démonstration. En reprenant les notations de la démonstration précédente.
Si $\deg P < \deg Q$ (l'autre cas est symétrique), alors

$$(P+Q)(X) = (a_0 + b_0) + \cdots + (a_d + b_d)X^d + \cdots + b_e X^e \qquad \text{et} \qquad b_e \neq 0.$$

donc $\deg(P+Q) = \deg(Q)$.
Si $\deg P = \deg Q$, alors

$$(P+Q)(X) = (a_0 + b_0) + \cdots + (a_d + b_d)X^d,$$

donc $\deg(P+Q) \leq d$ et l'on a $\deg(P+Q) < d$ si, et seulement si $a_d + b_d = 0$. ∎

D 11 Soit $P = \sum_{n \geq 0} a_n X^n \in \mathbb{K}[X]$ et $x \in \mathbb{K}$.

- On note

$$\widetilde{P}(x) = \sum_{n=0}^{\deg P} a_n x^n \in \mathbb{K}.$$

$\widetilde{P}(x)$ s'appelle l'**élément de $\mathbb{K}$ déduit par substitution de x à X dans P**, ou encore la **valeur de P en x**. Plus simplement, on peut noter

$$\widetilde{P}(x) = P(x) = \sum_{n \geq 0} a_n x^n.$$

- L'application

$$\widetilde{P} : \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & \widetilde{P}(x) \end{array}$$

s'appelle la **fonction polynômiale** définie par P.

P 12 *Quels que soient les polynômes P et Q de $\mathbb{K}[X]$, et le scalaire $\lambda \in \mathbb{K}$, on a*

$$\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}, \quad \widetilde{\lambda \cdot P} = \lambda \cdot \widetilde{P} \quad \text{et} \quad \widetilde{P \times Q} = \widetilde{P} \times \widetilde{Q}.$$

Remplaçons en effet $5x^4 - 4x^3 + 3x^2 - 2x + 1$ par l'expression équivalente

$$x(x(x(x \times 5 - 4) + 3) - 2) + 1,$$

On économise donc des multiplications, qui sont des opérations longues à réaliser.

P 13

$$\sum_{n=0}^{d} a_n x^n = x\left(\ldots\left(x\left(x\left(x \times a_d + a_{d-1}\right) + a_{d-2}\right) + a_{d-3}\right)\cdots + a_1\right) + a_0.$$

D 14 Soit $(P, Q) \in \mathbb{K}[X]^2$, avec $P = \sum\limits_{n \geq 0} a_n X^n$. On appelle polynôme composé des deux polynômes P et Q, et on note $P \circ Q$ ou encore $P(Q)$ le polynôme défini par

$$P \circ Q = P(Q) = \sum_{n=0}^{\deg P} a_n Q^n$$

que l'on écrit plus simplement

$$P \circ Q = \sum_{n \geq 0} a_n Q^n.$$

On a bien sûr $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$.

D 15

- Un polynôme P est **pair** si $P(-X) = P(X)$.
- Un polynôme P est **impair** si $P(-X) = -P(X)$.

P 16 *Soit* $P = \sum_{n \geq 0} a_n X^n \in \mathbb{K}[X]$.

- P *est impair si et seulement si* P *ne contient que des termes non nuls de degré impairs, c'est-à-dire*
$$\forall n \in \mathbb{N}, n \in 2\mathbb{N} \implies a_n = 0.$$
- P *est pair si et seulement si* P *ne contient que des termes non nuls de degré pairs, c'est-à-dire*
$$\forall n \in \mathbb{N}, n \notin 2\mathbb{N} \implies a_n = 0.$$

D 17 Soient $A, B \in \mathbb{K}[X]$. On dit que $\boldsymbol{A}$ **divise** $\boldsymbol{B}$ lorsqu'il existe un polynôme Q vérifiant $B = AQ$. On note cette relation $A \mid B$. On dit aussi que B est un **multiple** de A.

Lorsque $A \neq 0$, le polynôme Q est unique car $\mathbb{K}[X]$ est intègre et s'appelle **quotient exact** de la division de B par A. Dans ce cas, on a

$$\deg A \leq \deg B \qquad \text{et} \qquad \deg Q = \deg B - \deg A.$$

E 18

1. $X - 1 \mid X^5 - 1$ car $X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1)$.
2. On a $X \mid 3X$, mais aussi $3X \mid X$ car $X = \frac{1}{3}3X$. Plus généralement, $\lambda P \mid P$ pour tout $\lambda \in \mathbb{K}^\star$.
3. Le polynôme nul $\mathbf{0}$ est multiple de tout polynôme (car $\mathbf{0} = A \times \mathbf{0}$) mais il ne divise que lui-même (car $B = Q \times \mathbf{0}$ implique $B = \mathbf{0}$).
4. Un polynôme de degré 0 divise tous les polynômes et n'est multiple que des polynômes de degré 0.
5. On a bien $3 \mid 2$ dans $\mathbb{K}[X]$ bien que cette relation soit fausse dans $\mathbb{N}$.

P 19 **Caractérisation des polynômes associés**

Soit A, B deux polynômes non nuls de $\mathbb{K}[X]$. Les assertions suivantes sont équivalentes

1. $A \mid B$ *et* $B \mid A$;
2. $A \mid B$ *et* $\deg A = \deg B$;
3. $\exists \lambda \in \mathbb{K} \setminus \{0\}, A = \lambda B$.

D 20 On dit que deux polynômes A et B sont **associés** lorsqu'il existe un scalaire non nul $\lambda \in \mathbb{K} \setminus \{0\}$ tel que $A = \lambda B$.

On note alors $A \sim B$. La relation $\sim$ est clairement une relation d'équivalence sur $\mathbb{K}[X]$.

T 21 *Soit* $A, B \in \mathbb{K}[X]$ *avec* $B \neq 0$. *Il existe un unique couple de polynômes* $(Q, R) \in \mathbb{K}[X]^2$ *tels que*

$$A = BQ + R \qquad \textit{et} \qquad \deg R < \deg B.$$

On appelle Q *le* ***quotient*** *de la division euclidienne de* A *par* B.
Le polynôme $R = A - BQ$ *est le* ***reste*** *de la division euclidienne de* A *par* B.

E 22 En suivant l'algorithme décrit dans la démonstration :

$$
\begin{array}{rrrrr|l}
2X^4 & +5X^3 & -X^2 & +2X & +1 & 2X^2-3X+1 \\
\cline{6-6}
+2X^4 & -3X^3 & +X^2 & & & X^2 \\
\cline{1-5}
 & 8X^3 & -2X^2 & +2X & +1 & \\
 & 8X^3 & -12X^2 & +4X & & +4X \\
\cline{2-5}
 & & 10X^2 & -2X & +1 & \\
 & & 10X^2 & -15X & +5 & +5 \\
\cline{3-5}
 & & & 13X & -4 &
\end{array}
$$

Ici $A = 2X^4 + 5X^3 - X^2 + 2X + 1$, $B = 2X^2 - 3X + 1$, $Q = X^2 + 4X + 5$, $R = 13X - 4$.

T 23 Effectuer la division euclidienne de $A = X^7 + X + 1$ par $B = X^3 + X + 1$.

T 24 *Soit $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Alors $B \,\Big|\, A$ si et seulement si le reste de la division euclidienne de A par B est nul.*

R Soit $A, B \in \mathbb{R}[X]$. Le quotient et le reste de la division euclidienne de B par A sont identique dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$.
Ainsi, si $A \,\Big|\, B$ dans $\mathbb{C}[X]$, c'est-à-dire $B = AQ$ avec $Q \in \mathbb{C}[X]$, alors $A \,\Big|\, B$ dans $\mathbb{R}[X]$, c'est-à-dire que $Q \in \mathbb{R}[X]$.

T 25 Soit $a \in \mathbb{K}$.

P 26 *Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.*
Le reste de la division euclidienne de $P(X)$ par $X - a$ est $\tilde{P}(a)$. On a donc l'équivalence

$$(X - a) \,\Big|\, P \iff \widetilde{P}(a) = 0.$$

D 27 Lorsque $\widetilde{P}(a) = 0$, on dit que a est **une racine** ou **un zéro** de P.

D 28 Soit $P \in \mathbb{K}[X]$ un polynôme non nul et soit $a \in \mathbb{K}$.

- On dit que a est **une racine** ou **un zéro** de P si $\widetilde{P}(a) = 0$.
  Pour que a soit un zéro de P, il faut, et il suffit, que $X - a$ divise P.
- On suppose que a est un zéro de P. Il existe alors un unique entier m tel que P est divisible par $(X-a)^m$ mais pas par $(X-a)^{m+1}$. On a $1 \leq m \leq \deg P$.
  L'entier m est appelé l'**ordre** ou la **multiplicité** de la racine a. La racine a est dite **simple** si $m = 1$, et **multiple** sinon.

T 29 *Soit $P \in \mathbb{K}[X]$ un polynôme non nul et soit $a \in \mathbb{K}$.*
a est une racine de multiplicité m si, et seulement si il existe un polynôme $Q \in \mathbb{K}[X]$ tel que

$$P = (X-a)^m Q \qquad \text{et} \qquad \widetilde{Q}(a) \neq 0.$$

E 30 Déterminons la multiplicité de 1 relativement aux polynômes $P = X^3 - 3X^2 + 2$ et $Q = X^3 - 4X^2 + 5X - 2$.

L 31 *Soient* $a_1, a_2, \dots, a_k$ *des racines deux à deux distinctes du polynôme non nul* P *et soient* $m_1, m_2, \dots, m_k$ *leurs multiplicités. Alors*

$$P(X) = \left(X - a_1\right)^{m_1} \left(X - a_2\right)^{m_2} \dots \left(X - a_k\right)^{m_k} Q(X) \quad \text{où} \quad Q(a_1) \neq 0, \dots, Q(a_k) \neq 0.$$

Soient $a_1, a_2, \dots, a_k$ toutes les racines de P et soient $m_1, m_2, \dots, m_k$ leurs multiplicités. L'expression **le nombre de racines de P comptées avec leurs multiplicités** désigne alors la somme $m_1 + m_2 + \cdots + m_k$ de ces multiplicités.

T 32 *Le nombre de racines d'un polynôme non nul P, comptées avec leurs multiplicités, est inférieur ou égal à $\deg(P)$.*

C 33 *Soit $n \in \mathbb{N}$. Si $\deg P \leq n$ et si P admet au moins $n+1$ racines distinctes alors $P = 0$.*

C 34 *Soient $P, Q \in \mathbb{K}[X]$ de degré $\leq n$. S'il existe $n+1$ éléments $x_1, \cdots, x_{n+1}$ de $\mathbb{K}$, deux à deux distincts, tels que $P(x_i) = Q(x_i)$ pour $1 \leq i \leq n+1$, on a $P = Q$.*

C 35 *Soient $P, Q \in \mathbb{K}[X]$ tels qu'il existe une partie infinie de $\mathbb{K}$ sur laquelle $\widetilde{P}$ et $\widetilde{Q}$ coïncident. Alors $P = Q$.*
En particulier, l'application $P \in \mathbb{K}[X] \mapsto \widetilde{P} \in \mathscr{F}(\mathbb{K}, \mathbb{K})$ est injective.

T 36 *Soient $(x_1, x_2, \dots, x_n)$ des éléments deux à deux distincts de $\mathbb{K}$. Pour $j \in [\![1, n]\!]$, on pose*

$$L_j = \prod_{k \in [\![1,n]\!] \setminus \{ j \}} \left(\frac{X - x_k}{x_j - x_k} \right).$$

Ces polynômes sont de degré $n-1$ et

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

T 37 **Polynôme d'interpolation de Lagrange**

Soient $(x_1, x_2, \dots, x_n)$ des éléments deux à deux distincts de $\mathbb{K}$ et $(y_1, y_2, \dots, y_n) \in \mathbb{K}^n$. L'unique polynôme P tel que

$$\deg(P) \leq n-1 \;\text{ et }\; P(x_1) = y_1 \;\text{ et }\; P(x_2) = y_2 \;\text{ et }\; \dots \;\text{ et }\; P(x_n) = y_n$$

est le polynôme

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

D 38 Un polynôme non nul P est dit **scindé** s'il est produit de polynômes du premier degré (ou, de manière équivalente, s'il admet $\deg(P)$ racines comptées avec leurs multiplicités).

Soit P un polynôme scindé de $\mathbb{K}[X]$ de degré $n \geq 1$, $x_1, \ldots, x_n$ ses zéros comptés avec leur ordre de multiplicité. Les éléments $x_1, \ldots, x_n$ sont éléments de $\mathbb{K}$ distincts ou non. On a deux écritures possibles

$$P = a_0 + a_1 X + \cdots + a_n X^n = a_n(X - x_1)(X - x_2) \cdots (X - x_n)$$

Quelles relations y-a-t-il entre $x_1, x_2, \ldots, x_n$ et $a_0, \ldots, a_n$?

P 39 **Cas $n = 2$**

Soit

$$P = a_0 + a_1 X + a_2 X^2 = a_2(X - x_1)(X - x_2)$$

un polynôme scindé de degré 2. *Alors*

$$x_1 x_2 = \frac{a_0}{a_2} \qquad \textit{et} \qquad x_1 + x_2 = -\frac{a_1}{a_2}.$$

P 40 **Cas $n = 3$**

Soit

$$P = a_0 + a_1 X + a_2 X^2 + a_3 X^3 = a_3(X - x_1)(X - x_2)(X - x_3)$$

un polynôme scindé de degré 3. *Alors*

$$x_1 x_2 x_3 = -\frac{a_0}{a_3} \quad x_1 x_2 + x_1 x_3 + x_2 x_3 = \frac{a_1}{a_3} \qquad x_1 + x_2 + x_3 = -\frac{a_2}{a_3}.$$

D 41 Soient $n \in \mathbb{N}^\star$, et $x_1, \dots, x_n$ dans $\mathbb{K}$. On note pour tout entier k compris entre 1 et n, [a]

$$\sigma_k(x_1, \dots, x_n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k} = \sum_{\substack{H \subset [\![1,n]\!] \\ \operatorname{card} H = k}} \prod_{i \in H} x_i.$$

La fonction $\sigma_k : \mathbb{K}^n \to \mathbb{K}$, s'appelle **fonction symétrique élémentaire de degré k**.

[a]41. Cette somme contient $\binom{n}{k}$ termes.

On écrira souvent σ_k au lieu de $\sigma_k(x_1, \dots, x_n)$ afin d'alléger les notations. On a par exemple

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + \cdots x_n \\
\sigma_2 &= \sum_{1 \leq i < j \leq n} x_i x_j = x_1 x_2 + x_1 x_3 + x_2 x_3 + \cdots + x_{n-1} x_n \\
&\vdots \\
\sigma_n &= x_1 x_2 \cdots x_n.
\end{aligned}$$

Lorsqu'il convient de préciser l'entier n, on écrit $\sigma_{k,n}$ pour σ_k.

T 42 **Relations coefficient-racines (Formules de Viète)**

Soit $P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ un polynôme scindé de $\mathbb{K}[X]$ de degré $n \geq 1$; on note $x_1, \ldots, x_n$ ses zéros comptés avec leur ordre de multiplicité.
Alors, pour $k = 1, \ldots, n$,

$$\sigma_{k,n} = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k} = (-1)^k \frac{a_{n-k}}{a_n}.$$

On peut donc écrire

$$P = a_n \left(X^n - \sigma_1 X^{n-1} + \cdots + (-1)^{n-1} \sigma_{n-1} X + (-1)^n \sigma_n \right).$$

E 43

- $n = 4, k = 2$: on a $\dfrac{a_2}{a_4} = x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4.$
- $k = 1$: $-\dfrac{a_{n-1}}{a_n} = \displaystyle\sum_{i=1}^{n} x_i.$
- $k = n$: $(-1)^n \dfrac{a_0}{a_n} = x_1 x_2 \cdots x_n.$

C 44 Somme et produit des racines

Soit

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_{n-1} X^{n-1} + a_n X^n = a_n (X - x_1)(X - x_2) \dots (X - x_n)$$

un polynôme scindé de $\mathbb{K}[X]$ *de degré* $n \geq 1$*; avec* $x_1, \dots, x_n$ *ses zéros comptés avec leur ordre de multiplicité. Alors*

$$x_1 x_2 \dots x_n = (-1)^n \frac{a_0}{a_n} \qquad \textit{et} \qquad x_1 + x_2 + \cdots + x_n = -\frac{a_{n-1}}{a_n}.$$

E 45 Soit $P = X^4 + 4X^3 + 2X^2 + 7X + 12 \in \mathbb{C}[X]$, x_1, x_2, x_3, x_4 ses zéros.
Calculer $x_1^3 + x_2^3 + x_3^3 + x_4^3$.
Il existe des formules permettant de résoudre une équation algébrique du 4-ième degré (c'est même la plus grande valeur des degrés pour lesquels des formules sont possibles). On se doute que ces formules sont d'une utilisation extrêmement malaisée, voire même impossible dans la pratique. Mais dans le cas présent, on peut écrire

$$\begin{aligned}
\sigma_1^3 = \left(\sum_{i=1}^4 x_i\right)^3 &= \sum_{i=1}^4 x_i^3 + 3\sum_{1\le i<j\le 4} x_i^2 x_j + 3\sum_{1\le i<j\le 4} x_i x_j^2 + 6\sum_{1\le i<j<k\le 4} x_i x_j x_k \\
&= \sum_{i=1}^4 x_i^3 + 3\left(\sum_{1\le i<j\le 4} x_i x_j (x_i + x_j)\right) + 6\sigma_3 \\
&= \sum_{i=1}^4 x_i^3 + 3\left(\sum_{1\le i<j\le 4} x_i x_j \sigma_1\right) - 3\times 3\left(\sum_{1\le i<j<k\le 4} x_i x_j x_k\right) + 6\sigma_3 \\
&= \sum_{i=1}^4 x_i^3 + 3\sigma_2\sigma_1 - 3\sigma_3.
\end{aligned}$$

Or on a $\sigma_1 = -4$, $\sigma_2 = 2$, $\sigma_3 = -7$, $\sigma_4 = 12$, d'où

$$\sum_{i=1}^4 x_i^3 = \sigma_1^3 - 3\sigma_2\sigma_1 + 3\sigma_3 = -61.$$

D 46 Soit $P = \sum_{n\geq 0} a_n X^n \in \mathbb{K}[X]$. On appelle **dérivée formelle de P** ou **polynôme dérivé de P**, le polynôme

$$P' = \sum_{n\geq 0} (n+1) a_{n+1} X^n.$$

Si $P = a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d$, alors

$$P' = a_1 + 2a_2 X + \cdots + d a_d X^{d-1} = \sum_{n=0}^{d-1} (n+1) a_{n+1} X^n = \sum_{n=1}^{d} n a_n X^{n-1}.$$

On utilise donc également la notation

$$P' = \sum_{n\geq 1} n a_n X^{n-1}.$$

R Il s'agit d'une dérivation formelle définie algébriquement. Bien sûr, dans le cas réel, on a pour $x \in \mathbb{R}$,

$$\widetilde{(P')}(x) = \left(\widetilde{P}\right)'(x).$$

T 47 *La dérivation* $\mathrm{D} : \mathbb{K}[X] \to \mathbb{K}[X]$ *est une application linéaire, c'est-à-dire,*

$$\forall(\alpha, \beta) \in \mathbb{K}^2, \forall(P, Q) \in \mathbb{K}[X]^2, (\alpha P + \beta Q)' = \alpha P' + \beta Q'.$$

De plus, la dérivation satisfait la règle de Leibniz:

$$\forall(P, Q) \in \mathbb{K}[X]^2, (PQ)' = P'Q + PQ'.$$

Démonstration. La linéarité de $P \mapsto P'$ est évidente.
Supposons $P = X^p$ et $Q = X^q$ avec $p, q \geq 1$. On a alors

$$(PQ)' = (p+q)X^{p+q-1} = pX^{p-1}X^q + X^p(qX^{q-1}) = P'Q + PQ'.$$

Supposons $P = X^p$ et $Q = \sum_{q\geq 0} b_q X^q$, alors

$$\begin{aligned}(PQ)' &= \left(\sum_{q\geq 0} b_q P X^q\right)' = \sum_{q\geq 0} b_q \,(PX^q)' \\ &= \sum_{q\geq 0} b_q \left(P'X^q + P(X^q)'\right) = P' \sum_{q\geq 0} b_q X^q + P \sum_{q\geq 0} b_q (X^q)' = P'Q + PQ'.\end{aligned}$$

Supposons $P = \sum_{p\geq 0} a_p X^p$ et $Q = \sum_{q\geq 0} b_q X^q$, alors

$$(PQ)' = \sum_{p\geq 0} a_p \,(X^p Q)' = \sum_{p\geq 0} a_p (X^p)' Q + \sum_{p\geq 0} a_p X^p Q' = P'Q + PQ'.$$

∎

T 48 *Soient $P, Q \in \mathbb{K}[X]$.*

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

En particulier, pour $m \geq 1$, $(P^m)' = mP^{m-1}P'$.

D 49 On définit par récurrence le **polynôme dérivé d'ordre k** de P, notée $P^{(k)}$ ou $\mathrm{D}^k(P)$, comme suit

- On pose $P^{(0)} = P$,
- pour $k \in \mathbb{N}$, on pose $P^{(k+1)} = \left(P^{(k)}\right)'$.

T 50 Quelles sont les dérivées successives de $P = X^m$? De $Q = (X - a)^m$?

T 51 **Formule de Leibniz pour les polynômes**

Soient $(P,Q) \in \mathbb{K}[X]^2$ *et* $k \in \mathbb{N}$. *Alors*

$$(PQ)^{(k)} = \sum_{j=0}^{k} \binom{k}{j} P^{(k-j)} \times Q^{(j)}.$$

T 52 **Formules de Taylor pour les polynômes**

Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors

$$P(X) = \sum_{n \geq 0} \frac{P^{(n)}(a)}{n!}(X-a)^n = P(a) + P'(a)(X-a) + \cdots + \frac{P^{(d)}(a)}{d!}(X-a)^d,$$

où $d = \deg(P)$.

On a donc en particulier

$$P(X) = \sum_{n \geq 0} \frac{P^{(n)}(0)}{n!} X^n = P(0) + P'(0)X + \cdots + \frac{P^{(d)}(0)}{d!} X^d$$

et aussi

$$P(X+a) = \sum_{n \geq 0} \frac{P^{(n)}(a)}{n!} X^n = P(a) + P'(a)X + \cdots + \frac{P^{(d)}(a)}{d!} X^d.$$

T 53 *Soit P un polynôme non nul sur le corps $\mathbb{K}$.*

1. *Pour que $a \in \mathbb{K}$ soit racine multiple de P, il faut, et il suffit, que a soit racine de P et de P'.*
2. *Soit m un entier non nul. Pour que $a \in \mathbb{K}$ soit racine de P d'ordre m, il faut, et il suffit que*

$$P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0 \qquad \text{et} \qquad P^{(m)}(a) \neq 0.$$

C 54 *$a \in \mathbb{K}$ est racine simple de P si et seulement si $P(a) = 0$ et $P'(a) \neq 0$.*

E 55 Déterminons la multiplicité de 1 relativement aux polynômes $P = X^3 - 3X^2 + 2$ et $Q = X^3 - 4X^2 + 5X - 2$.

1. On a $P(1) = 0$, $P' = 3X^2 - 6X$, $P'(1) = -3 \neq 0$: 1 est donc racine simple de P.
2. On a $Q(1) = 0$, $Q' = 3X^2 - 8X + 5$, $Q'(1) = 0$, $Q'' = 6X - 8$, $Q''(1) = -2 \neq 0$: 1 est racine double de Q.

D 56 Un polynôme P non constant est dit **irréductible** ou **premier** si les seuls diviseurs de P sont les polynômes associés à P et les polynômes inversibles.
Dans le cas contraire, on dit que P est **réductible**.

Ainsi, le polynôme P de degré supérieur ou égal à 1 est irréductible si, et seulement si l'on a l'implication

$$\forall (A, B) \in \mathbb{K}[X]^2, P = AB \implies \deg A = 0 \text{ ou } \deg B = 0.$$

E 57 **Cas importants**

1. Un polynôme constant n'est ni réductible ni irréductible.
2. Tout polynôme de degré 1 est irréductible.
3. Le polynôme $X^2 + 1$ de $\mathbb{R}[X]$ est irréductible. Mais le même polynôme $X^2 + 1$, considéré comme élément de $\mathbb{C}[X]$, se factorise en $(X + i)(X - i)$. La notion de polynôme irréductible est donc relative au corps de base $\mathbb{K}$.
4. Un polynôme de degré 2 est irréductible dans $\mathbb{K}[X]$ si, et seulement s'il n'a pas de racine dans $\mathbb{K}$.

T 58 *Tout polynôme non constant est produit de polynômes irréductibles.*

Dans cette partie, on note $\mathrm{Div}(A)$ l'ensemble des polynômes divisant A et $\mathrm{Div}(A, B)$ l'ensemble des polynômes divisant à la fois A et B, c'est-à-dire

$$\mathrm{Div}(A, B) = \mathrm{Div}(A) \cap \mathrm{Div}(B).$$

P 59 *Soient A, B, P, Q, U, V des polynômes.*

1. *Si $P \in \mathrm{Div}(A, B)$ et $Q \mid P$, alors $Q \in \mathrm{Div}(A, B)$.*
2. *Si P et Q sont associés : $(P \in \mathrm{Div}(A, B)) \iff (Q \in \mathrm{Div}(A, B))$.*
3. *Si $P \in \mathrm{Div}(A, B)$, alors $P \mid UA + VB$.*
4. $\mathrm{Div}(A, B - UA) = \mathrm{Div}(A, B)$.

D 60 Soit A et B deux polynômes dont l'un au moins est non nul.

- On dit que A et B sont premiers entre eux lorsqu'ils n'ont pas de diviseur commun non inversible.
- On appelle **plus grand commun diviseur** de A et B, ou **pgcd** de A et B, tout polynômes de degré maximum parmi les diviseurs commun à A et B.

Cette définition a un sens car $\mathrm{Div}(A, B)$ est non vide (il contient 1) et les degrés des éléments de $\mathrm{Div}(A, B)$ sont majorés par $\min\left(\deg(A), \deg(B)\right)$.

R

1. Dire que A et B sont premiers entre eux revient à dire que 1 est un pgcd de A et B.
2. Si $A \mid B$, alors A est un pgcd de A et B.

T 61 *Soient A et B des polynômes non nuls. Un pgcd de A et B est un polynômes $D = A_{m-1}$ où $\left(A_k\right)_{k\in\mathbb{N}}$ est la suite de polynômes telle que*

- $A_0 = A$,
- $A_1 = B$,
- *Pour $k \geq 2$, A_k est le reste de la division euclidienne de A_{k-2} par A_{k-1}.*
- $A_m = 0$ *et si* $k < m$, *alors* $A_k \neq 0$.

Démonstration. Supposons que $A_0, A_1, \dots, A_n$ soient non nuls, alors

$$\deg A_1 > \deg A_2 > \dots \deg A_n.$$

Ceci n'est pas possible indéfiniment, donc $n \leq \deg(A_1)$. Il existe donc $m \geq 2$ tel que $A_m = 0$. Cela signifie que A_{m-1} divise A_{m-2}.
Or, pour $k = 1, 2, \dots m-2$, on a $\mathrm{Div}(A_{k+1}, A_k) = \mathrm{Div}(A_k, A_{k-1})$. Donc $\mathrm{Div}(A, B) = \mathrm{Div}(A_{m-2}, A_{m-1})$. Finalement, A_{m-1} est un pgcd de A et B. ∎

T 62 *Soient A et B des polynômes non nuls.*

1. *Les pgcd de A et B sont deux à deux associés.*
2. *Un polynôme D est un pgcd de A et B si, et seulement si*

$$D \,\Big|\, A \text{ et } D \,\Big|\, B \text{ et } \exists (U,V) \in \mathbb{K}[X]^2, UA + VB = D.$$

3. *Si D est un pgcd de A et B, alors l'ensemble des diviseur communs à A et B est l'ensemble des diviseurs de D.*

D 63 Tous les pgcd de A et B sont associés. On appellera celui qui est unitaire **le pgcd** de A et B et on le notera $\mathrm{pgcd}(A, B)$ ou $A \wedge B$.

On conviendra que $\mathrm{pgcd}(0, 0) = 0$ (qui n'est pas unitaire!).

T 64 **Théorème de Bézout**

Deux polynômes A et B sont premiers entre eux si, et seulement si il existe des polynômes U et V tels que

$$UA + VB = 1.$$

T 65 **Lemme de Gauß pour les polynômes**

Soient A, B, C des polynômes non nuls.

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

T 66 **Lemme d'Euclide pour les polynômes**

Soit P un polynôme irréductible.

$$\forall (A, B) \in \mathbb{K}[X]^2, P \,\Big|\, AB \implies P \,\Big|\, A \text{ ou } P \,\Big|\, B.$$

T 67 *Si A est premier avec B et C, alors A est premier avec BC.*

D 68 Soient A et B des polynômes non nuls. Un **plus petit commun multiple** de A et B, ou **ppcm** de A et B est un polynôme non nul C qui est multiple de A et multiple de B et qui est de degré minimum parmi leurs multiples communs non nuls.

T 69 *Soient A et B des polynômes non nuls. Soit M un ppcm de A et B.*

1. *Les autres ppcm de A et B sont les polynômes associés à M. En particulier, il existe un et un seul ppcm unitaire de A et B.*
2. *Soit D un pgcd de A et B, alors MD et AB sont associés.*
3. *L'ensemble des multiples communs à A et B est l'ensemble des multiples de M.*

D 70 Soient $A_1, A_2, \ldots, A_r \in \mathbb{K}[X]$ dont l'un au moins est non nul.

- On appelle **plus grand commun diviseur** de $A_1, A_2, \ldots, A_r$ tout diviseur commun de $A_1, A_2, \ldots, A_r$ de degré maximal.
- Les pgcd de $A_1, A_2, \ldots, A_r$ sont associés. Un seul d'entre eux est unitaire, on l'appelle **le pgcd** de $A_1, A_2, \ldots, A_r$ et on le note

$$A_1 \wedge A_2 \wedge \cdots \wedge A_r \quad \text{ou} \quad \operatorname{pgcd}(A_1, A_2, \ldots, A_r).$$

On pose par convention $\operatorname{pgcd}(0, 0, \ldots, 0) = 0$.

P 71 *Soient $A_1, A_2, \dots, A_r \in \mathbb{K}[X]$.*

1. *Les diviseurs communs de $A_1, A_2, \dots, A_r$ sont exactement les diviseur de $\operatorname{pgcd}(A_1, A_2, \dots, A_r)$.*
2. *Il existe des polynômes $U_1, U_2, \dots, U_r \in \mathbb{K}[X]$ pour lesquels*

$$U_1A_1 + U_2A_2 + \cdots + U_rA_r = \operatorname{pgcd}(A_1, A_2, \dots, A_r).$$

Une telle relation est appelée ***une relation de Bézout*** *pour $A_1, A_2, \dots, A_r$.*

D 72

- On dit que $A_1, A_2, \dots, A_r$ sont **premiers entre eux dans leur ensemble** si 1 est leur seul diviseur commun unitaire, c'est-à-dire lorsque $\mathrm{pgcd}(A_1, A_2, \dots, A_r) = 1$.
- On dit que $A_1, A_2, \dots, A_r$ sont **premiers entre eux deux à deux** si pour tous $i, j \in [\![1, r]\!]$ distincts, les polynômes A_i et A_j sont premiers entre eux.

Si les polynômes $A_1, A_2, \dots, A_r$ sont premiers entre eux deux à deux, alors ils sont premiers entre eux dans leur ensemble. La réciproque est fausse.

T 73 *Tout polynôme non nul P admet une factorisation*

$$P = C P_1 \dots P_r,$$

où $C \in \mathbb{K}^\star$ et où $P_1, \dots, P_r$ sont irréductibles unitaires. Cette décomposition est unique à l'ordre près des facteurs irréductibles.

T 74 **Théorème de d'Alembert-Gauß ou T.F.A**

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

Démonstration. Théorème admis. ∎

T 75 *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*

C 76 *Deux polynômes de $\mathbb{C}[X]$ sont premiers entre eux si, et seulement si ils n'ont pas de racine commune.*

T 77 *Soit $P \in \mathbb{C}[X]$ un polynôme non nul alors P se décompose en facteurs irréductibles*

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

où $a_1, a_2, \ldots, a_k$ sont des scalaires distincts qui sont les zéros de P, et pour tout j, m_j est l'ordre de multiplicité de x_j comme zéro de P, et C est le coefficient directeur de P.

Cette décomposition est unique, à l'ordre des facteurs près.

E 78 Soit $P = X^3 - 2$. Ses racines sont $\sqrt[3]{2}$, $j\sqrt[3]{2}$, $j^2\sqrt[3]{2}$ et

$$X^3 - 2 = 1\left(X - \sqrt[3]{2}\right)\left(X - j\sqrt[3]{2}\right)\left(X - j^2\sqrt[3]{2}\right).$$

E 79 Décomposons $P = X^n - 1$ dans $\mathbb{C}[X]$.
Pour tout $k \in [\![0, n-1]\!]$, $\omega_k = e^{2ik\pi/n}$ est une racine de P. Puisque les ω_k sont distincts deux à deux, P possède $n = \deg P$ racines distinctes. De plus, le coefficient dominant de P est 1, on a donc

$$P = X^n - 1 = \prod_{k=0}^{n-1} \left(X - e^{2ik\pi/n} \right).$$

L 80 *Soit P un polynôme réel et a un zéro complexe de P. Alors $\overline{a}$ est un zéro de P et les ordres de multiplicité de a et $\overline{a}$ sont égaux.*

T 81 *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant est strictement négatif.*

Un polynôme réel de degré > 2 n'est *jamais* irréductible dans $\mathbb{R}[X]$, même s'il n'a aucune racine réelle. Par exemple, $X^4 + 3X^2 + 2 = (X^2 + 1)(X^2 + 2)$.

M ## Décomposition en produit de polynômes irréductibles

Soit $P \in \mathbb{R}[X]$. On note $a_1, a_2, \dots, a_k$ les racines réelles de P, d'ordre de multiplicité $m_1, m_2, \dots, m_k$. Il existe donc $Q \in \mathbb{R}[X]$ n'ayant aucun zéro réel tel que

$$P(X) = \prod_{k=1}^{s} (X - a_k)^{m_k} \times Q(X).$$

Le polynôme Q est forcément de degré pair puisque tout polynôme de $\mathbb{R}[X]$ de degré impair admet au moins un zéro réel (pourquoi?). Soit $c_1, \dots, c_r$ les zéros complexes de Q de partie imaginaire > 0. Notons v_i l'ordre de multiplicité de c_i. Les autres zéros de Q sont les conjugués des c_i ; on sait que $\bar{c}_i$ a pour ordre de multiplicité v_i. Donc

$$Q = \lambda(X - c_1)^{v_1}(X - c_2)^{v_2} \cdots (X - c_r)^{v_r}(X - \bar{c}_1)^{v_1}(X - \bar{c}_2)^{v_2} \cdots (X - \bar{c}_r)^{v_r}$$

On regroupe $(X - c_i)(X - \bar{c}_i) = X^2 - 2\,\mathfrak{Re}(c_i) + |c_i|^2 = X^2 + p_i X + q_i$ où p_i et q_i sont des réels tels que $p_i^2 - 4q_i < 0$.

T 82 *Tout polynôme $P \in \mathbb{R}[X]$ non nul s'écrit*

$$C \prod_{k=1}^{s} (X - a_k)^{m_k} \prod_{i=1}^{r} (X^2 + p_i X + q_i)^{v_i}$$

où C est le coefficient directeur de P, les $a_k \in \mathbb{R}$ sont des réels distincts, les $(p_i, q_i) \in \mathbb{R}^2$ sont des couples distincts de réels tels que $p_i^2 - 4q_i < 0$. Cette décomposition est unique, à l'ordre des facteurs près.

E 83 Soit $P = X^4 + 1$. Les racines de P sont les racines quatrièmes de $-1 = \mathrm{e}^{i\pi}$, c'est-à-dire les $\mathrm{e}^{i(2k+1)\pi/4}$, $k \in [\![0, 3]\!]$. Le coefficient dominant de P est 1, donc

$$\begin{aligned} P &= \left(X - \mathrm{e}^{i\pi/4}\right)\left(X - \mathrm{e}^{7i\pi/4}\right)\left(X - \mathrm{e}^{3i\pi/4}\right)\left(X - \mathrm{e}^{5i\pi/4}\right) \\ &= \left(X^2 - 2\,\mathfrak{Re}\left(\mathrm{e}^{i\pi/4}\right)X + 1\right)\left(X^2 - 2\,\mathfrak{Re}\left(\mathrm{e}^{3i\pi/4}\right)X + 1\right) \\ &= \left(X^2 - \sqrt{2}X + 1\right)\left(X^2 + \sqrt{2}X + 1\right). \end{aligned}$$

E 84 On veut décomposer le polynôme $P = X^n - 1$ dans $\mathbb{R}[X]$. La décomposition de P dans $\mathbb{C}[X]$ est

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

Le conjugué de $\omega_k = e^{2ik\pi/n}$ est $\mathrm{e}^{-2ik\pi/n} = \mathrm{e}^{2i(n-k)\pi/n} = \omega_{n-k}$. On calcule

$$(X - \omega_k)(X - \omega_{n-k}) = X^2 - 2X \cos\left(\frac{2k\pi}{n}\right) + 1. \tag{1}$$

Si n est impair, donc $n = 2m + 1$ où m est entier,

- $\omega_0 = 1$ est la seule racine réelles ;
- Les racines non réelles de P sont les ω_k avec $1 \leq k \leq m$ et leurs conjuguées.

On obtient donc

$$X^{2m+1} - 1 = (X - 1) \prod_{k=1}^{m} \left(X^2 - 2\cos\left(\frac{2k\pi}{2m+1}\right) X + 1\right). \tag{2}$$

E 84 On veut décomposer le polynôme $P = X^n - 1$ dans $\mathbb{R}[X]$. La décomposition de P dans $\mathbb{C}[X]$ est

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

Le conjugué de $\omega_k = e^{2ik\pi/n}$ est $\mathrm{e}^{-2ik\pi/n} = \mathrm{e}^{2i(n-k)\pi/n} = \omega_{n-k}$. On calcule

$$(X - \omega_k)(X - \omega_{n-k}) = X^2 - 2X\cos\left(\frac{2k\pi}{n}\right) + 1. \tag{1}$$

Si n est pair, donc $n = 2m$ où m est entier,

- Les racines réelles de P sont $\omega_0 = 1$ et $\omega_m = -1$;
- les racines non réelles de P sont les ω_k avec $1 \leq k \leq m-1$, et leurs conjuguées.

On a donc

$$X^{2m} - 1 = (X-1)(X+1)\prod_{k=1}^{m-1}\left(X^2 - 2\cos\left(\frac{k\pi}{m}\right)X + 1\right). \tag{3}$$