Table des matières

Chapitre 14

Polynômes

Dans toute la suite $\mathbb{K}$ désigne le corps $\mathbb{R}$ ou $\mathbb{C}$

14.1 Polynômes à une indéterminée

14.1.1 Définitions - Structures

Définition 14.1.1 *On note $\mathbb{K}^{(\mathbb{N})}$ l'ensemble des familles (ou suites) $(a_n)_{n\in\mathbb{N}}$ indexée par $\mathbb{N}$ presque nulle (ou nulle apcr) :*

$$\exists N \in \mathbb{N};\quad \forall n \geq n,\quad a_n = 0$$

♠

Définition 14.1.2 *On défini sur $\mathbb{K}^{(\mathbb{N})}$ deux $\ell.c.i$ $+$ et $\times$*

$$\forall (a,b) \in \mathbb{K}^{(\mathbb{N})} \times \mathbb{K}^{(\mathbb{N})},\qquad (a+b)_n = a_n + b_n \quad et \quad (a\times b)_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{n} a_{n-k} b_k$$

♠

Preuve la deuxième formule du produit s'obtient par le changement d'indice $k \mapsto n-k$.
Soient a, b deux suites presque nulles, on a pour un certain $M \in \mathbb{N}$ et $N \in \mathbb{N}$

$$\forall n > M,\quad a_n = 0 \qquad \text{et} \qquad \forall n > N,\quad b_n = 0$$

Montrons que $a+b$ (resp. $a\times b$) est presque nulle.
En effet

$$(*) \qquad \forall n > \max(N,M),\quad (a+b)_n = a_n + b_n = 0$$

$$(**) \qquad resp.\quad \forall n > N+M,\quad (a\times b)_n = \sum_{k=0}^{M} a_k \underbrace{b_{n-k}}_{=0} + \sum_{k=M+1}^{n} \underbrace{a_k}_{=0} b_{n-k} = 0$$

•

Remarque 14.1.1 *la loi $+$ n'est rien d'autre que la loi additive usuelle sur l'ensemble des suites. En revanche la loi $\times$ ci-dessus n'a rien à voir avec la loi produit usuelle sur l'ensemble des suites.*

$$(a\times b)_n = \sum_{p+q=n} a_p b_q$$

∗

Proposition 14.1.1 *On note X l'élément de $\mathbb{K}^{(\mathbb{N})}$ défini par*

$$X_1 = 1 \quad et \quad \forall n \neq 1,\quad X_n = 0$$

$$X = (0, 1, 0, 0, \ldots)$$

Si on note X^p la puissance p-ième de X pour $p \in \mathbb{N}^*$, on a

$$(X^p)_p = 1 \qquad et \qquad \forall n \neq p, \quad (X^p)_n = 0$$

$$X^p = (0, 0, 0, 0, \underbrace{1}_{p-ieme}, 0, 0, \ldots)$$

On note de même $\mathbf{1} := (1, 0, 0, \ldots)$ ♣

Proposition 14.1.2 $(\mathbb{K}^{(\mathbb{N})}, +, \times)$ *est un anneau commutatif, noté* $\mathbb{K}[X]$.
On l'appelle l'ensemble des polynômes à une indéterminée X (où X est défini comme-ci dessus) ♣

Démonstration
• $(\mathbb{K}^{(\mathbb{N})}, +)$ est un sous-groupe de $(\mathbb{K}^{\mathbb{N}}, +)$. En effet $\mathbf{0} = (0, 0, 0, \ldots) \in \mathbb{K}^{(\mathbb{N})}$ et (d'après l'analogue de $(*)$)

$$\forall (a, b) \in \mathbb{K}^{(\mathbb{N})} \times \mathbb{K}^{(\mathbb{N})}, \quad a - b \in \mathbb{K}^{(\mathbb{N})}$$

• $+$ et $\times$ sont commutatifs (trivial).
• $\mathbf{1} = (1, 0, 0, 0,) \in \mathbb{K}^{(\mathbb{N})}$ est élément neutre de $(\mathbb{K}^{(\mathbb{N})}, \times)$

$$\forall a \in \mathbb{K}^{(\mathbb{N})}, \quad \forall n \in \mathbb{N}, \quad (a \times \mathbf{1})_n = \sum_{k \in [|0, n-1|]} a_k \cdot \underbrace{\mathbf{1}_{n-k}}_{=0} + a_n \cdot \mathbf{1}_0 = a_n \cdot 1 = a_n$$

(la somme ci-dessus est éventuellement vide). La deuxième relation $\mathbf{1} \times a = a$ s'obtient par commutativité
• $\times$ est associative.
Soient a, b, c dans $\mathbb{K}^{(\mathbb{N})}$

$$([a \times b] \times c)_n = \sum_{r=0}^{n} \Big[\sum_{p+q=n-r} a_p b_q \Big] c_r = \sum_{p+q+r=n} a_p b_q c_r = (a \times [b \times c])_n$$

• $\times$ est distributive par rapport à $+$.
Soient a, b, c dans $\mathbb{K}^{(\mathbb{N})}$.

$$\forall n \in \mathbb{N}, \quad (a \times [b + c])_n = \sum_{p+q=n} a_p \cdot [b_q + c_q] = \sum_{p+q=n} a_p \cdot b_q + \sum_{p+q=n} a_p \cdot c_q = (a \times b + a \times c)_n$$

De même par commutativité $[b + c] \times a = b \times a + c \times a$ •

Remarque: $(\mathbb{K}[X], +, \times)$ n'est pas un sous-anneau de $(\mathbb{K}^{\mathbb{N}}, +, \times)$ (les lois $\times$ ne coïncident pas)

Proposition 14.1.3 *l'application $\varphi : \mathbb{K} \to \mathbb{K}[X]$ défini par*

$$\forall x \in \mathbb{K}, \quad \varphi(x) = (x, 0, \ldots)$$

est un morphisme d'anneaux injectif. ♣

Démonstration Soient x, y dans $\mathbb{K}$.

$$\varphi(x + y) = (x + y, 0, 0, \ldots) = (x, 0, 0, \ldots) + (y, 0, 0, \ldots) = \varphi(x) + \varphi(y)$$

Et puis d'après $(**)$

$$\varphi(x \times y) = (x \times y, 0, 0, \ldots) = (x, 0, 0, \ldots) \times (y, 0, 0, \ldots) = \varphi(x) \times \varphi(y)$$

$$\varphi(1) = (1, 0, 0, \ldots) = \mathbf{1}$$

C'est donc un morphisme. Montrons l'injectivité

$$x \in \ker \varphi \Longrightarrow \varphi(x) = \mathbf{0} \Longrightarrow x = (\varphi(x))_0 = 0$$

Et donc $\ker \varphi = \{0\}$ (l'inclusion réciproque provenant du fait que $(\ker \varphi, +)$ est un groupe) •

Remarque 14.1.2 *En particulier* $(\mathbb{K},+,\times)$ *est isomorphe à* $(\varphi(\mathbb{K}),+,\times)$.
Ceci nous permet d'identifier $\lambda\in\mathbb{K}$ *au polynôme constant* $(\lambda,0,0,\ldots)$.

$$\forall\lambda\in\mathbb{K},\forall P\in\mathbb{K}[X],\quad\left\{\begin{array}{lcl}\lambda\times P&:=&\varphi(\lambda)\times P=(\lambda P_0,\lambda P_1,\ldots,\lambda_k P_k,\ldots)\\ \lambda+P&:=&\varphi(\lambda)+P=(\lambda+P_0,P_1,P_2,\ldots)\end{array}\right.$$

*

Proposition 14.1.4 (Espace Vectoriel)
le produit défini une loi de composition externe $"\cdot"$ *sur* $\mathbb{K}[X]$ *définie sur* $\mathbb{K}$.
$(\mathbb{K}[X],+,\cdot)$ *est un* $\mathbb{K}$*-espace vectoriel* ♣

14.1.2 Base canonique - Degré

Proposition 14.1.5 *Tout polynôme* $P\in\mathbb{K}[X]$ *non nul (différent de* $\boldsymbol{0}$*) admet une décomposition unique sous la forme.*

$$P=\sum_{k=0}^{n}a_kX^k\qquad avec\quad n\in\mathbb{N}\quad(a_0,\ldots,a_n)\in\mathbb{K}^{n+1}\quad et\quad a_n\neq 0$$

n est alors ce qu'on appelle le degré de P*, on note* $\deg(P)=n$.
Par convention on pose $\deg(\boldsymbol{0})=-\infty$ ♣

Démonstration
• Existence
Soit $A:=\{n\in\mathbb{N},\quad P_n\neq 0\}$ c'est une partie non vide ($P\neq\mathbf{0}$) majorée (par définition de $\mathbb{K}^{(\mathbb{N})}$) soit n sont plus grand élément, en posant pour tout $k\in[|0,n|]$ $a_k=P_k$

$$\sum_{k=0}^{n}a_kX^k=\sum_{k=0}^{n}a_k(0,\ldots,0,\underbrace{1}_{k-ieme},0,0,\ldots)=\sum_{k=0}^{n}(0,\ldots,0,\underbrace{a_k}_{k-ieme},0,0,\ldots)=(a_0,a_1,\ldots,a_k,\ldots,a_n,0,0,\ldots)=P$$

• Unicité
Soient $\sum_{k=0}^{n}a_kX^k$ et $\sum_{k=0}^{m}b_kX^k$ sont deux décompositions distinctes de P avec par exemple $n\leq m$.

$$\mathbf{0}=\sum_{k=0}^{n}a_kX^k-\sum_{k=0}^{m}b_kX^k=\sum_{k=0}^{n}(a_k-b_k)X^k-\sum_{k=n+1}^{m}b_kX^k$$

Dans le cas où $n<m$ la deuxième somme est non vide et $-b_m=\mathbf{0}_m=0$ ce qui est absurde, d'où $n=m$ et donc

$$\forall k\in[|0,n|],\quad a_k-b_k=\mathbf{0}_k=0$$

ce qui est encore contradictoire car les décompositions sont supposées distinctes. •

Remarque 14.1.3
Avec les notations ci-dessus $deg(P)=\max\{n\in\mathbb{N}\mid a_n\neq 0\}$ *et pour tout* $n\in[|0,n|]$, $\quad a_n=P_n$

$$\forall N\in\mathbb{N},\quad\boldsymbol{0}=\sum_{k=0}^{N}0X^k$$

*

Remarque: $\forall p\in\mathbb{N},\quad\deg(X^p)=p$

Proposition 14.1.6 *Soient* P *et* Q *dans* $\mathbb{K}[X]$ *quelconque.*

$$\deg(P+Q)\leq\max(\deg P,\deg Q)\qquad et\qquad\deg(P\times Q)=\deg P+\deg Q$$

les relations étant considérée dans $\mathbb{R}\cup\{-\infty\}$ ♣

Démonstration Notons $M = \deg P$ et $N = \deg Q$

$$P = \sum_{k \leq M} a_k X^k \quad \text{et} \quad Q = \sum_{k \leq N} b_k X^k$$

(Ces sommes sont éventuellement vides) avec $(a_k)_{k\in\mathbb{N}}$ et $(b_k)_{k\in\mathbb{N}}$ dans $\mathbb{K}^{(\mathbb{N})}$.
Puisque

$$\forall n > M, \quad a_n = 0 \qquad \text{et} \qquad \forall n > N, \quad b_n = 0$$

on en déduit d'après $(*)$ et $(*)$

$$\deg(P+Q) \leq \max(N, M) \quad \text{et} \quad \deg(P \times Q) \leq N + M$$

Par ailleurs :
Si P ou Q est nulle, puisque $\mathbf{0}$ est absorbant $P \times Q = \mathbf{0}$ d'où $\deg P \times Q = -\infty = \infty + (N \quad \text{ou} \quad M)$
Si P et Q non nuls, $(PQ)_{N+M} = a_M b_N \neq 0$, d'où $\deg(P \times Q) \geq M + N$ •

Remarque: Si $\deg P \neq \deg Q$ alors $\deg(P+Q) = \max(\deg P, \deg Q)$

Définition 14.1.3
Pour tout $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n.
En particulier $\mathbb{K}_0[X] = \mathbb{K}$ ♠

Proposition 14.1.7 *Pour tout $n \in \mathbb{N}$ $(\mathbb{K}_n[X], +, \cdot)$ est un $\mathbb{K}$-sous espace vectoriel de $(\mathbb{K}[X], +, \cdot)$* ♣

Démonstration 0 est dans $\mathbb{K}_n[X]$.
Soient P, Q dans $\mathbb{K}_n[X]$ et λ, μ dans $\mathbb{K}$ quelconques

$$\deg(\lambda P + \mu Q) \leq \max(\deg \lambda P, \deg \mu Q)$$

Or $\deg(\lambda P) = \deg(\lambda) + \deg(P) \leq \deg(P)$ et $\deg(\mu Q) = \deg(\mu) + \deg(Q) \leq \deg(Q)$

$$\deg(\lambda P + \mu Q) \leq \max(\deg P, \deg Q) \leq n$$

•

Remarque: $(1, X, \ldots, X^n)$ est une base de $\mathbb{K}_n[X]$

Exercice: Montrer que pour tout $a \in \mathbb{K}$, $(1, X-a, \ldots, (X-a)^n)$ est une base de $\mathbb{K}_n[X]$

Solution :
Soit $Q \in \mathbb{K}_[X]$, montrons que Q admet une décomposition unique sous la forme

$$Q(X) = \sum_{k=0}^{n} a_k (X-a)^k \qquad \text{avec } (a_0, \ldots, a_n) \in \mathbb{K}^{n+1}$$

⋆ Montrons l'existence.
Puisque $\widehat{Q} := Q(X+a) \in \mathbb{K}_n[X]$, on a

$$Q(X+a) = \sum_{k=0}^{n} a_k X^k v \quad \text{D'où} \quad Q(X) = \widehat{Q}(X-a) = \sum_{k=0}^{n} a_k (X-a)^k$$

⋆ Montrons l'unicité.
Si

$$Q(X) = \sum_{k=0}^{n} a_k (X-a)^k = \sum_{k=0}^{n} b_k (X-a)^k \qquad \text{avec } (a_0, \ldots, a_n) \neq (b_0, \ldots, b_n)$$

Posons

$$R := \sum_{k=0}^{n} (a_k - b_k)(X-a)^k$$

On a $R = 0$ et donc $R(X+a) = 0$, d'où

$$\sum_{k=0}^{n} (a_k - b_k) X^k = 0$$

D'où puisque $(1, X, \ldots, X^n)$ est une base de $\mathbb{K}_n[X]$

$$\forall k \in [|0, n|], \qquad a_k - b_k = 0$$

Définition 14.1.4 *Soient P et Q deux polynômes avec*

$$Q = \sum_{k=0}^{n} b_k X^k \qquad où \quad n \in \mathbb{N} \quad et \quad (b_0, \dots, b_n) \in \mathbb{K}^{n+1}$$

On note $Q \circ P$ ou $Q(P)$ le polynôme

$$Q(P) := \sum_{k=0}^{n} b_k P^k$$

♠

Exercice: Montrer que $\deg(P \circ Q) = \deg P \times \deg Q$

Remarque: En particulier on a pour $P \in \mathbb{K}[X]$ quelconque $P = P(X)$

14.2 Arithmétique dans $\mathbb{K}[X]$

14.2.1 Divisibilité

Proposition 14.2.1 *$(\mathbb{K}[X], +, \times)$ est un anneau commutatif intègre, i.e.*

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

Les seuls éléments inversibles sont les polynômes constants non nuls $\mathbb{K}^*$ ♣

Définition 14.2.1 *Soient A et B deux polynômes de $\mathbb{K}[X]$.*
On dit que B est un multiple de A ou encore que A divise B (et on note $A \mid B$) lorsque :

$$\exists Q \in \mathbb{K}[X], \qquad B = QA$$

On dit aussi que A est un diviseur de B ♠

Remarque: $A \cdot \mathbb{K}[X]$ est l'ensemble des multiples de A :

$$A \mid B \Longleftrightarrow B \in A \cdot \mathbb{K}[X] \Longleftrightarrow B \cdot \mathbb{K}[X] \subset A \cdot \mathbb{K}[X]$$

Exercice: Pour tout A, B dans $\mathbb{K}[X]$, on a $A \cdot \mathbb{K}[X]$ est sous-groupe stable par multiplications de $(\mathbb{K}[X], +, \times)$ (c'est un pseudo-anneau) et

$$A \cdot \mathbb{K}[X] = B \cdot \mathbb{K}[X] \Longleftrightarrow \exists \lambda \in \mathbb{K}^*, \quad A = \lambda B$$

Définition 14.2.2 (Polynômes associés)
Soient A et B deux polynômes, on dit que A et B sont associés lorsque l'on peut trouver $\lambda \in \mathbb{K}^*$ tel que

$$A = \lambda B$$

Lorsque P est un polynôme non nul dont le coefficient dominant (coefficient d'indice $\deg P$) est 1, on dit que P est unitaire. ♠

Remarque: **Si** $A \mid B$ **Alors** $\deg A \leq \deg B$. et **Si** A et B sont associés **Alors** $\deg A = \deg B$

Exercice: Et les réciproques ?

Remarque: Si A est un polynôme non nul il existe un unique polynôme unitaire associé à A

$$a_n X^n + a_{n-1} X^{n-1} + ... + a_0 = a_n (X^n + \frac{a_{n-1}}{a_n} X^{n-1} + ... + \frac{a_0}{a_n})$$

Proposition 14.2.2 *Pour tout A, B, C dans $\mathbb{K}[X]$.*

- $A \mid A$
- $A \mid B \quad et \quad B \mid A \Longrightarrow \exists \lambda \in \mathbb{K}^*, \quad A = \lambda B$
- $A \mid B \quad et \quad B \mid C \Longrightarrow A \mid C$

♣

Démonstration
- $A \mid A \iff A \cdot \mathbb{K}[X] \subset A \cdot \mathbb{K}[X]$
- $A \mid B \quad \text{et} \quad B \mid A \Longrightarrow B \cdot \mathbb{K}[X] \subset A \cdot \mathbb{K}[X] \subset B \cdot \mathbb{K}[X] \iff \exists \lambda \in \mathbb{K}^*, \quad A = \lambda B$
- $A \mid B \quad \text{et} \quad B \mid C \Longrightarrow C \cdot \mathbb{K}[X] \subset B \cdot \mathbb{K}[X] \subset A \cdot \mathbb{K}[X] \iff A \mid C$

•

Proposition 14.2.3 *Soient A, B, C, D dans $\mathbb{K}[X]$.*

$$\forall (U,V) \in (\mathbb{K}[X])^2, \quad D \mid A \quad et \quad D \mid B \Longrightarrow D \mid UA + VB$$

$$\forall C \in \mathbb{K}[X] \setminus \{0\}, \qquad A \mid B \iff AC \mid BC$$

♣

Exercice: le prouver

Remarque 14.2.1 *Ceci se traduit par :*
$D \cdot \mathbb{K}[X]$ est stable par $\mathbb{K}[X]$-combinaison linéaire

$$\forall (U,V) \in (\mathbb{K}[X])^2, \quad A \in D \cdot \mathbb{K}[X] \quad et \quad B \in D \cdot \mathbb{K}[X] \Longrightarrow UA + VB \in D \cdot \mathbb{K}[X]$$

et par dilatation non nulle

$$\forall C \in \mathbb{K}[X] \setminus \{0\}, \qquad B \in A \cdot \mathbb{K}[X] \iff BC \in AC \cdot \mathbb{K}[X]$$

*

14.2.2 Division Euclidienne

Théorème 14.2.4 (Division Euclidienne) *Soient A, B dans $\mathbb{K}[X]$ avec $B \neq 0$, il existe un unique couple $(Q,R) \in (\mathbb{K}[X])^2$ tel que*

$$A = BQ + R \qquad et \qquad \deg R < \deg B$$

Cette décomposition porte le nom de division euclidienne de A par B.
Q est le quotient et R le reste.
On note parfois

$$A \equiv R \quad [B]$$

♣

Démonstration
⋆ Existence
Soit $B = \sum_{k=0}^{m} b_k X^k$ avec $m \geq 0$ et $b_m \neq 0$.

$$\mathcal{H}(n) : \text{"}\forall A \in \mathbb{K}_n[X], \quad \exists !(Q,R) \in (\mathbb{K}[X])^2; \qquad A = BQ + R \quad \text{et} \quad \deg R < \deg B\text{"}$$

• $\mathcal{H}(0), \ldots, \mathcal{H}(m-1)$ sont vérifiés il suffit de prendre $R := A$ et $Q := 0$
• supposons $\mathcal{H}(n)$ vérifié pour $n \geq \max(0, m-1)$.
Soit $A = \sum_{k=0}^{n+1} a_k X^k$ (ici on peut avoir $a_{n+1} = 0$).
On applique $\mathcal{H}(n)$ à

$$A_1 = A - \frac{a_{n+1}}{b_m} X^{n-m+1} B = (a_{n+1} - a_{n+1}) X^{n+1} + \sum_{k=n-m+1}^{n} (a_k - \frac{a_{n+1} b_{k-n+m-1}}{b_m}) X^k \in \mathbb{K}_n[X]$$

On peut trouver $(Q_1, R) \in (\mathbb{K}[X])^2$ tq

$$A_1 = A - \frac{a_{n+1}}{b_m} X^{n-m+1} B = BQ_1 + R \qquad \text{et} \qquad \deg R < \deg B$$

Et donc

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

avec $Q = Q_1 + \frac{a_{n+1}}{b_m} X^{n-m+1}$

$\star$ Unicité

Supposons avoir deux couples $(Q_1, R_1), (Q_2, R_2)$ vérifiant la décomposition.

$$A = BQ_1 + R_1 = BQ_2 + R_2 \qquad \text{et} \qquad \deg R_1, \deg R_2 < \deg B$$

Alors

$$\deg B + \deg(Q_1 - Q_2) = degB(Q_1 - Q_2) = \deg R_2 - R_1 \leq \max(\deg R_1, \deg R_2) < \deg B$$

D'où $\deg(Q_1 - Q_2) = -\infty$, soit $Q_1 - Q_2 = 0$ et donc

$$R_1 = A - BQ_1 = A - BQ_2 = R_2$$

•

Exemple:

$$A = X^5 + 4X^4 + 2X^3 + X^2 - X - 1 \quad \text{et} \quad B = X^3 - 2X + 3$$

Par des soustractions de multiples de B on "abaisse" le degré de A

$$A = \underbrace{(4X^4 + 4X^3 - 2X^2 - X - 1)}_{A_1 = A - X^2 B} + X^2 B$$

$$A_1 = \underbrace{(4X^3 + 6X^2 + 13X - 1)}_{A_2 = A_1 - 4XB} + 4XB$$

$$A_2 = \underbrace{(6X^2 - 5X - 13)}_{A_3 = A_2 - 4B} + 4$$

Comme $\deg A_3 < \deg B$ Au final

$$A = A_1 + X^2 B = A_2 + 4XB + X^2 B = A_3 + 4 + 4XB + X^2 B = \underbrace{(6X^2 - 5X - 13)}_{R} + \underbrace{(X^2 + 4X + 4)}_{Q} B$$

Remarque 14.2.2 (Algorithme Naïf)

Procédure *division(A, B)*
©*omentaire* $A = a_0 + a_1 X + \ldots a_n X^n, B = b_0 + b_1 X + \ldots b_m X^m$ *et* $b_m \neq 0$
. *variables locales :* $k, R = r_0 + \ldots + r, Q$
©*omentaire* $R = r_0 + r_1 X + \ldots r_m X^m, Q = q_0 + q_1 X + \ldots q_{n-m} X^{n-m}$
. $R \leftarrow A$; $Q \leftarrow 0$
. ***Pour*** i ***allant de*** $n - m$ ***à*** 0 ***aavec un pas de*** -1 ***faire***
. $q_k \leftarrow r_{k+m}/b_m$ $R \leftarrow R - q_k X^k B$ ***Fin du Pour***
Retourne (Q, R)
Fin de la procédure

*

Remarque: Voir les commandes MAPLE *quo* et *rem*

14.2.3 Dérivation

Définition 14.2.3 *Soit* $P \in \mathbb{K}[X]$ *, on appelle polynome dérivée le polynome noté* P' *défini par. Si* $P = \sum_{k=0}^{n} a_k X^k$ *alors*

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

♠

Remarque: $\deg(P') = \deg P - 1$

Exemple: $(1 + 2X + 3X^2 + iX^7)' = 2 + 6X + 7iX^6$

Proposition 14.2.5 *l'application $D : \mathbb{K}[X] \to \mathbb{K}[X]$ est un morphisme de K-ev (i.e. elle est $\mathbb{K}$-linéaire)* ♣

Remarque: il en va de même pour $D^n = \underbrace{D \circ \ldots \circ D}_{n\ fois}$, on note $P^{(n)} = D^n P$

Remarque: $D^0 = Id$ par convention

Proposition 14.2.6 *Soient $A, B \in \mathbb{K}[X]$* $\qquad (AB)' = A'B + AB'$
Et plus généralement on a la formule de Leibniz, pour tout $n \in \mathbb{N}$

$$(AB)^{(n)} = \sum_{k=0}^{n} C_n^k A^{(k)} B^{(n-k)}$$

♣

Remarque: On ne connaît pas de facon générale $D(P \circ Q)$, mais

$$D(P(\alpha X + \beta)) = \alpha P'(\alpha X + \beta)$$

14.3 Fonctions Polynômiales

14.3.1 Formule de Taylor

Définition 14.3.1 *Soit*

$$\Psi : \begin{array}{ccc} \mathbb{K}[X] & \to & \mathcal{F}(\mathbb{K}, \mathbb{K}) \\ P & \mapsto & \widetilde{P} \end{array}$$

Où pour $P = \sum_{k=0}^{n} a_k X^k$, $\widetilde{P}$ est défini par

$$\forall x \in \mathbb{K}, \qquad \widetilde{P}(x) = \sum_{k=0}^{n} a_k x^k$$

Ψ est un morphisme d'anneaux (resp. d'espaces-vectoriels) ♠

Démonstration Pour $(P, Q) \in (\mathbb{K}[X])^2$ et $\lambda \in \mathbb{K}$ quelconques

$$\Psi(P + Q) = \widetilde{P + Q} = \widetilde{P} + \widetilde{Q} = \Psi(P) + \Psi(Q)$$
$$\Psi(P \times Q) = \widetilde{P \times Q} = \widetilde{P} \times \widetilde{Q} = \Psi(P) \times \Psi(Q)$$
$$\Psi(1_{\mathbb{K}[X]}) = 1_{\mathcal{F}(\mathbb{K},\mathbb{K})}$$
$$resp. \quad \Psi(\lambda \cdot P) = \widetilde{\lambda \cdot P} = \lambda \cdot \widetilde{P} = \lambda \cdot \Psi(P)$$

•

Remarque: $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$ d'où le "morphisme" $\Psi(P \circ Q) = \Psi(P) \circ \Psi(Q)$

Remarque: $\widetilde{P'} = P'$ et De façon générale, pour tout $n \in \mathbb{N}$, $D^n \circ \Psi = \Psi \circ D^n$

Proposition 14.3.1 (Formule de Taylor) *Soit $n \in \mathbb{N}$ et $P \in \mathbb{K}_n[X]$*

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

Et plus généralement pour tout $a \in \mathbb{K}$, on a

$$P(X) = \sum_{k=0}^{n} \frac{\widetilde{P}^{(k)}(a)}{k!} (X - a)^k = \sum_{k=0}^{n} \frac{\widetilde{P^{(k)}}(a)}{k!} (X - a)^k$$

♣

Démonstration il suffit de Montrer que pour $P = \sum_{k=0}^{n} a_k X^k$ quelconque, on a

$$\forall k \in [|0, n|], \qquad a_k = \frac{\widetilde{D^k P}(0)}{k!}$$

.
Or par linéarité des applications $\Psi \circ D^0, \Psi \circ D^1, \Psi \circ D^2, \ldots, \Psi \circ D^n, \ldots$, il suffit de Montrer que

$$\forall (k,p) \in [|0,n|]^2, \qquad \frac{\widetilde{D^k X^p}(0)}{k!} = 1 \quad \textbf{Si } k = n \qquad \frac{\widetilde{D^k X^p}(0)}{k!} = 0 \quad sinon$$

ceci découle de

$$D^k X^p = \begin{cases} p(p-1)\cdots(p-k+1)X^{p-k} & si \quad k \leq p \\ 0 & sinon \end{cases}$$

La dernière Formule s'obtient en appliquant ce qui prècède à $Q = P(X+a)$

$$Q(X) = \sum_{k=0}^{n} \frac{\widetilde{Q^{(k)}}(0)}{k!} X^k = \sum_{k=0}^{n} \frac{\widetilde{P^{(k)}(X+a)}(0)}{k!} X^k = \sum_{k=0}^{n} \frac{\widetilde{P^{(k)}}(a)}{k!} X^k$$

D'où

$$P(X) = Q(X-a) = \sum_{k=0}^{n} \frac{\widetilde{P^{(k)}}(a)}{k!} (X-a)^k$$

•

Remarque: Pour tout $P \in \mathbb{K}[X], \quad P = \sum_{k\in\mathbb{N}} \frac{\widetilde{P}^{(k)}(0)}{k!} X^k$

Remarque 14.3.1 *Soit $P = \sum_{k=0}^{n} a_k X^k$ alors*

$$\forall k \in [|0, n|], \qquad a_k = \frac{\widetilde{P}^{(k)}(0)}{k!}$$

∗

Proposition 14.3.2 *Im Ψ est ce qu'on appelle l'ensemble des fonctions polynômiales c'est un sous-anneau (resp. sous-ev) de $\mathcal{F}(\mathbb{K}, \mathbb{K})$.*

L'application Ψ est injective, elle induit donc un isomorphisme entre $\mathbb{K}[X]$ et l'ensemble des fonctions polynômiales à coefficients dans $\mathbb{K}$ ♣

Démonstration Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ d'après la formule de Taylor

$$P \in \ker \Psi \Longrightarrow \widetilde{P} \equiv 0 \Longrightarrow \forall k \in [|0, n|], \quad a_k = \frac{\widetilde{D^k(P)}}{k!} = \frac{D^k(\widetilde{P})}{k!} = 0$$

D'où $\ker \Psi = \{0\}$ •

Remarque: Etant donné cet isomorphisme on note parfois indistinctement P et $\widetilde{P}$ pour désigner le polynôme P et sa fonction polynômiale associée.

14.3.2 Racines

Remarque 14.3.2 *Soit P un polynôme et $a \in X$ on par division euclidienne*

$$P \equiv P(a) \quad [X-a]$$

D'où $X - a \mid P$ si et seulement si $P(a) = 0$ ∗

Définition 14.3.2 *On appelle équation algébrique sur $\mathbb{K}$ d'inconnue x toute équation du type*

$$P(x) = 0$$

où $P \in \mathbb{K}[X]$ ♠

Définition 14.3.3 *On dit que $r \in \mathbb{K}$ est une racine de P lorsque $P(r) = 0$.*
Si de plus pour un certain $n \geq 1$, on a

$$(X-r)^n \mid P \qquad et \qquad (X-r)^{n+1} \nmid P$$

On dit que r est une racine d'ordre n (n est la multiplicité de r) ♠

Remarque: r racine d'ordre n de P si et seulement si

$$\exists Q \in \mathbb{K}[X]; \quad P = (X-a)^n Q \qquad \text{et} \qquad Q(a) \neq 0$$

Proposition 14.3.3 *Soit P un polynome.*
a est racine d'ordre α si et seulement si

$$P(a) = \ldots = P^{(\alpha-1)}(a) = 0 \quad et \quad P^{(\alpha)}(a) \neq 0$$

♣

Démonstration
$\Longrightarrow$
Supposons que

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

D'après la formule de Taylor

$$P = (X-a)^\alpha \sum_{i \geq \alpha} \frac{\widetilde{P^{(i)}}(a)}{i!}(X-a)^{k-\alpha} + \underbrace{\sum_{i<\alpha} \frac{\widetilde{P^{(i)}}(a)}{i!}(X-a)^i}_{\deg < \alpha}$$

D'où par unicité dans la division Euclidienne

$$Q = \sum_{i \geq \alpha} \frac{\widetilde{P^{(i)}}(a)}{i!}(X-a)^{k-\alpha} \qquad \text{et} \qquad 0 = \sum_{i<\alpha} \frac{\widetilde{P^{(i)}}(a)}{i!}(X-a)^i$$

Soit (puisque $(1, X-a, \ldots, (X-a)^n)$ est une base de $\mathbb{K}_n[X]$)

$$0 \neq Q(a) = \frac{\widetilde{P^{(\alpha)}}(a)}{\alpha!} \qquad \text{et} \qquad \forall i < \alpha, \quad \frac{\widetilde{P^{(i)}}(a)}{i!} = 0$$

$\Longleftarrow$
Supposons

$$P(a) = \ldots = P^{(\alpha-1)}(a) = 0 \quad \text{et} \quad P^{(\alpha)}(a) \neq 0$$

Alors par Taylor Si on pose

$$Q = \sum_{i \geq \alpha} \frac{\widetilde{P^{(i)}}(a)}{i!}(X-a)^{k-\alpha}$$

on a

$$P = (X-a)^\alpha Q \qquad \text{et} \qquad Q(a) = \frac{\widetilde{P^{(\alpha)}}(a)}{\alpha!} \neq 0$$

•

Proposition 14.3.4
Si P est non nul de degré $n \geq 0$, alors P admet au plus n racines (comptées avec multiplicité).
Plus précisément si on note $r_1, \ldots, r_p$ les multiplicités des p racines distinctes $\alpha_1, \ldots, \alpha_p$ de P alors

$$r_1 + \ldots + r_p \leq n \quad et \quad \prod_{i=1}^{p} (X-r_i)^{\alpha_i} \mid P$$

♣

Démonstration Il suffit de montrer la divisibilité entre polynômes car l'inégalité s'obtiendra en comparant les degrés.

Soit $\mathcal{H}(p)$ la propriété définie pour $p \geq 1$ par :

"Pour tout polynôme P admettant $\alpha_1, \ldots, \alpha_p$ pour racines distinctes, de multiplicités respectives $r_1, \ldots, r_p$ on a $\prod_{i=1}^{p}(X-\alpha_i)^{r_i} \mid P$"

• $\mathcal{H}(1)$ vrai par définition
• supposons $\mathcal{H}(p)$ vérifié pour un $p \in \mathbb{N}^*$ fixé.

Soit P ayant $\alpha_1, \ldots, \alpha_p, \alpha_{p+1}$ pour racines distinctes, de multiplicités respectives $r_1, \ldots, r_p, r_{p+1}$

D'après l'hypothèse de récurrence

$$P = Q\prod_{i=1}^{p}(X-\alpha_i)^{r_i}$$

D'après la formule de Taylor

$$Q = \sum_{k\in\mathbb{N}} \frac{Q^{(k)}(\alpha_{p+1})}{k!}(X-\alpha_{p+1})^k = \sum_{k\geq r} \frac{Q^{(k)}(\alpha_{p+1})}{k!}(X-\alpha_{p+1})^k$$

où r est le plus petit indice k tel que $Q^{(k)}(\alpha_{p+1}) \neq 0$

$$Q = (X-\alpha_{p+1})^r R \qquad \text{et} \qquad R(\alpha_{p+1}) \neq 0$$

D'où

$$P = (X-\alpha_{p+1})^r \times \underbrace{R\prod_{i=1}^{p}(X-\alpha_i)^{r_i}}_{S} \qquad \text{et} \qquad S(\alpha_{p+1}) \neq 0$$

Donc α_{p+1} racine d'ordre $r = r_{p+1}$... CQFD
• Conclusion... •

14.4 Polynômes Scindés

14.4.1 Coefficients et Racines

Définition 14.4.1 (Polynômes Scindés) *On dit que P est un polynôme est scindé dans $\mathbb{K}[X]$, lorsqu'il est associé à un produit de monomes, c'est à dire.*

$$\exists \lambda \in \mathbb{K}^*; \quad \exists (\alpha_1, \ldots, \alpha_n) \in \mathbb{K}^n; \qquad P = \lambda\prod_{k=1}^{n}(X-\alpha_k)$$

(En particulier $\alpha_1, \ldots, \alpha_n$ sont des racines (dans $\mathbb{K}$) non forcément distinctes de P) ♠

Exemple: les polynômes $X+1$, $X^2-1=(X-1)(X+1)$ et $2X^2-4X+2=2(X-1)^2$ sont scindés dans $\mathbb{R}[X]$

Exemple: les polynômes de degré 1 sont scindés dans $\mathbb{K}[X]$

Exercice: les polynômes de degré 2 sont scindés dans $\mathbb{R}[X]$ si et seulement si P admet une racine réelle.

Exercice: Tout polynôme de degré n dans $\mathbb{K}[X]$ est scindé si et seulement si il admet n racines comptées avec leur multiplicité.

Proposition 14.4.1 *Tout Polynôme P, scindé dans $\mathbb{K}[X]$, dont les racines (non forcément distinctes) sont notées $\alpha_1, \ldots, \alpha_n$ s'écrit*

$$P = \lambda\Big(X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} + \ldots + (-1)^n\sigma_n\Big) = \lambda\Big(X^n + \sum_{p=0}^{n-1}(-1)^{n-p}\sigma_{n-p}X^p\Big)$$

Où λ est le coefficient dominant de P, et les $\sigma_1, \ldots, \sigma_n$ sont définis par

$$\begin{aligned}
\sigma_1 &= \sum_{i=1}^{n} \alpha_i \\
&\vdots \quad \vdots \quad \vdots \\
\sigma_p &= \sum_{1 \le i_1 < \ldots < i_p \le n} \alpha_{i_1} \cdots \alpha_{i_p} \\
&\vdots \quad \vdots \quad \vdots \\
\sigma_n &= \prod_{i=1}^{n} \alpha_i
\end{aligned}$$

il s'agit des fonctions symétriques élémentaires des racines de P ♣

Remarque: Dans la formule de σ_p ci-dessus il y a C_n^p termes (autant que de parties à p-combinaisons parmi n)

Preuve Soit P scindé tel que ci-dessus

$$P = \lambda \prod_{k=1}^{n} (X - \alpha_k)$$

Supposons avoir démontré la décomposition pour tous les polynômes scindes de degré $\le n-1$, En particulier

$$\widehat{P} := \lambda \prod_{k=1}^{n-1} (X - \alpha_k) = \lambda\Big(X^{n-1} - \widehat{\sigma}_1 X^{n-2} + \widehat{\sigma}_2 X^{n-3} + \ldots + (-1)^{n-2}\widehat{\sigma}_{n-2} X + (-1)^{n-1}\widehat{\sigma}_{n-1}\Big)$$

avec

$$\forall p \in [|1, n-1|], \qquad \widehat{\sigma}_p = \sum_{1 \le i_1 < \ldots < i_p \le n-1} \alpha_{i_1} \cdots \alpha_{i_p}$$

$$\begin{aligned}
P = (X - \alpha_n)\widehat{P} = \lambda \prod_{k=1}^{n-1} (X - \alpha_k) &= \lambda\Big(X^n - \widehat{\sigma}_1 X^{n-1} + \widehat{\sigma}_2 X^{n-2} + \ldots + (-1)^{n-1}\widehat{\sigma}_{n-1} X\Big) \\
&- \lambda\Big(\alpha_n X^{n-1} - \alpha_n\widehat{\sigma}_1 X^{n-2} + \ldots + (-1)^{n-2}\alpha_n\widehat{\sigma}_{n-2} X + (-1)^{n-1}\alpha_n\widehat{\sigma}_{n-1}\Big)
\end{aligned}$$

D'où

$$P = \lambda\Big(X^n - \underbrace{(\widehat{\sigma}_1 + \alpha_n)}_{\sigma_1} X^{n-1} + \underbrace{(\widehat{\sigma}_2 + \alpha_n\widehat{\sigma}_1)}_{\sigma_2} X^{n-2} + \ldots + (-1)^{n-1} \underbrace{(\widehat{\sigma}_{n-1} + \alpha_n\widehat{\sigma}_{n-2})}_{\sigma_{n-1}} X + (-1)^n \underbrace{\alpha_n\widehat{\sigma}_{n-1}}_{\sigma_n}\Big)$$

Pour une preuve rigoureuse, il s'agit de faire une récurrence et montrer (par une sommation par paquets) les égalités sous les accolades. •

Exemple:

$$\lambda(X - \alpha_1)(X - \alpha_2) = \lambda\Big(X^2 - \underbrace{(\alpha_1 + \alpha_2)}_{\sigma_1} X + \underbrace{\alpha_1\alpha_2}_{\sigma_2}\Big)$$

$$\lambda(X - \alpha_1)(X - \alpha_2)(X - \alpha_3) = \lambda\Big(X^3 - \underbrace{(\alpha_1 + \alpha_2 + \alpha_3)}_{\sigma_1} X^2 + \underbrace{(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)}_{\sigma_2} X - \underbrace{\alpha_1\alpha_2\alpha_3}_{\sigma_3}\Big)$$

Corollaire 14.4.2 (Relations entre Coefficients et Racines) *Soit $P = a_0 + a_1 X + \ldots + a_n X^n$ un polynôme scindé dans $\mathbb{K}[X]$, dont les racines (comptées avec multiplicité) sont notées $\alpha_1, \ldots, \alpha_n$ On a*

$$P = a_n(X - \alpha_1) \cdots (X - \alpha_n)$$

Et plus précisément

$$\begin{array}{rcl}
\sigma_1 = & \sum_{i=1}^{n} \alpha_i & = -\dfrac{a_{n-1}}{a_n} \\
\vdots & \vdots & \vdots \\
\sigma_p = & \displaystyle\sum_{1\le i_1<\ldots<i_p\le n} \alpha_{i_1}\cdots\alpha_{i_p} & = (-1)^p \dfrac{a_{n-p}}{a_n} \\
\vdots & \vdots & \vdots \\
\sigma_n = & \displaystyle\prod_{i=1}^{n} \alpha_i & = (-1)^n \dfrac{a_0}{a_n}
\end{array}$$

♣

14.4.2 Polynômes irréductibles

Définition 14.4.2 *On dit qu'un polynôme P, **non constant**, est irréductible dans $\mathbb{K}[X]$ lorsque ses seules diviseurs sont les polynômes constants et les polynômes associés à P* ♠

Exemple: les polynômes de degré 1 sont des polynômes irréductibles de $\mathbb{K}[X]$

Exercice: Si P admet au moins une racine (dans $\mathbb{K}$) et n'est pas de degré 1, alors P n'est pas irréductible dans $\mathbb{K}[X]$

Théorème 14.4.3 (d'Alembert Gauss (Admis))
Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine dans $\mathbb{C}$ ♣

Corollaire 14.4.4 *Tout polynôme non constant de $\mathbb{C}[X]$ est scindé dans $\mathbb{C}[X]$* ♣

Démonstration le résultat est évident pour les polynômes de degré 1
Supposons le résultat vérifié pour les polynômes de degré $n \geq 1$.
Tout polynôme P de degré $n+1$ (donc non constant)admet au moins une racine β d'où

$$P = (X-\beta)Q \qquad \text{et} \qquad \deg(Q) = n$$

D'où d'après la "propriéèté" de récurrence

$$P = (X-\beta) \times \lambda \prod_{k=1}^{n} (X-\alpha_k)$$

•

Corollaire 14.4.5 *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.* ♣

Démonstration les polynômes sont irréductibles.
Pour P de degré $n \geq 2$ etant divisible par $(X-\alpha)(X-\beta)$ (car admet au moins deux racines avec multiplicité).
Et donc $(X-\alpha)$ est un diviseurs propre de P, il n'est donc pas irréductible. •

Définition 14.4.3 *Pour $P = a_0 + \ldots + a_n X^n \in \mathbb{C}[X]$ on note $\overline{P}$ le polynôme conjugué de P*

$$\overline{P} = \overline{a_0} + \ldots + \overline{a_n} X^n$$

En particulier $P \in \mathbb{R}[X] \Longleftrightarrow \overline{P} = P$.
Par ailleurs $P \mapsto \overline{P}$ est un morphisme d'anneaux de $\mathbb{C}[X]$ ♠

Lemme 14.4.6 *Soit $A \in \mathbb{R}[X]$, en particulier on a aussi $A \in \mathbb{C}[X]$.*
Si A admet une racine complexe α, alors $\overline{\alpha}$ est également une racine de A
Si $B \in \mathbb{R}[X] \setminus \{0\}$ divise A dans $\mathbb{C}[X]$, alors B divise A dans $\mathbb{R}[X]$ ♣

Démonstration

$$0 = A(\alpha_k) = \overline{A(\alpha_k)} = \overline{A}(\overline{\alpha_k}) = A(\overline{\alpha_k})$$

Et donc $\overline{\alpha}$ est également une racine.
Si $B \mid A$ dans $\mathbb{C}[X]$, alors

$$A = QB \quad avec \quad Q \in \mathbb{C}[X]$$

D'où

$$\overline{Q}B = \overline{Q} \cdot \overline{B} = \overline{QB} = \overline{A} = A = QB \quad \text{d'où} \quad (Q - \overline{Q})B = 0$$

Et donc puisque $\mathbb{C}[X]$ est intègre, on en déduit :

$$\overline{Q} = Q$$

D'où $Q \in \mathbb{R}[X]$, et donc $B \mid A$ dans $\mathbb{R}[X]$ •

Proposition 14.4.7 *les Polynômes irréductibles de $\mathbb{R}[X]$ sont sont les polynômes de degré 1. et ceux de degré 2 dont le discriminant est strictement négatif* ♣

Démonstration
⋆ Cherchons les polynômes A irréductibles de $\mathbb{R}[X]$.
• Supposons par l'absurde $\deg A \geq 3$.
A ne peut admettre de racine réelle (puisqu'irréductible de degré ≥ 2), il admet donc deux racines complexes distinctes α et $\overline{\alpha}$ et puisque A est scindé dans $\mathbb{C}[X]$,

$$B := (X - \alpha)(X - \overline{\alpha}) = \underbrace{X^2 - 2Re(\alpha)X + |\alpha|^2}_{\in \mathbb{R}[X]} \quad divise \quad A \quad dans \ \ \mathbb{C}[X]$$

Et donc B est un diviseur propre de A dans $\mathbb{R}[X]$... d'où la contradiction. • Supposons par l'absurde $\deg A = 2$ de déterminant négatif ou nul.
alors A admet au moins une racine réelle α et donc

$$B := (X - \alpha) \quad divise \quad A \quad dans \ \ \mathbb{R}[X]$$

D'où la contradiction.
• Conclusion : Si A est irréductible alors nécessairement A est de degré 1 ou de degré 2 dont le discriminant est strictement négatif.

⋆ Réciproquement Soit A dans $\mathbb{R}[X]$ de degré 1 ou 2 dont le discriminant est strictement négatif.
• si le degré est 1, A est irréductible.
• si il est de degré 2 et si par l'absurde A n'est pas irréductible alors il admet un diviseur propre de degré 1 (car non constant et non associé à A de degré 2), ce diviseur s'écrit $aX + b$ avec $(a, b) \in \mathbb{R}^* \times \mathbb{R}$ et donc en particulier $-b/a$ est une racine réelle de A... contradiction. •

Proposition 14.4.8 (Admis)
Dans $\mathbb{K}[X]$, tout polynôme A non nul est associé à un produit de polynômes irréductibles de $\mathbb{K}[X]$.
Plus précisément, on peut trouver $\lambda \in \mathbb{K}^*$ et $(P_i)_{i \in I}$ une famille (éventuellement vide) de polynômes irréductibles unitaires dans $\mathbb{K}[X]$ (non forcément distincts) tel que

$$A = \lambda \prod_{i \in I} P_i$$

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

Exemple: Comme tout polynôme dans $\mathbb{C}[X]$ $X^n - 1$ admet une décomposition en facteurs irréductibles

$$X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega) = \prod_{k=0}^{n} (X - e^{\frac{2ik\pi}{n}})$$

Exercice: Montrer que

$$\prod_{\omega \in \mathbb{U}_n} \omega = (-1)^{n+1}$$

Et en notant $\mathbb{U}_n = \{\omega_k \mid k \in [|0, n-1|]\}$

$$\forall p \in [|1, n-1|], \qquad \sum_{0 \leq k_1 < \ldots < k_p \leq n} \omega_{k_1} \cdots \omega_{k_p} = 0$$

Remarque 14.4.1 *Si $P \in \mathbb{R}[X]$ non constant alors P admet q racines réelles $\alpha_1, \ldots, \alpha_q$ et $2p$ racines complexes non réelles $\omega_1, \ldots, \omega_p, \overline{\omega_1}, \ldots, \overline{\omega_p}$ (éventuellement $p = 0$ ou $q = 0$).*
Sa décomposition dans $\mathbb{C}[X]$ s'écrit.

$$P = \lambda \prod_{i=1}^{q} (X - \alpha_i)^{r_i} \prod_{j=1}^{p} (X - \omega_j)^{s_j} (X - \overline{\omega_j})^{s_j}$$

$\lambda \in \mathbb{R}$ est le coefficient dominant de P et $r_1, \ldots, r_q$ resp. $s_1, \ldots, s_p$ sont les multiplicités de $\alpha_1, \ldots, \alpha_q$ resp $\omega_1, \ldots, \omega_p$.

$$r_1 + \cdots + r_q + 2(s_1 + \cdots + s_p) = \deg P$$

La décomposition de P dans $\mathbb{R}[X]$ s'écrit alors

$$P = \lambda \prod_{i=1}^{q} (X - \alpha_i)^{r_i} \prod_{j=1}^{p} (X^2 - 2Re(\omega_j) + |\omega_j|^2)^{s_j}$$

*

Exemple:

$$X^4 + 1 = \underbrace{(X - e^{i\frac{5\pi}{4}})(X - e^{-i\frac{5\pi}{4}})}_{X^2 + \sqrt{2}X + 1} \underbrace{(X - e^{i\frac{7\pi}{4}})(X - e^{-i\frac{7\pi}{4}})}_{X^2 - \sqrt{2}X + 1}$$

Exercice: Donner la décomposition dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$ de

$$X^8 - 1 \qquad \text{et} \qquad X^5 + 1$$