

# Chapitre 16

## Arithmétique des polynômes

<b>16 Arithmétique des polynômes</b>	<b>1</b>
16.1 Division euclidienne	2
16.7 Proposition 16.7	2
16.15 Principalité de $\mathbb{K}[X]$	3
16.17 Existence de $\text{pgcd}$	4
16.18 Principalité de $\mathbb{K}[X]$	4
16.24 Lemme de préparation au calcul pratique du PGCD unitaire	4
16.26 Exemple	5
16.27 Propriétés du PGCD	5
16.29 Existence de PPCM	5
16.30 Caractérisation des PPCM par les idéaux	6
16.42 Cas d'unicité d'une relation de Bézout	6
16.43 Corollaire	7
16.44 Caractérisation des PGCD et PPCM	7
16.53 Caractérisation des racines par la divisibilité	8
16.56 Formule de Taylor pour les polynômes	9
16.57 Caractérisation de la multiplicité par les dérivées	9
16.59 Caractérisation de la multiplicité des racines par la divisibilité	10
16.63 Polynômes formels et fonctions polynomiales	10
16.66 Caractérisation des polynômes interpolateurs	10
16.69 Corollaire	11
16.74 Proposition	11
16.76 Relation de Viète	11
16.88 Lemme	12
16.98 Caractérisation de la divisibilité dans $\mathbb{C}[X]$ par les racines	12
16.99 Caractérisation des polynômes à coefficients réels	12
16.10 Racine complexe d'un polynôme réel	13
16.10 Polynômes irréductibles de $\mathbb{R}[X]$	13

## 16.1 Division euclidienne

### Théorème 16.1

Soit  $A \in \mathbb{K}[X]$  et  $B \in \mathbb{K}[X]$  non nul, il existe un unique couple de polynômes  $(Q, R)$  tel que  $A = BQ + R$  avec  $\deg R < \deg B$ . Le polynôme  $Q$  est appelé **quotient** et  $R$  le **reste**.

#### Existence :

On raisonne par récurrence sur le degré de  $A$ .

- Pour  $n = \deg A = 0$ . Soit  $A \in \mathbb{K}[X]$ .
  - Si  $\deg B > 0$ , alors  $(0, A)$  convient.
  - Si  $\deg B = 0$ , le couple  $(B^{-1} \times A, 0)$  convient (comme  $B$  est constant et non nul), alors  $B \in \mathbb{K}^*$  donc inversible).
- On suppose le résultat vrai pour tout  $A \in \mathbb{K}_n[X]$ .  
 Soit  $A \in \mathbb{K}_{n+1}[X]$  avec  $\deg A = n + 1$ .  
 On écrit  $A = \underbrace{a}_{\neq 0} X^{n+1} + A_1$  avec  $A_1 \in \mathbb{K}_n[X]$ .
  - Si  $\deg A < \deg B$ , le couple  $(0, A)$  convient.
  - Si  $\deg A \geq \deg B$  et on note  $b$  le coefficient dominant de  $B$  :

$$A - ab^{-1}B \times X^{n+1-\deg B} \in \mathbb{K}_n[X]$$

D'après l'hypothèse de récurrence, on choisit  $(Q, R) \in \mathbb{K}[X]^2$  tel que  $\deg R < \deg B$  et  $A - ab^{-1}B \times X^{n+1-\deg B} = QB + R$ .

Donc :

$$A = [Q + ab^{-1}X^{n+1-\deg A}] \times B + R$$

#### Unicité :

On suppose que  $A = BQ + R = BQ_1 + R_1$ .

Donc :

$$\begin{aligned} B(Q - Q_1) &= R_1 - R \\ \text{donc } \underbrace{\deg(B(Q - Q_1))}_{\deg B + \deg Q - Q_1} &= \deg(R_1 - R) \\ &\leq \max(\deg R_1, \deg R) \\ &< \deg B \\ \text{donc } \deg(Q - Q_1) &< 0 \\ \text{donc } Q - Q_1 &= 0 \\ \text{puis } R_1 - R &= 0 \end{aligned}$$

## 16.7 Proposition 16.7

### Proposition 16.7

On a :

1. Soit  $A$  et  $P$  deux polynômes non nuls. Si  $A|P$  et si  $P|A$ , alors il existe  $\alpha \in \mathbb{K}^*$  tel que  $P = \alpha A$ . (La relation de divisibilité n'est pas antisymétrique)
2. Si  $A|B$  et si  $B|C$ , alors  $A|C$ . La relation de divisibilité est transitive.
3. Pour tout  $A \in \mathbb{K}[X]$  non nul,  $A|A$ . La relation de divisibilité est réflexive.

1.  $P \neq 0, A \neq 0$ . Si  $A|P$  et  $P|A$ , alors (16.6.2) :

$$\deg A \leq \deg P \text{ et } \deg P \leq \deg A$$

Donc :

$$\deg P = \deg A$$

Or  $A|P$ , alors :

$$P = A \times Q$$

Puis :

$$\deg P = \deg(AQ) = \deg A + \deg Q \text{ } (\mathbb{K} \text{ est int\`egre})$$

Donc :

$$\deg Q = 0$$

Donc :

$$Q = \alpha \in \mathbb{K}^*$$

2. RAS

3. RAS

## 16.15 Principauté de $\mathbb{K}[X]$

### Théorème 16.15

Soit  $I$  un idéal de  $\mathbb{K}[X]$  non réduit à  $\{0\}$ . Il existe un unique polynôme unitaire  $D$  tel que

$$I = D\mathbb{K}[X]$$

Existence :

Soit  $I \neq \{0\}$  un idéal.

On note  $A = \{\deg P, P \in I \setminus \{0\}\} \subset \mathbb{N}$ .

$A \neq \emptyset$  ( $I \neq \{0\}$ ), d'après la propriété fondamentale de  $\mathbb{N}$ ,  $A$  possède un plus petit élément noté  $n \geq 0$ .

Comme  $n \in A$ , on choisit  $D \in I$  tel que  $\deg D = n$ .

Comme  $I$  est un idéal de  $\mathbb{K}[X]$  et que  $\mathbb{K} = \mathbb{K}_0[X] \subset \mathbb{K}[X]$ , on a :

$$\forall \alpha \in \mathbb{K}, \alpha D \in I$$

On peut donc supposer  $D$  unitaire. Comme  $I$  est un idéal de  $\mathbb{K}[X]$ , on a :

$$D \times \mathbb{K}[X] \subset I$$

Soit  $P \in I$ . On effectue la division euclidienne de  $P$  par  $D$  ( $\neq 0$ ) :

$$P = BD + R$$

avec  $\deg R < \deg D$ .

Or :

$$R = \underbrace{P}_{\in I} - \underbrace{BD}_{\in I} \in I$$

Par définition de  $\deg D = n$ ,  $R = 0$ .

Unicité :

$$I = D\mathbb{K}[X] = J\mathbb{K}[X]$$

avec  $D$  et  $J$  unitaires.

Or ils sont associés, donc égaux.

## 16.17 Existence de $\text{pgcd}$

### Proposition 16.17

Si  $A$  et  $B$  sont deux polynômes non nuls, de tels PGCD existent.

Soit  $A, B$  dans  $\mathbb{K}[X]$ ,  $(A, B) \neq (0, 0)$ .

On note  $\mathcal{C} = \{\deg P, P|A \text{ et } P|B \text{ et } P \neq 0\} \subset \mathbb{N}$ .

$\mathcal{C} \neq \emptyset$  car  $0 \in \mathcal{C}$  et  $\mathcal{C}$  est majoré par  $\deg B$  ( $\max(\deg A, \deg B)$ ).

L'existence est assurée par la propriété fondamentale de  $\mathbb{N}$ .

## 16.18 Principauté de $\mathbb{K}[X]$

### Proposition 16.18

Soit  $A$  et  $B$  deux polynômes non tous deux nuls. Soit  $D \in \mathbb{K}[X]$ . Alors  $D$  est un PGCD de  $A$  et  $B$  si et seulement si

$$A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X].$$

D'après (16.15), on choisit  $F \in \mathbb{K}[X]$  tel que :

$$A\mathbb{K}[X] + B\mathbb{K}[X] = F\mathbb{K}[X]$$

Soit  $D \in \mathbb{K}[X]$ .

$\Rightarrow$

On suppose que  $D$  est un PGCD.

Donc  $D|A$  et  $D|B$ .

Donc  $D|F$  (combinaison  $F \in A\mathbb{K}[X] + B\mathbb{K}[X]$ ).

Or  $F|A$  et  $F|B$  ( $A \in F\mathbb{K}[X]$ ,  $B \in F\mathbb{K}[X]$ ).

Par maximalité de  $\deg D$ , on a  $F$  et  $D$  associés.

$\Leftarrow$

$$D\mathbb{K}[X] = A\mathbb{K}[X] + B\mathbb{K}[X] = F\mathbb{K}[X]$$

Donc  $D|A$  et  $D|B$ .

Pour tout diviseur commun  $P$  de  $A$  et  $B$ ,  $P|A$  et  $P|B$ .

Donc  $P|D$  ( $D \in A\mathbb{K}[X] + B\mathbb{K}[X]$ ).

Donc  $\deg D$  est maximal pour la divisibilité.

## 16.24 Lemme de préparation au calcul pratique du PGCD unitaire

### Lemme 16.24

Soit  $A$  et  $B$  deux polynômes tels que  $B \neq 0$ . Pour tout  $Q \in \mathbb{K}[X]$ , on a  $A \wedge B = (A - BQ) \wedge B$ .

En particulier, si  $Q$  et  $R$  sont le quotient et le reste de la division euclidienne de  $A$  par  $B$  Alors  $A \wedge B = B \wedge R$ .

$$\begin{aligned} (A \wedge B)\mathbb{K}[X] &= A\mathbb{K}[X] + B\mathbb{K}[X] \\ &= (A - BQ)\mathbb{K}[X] + B\mathbb{K}[X] \\ &= ((A - BQ) \wedge B)\mathbb{K}[X] \end{aligned}$$

Donc  $A \wedge B$  et  $(A - BQ) \wedge B$  sont associés, unitaires par définition, donc égaux.

## 16.26 Exemple

### Exemple alternatif 16.26

Trouver les PGCD de  $A = X^5 + 2X$  et de  $B = X^4 + 2X^3 + 4$  et une relation de Bézout.

$$\begin{aligned} X^5 + 2X &= (X^4 + 2X^3 + 4)(X - 2) + 4X^3 - 2X + 8 \\ X^4 + 2X^3 + 4 &= (4X^3 - 2X + 8)\left(\frac{1}{4}X + \frac{1}{2}\right) + \frac{1}{2}X^2 - X \\ 4X^3 - 2X + 8 &= \left(\frac{1}{2}X^2 - X\right)(8X + 16) + 14X + 8 \\ \frac{1}{2}X^2 - X &= (14X + 8)\left(\frac{1}{28}X - \frac{9}{14 \times 7}\right) + \frac{9 \times 4}{7^2} \\ A \wedge B &= 1 \end{aligned}$$

$$\begin{aligned} \frac{9 \times 4}{7^2} &= \frac{1}{2}X^2 - X - (14X + 8)\left(\frac{1}{28}X - \frac{9}{2 \times 7^2}\right) \\ &= \frac{1}{2}X^2 - X - (4X^3 - 2X + 8 - \left(\frac{1}{2}X^2 - X\right)(8X + 16))\left(\frac{1}{28}X - \frac{9}{2 \times 7^2}\right) \end{aligned}$$

## 16.27 Propriétés du PGCD

### Proposition 16.27

L'opération  $\wedge$  est commutative et associative. Par ailleurs, si  $C$  est unitaire, alors  $(A \wedge B)C = (AC) \wedge (BC)$ .

Soit  $(A, B, C) \in \mathbb{K}[X]^3$  non tous nuls.

$$\begin{aligned} (A \wedge B)\mathbb{K}[X] &= A\mathbb{K}[X] + B\mathbb{K}[X] \\ &= B\mathbb{K}[X] + A\mathbb{K}[X] \\ &= (B \wedge A)\mathbb{K}[X] \end{aligned}$$

Donc  $A \wedge B$  et  $B \wedge A$  sont associés et unitaires donc égaux.

$$\begin{aligned} ((A \wedge B) \wedge C)\mathbb{K}[X] &= (A \wedge B)\mathbb{K}[X] + C\mathbb{K}[X] \\ &= A\mathbb{K}[X] + B\mathbb{K}[X] + C\mathbb{K}[X] \\ &= (A \wedge (B \wedge C))\mathbb{K}[X] \end{aligned}$$

Donc  $A \wedge (B \wedge C)$  et  $(A \wedge B) \wedge C$  sont associés et unitaires donc égaux.

On suppose  $C$  unitaire.

On a :

$$\begin{aligned} (A \wedge B)\mathbb{K}[X] &= A\mathbb{K}[X] + B\mathbb{K}[X] \\ \text{donc } (A \wedge B)C\mathbb{K}[X] &= AC\mathbb{K}[X] + BC\mathbb{K}[X] \\ &= ((AC) \wedge (BC))\mathbb{K}[X] \end{aligned}$$

Ainsi  $C(A \wedge B)$  et  $(AC) \wedge (BC)$  sont associés et unitaires donc égaux.

## 16.29 Existence de PPCM

### Proposition 16.29

Soit  $\mathbb{K}$  un corps. Soit  $A$  et  $B$  deux polynômes non nuls de  $\mathbb{K}[X]$ . Alors  $A$  et  $B$  admettent des PPCM.

On note  $\mathcal{D} = \{\deg P, A|P, B|P, P \neq 0\} \subset \mathbb{N}$ .

$$\deg AB \in \mathcal{D} \neq \emptyset$$

On conclut avec la propriété fondamentale de  $\mathbb{N}$ .

## 16.30 Caractérisation des PPCM par les idéaux

### Proposition 16.30

Soit  $A$  et  $B$  deux polynômes non nuls de  $\mathbb{K}[X]$  et soit  $P \in \mathbb{K}[X]$ . Alors  $P$  est un PPCM de  $A$  et  $B$  si et seulement si

$$A\mathbb{K}[X] \cap B\mathbb{K}[X] = P\mathbb{K}[X].$$

$A\mathbb{K}[X] \cap B\mathbb{K}[X]$  est un idéal de  $\mathbb{K}[X]$ , donc de la forme  $M\mathbb{K}[X]$  (16.15).

Montrons que  $P$  est un PPCM de  $A$  et  $B$  si et seulement si  $P$  et  $M$  sont associés.

$\Rightarrow$

On a donc :

$$\begin{aligned} P &\in A\mathbb{K}[X] \cap B\mathbb{K}[X] \\ &\in M\mathbb{K}[X] \end{aligned}$$

Donc  $M|P$ .

Or  $M$  est un multiple commun à  $A$  et  $B$ , donc par définition de  $P$ , on a :

$$\deg P \leq \deg M$$

Donc  $P$  et  $M$  sont associés.

$\Leftarrow$

On suppose  $P$  et  $M$  associés, donc :

$$\begin{aligned} P\mathbb{K}[X] &= M\mathbb{K}[X] \\ &= A\mathbb{K}[X] \cap B\mathbb{K}[X] \end{aligned}$$

En particulier,  $P$  est un multiple commun à  $A$  et  $B$  et pour tout  $Q \in A\mathbb{K}[X] \cap B\mathbb{K}[X]$ , donc  $P|Q$ .

Donc :

$$\deg P \leq \deg Q$$

## 16.42 Cas d'unicité d'une relation de Bézout

### Proposition 16.42

Soit  $A$  et  $B$  non constants et premiers entre eux. Il existe un unique couple  $(U, V) \in \mathbb{K}[X]^2$  tel que

$$AU + BV = 1 \text{ et } \deg U < \deg B \text{ et } \deg V < \deg A.$$

Existence :

Soit  $(C, D) \in \mathbb{K}[X]^2$  tel que (16.37 - Bézout) :

$$AC + BD = 1$$

On effectue la division euclidienne de  $C$  par  $B$  :

$$\begin{aligned} C &= BE + U \text{ avec } \deg U < \deg B \\ \text{donc } AU + B \underbrace{(D + AE)}_V &= 1 \\ \text{donc } \deg(AU + BV) &= 0 \end{aligned}$$

Si  $\deg V \geq \deg A$ , alors :

$$\begin{aligned} \deg B + \deg V &\geq \deg B + \deg A \\ &> \deg U + \deg B \\ &= \deg AU \end{aligned}$$

Donc  $\deg(AU + BV) = \deg BV > 0$ .

Absurde.

L'existence est prouvée.

Unicité :

Avec les hypothèses correspondantes :

$$\begin{aligned} AU_1 + BV_1 &= 1 = AU_2 + BV_2 \\ \text{donc } A(U_1 - U_2) &= B(V_2 - V_1) \\ \text{donc } A|B(V_2 - V_1) \end{aligned}$$

Or  $A \wedge B = 1$ , donc  $A|(V_2 - V_1)$ .

Or  $\deg(V_2 - V_1) < \deg A$ .

Donc  $V_2 - V_1 = 0$ .

Puis  $A(U_1 - U_2) = 0$ , donc  $U_1 - U_2 = 0$  car  $\mathbb{K}[X]$  est intègre avec  $A \neq 0$ .

## 16.43 Corollaire

### Corollaire 16.43

Soit  $A$ ,  $B$  et  $C$  trois polynômes avec  $A$  et  $B$  premiers entre eux. Alors  $A \wedge (BC) = A \wedge C$ .

—  $A \wedge C|A$  donc  $A \wedge C|A \wedge (BC)$ . Donc  $A \wedge C|BC$ .

—  $A \wedge (BC)|A$ . Or  $A \wedge B = 1$  donc on peut écrire  $AU + BV = 1$ . Donc  $ACU + BCV = C$ .

Or  $A \wedge (BC)|ACU + BCV$  soit  $A \wedge (BC)|C$ . Donc  $A \wedge (BC)|A \wedge C$ .

Ainsi,  $A \wedge C$  et  $A \wedge (BC)$  sont associés et unitaires donc égaux.

## 16.44 Caractérisation des PGCD et PPCM

### Proposition 16.44

Soit  $A$  et  $B$  deux polynômes non nuls,  $M$  et  $D$  deux polynômes. Alors

$$M = A \vee B \Leftrightarrow (M \text{ unitaire et } \exists (U, V) \in \mathbb{K}[X]^2, M = AU = BV \text{ et } U \wedge V = 1).$$

$$D = A \wedge B \Leftrightarrow (D \text{ unitaire et } \exists (U, V) \in \mathbb{K}[X]^2, A = DU \text{ et } B = DV \text{ et } U \wedge V = 1).$$

—  $\boxed{\Rightarrow}$

$M = A \vee B$ . On écrit  $M = AU + BV$  avec  $(U, V) \in \mathbb{K}[X]^2$ .

On note  $R = U \wedge V$ . On écrit  $U = RU_1$  et  $V = RV_1$ .

Ainsi :

$$\begin{aligned} M &= RAU_1 = RBV_1 \\ \text{donc } R(AU_1 - BV_1) &= 0 \\ \text{donc } AU_1 &= BV_1 \text{ (}\mathbb{K}[X]\text{ est intègre)} \end{aligned}$$

Donc  $M_1 = AU_1 = BV_1$  est un multiple commun et par minimalité des degrés :

$$RM_1 = M|M_1 \text{ donc } R = 1$$

⇐

Par hypothèse,  $M$  est un multiple commun, donc :

$$M \in A\mathbb{K}[X] \cap B\mathbb{K}[X] = (A \vee B)\mathbb{K}[X]$$

Donc  $A \vee B | M$ .

Donc  $M = D \times A \vee B$ .

Or  $A \vee B = AU_1 = BV_1$ .

Donc  $M = DAU_1 = DBV_1 = AU = BV$ .

Donc :

$$A(DU_1 - U) = 0$$

$$B(DV_1 - V) = 0$$

Or  $\mathbb{K}[X]$  est intègre donc  $DU_1 = U$  et  $DV_1 = V$ .

Donc  $D|U \wedge V = 1$ .

—

⇒

$D = A \wedge B$ . On écrit  $A = DU$  et  $B = DV$ .

Or pour  $R = U \wedge V$ , on écrit  $U = RU_1$  et  $V = RV_1$ .

Donc  $A = DRU_1$  et  $B = DRV_1$ .

Donc  $DR|A$  et  $DR|B$ .

Donc  $DR|D$ .

Nécessairement,  $R = 1$ .

⇐

Par hypothèse,  $D|A$  et  $D|B$ , donc  $D|A \wedge B$ .

Comme  $U \wedge V = 1$ , d'après le théorème de Bézout :

$$UU_1 + VV_1 = 1$$

$$\text{donc } DUU_1 + DVV_1 = D$$

$$\text{soit } AU_1 + BV_1 = D$$

$$\text{donc } A \wedge B | D$$

Ainsi,  $A \wedge B$  et  $D$  sont associés. Or ils sont unitaires, donc égaux.

## 16.53 Caractérisation des racines par la divisibilité

### Théorème 16.53

Soit  $\mathbb{K}$  un corps,  $P \in \mathbb{K}[X]$  et  $r \in \mathbb{K}$ . Alors  $r$  est racine de  $P$  si et seulement si  $X - r$  divise  $P$ . Donc s'il existe  $Q \in \mathbb{K}[X]$  tel que  $P = (X - r)Q$ .

⇐

Si  $P = (X - r)Q$ , alors :

$$\tilde{P}(r) = (X - r)\tilde{Q}(r)$$

$$= 0 \times \tilde{Q}(r)$$

$$= 0$$

⇒

On suppose  $r$  racine de  $P$ .

On effectue la division euclidienne de  $P$  par  $X - r$  :

$$P = (X - r)Q + R, R \in \mathbb{K}_0[X]$$

Donc  $0 = \tilde{P}(r) = \tilde{R}(r)$ .

Donc  $R = 0$ .

Donc  $X - r | P$ .



## 16.56 Formule de Taylor pour les polynômes

### Théorème 16.56

Soit  $\mathbb{K}$  un corps de caractéristique nulle,  $P$  un polynôme de  $\mathbb{K}[X]$  de degré  $d$  et  $a \in \mathbb{K}$ , alors

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

On note  $E_k = X^k$ , pour  $k \in \mathbb{N}$ .

On a, pour  $i \in \mathbb{N}$  :

$$E_k^{(i)} = \begin{cases} \frac{k!}{(k-i)!} X^{k-i} & \text{si } i \leq k \\ 0 & \text{si } i > k \end{cases}$$

Ainsi :

$$\begin{aligned} E_k(X + a) &= (X + a)^k \\ &= \sum_{i=0}^k \binom{k}{i} a^{k-i} X^i \\ &= \sum_{i=0}^k \frac{k!}{i!(k-i)!} a^{k-i} X^i \\ &= \sum_{i=0}^k \frac{E_k^{(i)}(a)}{i!} X^i \end{aligned}$$

Soit  $P = \sum_{k=0}^d a_k X^k = \sum_{k=0}^d a_k E_k$ .

Ainsi :

$$\begin{aligned} P(x + a) &= \sum_{k=0}^d a_k E_k(X + a) \\ &= \sum_{k=0}^d a_k \sum_{i=0}^k \frac{E_k^{(i)}(a)}{i!} X^i \\ &= \sum_{i=0}^d \frac{1}{i!} \left( \sum_{k=i}^d a_k E_k^{(i)}(a) \right) X^i \\ &= \sum_{i=0}^d \frac{1}{i!} \left( \sum_{k=0}^d a_k E_k^{(i)}(a) \right) X^i \\ &= \sum_{i=0}^d \frac{1}{i!} P^{(i)}(a) X^i \end{aligned}$$

## 16.57 Caractérisation de la multiplicité par les dérivées

### Théorème 16.57

Soit  $\mathbb{K}$  un corps de caractéristique nulle,  $P \in \mathbb{K}[X]$  et  $a \in \mathbb{K}$ . Le réel  $a$  est racine d'ordre multiplicité  $k$  de  $P$  si et seulement si

$$P(a) = P'(a) = \dots = P^{(k-1)}(a) = 0 \text{ et } P^{(k)}(a) \neq 0.$$



D'après la formule de Taylor :

$$\begin{aligned}
 P &= \sum_{i=0}^d \frac{P^{(i)}(a)}{i!} (X-a)^i \\
 &= \sum_{i=k}^d \frac{P^{(i)}(a)}{i!} (X-a)^i \\
 &= (X-a)^k \underbrace{\sum_{i=k}^d \frac{P^{(i)}(a)}{i!} (X-a)^{i-k}}_{=Q} \\
 Q(a) &= \frac{P^{(k)}(a)}{k!} \neq 0
 \end{aligned}$$

$$P = \underbrace{(X-a)^k}_B Q \text{ avec } Q(a) \neq 0.$$

Pour tout  $i \in \llbracket 0, k-1 \rrbracket$  :

$$\begin{aligned}
 P^{(i)} &= (BQ)^{(i)} \\
 &= \sum_{l=0}^i \binom{i}{l} B^{(l)} Q^{(i-l)} \\
 P^{(i)}(a) &= 0 \\
 P^{(k)} &= \binom{k}{k} B^{(k)}(a) \times Q^{(k-k)}(a) \\
 &= k! \times Q(a) \neq 0
 \end{aligned}$$

## 16.59 Caractérisation de la multiplicité des racines par la divisibilité

### Théorème 16.59

Soit  $\mathbb{K}$  un corps. Soit  $P \in \mathbb{K}[X]$  et  $r_1, \dots, r_k$  des racines deux à deux distinctes de  $P$ , de multiplicités respectives  $a_1, \dots, a_k$ . Alors  $(X-r_1)^{a_1} \dots (X-r_k)^{a_k}$  divise  $P$  et  $r_1, \dots, r_k$  ne sont pas racines du quotient.

RAF :

$$(X-r_i)^{\alpha_1} \wedge (X-r_k)^{\alpha_k} = 1 \text{ si } i \neq k$$

## 16.63 Polynômes formels et fonctions polynomiales

### Théorème 16.63

Soit  $\mathbb{K}$  un corps infini. Alors l'application de  $\mathbb{K}[X]$  dans  $\mathbb{K}[x]$  qui à un polynôme formel associe sa fonction polynomiale est un isomorphisme d'anneaux.

RAF :  $\varphi(P) = \varphi(Q)$  donc  $\varphi(P-Q) = 0$   
 $\tilde{P} - \tilde{Q}$  s'annule sur  $\mathbb{K}$  infini et on applique (16.62).

## 16.66 Caractérisation des polynômes interpolateurs

### Lemme 16.66

Le polynôme  $L_i$  est l'unique polynôme de degré au plus  $n$  tel que pour tout  $j \in \llbracket 0, n \rrbracket$ ,  $L_i(x_j) = \delta_{ij}$ .

Existence : RAF

Unicité : (16.61.3)

## 16.69 Corollaire

### Corollaire 16.69

Soit  $P$  le polynôme d'interpolation de Lagrange associé à la famille  $(x_i)_{0 \leq i \leq n}$  et aux valeurs  $(y_i)_{0 \leq i \leq n}$ . Soit  $P_0 = (X - x_0) \dots (X - x_n)$ . L'ensemble  $E$  des polynômes  $Q$  (sans restriction de degré) tel que pour tout  $i \in \llbracket 0, n \rrbracket$ ,  $Q(x_i) = y_i$  est décrit par

$$E = P + (P_0) = \{P + (X - x_0) \dots (X - x_n)R, R \in \mathbb{K}[X]\}$$



Si  $Q = P + (X - x_0) \dots (X - x_n)R$ , alors :

$$\forall i \in \llbracket 0, n \rrbracket, Q(x_i) = P(x_i) = y_i$$

Donc  $Q \in E$ .



Soit  $Q \in E$ , alors  $x_0, \dots, x_n$  sont racines de  $Q - P$ .

Donc  $(X - x_0) \dots (X - x_n) \mid Q - P$ .

## 16.74 Proposition

### Proposition 16.74 (HP)

Soit  $P$  un polynôme scindé non constant de  $\mathbb{R}[X]$  à racines simples. Alors  $P'$  est scindé, et ses racines séparent celles de  $P$ .

Soit  $P = \prod_{k=1}^n (x - x_k)$  avec  $x_1 < \dots < x_n$ .

D'après le théorème de Rolle, comme  $P(x_1) = P(x_2) = \dots = P(x_n) = 0$  pour tout  $k \in \llbracket 1, n-1 \rrbracket$ , on choisit  $y_k \in ]x_k, x_{k+1}[$  tel que  $P'(y_k) = 0$ .

On a donc :

$$x_1 < y_1 < x_2 < y_2 < \dots < y_{n-1} < x_n$$

et  $y_1, \dots, y_{n-1}$  sont  $n-1$  racines distinctes de  $P'$  de degré  $n-1$  ( $\mathbb{R}$  de caractéristique nulle).

Donc  $P'$  est scindé (à racines simples).

## 16.76 Relation de Viète

### Théorème 16.76

Soit  $P = \sum_{k=0}^n a_k X^k$  un polynôme de degré  $n$ , scindé, de racines (éventuellement non distinctes, apparaissant dans la liste autant de fois que sa multiplicité)  $r_1, \dots, r_n$  alors pour tout  $k \in \llbracket 0, n \rrbracket$  :

$$\sum_{1 \leq i_1 < \dots < i_k \leq n} r_{i_1} \dots r_{i_k} = (-1)^k \frac{a_{n-k}}{a_n}$$

$$\begin{aligned} P &= \sum_{k=0}^n a_k X^k \\ &= a_n \prod_{k=1}^n (X - r_k) \end{aligned}$$

Les relations de Viète consistent simplement à développer l'expression de droite et à identifier les mnômes de degré  $n - k$ .

$$a_{n-k} = (-1)^k a_n \sum_{1 \leq i_1 < \dots < i_k \leq n} r_{i_1} \dots r_{i_k}$$

## 16.88 Lemme

### Lemme 16.88

Soit  $P$  un polynôme irréductible de  $\mathbb{K}[X]$  et  $A$  un polynôme non multiple de  $P$ . Alors  $A$  et  $P$  ont premiers entre eux.

Soit  $D$  unitaire  $\in \mathcal{D}_{A,P}$ .

Si  $P \nmid A$ , alors  $D \neq U(P)$ .

Donc  $D = 1$ .

Donc  $P \wedge A = 1$ .

## 16.98 Caractérisation de la divisibilité dans $\mathbb{C}[X]$ par les racines

### Théorème 16.98

Soit  $P$  et  $Q$  deux polynômes de  $\mathbb{C}[X]$ . Alors  $P$  divise  $Q$  si et seulement si toute racine de  $P$  est aussi une racine de  $Q$ , et que sa multiplicité dans  $Q$  est supérieure ou égale à sa multiplicité dans  $P$ .

$\Rightarrow$

Supposons  $P|Q$ .

Soit  $r$  une racine de  $P$  de multiplicité  $\alpha$ . Donc :

$$(X - r)^\alpha | P \\ \text{donc } (X - r)^\alpha | Q$$

Donc  $r$  est racine de  $Q$  de multiplicité supérieure à  $\alpha$ .

$\Leftarrow$

On décompose  $P = \lambda \prod_{i=1}^n (X - r_i)^{\alpha_i}$  ( $P$  est scindé sur  $\mathbb{C}$ ).

Par hypothèse,  $\prod_{i=1}^n (X - r_i)^{\alpha_i} | Q$ .

Donc  $P|Q$ .

## 16.99 Caractérisation des polynômes à coefficients réels

### Théorème 16.99

Soit  $P \in \mathbb{C}[X]$ . Les propositions sont équivalentes :

1.  $P$  est à coefficients réels ;
2.  $P(\mathbb{R}) \subset \mathbb{R}$  ;
3. pour tout  $z \in \mathbb{C}$ ,  $\overline{P(z)} = P(\bar{z})$ .

$1 \Rightarrow 2$

RAF

$2 \Rightarrow 1$

On suppose que  $P(\mathbb{R}) \subset \mathbb{R}$ .

Soit  $z \in \mathbb{C}$ .

$$\begin{aligned} P &= \sum_{k=0}^n a_k X^k \\ \overline{P(z)} &= \overline{\sum_{k=0}^n a_k z^k} \\ &= \sum_{k=0}^n \overline{a_k} (\overline{z})^k \end{aligned}$$

Par hypothèse, pour  $z \in \mathbb{R}$ ,  $P(z) \in \mathbb{R}$ , soit  $\overline{P(z)} = P(z)$ .  
Ainsi, pour  $z \in \mathbb{R}$  :

$$\sum_{k=0}^n \overline{a_k} z^k = \sum_{k=0}^n a_k z^k$$

Les deux polynômes  $\sum_{k=0}^n \overline{a_k} X^k$  et  $\sum_{k=0}^n a_k X^k$  coïncident sur une infinité de valeurs, donc (théorème de rigidité) ils sont égaux.  
Donc :

$$\forall k \in \llbracket 0, n \rrbracket, a_k = \overline{a_k}$$

Donc  $P \in \mathbb{R}[X]$ .

$1 \Rightarrow 3$

RAF

$3 \Rightarrow 2$

Si  $\overline{P(z)} = P(\overline{z})$  pour tout  $z \in \mathbb{C}$ , alors en particulier pour  $z \in \mathbb{R}$ ,  $\overline{P(z)} = P(z)$  soit  $P(z) \in \mathbb{R}$ .

## 16.100 Racine complexe d'un polynôme réel

### Corollaire 16.100

Soit  $P$  un polynôme à coefficients réels et  $r$  une racine de  $P$  dans  $\mathbb{C}$ . Si  $r \notin \mathbb{R}$ , alors  $\bar{r}$  est aussi une racine de  $P$  et elles ont la même multiplicité.

Soit  $r$  une racine complexe de  $P$ .

Donc  $P(r) = 0$ .

Donc  $\overline{P(r)} = 0$ .

Donc (16.99.3)  $P(\bar{r}) = 0$ .

Donc  $\bar{r}$  est aussi une racine de  $P$ .

Donc  $(X - \bar{r})(X - r) \mid P$ .

Donc  $P = (X - \bar{r})(X - r)Q$  et si  $r$  est une racine de  $Q$ ,  $\bar{r}$  également, ce qui justifie que  $\bar{r}$  a la même multiplicité que  $r$ .

## 16.101 Polynômes irréductibles de $\mathbb{R}[X]$

### Théorème 16.101

1. Les polynômes irréductibles de  $\mathbb{R}[X]$  sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif.
2. Ainsi, tout polynôme  $P \in \mathbb{R}[X]$  peut être factorisé en produit de polynômes de  $\mathbb{R}[X]$  de degré 1 ou de degré 2, de discriminant strictement négatif.

1. Les polynômes annoncés sont bien les seuls irréductibles dans  $\mathbb{R}_2[X]$ .

Soit  $P \in \mathbb{R}[X]$ , avec  $\deg P \geq 3$ . Dans  $\mathbb{C}[X]$ ,  $P$  est scindé.

Si  $P$  admet une racine dans  $\mathbb{R}$ ,  $P$  est réductible.

Supposons maintenant que toutes les racines de  $P$  sont complexes. Soit  $r$  l'une d'entre elles.

Alors  $\bar{r} \neq r$  est aussi une racine de  $P$ .

Donc  $(X - r)(X - \bar{r})|P$ .

Donc :

$$\begin{aligned} P &= (X - r)(X - \bar{r})Q \text{ avec } Q \in \mathbb{C}[X] \\ &= \underbrace{(x^2 - 2\operatorname{Re}(r)X + |r|^2)}_{:=R \in \mathbb{R}[X]}Q \end{aligned}$$

Donc  $P = RQ$  est la division euclidienne de  $P$  par  $R$  dans  $\mathbb{C}[X]$  et aussi dans  $\mathbb{R}[X]$ .

Par unicité, on a donc  $Q \in \mathbb{R}[X]$  et  $P$  est réductible dans  $\mathbb{R}[X]$ .

2. RAF