

# Chapitre 1

## Polynômes

Pour le contenu du chapitre “Polynômes”, on peut se reporter au chapitre 10 du Cours de mathématiques – Algèbre 1<sup>re</sup> année de F. Liret et D. Martinais (éditions Dunod), ou au chapitre 13 du livre “Toute l’algèbre du 1<sup>er</sup> cycle” de J.-P. Escofier (éditions Dunod).

### 1.1 Généralités

Un polynôme à une variable sur un corps  $\mathbb{K}$  (nous serons essentiellement intéressés par les cas où  $\mathbb{K}$  est  $\mathbb{R}$  ou  $\mathbb{C}$ ) est une expression

$$a_0 + a_1X + \cdots + a_nX^n ,$$

où les  $a_i$  sont des éléments de  $\mathbb{K}$  (les *coefficients* du polynôme). Formellement, on peut définir un polynôme comme la suite infinie  $(a_0, a_1, \dots, a_n, \dots)$  de ses coefficients, tous nuls à partir d’un certain rang. Par exemple, le polynôme  $1 + 2X^2 - X^3$  est codé par la suite  $(1, 0, 2, -1, 0, 0, \dots)$ .

On note  $\mathbb{K}[X]$  l’ensemble des polynômes sur  $\mathbb{K}$ . Il est muni des deux opérations de l’addition et de la multiplication, qui en font un anneau commutatif, comme  $\mathbb{Z}$ .

On identifie un élément  $a$  de  $\mathbb{K}$  au polynôme constant (codé  $(a, 0, 0, \dots)$ ). La multiplication par les éléments de  $\mathbb{K}$  munit alors  $\mathbb{K}[X]$  d’une structure d’espace vectoriel sur  $\mathbb{K}$ .

Soit  $P$  un polynôme non nul. Le *degré* de  $P$  est le plus grand entier  $n$  tel que le coefficient  $a_n$  de  $X^n$  dans  $P$  soit non nul. Ce coefficient  $a_n$  s’appelle alors le *coefficient dominant* de  $P$ , et on dit que  $P$  est *unitaire* si son coefficient dominant est 1. Par convention on peut décréter que le degré du polynôme nul est  $-\infty$ . On a

$$\begin{aligned} \deg(P + Q) &\leq \max(\deg(P), \deg(Q)) \quad (\text{égalité si } \deg(P) \neq \deg(Q)) \\ \deg(PQ) &= \deg(P) + \deg(Q) . \end{aligned}$$

On dit qu’un polynôme  $B$  *divise* un polynôme  $A$  s’il existe un polynôme  $Q$  tel que  $A = BQ$ . Noter que le fait qu’à la fois  $B$  divise  $A$  et  $A$  divise  $B$  équivaut au fait qu’il existe une constante  $c \neq 0$  telle que  $A = cB$ . Noter aussi que si  $B$  divise  $A$  et  $\deg(A) < \deg(B)$ , alors  $A = 0$ .

Soit  $c \in \mathbb{K}$  et  $P = a_0 + a_1X + \cdots + a_nX^n$  un polynôme sur  $\mathbb{K}$ . On pose  $P(c) = a_0 + a_1c + \cdots + a_nc^n$ . On dit que  $c$  est *racine* de  $P$  quand  $P(c) = 0$ . L'application  $c \mapsto P(c)$  de  $\mathbb{K}$  dans lui-même est la *fonction polynôme* associée au polynôme  $P$ .

On peut *substituer* un polynôme  $Q$  à la variable  $X$  dans un autre polynôme  $P$  pour obtenir un nouveau polynôme  $P(Q)$  (noté aussi  $P \circ Q$  chez Liret-Martinai) : si  $P = a_0 + a_1X + \cdots + a_nX^n$ , alors  $P(Q) = a_0 + a_1Q + \cdots + a_nQ^n$ . On a  $P_1(Q) + P_2(Q) = (P_1 + P_2)(Q)$  et  $P_1(Q) \times P_2(Q) = (P_1P_2)(Q)$ .

**Exercice 1.1**

Calculer par récurrence  $(1 + X)(1 + X^2)(1 + X^4) \cdots (1 + X^{2^n})$ .

**Exercice 1.2**

Si  $P$  est un polynôme de degré  $n$  à coefficients dans  $\mathbb{K}$  et  $c$  un élément de  $\mathbb{K}$ , combien faut-il d'opérations (additions et multiplications) dans  $\mathbb{K}$  pour calculer  $P(c)$  ?

Combien faut-il d'opérations dans  $\mathbb{K}$  pour multiplier deux polynômes de degré  $n$  ?

**Exercice 1.3**

Soient  $A, B, C, U, V$  des polynômes de  $\mathbb{K}[X]$ . Montrer que si  $A$  divise  $B$  et  $C$ , il divise aussi  $UB + VC$ .

**Exercice 1.4**

Montrer que, si les trois polynômes  $P, Q, R$  de  $\mathbb{R}[X]$  vérifient la relation

$$P^2(X) - XQ^2(X) = XR^2(X),$$

ils sont nuls (*faire jouer la parité du degré et les signes des coefficients dominants*). Est-ce encore vrai dans  $\mathbb{C}[X]$  ?

**Exercice 1.5**

Soit  $a \in \mathbb{K}$ . Montrer que  $P(X) = X(X + a)(X + 2a)(X + 3a) + a^4$  est un carré dans  $\mathbb{K}[X]$ . En déduire une décomposition de  $Q(X) = X(X + 1)(X + 2)(X + 3) - 8$  en produit dans  $\mathbb{R}[X]$ .

**Exercice 1.6**

Soient  $P$  et  $Q$  des polynômes de  $\mathbb{K}[X]$ .

1. Montrer que  $P(X) - X$  divise  $Q(P(X)) - Q(X)$ .
2. Montrer que  $P(X) - X$  divise  $P(P(X)) - X$ .

**Exercice 1.7**

Montrer que l'application  $P \mapsto P(X + a)$  est une bijection de  $\mathbb{K}[X]$  sur lui-même. Quelle est la bijection réciproque ?

## 1.2 Division euclidienne, pgcd de deux polynômes

Un point important qui fait que l'anneau des polynômes à une variable sur un corps  $\mathbb{K}$  est très semblable à  $\mathbb{Z}$  est l'existence d'une division euclidienne.

**Théorème 1.1** *Soient  $A$  et  $B$  deux polynômes de  $\mathbb{K}[X]$ , avec  $B$  différent du polynôme nul. Alors il existe des polynômes  $Q$  (quotient) et  $R$  (reste) tels que*

$$A = BQ + R \quad \text{avec } \deg R < \deg B \text{ ou } R = 0.$$

*De plus, le couple  $(Q, R)$  vérifiant ces propriétés est unique.*

**Proposition 1.2** *Le reste de la division euclidienne de  $P$  par  $X - c$  est  $P(c)$ . En conséquence, un élément  $c \in \mathbb{K}$  est racine de  $P$  si et seulement si  $P$  est divisible par  $X - c$ .*

**Définition 1.3** *Si  $A$  et  $B$  sont deux polynômes de  $\mathbb{K}[X]$ , on dit que le polynôme  $D$  est un plus grand commun diviseur (en abrégé, pgcd) de  $A$  et  $B$  quand*

1.  $D$  est un diviseur commun de  $A$  et  $B$ ,
2. tout diviseur commun de  $A$  et  $B$  divise  $D$ .

*Autrement dit, l'ensemble des diviseurs de  $D$  est égal à celui des diviseurs communs de  $A$  et  $B$ .*

Ceci ne définit pas le pgcd de manière unique, mais à un facteur constant non nul près. L'existence du pgcd est établie, comme pour les entiers, par l'algorithme d'Euclide. Soient  $A$  et  $B$  deux polynômes. On pose

$$R_0 = A \quad R_1 = B$$

et, pour  $n \geq 1$ , tant que  $R_n$  est non nul, on définit  $R_{n+1}$  comme le reste de la division euclidienne de  $R_{n-1}$  par  $R_n$  :

$$R_{n-1} = R_n Q_n + R_{n+1} \quad \text{avec } \deg(R_{n+1}) < \deg(R_n) \text{ ou } R_{n+1} = 0.$$

Comme la suite  $\deg R_1, \deg R_2, \dots$  est strictement décroissante, l'algorithme s'arrête au bout d'un nombre fini  $N$  d'étapes avec  $R_{N+1} = 0$ .

**Théorème 1.4** *Le polynôme  $R_N$  obtenu à la fin de l'algorithme (c'est le dernier reste non nul, si  $A$  et  $B$  sont différents de 0) est un pgcd de  $A$  et  $B$ .*

Si  $A$  et  $B$  sont tous les deux nuls,  $\text{pgcd}(A, B) = 0$ . Sinon, un pgcd est un polynôme de degré maximal parmi ceux qui divisent à la fois  $A$  et  $B$ ; on peut rendre le pgcd unique en demandant qu'il soit unitaire (c'est souvent comme cela que le pgcd est défini, par exemple chez Liret-Martinais).

Comme pour les entiers, on a :

**Théorème 1.5** *Soient  $A$  et  $B$  deux polynômes,  $D$  un pgcd de  $A$  et  $B$ . Il existe des polynômes  $U$  et  $V$  tels que  $D = UA + VB$ .*

**Définition 1.6** *Deux polynômes  $A$  et  $B$  sont dits premiers entre eux quand 1 est pgcd de  $A$  et  $B$ , autrement dit si et seulement si les seuls diviseurs communs de  $A$  et  $B$  sont les constantes non nulles.*

**Théorème 1.7 (Identité de Bezout)** Deux polynômes  $A$  et  $B$  sont premiers entre eux si et seulement s'il existe des polynômes  $U$  et  $V$  tels que  $UA + VB = 1$ .

**Corollaire 1.8** Soit  $A$  un polynôme premier avec chacun des polynômes  $B_1, \dots, B_r$ . Alors  $A$  est premier avec le produit  $B_1 \cdots B_r$ .

**Théorème 1.9 (Lemme de Gauss)** Soient  $A, B$  et  $C$  des polynômes tels que  $A$  et  $B$  soient premiers entre eux et que  $A$  divise le produit  $BC$ . Alors  $A$  divise  $C$ .

**Définition 1.10** Un polynôme  $M$  est un plus petit commun multiple (ppcm) de deux polynômes  $A$  et  $B$  si et seulement si

1.  $M$  est un multiple commun de  $A$  et  $B$ ,
2. tout multiple commun de  $A$  et  $B$  est multiple de  $M$ .

Si  $A$  ou  $B$  est nul, le ppcm de  $A$  et  $B$  est 0. Si  $A$  et  $B$  sont tous les deux non nuls, et si  $D$  est un pgcd de  $A$  et  $B$ , alors  $AB/D$  est un ppcm de  $A$  et  $B$ .

**Théorème 1.11** Soient  $A_1, \dots, A_r$  des polynômes premiers entre eux deux à deux ( $A_i$  premier avec  $A_j$  si  $i \neq j$ ). Si chaque  $A_i$  divise  $B$ , alors la produit  $A_1 \cdots A_r$  divise  $B$ .

Dans les exercices on dira “le pgcd” ou “le ppcm”, et on notera  $\text{pgcd}(A, B)$  ou  $\text{ppcm}(A, B)$  pour le pgcd ou le ppcm unitaire.

#### Exercice 1.8

Effectuer les divisions euclidiennes de

$$\begin{aligned} 2X^5 - 5X^3 - 8X & \text{ par } X + 3, \\ 4X^3 + X^2 & \text{ par } X + 1 + i, \\ X^5 - 2X^4 + 3X^3 - 4X^2 + 5X - 5 & \text{ par } X^2 + X + 1. \end{aligned}$$

En déduire  $\text{pgcd}(X^5 - 2X^4 + 3X^3 - 4X^2 + 5X - 5, X^2 + X + 1)$ .

#### Exercice 1.9

Calculer le reste de la division dans  $\mathbb{R}[X]$  de

1.  $(\cos a + X \sin a)^n$  par  $X^2 + 1$ ,
2.  $(X - 1)^m + X^m - 1$  par  $X^2 - X + 1$  selon la valeur de  $m$  modulo 6.

#### Exercice 1.10

Soit  $P(X) \in \mathbb{R}[X]$  et  $a$  et  $b$  deux nombres réels distincts. Calculer le reste  $R(X)$  de la division de  $P(X)$  par  $(X - a)(X - b)$  en fonction de  $P(a)$  et  $P(b)$ .

#### Exercice 1.11

Soit  $P(X) = 3X^3 + 2X^2 + 2$  et  $Q(X) = X^2 - 2$ .

1. Utiliser l'algorithme d'Euclide pour déterminer le pgcd  $D$  de  $P$  et  $Q$ .
2. En déduire deux polynômes  $U$  et  $V$  tels que  $UP + VQ = D$ .

**Exercice 1.12**

On note  $\mathbb{R}[X]$  l'ensemble des polynômes à coefficients réels et  $\deg P$  le degré d'un polynôme  $P$  de  $\mathbb{R}[X]$ . Soit  $A(X) = X^3 + 2X^2 - X - 2$  et  $B(X) = X^3 - 3X - 2$ .

1. Calculer  $D$  le pgcd unitaire de  $A$  et  $B$ .
2. Trouver deux polynômes  $U_0$  et  $V_0$  de  $\mathbb{R}[X]$  vérifiant  $AU_0 + BV_0 = D$  avec  $\deg U_0 < \deg B$  et  $\deg V_0 < \deg A$ .
3. Trouver le ppcm unitaire de  $A$  et  $B$ .

**Exercice 1.13**

On considère les polynômes  $A(X) = X^5 - X^4 + 2X^3 + 1$  et  $B(X) = X^5 + X^4 + 2X^2 - 1$ . Déterminer leur pgcd  $D$  et écrire  $D$  sous la forme  $AU + BV$ .

**Exercice 1.14**

Soient  $a$  et  $b$  deux entiers strictement positifs. Quel est le pgcd de  $X^a - 1$  et  $X^b - 1$  ?

**Exercice 1.15**

Soit  $D = \text{pgcd}(A, B)$  (où  $A$  et  $B$  ne sont pas nuls tous les deux), et soit  $(U, V)$  tels que  $AU + BV = D$ . Quel est le pgcd de  $U$  et  $V$  ?

**Exercice 1.16**

Soient  $A(X) = (X - 1)^2$  et  $B(X) = (X + 1)^2$ .

1. Calculer le pgcd unitaire  $D$  de  $A$  et  $B$ .
2. Trouver deux polynômes  $U$  et  $V$  de  $\mathbb{R}[X]$  tels que  $UA + VB = D$ .
3. Dédire une décomposition en éléments simples de  $\frac{1}{(X^2 - 1)^2}$ .

**Exercice 1.17**

Soit  $P$  et  $Q$  dans  $\mathbb{K}[X]$  deux polynômes premiers entre eux. Montrer que, si  $m$  et  $n$  sont des entiers strictement positifs,  $P^m$  est premier avec  $Q^n$ .

**Exercice 1.18**

Trouver un polynôme  $P$  unitaire de degré  $\leq 3$ , divisible par  $X - 1$  et tel que les restes dans la division de  $P$  par  $X - 2$ ,  $X - 3$  et  $X - 4$  soient égaux.

## 1.3 Décomposition en facteurs irréductibles

**Définition 1.12** *Un polynôme  $P \in \mathbb{K}[X]$  est dit irréductible si ce n'est pas une constante et si ses seuls diviseurs sont les constantes non nulles et les polynômes de la forme  $cP$  où  $c$  est une constante non nulle (autrement dit,  $\deg(P) > 0$  et il n'y a pas de factorisation  $P = Q_1Q_2$  avec  $\deg(Q_1) < \deg(P)$  et  $\deg(Q_2) < \deg(P)$ ).*

Un polynôme du premier degré est toujours irréductible. Soit  $P$  un polynôme irréductible. Si  $P$  ne divise pas le polynôme  $A$ , alors  $P$  est premier avec  $A$ . Si

$Q$  est un autre polynôme irréductible, alors ou bien il existe une constante non nulle  $c$  telle que  $Q = cP$ , ou bien  $P$  et  $Q$  sont premiers entre eux.

Les polynômes irréductibles jouent le rôle des nombres premiers.

**Théorème 1.13** *Soit  $A$  un polynôme non constant de  $\mathbb{K}[X]$ . Alors il existe une décomposition*

$$A = cP_1^{\alpha_1} \cdots P_k^{\alpha_k}$$

où  $c$  est une constante non nulle,  $P_1, \dots, P_k$  sont des polynômes irréductibles unitaires distincts de  $\mathbb{K}[X]$ , et  $\alpha_1, \dots, \alpha_k$  des entiers strictement positifs. De plus, une telle décomposition est unique, à l'ordre des facteurs irréductibles près.

L'identification des polynômes irréductibles sur  $\mathbb{C}$  et  $\mathbb{R}$  repose sur le fameux

**Théorème 1.14 (D'Alembert - Gauss)** *Tout polynôme non constant de  $\mathbb{C}[X]$  a une racine dans  $\mathbb{C}$ .*

La démonstration de ce théorème sort du cadre du cours. On en déduit :

**Théorème 1.15** *Sur  $\mathbb{C}$ , les polynômes irréductibles unitaires sont les  $X - c$  avec  $c \in \mathbb{C}$ . Sur  $\mathbb{R}$ , les polynômes irréductibles unitaires sont les  $X - c$  avec  $c \in \mathbb{R}$  et les  $X^2 + bX + c$  sans racine réelle (c.-à-d. avec  $b^2 - 4c < 0$ ).*

Rappelons que, si  $c$  est un nombre complexe,  $(X - c)(X - \bar{c}) = X^2 - 2 \operatorname{Re}(c)X + |c|^2 \in \mathbb{R}[X]$ .

**Exercice 1.19**

Soit  $P(X) = 3X^3 - 2X^2 - 7X - 2$  et  $Q(X) = 2X^2 + 3X + 1$ .

1. Utiliser l'algorithme d'Euclide pour déterminer le pgcd de  $P$  et  $Q$ .
2. Donner la décomposition de  $P$  en facteurs irréductibles dans  $\mathbb{R}[X]$ .
3. Quel est le ppcm de  $P$  et  $Q$  ?

**Exercice 1.20**

Décomposer dans  $\mathbb{R}[X]$  puis dans  $\mathbb{C}[X]$  les polynômes suivants en facteurs irréductibles

$$\begin{array}{ccc} X^3 + 1 & X^3 - 1 & X^3 + 2X^2 + 2X + 1 \\ X^4 + 1 & X^4 + X^2 + 1 & 1 + X + X^2 + X^3 + X^4 + X^5 \end{array}$$

**Exercice 1.21**

Décomposer dans  $\mathbb{R}[X]$ , puis dans  $\mathbb{Q}[X]$  le polynôme  $P(X) = X^4 + 1$ .

**Exercice 1.22**

Montrer qu'un polynôme de degré 2 ou 3 est irréductible sur un corps  $\mathbb{K}$  si et seulement s'il n'a pas de racine dans  $\mathbb{K}$ . En est-il de même pour un polynôme de degré 4 ?

**Exercice 1.23**

Soient  $m$  et  $n$  deux entiers naturels non nuls.

1. Déterminer le reste de la division euclidienne de  $P(X) = X^{2m} + (X+1)^n - 1$  par  $X(X+1)$ .

Dans toute la suite, on désigne par  $A(X)$  un polynôme de degré supérieur ou égal à 1 de  $\mathbb{C}[X]$  et on pose  $B(X) = [A(X)]^{2m} + (A(X) + 1)^n - 1$ .

2. Montrer que  $[A(X)]^2 + A(X)$  divise  $B(X)$ .
3. Montrer que, si  $x_0$  est racine de multiplicité 1 de  $A(X)$ , alors  $x_0$  est racine de multiplicité 1 de  $B(X)$ .
4. On suppose que  $A(X) = X^2 + 1$ ,  $m = 1$ , et  $n = 3$ . Donner la décomposition en produit de facteurs irréductibles du polynôme  $B(X)$  dans  $\mathbb{R}[X]$ , puis dans  $\mathbb{C}[X]$ .
5. On suppose que  $A(X) = 1 - X + X^2$ ,  $m = 1$  et  $n = 2$ .  
Donner la décomposition en produit de facteurs irréductibles du polynôme  $B(X)$  dans  $\mathbb{R}[X]$ , puis dans  $\mathbb{C}[X]$ .

**Exercice 1.24**

Soit  $P$  un polynôme à coefficients réels. Montrer que, si  $P(x) \geq 0, \forall x \in \mathbb{R}$ , alors il existe  $A$  et  $B$  dans  $\mathbb{R}[X]$  tels que  $P = A^2 + B^2$ .

On pourra montrer que, si  $A, B, C, D \in \mathbb{R}[X]$ , alors  $(A^2 + B^2)(C^2 + D^2)$  est encore une somme de deux carrés dans  $\mathbb{R}[X]$ .

Décomposer  $X^4 + X^2 + 1$  en une somme de deux carrés dans  $\mathbb{R}[X]$ .

## 1.4 Racines : multiplicité, relations coefficients-racines

**Définition 1.16** Soit  $c \in \mathbb{K}$ ,  $P$  un polynôme non nul de  $\mathbb{K}[X]$ . On dit que  $c$  est racine de multiplicité  $k$  de  $P$  si  $(X - c)^k$  divise  $P$  et  $(X - c)^{k+1}$  ne le divise pas. Autrement dit,  $P = (X - c)^k Q$  avec  $Q(c) \neq 0$ .

Une racine de multiplicité 1 est dite *simple*, et une racine de multiplicité  $> 1$  *multiple*.

**Définition 1.17** Soit  $P = a_0 + a_1 X + \dots + a_n X^n$ . Son polynôme dérivé est par définition  $P' = a_1 + 2a_2 X + \dots + na_n X^{n-1}$ . On note  $P'', \dots, P^{(k)}, \dots$  les polynômes dérivés successifs.

Les règles usuelles de dérivation de somme ou de produit s'appliquent.

Pour les deux résultats suivants, il faut supposer que  $\mathbb{K}$  contient  $\mathbb{Q}$  (par exemple  $\mathbb{K} = \mathbb{Q}, \mathbb{R}$  ou  $\mathbb{C}$ )

**Théorème 1.18** Soit  $P$  un polynôme de  $\mathbb{K}[X]$ , et  $c$  un élément de  $\mathbb{K}$ . Alors les propriétés suivantes sont équivalentes.

1.  $c$  est racine de multiplicité  $k$  de  $P$ .
2.  $P(c) = P'(c) = \dots = P^{(k-1)}(c) = 0$  et  $P^{(k)}(c) \neq 0$ .

En conséquence,  $c$  est racine de multiplicité  $\geq k$  de  $P$  si et seulement si  $P(c) = P'(c) = \dots = P^{(k-1)}(c) = 0$ .

**Théorème 1.19 (Formule de Taylor pour les polynômes)** Soit  $P$  un polynôme de  $\mathbb{K}[X]$  de degré inférieur ou égal à  $d$ , et  $c$  un élément de  $\mathbb{K}$ . Alors

$$P(X) = P(c) + P'(c)(X-c) + \frac{P''(c)}{2}(X-c)^2 + \frac{P^{(3)}(c)}{3!}(X-c)^3 + \dots + \frac{P^{(d)}(c)}{d!}(X-c)^d.$$

Soient  $c_1, \dots, c_p$  des éléments distincts de  $\mathbb{K}$ . Si  $c_i$  est racine de multiplicité  $k_i$  de  $P$ , pour  $i = 0, \dots, p$ , alors  $(X-c_1)^{k_1} \dots (X-c_p)^{k_p}$  divise  $P$ . En conséquence :

**Théorème 1.20** Un polynôme de degré  $n$  de  $\mathbb{K}[X]$  ne peut pas avoir plus de  $n$  racines comptées avec multiplicité dans  $\mathbb{K}$ .

Ce théorème est souvent employé sous la forme suivante : si un polynôme de degré  $\leq n$  a plus de  $n$  racines comptées avec multiplicité, alors c'est le polynôme nul. On en déduit par exemple la partie « unicité » du résultat suivant :

**Théorème 1.21 (Polynôme d'interpolation de Lagrange)** Soient  $c_0, c_1, \dots, c_n$  des éléments distincts de  $\mathbb{K}$ . Soient  $a_0, a_1, \dots, a_n$  des éléments de  $\mathbb{K}$  (pas forcément distincts). Alors il existe un unique polynôme  $P$  de degré inférieur ou égal à  $n$  tel que  $P(c_i) = a_i$  pour  $i = 0, \dots, n$ . Ce polynôme est donné par

$$P(X) = \sum_{i=0}^n \frac{\prod_{j \neq i} (X - c_j)}{\prod_{j \neq i} (c_i - c_j)} a_i.$$

Un polynôme de degré  $n > 0$  est dit *scindé* sur  $\mathbb{K}$  s'il a exactement  $n$  racines comptées avec multiplicité dans  $\mathbb{K}$ . Par exemple, le théorème de d'Alembert-Gauss entraîne que tout polynôme non constant est scindé sur  $\mathbb{C}$ .

**Théorème 1.22** Soit  $P = a_0 + \dots + a_{n-1}X^{n-1} + X^n$  un polynôme unitaire de degré  $n > 0$ , scindé sur  $\mathbb{K}$ . Soit  $c_1, \dots, c_n$  ses racines comptées avec multiplicité (une racine de multiplicité  $k$  figure  $k$  fois). Alors :

$$\begin{aligned} -a_{n-1} &= \sum_{1 \leq i \leq n} c_i \\ a_{n-2} &= \sum_{1 \leq i_1 < i_2 \leq n} c_{i_1} c_{i_2} \\ &\vdots \\ (-1)^k a_{n-k} &= \sum_{1 \leq i_1 < \dots < i_k \leq n} c_{i_1} c_{i_2} \dots c_{i_k} \\ &\vdots \\ (-1)^n a_0 &= c_1 c_2 \dots c_n. \end{aligned}$$

Autrement dit,  $(-1)^k a_{n-k}$  est la somme des produits  $k$  à  $k$  des racines. En particulier,  $a_{n-1}$  est l'opposé de la somme des racines et  $(-1)^n a_0$  est le produit des racines.

### Exercice 1.25

Soit  $P$  le polynôme de  $\mathbb{C}[X]$  donné par  $P(X) = 2X^3 + X^2 + X - 1$ .

1. Montrer que, si  $P$  admet une racine rationnelle écrite sous forme irréductible  $p/q$ , alors  $p$  divise 1 et  $q$  divise 2.
2. En déduire toutes les racines rationnelles de  $P$ .
3. Trouver toutes les racines de  $P$ .

1.4. RACINES : MULTIPLICITÉ, RELATIONS COEFFICIENTS-RACINES 11

**Exercice 1.26**

Soit  $m, n$  et  $p$  trois entiers naturels. Montrer que  $X^2 + X + 1$  divise  $X^{3m} + X^{3n+1} + X^{3p+2}$ . Factoriser  $X^8 + X^4 + X^3$ . (On ne demande pas une décomposition en facteurs irréductibles).

**Exercice 1.27**

On considère le polynôme  $P(X) = X^5 - 5X^4 + 7X^3 - 2X^2 + 4X - 8$ . Quelle est la multiplicité de 2 en tant que racine de  $P$  ?

**Exercice 1.28**

Trouver  $(a, b)$  pour que  $(X - 1)^2$  divise  $aX^4 + bX^3 + 1$ . Généraliser à  $aX^{n+1} + bX^n + 1$ .

**Exercice 1.29**

Trouver  $P(X)$  dans  $\mathbb{K}[X]$  tel que  $(X - 1)^3$  divise  $P(X) + 1$  et  $(X + 1)^3$  divise  $P(X) - 1$

1. en utilisant le polynôme dérivé  $P'$ .
2. en utilisant l'identité de Bezout.

**Exercice 1.30**

Trouver un polynôme  $P$  de  $\mathbb{R}[X]$  de degré inférieur ou égal à 4 tel que

$$\begin{aligned} X^3 & \text{ divise } P(X) + 1, \\ (X - 1)^2 & \text{ divise } P(X). \end{aligned}$$

Donner la décomposition en produits de facteurs irréductibles du polynôme  $P$  dans  $\mathbb{C}[X]$ .

**Exercice 1.31**

On considère le polynôme  $P(X) = X^6 - 6X^5 + 15X^4 - 20X^3 + 12X^2 - 4$  et on note  $P'$  son polynôme dérivé.

1. Déterminer le pgcd unitaire de  $P$  et  $P'$ .
2. Donner la décomposition en facteurs irréductibles de  $P$  dans  $\mathbb{R}[X]$  et dans  $\mathbb{C}[X]$ .

**Exercice 1.32**

On considère le polynôme  $P(X) = X^4 - 2X^3 + 3X^2 - 2X + 1$  et on note  $P'$  son polynôme dérivé.

1. Calculer  $D = \text{pgcd}(P, P')$ .  
Trouver deux polynômes  $U$  et  $V$  tels que  $D = UP + VP'$ .
2. En déduire les racines doubles de  $P$  dans  $\mathbb{C}[X]$  et ses décompositions en produits de facteurs irréductibles dans  $\mathbb{R}[X]$  et  $\mathbb{C}[X]$ .

**Exercice 1.33**

Soit  $A(X) = X^6 + aX^4 + bX^3 + c$  un polynôme de  $\mathbb{C}[X]$ .

1. Déterminer  $a$ ,  $b$  et  $c$  pour que 1 soit racine double de  $A$  et que  $j$  soit racine de  $A$ .
2. Montrer alors que  $A \in \mathbb{R}[X]$  et que  $j$  est racine double.
3. Décomposer  $A$  en produits de facteurs irréductibles dans  $\mathbb{C}[X]$  et  $\mathbb{R}[X]$ .

**Exercice 1.34**

Soit  $P(X) = 2X^3 - X^2 - 7X + a$ .

Déterminer  $a$  pour que  $P$  ait deux racines de somme 1.

**Exercice 1.35**

Soit  $P(X) = X^5 + 5X^4 + 9X^3 + 11X^2 + 7X + 3$ .

1. Calculer  $P(j)$  et  $P'(j)$ . En déduire que  $P$  admet une unique racine réelle négative. Calculer cette racine en utilisant un coefficient du polynôme. Vérifier le résultat à l'aide d'un autre coefficient.
2. Donner la décomposition de  $P$  en facteurs irréductibles sur  $\mathbb{R}[X]$ .
3. Quel est le pgcd de  $P$  et  $P'$  ?

**Exercice 1.36**

Résoudre, dans  $\mathbb{C}^3$ , les systèmes symétriques suivants

$$1) \begin{cases} x + y + z = 0 \\ xy + xz + yz = -13 \\ xyz = -12 \end{cases}, \quad 2) \begin{cases} x + y + z = -2 \\ x^2 + y^2 + z^2 = 0 \\ x^3 + y^3 + z^3 = 1 \end{cases}.$$

**Exercice 1.37**

Trouver un polynôme de degré trois dont les racines sont les carrés des racines du polynôme  $X^3 + X^2 - 2X - 1$ .