Chapitre 14

Polynômes

14.1 Définitions

Dans ce chapitre, $(\mathbb{K}, +, \times)$ désigne un corps commutatif (pour nous ce sera $\mathbb{R}$ ou $\mathbb{C}$).

Définition 14.1 : **Polynôme**
Un polynôme à coefficients dans $\mathbb{K}$ est suite $(a_0,a_1,\dots,a_n,0,\dots)$ d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang. On définit les opérations suivantes sur les polynômes. Soit $P = (a_0,a_1,\dots,a_n,\dots)$ et $Q = (b_0,b_1,\dots,b_n,\dots)$ deux polynômes. On pose :

$$P + Q = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, \dots)$$

$$\lambda.P = (\lambda a_0, \lambda a_1, \dots, \lambda a_n, \dots)$$

$$P \times Q = (c_0, c_1, \dots, c_n, \dots)$$

où les coefficients c_n du produit sont définis par la formule

$$\forall n \in \mathbb{N}, \quad c_n = \sum_{k=0}^{n} a_k b_{n-k}$$

On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$.

Théorème 14.1 : **L'algèbre des polynômes**
$\big(\mathbb{K}[X], +, \times, \cdot\big)$ est une $\mathbb{K}$-algèbre. Le vecteur nul est le polynôme $0 = (0,0,\dots)$ et l'élément neutre pour $\times$ est le polynôme
$1 = (1,0,\dots)$.

Remarque 143. En particulier, $(\mathbb{K}[X], +, \times)$ est un anneau commutatif, dans lequel on dispose de la formule du binôme. On sait également que $\big(\mathbb{K}[X], +, \cdot\big)$ est un $\mathbb{K}$-ev.

Notation définitive

Un polynôme $P = (a_0,a_1,\dots,a_n,0,\dots)$ s'écrira par la suite : $P = a_0 + a_1X + \cdots + a_nX^n$. On identifiera un scalaire $\lambda \in K$ avec le polynôme constant $P(X) = (\lambda,0,\dots) = \lambda$.

Définition 14.2 : **Degré, terme dominant**
Soit un polynôme $P = a_0 + a_1X + \cdots + a_nX^n$ avec $a_n \neq 0$.
- On appelle *degré* du polynôme P, l'entier n noté $\deg P$;
- Par convention, le degré du polynôme nul vaut $-\infty$;
- on appelle *terme dominant* de P, le monôme a_nX^n ;
- lorsque $a_n = 1$, on dit que le polynôme P est *normalisé* ou *unitaire*.

Théorème 14.2 : **Degré d'un produit, d'une somme**

1. $\deg\big(P + Q\big) \leq \max\big(\deg P, \deg Q\big)$
2. $\deg\big(PQ\big) = \deg P + \deg Q$

Remarque 144. La somme de polynômes de degré n peut être un polynôme de degré strictement inférieur à n si les termes dominants s'annulent. Lorsque $\deg P \neq \deg Q$, on a toujours $\deg(P + Q) = \max(\deg P, \deg Q)$. Si

l'on a k polynômes $(P_1,\dots,P_k)$ tous de degré n, pour montrer que la combinaison linéaire $Q=\sum_{i=1}^{k}\lambda_i P_i$ est de degré n, on utilise le théorème précédent pour justifier que $\deg Q \leq n$ et on calcule le coefficient de X^n du polynôme Q, en justifiant qu'il est non nul.

THÉORÈME 14.3 : **L'anneau des polynômes est intègre**
Soient trois polynômes $(P,Q,R)\in\mathbb{K}[X]^3$.

1. si $PQ=0$, alors $P=0$ ou $Q=0$;
2. si $PQ=PR$, et si $P\neq 0$, alors $Q=R$.

THÉORÈME 14.4 : **Polynômes inversibles**
Les éléments inversibles de l'anneau $\mathbb{K}[X]$ sont les polynômes constants non-nuls.

THÉORÈME 14.5 : **Espace des polynômes de degré inférieur à n**
On note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n. Cet ensemble est un sous-espace vectoriel de $\mathbb{K}[X]$. Le système $\left(1,X,X^2,\dots,X^n\right)$ forme une base de $\mathbb{K}_n[X]$ appelée *base canonique* de $\mathbb{K}_n[X]$.

THÉORÈME 14.6 : **Polynômes de degrés étagés**
On considère un système $S=(P_1,\dots,P_n)$ de polynômes non-nuls de degrés tous distincts. Alors S est un système libre de $\mathbb{K}[X]$.

Exercice 14-1
Soit $n\geq 1$ et pour $k\in[0,n]$, $P_k=X^k(1-X)^{n-k}$. Montrer que le système $\left(P_0,\dots,P_n\right)$ est libre dans $\mathbb{K}_n[X]$.

DÉFINITION 14.3 : **Composition des polynômes**
Si $P(X)=\sum_{k=0}^{n}a_kX^k$ et $Q\in\mathbb{K}[X]$ on définit le polynôme composé par la formule suivante :

$$P\circ Q=\sum_{k=0}^{n}a_kQ^k$$

Remarque 145. On a $\deg(P\circ Q)=\deg P\times\deg Q$.

Exercice 14-2
Soit un polynôme $P\in\mathbb{R}[X]$ tel que $P=P\circ(-X)$. Montrer qu'il existe un polynôme $Q\in\mathbb{R}[X]$ tel que $P=Q\circ(X^2)$.

Exercice 14-3
On considère le polynôme de $\mathbb{C}[X]$ défini par

$$P=(1+\lambda X)(1+\lambda^2X)\dots(1+\lambda^nX)$$

où $\lambda\in\mathbb{C}$, vérifie $|\lambda|\neq 1$. Déterminer les coefficients du polynôme P.

Exercice 14-4
Déterminer les polynômes $P\in\mathbb{R}[X]$ vérifiant $P\circ P=P$.

14.2 Arithmétique des polynômes

THÉORÈME 14.7 : **Division euclidienne**
Soient A,B deux polynômes de $\mathbb{K}[X]$ tels que $B\neq 0$. Alors il existe un unique couple (Q,R) de polynômes vérifiant :

1. $A=BQ+R$
2. $\deg R<\deg B$

Exercice 14-5
Soit $A=X^7-2X+1$ et $B=X^2+1$ deux polynômes à coefficients réels. Effectuer la division euclidienne de A par B.

Exercice 14-6

On dit qu'une partie $\mathcal{I}$ de $\mathbb{K}[X]$ est un *idéal* de l'anneau $(\mathbb{K}[X], +, \times)$ lorsque :

- $\mathcal{I}$ est un sous-groupe du groupe $(\mathbb{K}[X],+)$;
- $\mathcal{I}$ est *absorbant* : $\forall A \in \mathcal{I}$, $\forall P \in \mathbb{K}[X]$, $A \times P \in \mathcal{I}$.

Montrer que tout idéal de l'anneau $(\mathbb{K}[X], +, \times)$ est engendré par un polynôme : $\exists P \in \mathbb{K}[X]$ tel que

$$\mathcal{I} = \mathcal{I}(P) = \{Q \times P \ ; \ Q \in \mathbb{K}[X]\}$$

On dit que l'anneau $(\mathbb{K}[X], +, \times)$ est *principal*. Cette notion correspond aux sous-groupes de l'anneau $(\mathbb{Z}, +, \times)$ utilisés en arithmétique dans $\mathbb{Z}$.

DÉFINITION 14.4 : **Divisibilité**
Soient A,B deux polynômes. On dit que A divise B ssi il existe $Q \in \mathbb{K}[X]$ tel que $B = AQ$.

Exercice 14-7

Cette notion a un intérêt pratique important : si un polynôme A divise un polynôme B, cela signifie que l'on peut *mettre en facteur* le polynôme A dans le polynôme B.

THÉORÈME 14.8 : **Polynômes associés**
Soient deux polynômes $(P,Q) \in \mathbb{K}[X]$ non-nuls.

$$(P/Q \text{ et } Q/P) \iff (\exists \lambda \in K \setminus \{0\} \text{ tq } Q = \lambda P)$$

On dit alors que les deux polynômes P et Q sont *associés*.

DÉFINITION 14.5 : **Congruences**
Soit un polynôme $P \in \mathbb{K}[X]$ non-nul. Soient deux polynômes $(A,B) \in \mathbb{K}[X]^2$. On dit que A est *congru* à B modulo P et l'on note

$$A \equiv B \bmod (P)$$

ssi A et B ont même reste dans la division euclidienne par P.

THÉORÈME 14.9 : **Caractérisation des congruences**
Soient un polynôme non-nul $P \in \mathbb{K}[X]$ et deux polynômes $(A,B) \in \mathbb{K}[X]^2$,

$$\big(A \equiv B \bmod (P)\big) \iff \big(P/(B-A)\big)$$

THÉORÈME 14.10 : **Propriétés des congruences**
On suppose que $A \equiv B \bmod (P)$ et $A' \equiv B' \bmod (P)$. Alors :

- $A + A' \equiv B + B' \bmod (P)$.
- $AA' \equiv BB' \bmod (P)$.
- $\forall n \in \mathbb{N}$, $A^n \equiv B^n \bmod (P)$.

Exercice 14-8

Déterminer le reste de la division euclidienne de $A = X^{2000} - X^3 + X$ par $B = X^2 + 1$, puis par $C = X^2 + X + 1$.

Exercice 14-9

Soit un polynôme $P \in \mathbb{K}[X]$. Montrer que $(P - X) \ / \ (P \circ P - X)$.

PROPOSITION 14.11 : **Théorème d'Euclide**
Soient deux polynômes non nuls $(A,B) \in \mathbb{K}[X]$. On effectue la division euclidienne de A par B :

$$\begin{cases} A = BQ + R \\ \deg R < \deg B \end{cases}$$

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

$$\Big(\underset{(i)}{\begin{cases} D/A \\ D/B \end{cases}}\Big) \iff \Big(\underset{(ii)}{\begin{cases} D/B \\ D/R \end{cases}}\Big)$$

Définition 14.6 : **Algorithme d'Euclide, PGCD**
On considère deux polynômes non nuls $(A,B) \in \mathbb{K}[X]^2$. On définit une suite (R_n) de polynômes en posant $R_0 = A$, $R_1 = B$ et $\forall k \geq 1$,

$$R_{k-1} = Q_k R_k + R_{k+1},\ \deg(R_{k+1}) < \deg(R_k)$$

Comme la suite d'entiers $\big(\deg(R_k)\big)$ est strictement décroissante, il existe un entier $n \in \mathbb{N}$ tel que $R_n \neq 0$ et $R_{n+1} = 0$. On note $A \wedge B$ le polynôme R_n normalisé. On dit que le polynôme $\delta = A \wedge B$ est le pgcd des polynômes A et B.

Proposition 14.12 : **Caractérisation du pgcd**
Soient deux polynômes non nuls $(A,B) \in \mathbb{K}[X]^2$ et δ leur pgcd. Alors :

1. $\begin{cases} \delta/A \\ \delta/B \end{cases}$;
2. Si $D \in \mathbb{K}[X]$, $\begin{cases} D/A \\ D/B \end{cases} \Rightarrow D/\delta$.

En d'autres termes, δ est le « plus grand » commun diviseur normalisé des polynômes A et B.

Proposition 14.13 : **Propriété du pgcd**
Soient deux polynômes non nuls $(A,B) \in \mathbb{K}[X]^2$. Alors en notant δ leur pgcd, il existe deux polynômes $(U,V) \in \mathbb{K}[X]^2$ tels que

$$UA + VB = \delta$$

Remarque 146. On trouve en pratique un tel couple de polynômes (U,V) en utilisant l'algorithme d'Euclide et en éliminant les restes successifs. Si l'on veut écrire une procédure calculant ce couple (U,V), on pourra adapter l'algorithme vu pour les entiers.

Exercice 14-10
Déterminer le pgcd des polynômes $A = X^3 + X^2 + 2$ et $B = X^2 + 1$. Trouver ensuite un couple (U,V) tel que $AU + BV = \delta$.

Exercice 14-11
On considère deux entiers non nuls $(a,b) \in \mathbb{N}^{\star 2}$. On note $\delta = a \wedge b$ leur pgcd. Montrer, en utilisant l'algorithme d'Euclide que

$$(X^a - 1) \wedge (X^b - 1) = X^\delta - 1$$

Définition 14.7 : **Polynômes premiers entre eux**
On dit que deux polynômes non nuls A et B sont premiers entre eux lorsque $A \wedge B = 1$.

Théorème 14.14 : **Théorème de Bezout**
Soient deux polynômes non nuls A et B.

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

Théorème 14.15 : **Théorème de Gauss**
Soient trois polynômes non nuls $(A,B,C) \in \mathbb{K}[X]^3$.

$$\begin{cases} A/BC \\ A \wedge B = 1 \end{cases} \Rightarrow A/C$$

Remarque 147. On démontre ensuite de la même façon les théorèmes vus en arithmétique dans $\mathbb{Z}$. En particulier :

1. $(\lambda A) \wedge (\lambda B) = \lambda (A \wedge B)$;
2. $A \wedge (B \wedge C) = (A \wedge B) \wedge C$;
3. $\begin{cases} A \wedge B = 1 \\ A \wedge C = 1 \end{cases} \Rightarrow A \wedge (BC) = 1$;
4. Si $A \wedge B = 1$, alors $\forall (k,p) \in \mathbb{N}^{\star 2}$, $A^p \wedge B^k = 1$;
5. Si $\delta = A \wedge B$, alors on peut écrire $A = \delta A'$, $B = \delta B'$ avec $A' \wedge B' = 1$;

6. $\begin{cases} A/C \\ B/C \\ A \wedge B = 1 \end{cases} \Rightarrow (AB)/C.$

Exercice 14-12

Montrez que si $(a,b) \in \mathbb{K}^2$ sont deux scalaires distincts, alors pour tous entiers $k \geq 1$ et $p \geq 1$, les polynômes $A = (X-a)^k$ et $B = (X-b)^p$ sont premiers entre eux.

DÉFINITION 14.8 : **PPCM**

Soient deux polynômes (A,B) non nuls. Il existe un unique polynôme normalisé $\mu \in \mathbb{K}[X]$ tel que

1. A/μ, B/μ ;
2. $\forall M \in \mathbb{K}[X]$, $\begin{cases} A/M \\ B/M \end{cases} \Rightarrow \mu/M$

On appelle plus grand commun multiple des polynômes (A,B) ce polynôme μ, et on le note

$$\mu \ = \ A \vee B$$

Remarque 148. On montre que $A \vee (B \vee C) = (A \vee B) \vee C$, ce qui permet de définir le ppcm de n polynômes.

THÉORÈME 14.16 : **Relation entre PPCM et PGCD**

Soient deux polynômes non nuls $(A,B) \in \mathbb{K}[X]^2$.

1. Si $A \wedge B = 1$, alors il existe $\lambda \in \mathbb{K}^\star$ tel que $AB = \lambda(A \vee B)$;
2. Il existe $\lambda \in \mathbb{K}^\star$ tel que $AB = \lambda.(A \wedge B) \times (A \vee B)$.

14.3 Fonctions polynômiales. Racines d'un polynôme

DÉFINITION 14.9 : **Fonction polynômiale**

Soit un polynôme $P = a_0 + a_1 X + \cdots + a_n X^n$ de $\mathbb{K}[X]$. On définit à partir des coefficients de P, la *fonction polynômiale* associée :

$$\widetilde{P} : \left\{ \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \mapsto & a_0 + a_1 x + \cdots + a_n x^n \end{array} \right.$$

THÉORÈME 14.17 : **Les lois sur $\mathbb{K}[X]$ correspondent à celles sur $\mathcal{F}(\mathbb{K},\mathbb{K})$**

Soient $(P,Q) \in \mathbb{K}[X]^2$ et $(\lambda,\mu) \in \mathbb{K}^2$. On a les propriétés suivantes :

- $\widetilde{P \times Q} = \widetilde{P} \times \widetilde{Q}$;
- $\widetilde{\lambda P + \mu Q} = \lambda \widetilde{P} + \mu \widetilde{Q}$;
- $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$

Remarque 149. En d'autres termes, l'application

$$\phi : \left\{ \begin{array}{ccc} \big(\mathbb{K}[X], +, \times, \cdot\big) & \longrightarrow & \big(\mathcal{F}(\mathbb{K},\mathbb{K}), +, \times, \cdot\big) \\ P & \mapsto & \widetilde{P} \end{array} \right.$$

est un morphisme d'algèbres.

DÉFINITION 14.10 : **Racine d'un polynôme**

Soit un polynôme $P \in \mathbb{K}[X]$. On dit qu'un scalaire $\alpha \in \mathbb{K}$ est une *racine* de P lorsque $\widetilde{P}(\alpha) = 0$.

Exercice 14-13

Trouver un algorithme qui permet de trouver toutes les racines rationnelles d'un polynôme à coefficients rationnels. Appliquer cet algorithme pour trouver toutes les racines rationnelles du polynôme $P = 3X^3 - X + 1$.

THÉORÈME 14.18 : **Factorisation d'une racine**

Soit un polynôme $P \in \mathbb{K}[X]$ et un scalaire $\alpha \in \mathbb{K}$. Alors le scalaire α est racine du polynôme P si et seulement si l'on peut mettre en facteur le polynôme $(X-\alpha)$ dans le polynôme P :

$$\Big(\widetilde{P}(\alpha) = 0\Big) \Longleftrightarrow \Big((X-\alpha)/P\Big)$$

THÉORÈME 14.19 : **Un polynôme non nul de degré inférieur à n admet au plus n racines**
Soit un polynôme $P \in \mathbb{K}_n[X]$. Si le polynôme P admet au moins $(n+1)$ racines distinctes, alors il est nul.

Remarque 150. Ce théorème est très utilisé pour montrer des unicités.

Exercice 14-14
Soient deux polynômes $(P,Q) \in \mathbb{R}_2[X]^2$. Si $\widetilde{P}(0) = \widetilde{Q}(0), \widetilde{P}(1) = \widetilde{Q}(1)$ et $\widetilde{P}(2) = \widetilde{Q}(2)$, montrer que $P = Q$.

Exercice 14-15
Trouver les fonctions polynômiales à coefficients réels qui sont périodiques.

THÉORÈME 14.20 : **Relation entre polynômes et fonctions polynômes**
Si le corps $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$, alors pour tout polynôme $P \in \mathbb{K}[X]$, $\Big(\widetilde{P} = 0\Big) \iff \Big(P = 0\Big)$.

Remarque 151. C'est ce théorème qui permet de confondre un polynôme et sa fonction polynômiale associée. Lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, l'application

$$\Phi : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathcal{F}(K,K) \\ P & \mapsto & \widetilde{P} \end{array} \right.$$

est un morphisme d'algèbres injectif.

Exercice 14-16
Soit le polynôme $P(X) = X^{2n} + X^n + 1 \in \mathbb{C}[X]$. Trouver une CNS pour que le polynôme P soit divisible par le polynôme $X^2 + X + 1$.

Algorithme de Hörner

En Maple, un polynôme A est représenté par la liste de ses coefficients :

$$a = [a_1, \ldots, a_n] \quad A = a_1 + a_2 X + \cdots + a_n X^{n-1}$$

Si $x \in \mathbb{K}$, l'idée de l'algorithme d'Hörner est d'écrire :

$$\widetilde{A}(x) = \Big(\cdots \big(a_n * x + a_{n-1}\big) * x + \cdots \Big) * x + a_1$$

1. **Arguments :** a (liste) x (scalaire)
2. **Variables :** *valeur* (scalaire), n (entier)
3. **Initialisation :**
   - $n \leftarrow$ longueur(l)
   - $valeur \leftarrow a[n]$
4. **Corps :** Pour i de 1 à $n-1$ faire :
   - $valeur \leftarrow valeur * x + a[n-i]$
5. **Fin :** retourner *valeur*.

On montre par récurrence qu'après le ième passage dans la boucle for, la variable *valeur* contient

$$valeur_i = a_n x^i + a_{n-1} x^{i-1} + \cdots + a_{n-i}$$

Après le dernier passage, *valeur* contient donc $\widetilde{A}(x)$. Cet algorithme nécessite $n-1$ multiplications, lorsque $\deg A = n-1$.

14.4 Dérivation, formule de Taylor

DÉFINITION 14.11 : **Dérivée des polynômes**
Soit un polynôme $P = a_0 + a_1 X + \cdots + a_p X^p$. On définit le *polynôme dérivé* de P par

$$P' = a_1 + 2a_2 X + \cdots + p a_p X^{p-1}$$

On définit ensuite par récurrence, les polynômes $P'', \ldots, P^{(k)}$.

Remarque 152. La définition précédente est purement algébrique. Elle correspond à la dérivée des fonctions polynômes lorsque le corps $\mathbb{K}$ vaut $\mathbb{R}$. Si $P = (p_n)$, alors $P' = \big((n+1)p_{n+1}\big)$.

THÉORÈME 14.21 : **Dérivée d'un produit de polynômes**
L'application

$$D : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ P & \mapsto & P' \end{array} \right.$$

est linéaire et vérifie

$$(PQ)' = P'Q + PQ'$$

Remarque 153.

- $\deg(P') = \begin{cases} -\infty & \text{si } \deg(P) \leq 0 \\ \deg(P) - 1 & \text{si } \deg(P) \geq 1 \end{cases}$.
- $\mathrm{Ker}(D) = \mathbb{K}_0[X]$, $\mathrm{Im}(D) = \mathbb{K}[X]$, donc l'endomorphisme D est surjectif mais pas injectif.
- $\mathrm{Ker}(D^n) = \mathbb{K}_{n-1}[X]$.

THÉORÈME 14.22 : **Formule de Leibniz**
Soient deux polynômes $(P,Q) \in \mathbb{K}[X]^2$. On a la formule suivante pour la dérivée du polynôme produit :

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

Remarque 154. Si l'on considère un polynôme P, on peut exprimer ses coefficients à l'aide des dérivées de la fonction polynômiale en 0 :

$$\begin{aligned} P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \quad & P(0) = a_0 \\ P' = a_1 + 2a_2 X^2 + \cdots + n a_n X^{n-1} \quad & P'(0) = a_1 \\ P'' = 2a_2 + 2 \times 3X + \cdots + n(n-1) a_n X^{n-2} \quad & P''(0) = 2a_2 \\ \vdots & \\ P^{(k)} = k! a_k + \cdots + n(n-1)\ldots(n-k+1) a_n X^{n-k} \quad & P^{(k)}(0) = k! a_k \\ \vdots & \\ P^{(n)} = n! a_n \quad & P^{(n)}(0) = n! a_n \end{aligned}$$

Par conséquent, $\forall k \in [\![0,n]\!]$, $a_k = \dfrac{P^{(k)}(0)}{k!}$. Donc on peut écrire

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

La formule de Taylor est une généralisation de cette idée.

LEMME 14.23 : **Dérivées de** $(X-a)^n$
Soit $a \in \mathbb{K}$. On exprime pour $k \in \mathbb{N}$, la dérivée $k$ième du polynôme $(X-a)^n$:

$$\left[(X-a)^n\right]^{(k)} = \begin{cases} 0_{\mathbb{K}[X]} & \text{si } k > n \\ n! & \text{si } k = n \\ n(n-1)\ldots(n-k+1)(X-a)^{n-k} & \text{si } k < n \end{cases}$$

THÉORÈME 14.24 : **Formule de Taylor**
Soit un polynôme $P \in \mathbb{K}[X]$ de degré n et un scalaire $a \in \mathbb{K}$. On obtient la décomposition du polynôme P sur la base $\mathcal{B} = \left(1, \frac{(X-a)}{1!}, \ldots, \frac{(X-a)^n}{n!}\right)$:

$$\boxed{P(X) = P(a) + P'(a)(X-a) + \cdots + P^{(n)}(a)\frac{(X-a)^n}{n!}}$$

THÉORÈME 14.25 : **Deuxième formule de Taylor**
Lorsque le corps $\mathbb{K}$ vaut $\mathbb{R}$ ou $\mathbb{C}$ (corps infini), pour tout scalaire $a \in \mathbb{K}$ et tout polynôme P de degré n, on a la décomposition du polynôme $P \circ (X - a)$ sur la base canonique :

$$P(X + a) = P(a) + P'(a)X + \cdots + \frac{P^{(n)}(a)}{n!}X^n$$

THÉORÈME 14.26 : **Troisième formule de Taylor**
Soit un polynome $P \in \mathbb{K}[X]$ ($\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$), avec $n = \deg(P)$. Soit $a \in \mathbb{K}$. On a la formule de Taylor

$$P(X + a) = P + aP' + \frac{a^2}{2!}P'' + \cdots + \frac{a^n}{n!}P^{(n)}$$

DÉFINITION 14.12 : **Ordre de multiplicité d'une racine**
Soit un scalaire $\alpha \in \mathbb{K}$. On dit que α est *racine d'ordre k exactement* de P ssi $(X - \alpha)^k$ divise P et $(X - \alpha)^{k+1}$ ne divise pas P.

Remarque 155. Cela signifie que l'on peut mettre en facteur le polynôme $(X-\alpha)^k$ dans P, mais pas le polynôme $(X - \alpha)^{k+1}$. On dit que α est racine d'ordre au moins k lorsque $(X - \alpha)^k$ divise P.

THÉORÈME 14.27 : **Caractérisation des racines multiples**
Soit un polynôme $P \in \mathbb{K}[X]$ et un scalaire $\alpha \in \mathbb{K}$. On peut voir si α est une racine multiple de P en calculant les valeurs $P(\alpha)$, $P'(\alpha)$ ... :

- Le scalaire α est racine de P d'ordre k au moins si et seulement si
  1. $P(\alpha) = P'(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0_{\mathbb{K}}$.
- le scalaire α est racine de P d'ordre k exactement si et seulement si :
  1. $P(\alpha) = P'(\alpha) = \ldots = P^{(k-1)}(\alpha) = 0$;
  2. $P^{(k)}(\alpha) \neq 0$.

Remarque 156. Retenons qu'une formule de Taylor permet d'obtenir le reste et le quotient de la division d'un polynôme P par $(X - a)^k$.

Exercice 14-17
Trouver le reste de la division du polynôme $P = X^n + 1$ ($n \geq 2$) par le polynôme $(X - 1)^3$.

Exercice 14-18
On considère le polynôme $P(X) = (X + 1)^n - X^n - 1 \in \mathbb{C}[X]$ où l'entier n est strictement positif. Trouver une CNS sur n pour que P admette une racine multiple.

Exercice 14-19
Montrer qu'un polynôme $P \in \mathbb{C}[X]$ admet une racine multiple si et seulement si les polynômes P et P' ne sont pas premiers entre eux. Trouver une condition nécessaire et suffisante sur $\lambda \in \mathbb{C}$ pour que le polynôme $P = X^7 - X + \lambda$ admette une racine multiple.

14.5 Relations coefficients-racines pour les polynômes scindés

DÉFINITION 14.13 : **Polynôme scindé**
Soit $P \in \mathbb{K}[X]$, on dit que P est scindé si P s'écrit

$$P = a_p \prod_{i=0}^{p} (X - \alpha_i)$$

où les scalaires α_i sont les racines de P comptées avec leur ordre de multiplicité et a_p est le coefficient dominant du polynôme P.

La principale différence entre les corps $\mathbb{R}$ et $\mathbb{C}$ concernant les polynômes provient du théorème suivant :

THÉORÈME 14.28 : **Théorème de d'Alembert**
Soit un polynôme $P \in \mathbb{C}[X]$ tel que $\deg P \geq 1$. Alors P possède au moins une racine complexe $\alpha \in \mathbb{C}$.

Remarque 157. On en déduit que tout polynôme de $\mathbb{C}[X]$ est scindé. Ce résultat est faux pour $\mathbb{R}[X]$ comme le montre l'exemple $P(X) = X^2 + 1$.

Exercice 14-20

Soit un polynôme $P \in \mathbb{R}[X]$. Montrer que si P est scindé, alors P' est également scindé dans $\mathbb{R}[X]$.

Remarque 158. Le résultat précédent est faux dans un corps quelconque. Par exemple, $P(X) = X^3 - X = X(X-1)(X+1) \in \mathbb{Q}[X]$ est scindé dans $\mathbb{Q}[X]$, mais $P'(X) = 3X^2 - 1$ n'est pas scindé dans $\mathbb{Q}[X]$, car les racines de P' sont $1/\sqrt{3}$ et $-1/\sqrt{3}$ qui ne sont pas rationnels.

Relations entre coefficients et racines d'un polynôme scindé

Remarque 159. Commençons par un exemple simple avec un polynôme de degré 2, $P(x) = \lambda(X-\alpha_1)(X-\alpha_2) = a_2X^2 + a_1X + a_0$. En développant et en identifiant les coefficients, on trouve que

$$\alpha_1 + \alpha_2 = -\frac{a_1}{a_2} \text{ et } \alpha_1\alpha_2 = \frac{a_0}{a_2}$$

DÉFINITION 14.14 : **Fonctions symétriques élémentaires des racines**

Considérons maintenant un polynôme scindé $P \in \mathbb{K}[X]$ de degré p, s'écrivant

$$P = a_pX^p + a_{p-1}X^{p-1} + \cdots + a_0$$

Notons $\alpha_1,\alpha_2,\ldots,\alpha_p$ ses racines. On définit les *fonctions symétriques élémentaires des racines* :

$$\begin{aligned}
\sigma_1 &= \alpha_1 + \cdots + \alpha_p \\
\sigma_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{p-1}\alpha_p \\
&\cdots \\
\sigma_k &= \sum_{1\le i_1<\cdots<i_k\le p} a_{i_1}\ldots a_{i_k} \\
&\cdots \\
\sigma_n &= \alpha_1\ldots\alpha_p
\end{aligned}$$

THÉORÈME 14.29 : **Relations coefficients-racines**

Les formules suivantes relient les coefficients d'un polynôme scindé avec ses racines :

$$\forall k \in [1,n], \quad \boxed{\sigma_k = (-1)^k \frac{a_{p-k}}{a_p}}$$

Remarque 160. Un célèbre résultat de Galois dit qu'il n'existe pas d'algorithme qui permet d'exprimer les racines d'un polynôme quelconque à coefficients réels de degré supérieur à 5 à partir des coefficients du polynôme. C'est la principale limitation sur les calculs des polynômes et fractions rationnelles en calcul formel.

Par contre, on montre que toute expression polynômiale en les racines d'un polynôme qui est invariante par permutations peut s'exprimer à l'aide des fonctions symétriques élémentaires, c'est à dire à l'aide des coefficients du polynôme. Par exemple, la somme et le produit des racines s'expriment facilement sans calculer explicitement celles-ci. De même, si $(\alpha_1,\ldots,\alpha_n)$ sont les racines d'un polynôme de degré n, on peut exprimer les quantités

$$S_k = \alpha_1^k + \cdots \alpha_n^k \quad (k \in \mathbb{N})$$

à l'aide des coefficients du polynôme P.

Exercice 14-21

Trouver $(a,b,c) \in \mathbb{C}^3$ tels que

$$a + b + c = 1, \quad a^2 + b^2 + c^2 = 3 \quad a^3 + b^3 + c^3 = 1$$

14.6 Décomposition d'un polynôme en facteurs irréductibles

DÉFINITION 14.15 : **Polynômes irréductibles**

Soit $P \in \mathbb{K}[X]$, un polynôme non constant. On dit que P est *irréductible* ssi $P = QH$ implique $Q \in \mathbb{K}$ ou $H \in \mathbb{K}$.

Remarque 161. Cette notion correspond aux nombres premiers en arithmétique des entiers.

THÉORÈME 14.30 : **Les polynômes de degré 1 sont irréductibles**
Quel que soit le corps $\mathbb{K}$, pour tout scalaire $\alpha \in \mathbb{K}$, le polynôme $P = X - \alpha$ est irréductible dans $\mathbb{K}[X]$.

THÉORÈME 14.31 : **Décomposition d'un polynôme en facteurs irréductibles**
Soit un polynôme $P \in \mathbb{K}[X]$. Alors P s'écrit de façon unique à l'ordre près comme produit de polynômes irréductibles normalisés dans $\mathbb{K}[X]$:

$$P = \lambda P_1 \times \cdots \times P_n \text{ où } \lambda \in \mathbb{K}^\star$$

THÉORÈME 14.32 : **Décomposition dans $\mathbb{C}[X]$**

1. Dans $\mathbb{C}[X]$, les polynômes irréductibles unitaires sont les polynômes de degré 1 : $X - \alpha$, $(\alpha \in \mathbb{C})$;
2. Tout polynôme de $\mathbb{C}[X]$ s'écrit de façon unique (à l'ordre près) sous la forme :

$$P(X) = \lambda(X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_n)$$

(les complexes α_i ne sont pas forcément distincts).

THÉORÈME 14.33 : **Décomposition dans $\mathbb{R}[X]$**

1. Dans $\mathbb{R}[X]$, les polynômes irréductibles normalisés sont :
   (a) Les polynômes de degré 1 de la forme $(X - \alpha)$ $(\alpha \in \mathbb{R})$;
   (b) Les polynômes de degré 2 à discriminant strictement négatif de la forme $X^2 + pX + q$, avec $(p^2 - 4q < 0)$.
2. Tout polynôme de $\mathbb{R}[X]$ s'écrit de façon unique (à l'ordre près) sous la forme :

$$P(X) = \lambda(X - \alpha_1)\dots(X - \alpha_p)(X^2 + p_1X + q_1)\dots(X^2 + p_rX + q_r)$$

où tous les facteurs sont irréductibles normalisés et $\lambda \in \mathbb{R}$.

Remarque 162. D'après le théorème précédent, un polynôme bicarré $X^4 + pX^2 + q$ n'est pas irréductible dans $\mathbb{R}[X]$. Pour obtenir sa factorisation lorsque $p^2 - 4q < 0$, regrouper le terme en X^4 et le terme constant, faire apparaître un début de carré, puis utiliser l'identité $A^2 - B^2 = (A - B)(A + B)$.

Exercice 14-22
On considère les polynômes $P(X) = X^{2n} - 1$ et $Q(X) = X^{2n+1} - 1$. Factoriser P et Q dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.