Les Polynômes

MPSI-1 Prytanée National Militaire

Pascal Delahaye - D'après le cours d'Alain Soyeur

14 février 2011

1 Définitions

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

Définition 1 : On appelle polynôme à coefficient dans $\mathbb{K}$ tout élément de la forme :

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \quad \text{où} \quad \begin{cases} n \in \mathbb{N} \\ (a_0, a_1, \ldots, a_n) \in \mathbb{K}^n \end{cases}$$

1. X est appelée l'*indéterminée*.
2. L'ensemble des polynômes à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$.

Remarque 1.

1. En fait, un polynôme est défini comme une suite presque nulle d'éléments de $\mathbb{K}$, mais cette définition officielle n'est pas au programme.
   X représente la suite de termes successifs : 0, 1, 0, 0, ... Il ne s'agit donc pas d'une variable à laquelle à pourra donner des valeurs.
2. Par définition, l'écriture d'un polynôme sous la forme $P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ est unique.
   Ainsi, on aura : $P = 0 \iff \forall k \in \mathbb{N},\ a_k = 0$.

Théorème Fondamental 1 : **L'algèbre des polynômes**
On munit l'ensemble $\mathbb{K}[X]$ de l'addition, de la multiplication et la lce "usuelles".

$$\text{Ainsi,} \quad \begin{cases} \big(\mathbb{K}[X], +, \cdot\big) \text{ est un } \mathbb{K}\text{-ev} \\ \big(\mathbb{K}[X], +, \times\big) \text{ est un anneau commutatif} \end{cases}$$

Comme d'autre part, on a $\lambda(P \times Q) = (\lambda P) \times Q = P \times (\lambda Q)$ alors $\big(\mathbb{K}[X],\ +,\ \times,\ \cdot\big)$ est une $\mathbb{K}$-algèbre associative et unitaire.
Le vecteur nul est le polynôme $P = 0$ et l'élément neutre pour $\times$ est le polynôme $P = 1$.

Preuve 1 : On doit vérifier une à une toutes les propriétés d'un espace vectoriel et d'un anneau commutatif ...

Remarque 2. Ce théorème donne en particulier la stabilité de l'ensemble $\mathbb{K}[X]$ par les opérations usuelles $(+, \times, .)$.

Remarque 3. $(\mathbb{K}[X], +, \times)$ étant un anneau commutatif, on pourra utiliser la formule du binôme :

$$\begin{cases} \forall (P, Q) \in \mathbb{K}[X]^2 \\ \forall n \in \mathbb{N} \end{cases}, \quad \text{on a :} \quad (P+Q)^n = \sum_{k=0}^{n} \binom{n}{k} P^k Q^{n-k}$$

Définition 2 : **Degré, valuation, terme dominant**
Soit un polynôme $P = a_0 + a_1X + \cdots + a_nX^n$ avec $a_n \neq 0$.

1. On appelle *degré* du polynôme P, l'entier n noté $\deg P$.
2. On appelle *valuation* du polynôme P, le plus petit entier k tel que $a_k \neq 0$ noté $val(P)$.
3. Par convention, le degré du polynôme nul vaut $-\infty$.
4. On appelle *terme dominant* de P, le monôme a_nX^n.
5. Lorsque $a_n = 1$, on dit que le polynôme P est *normalisé* ou *unitaire*.

Théorème 2 : **Degré d'un produit, d'une somme**

1. $\deg(P+Q) \leq \max(\deg P,\ \deg Q)$
2. $\deg(PQ) = \deg P + \deg Q$ Ces formules sont valables même si P et/ou Q est nul.

Preuve 2 :
On écrit P et Q sous leur forme générale et on s'intéresse aux termes dominants de $P+Q$ et de PQ.

Remarque 4.

1. La somme de polynômes de degré n peut être un polynôme de degré strictement inférieur à n si les termes dominants s'annulent.
2. Lorsque $\deg P \neq \deg Q$, on a toujours $\deg(P+Q) = \max(\deg P,\ \deg Q)$.
3. Si l'on a k polynômes $(P_1,\ \ldots,\ P_k)$ tous de degré n, pour montrer que la combinaison linéaire $Q = \sum_{i=1}^{k} \lambda_i P_i$ est de degré n on pourra :
   (a) utiliser le théorème précédent pour justifier que $\deg Q \leq n$, puis
   (b) calculer le coefficient de X^n du polynôme Q, pour justifier qu'il est non nul.

Remarque 5. Le degré est un outil d'analyse performant dans la recherche de polynômes vérifiant une ou des conditions données (analyse / synthèse).

`Exemple 1.` $(*)$ Déterminer tous les couples de polynômes $(P,\ Q) \in \mathbb{K}[X]^2$ tels que $Q^2 = XP^2$.

Théorème 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 $Q = R$.

Preuve 3 :

1. Par l'absurde en utilisant la fonction degrée
2. Conséquence immédiate du premier résultat

Théorème 4 : **Polynômes inversibles**
Les éléments inversibles de l'anneau $\mathbb{K}[X]$ sont les polynômes constants non-nuls.

Preuve 4 : On utilise de nouveau la fonction degrée.

Théorème Fondamental 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.

1. Cet ensemble est un sous-espace vectoriel de $\mathbb{K}[X]$.
2. Le système $\left(1,\ X,\ X^2,\ \ldots,\ X^n\right)$ forme une base de $\mathbb{K}_n[X]$ appelée *base canonique* de $\mathbb{K}_n[X]$.

Preuve 5 : On a $\mathbb{K}_n[X] = \text{Vect}(1,\ X,\ \ldots,\ X^n)$ et la famille $(1,\ X,\ \ldots,\ X^n)$ est libre.

Théorème 6 : **Polynômes de degrés étagés**
On considère un système $S = (P_1,\ \ldots,\ P_n)$ de polynômes non-nuls de degrés tous distincts.
Alors S est un système libre de $\mathbb{K}[X]$.

Preuve 6 : On peut commencer par ordonner les polynôme P_k en fonction de leur degré.
Soit $P = \sum_{k=0}^{n} \lambda_k.P_k$ une CL nulle des polynômes de S. Soit D_k le terme dominant du polynôme P_k. On montre, en utilisant les termes D_k et la fonction degrée que chacun des λ_k est nul pour k allant de n à 0.

Remarque 6. Ce théorème est très utilisé en pratique pour prouver qu'une famille de polynômes est libre.

`Exemple 2.` (∗) Soit $n \geq 1$ et pour $k \in [\![0,n]\!]$, on définit les polynômes $P_k = (X+1)^{k+1} - X^{k+1}$.
Le théorème précédent permet de montrer que le système $(P_0, \ldots, P_n)$ est libre dans $\mathbb{K}_n[X]$.

Exercice : 1
(∗∗) Soit $n \geq 1$ et pour $k \in [\![0,n]\!]$, on définit les polynômes $P_k = X^k(1-X)^{n-k}$.
Montrer que le système $(P_0, \ldots, P_n)$ est libre dans $\mathbb{K}_n[X]$.

Définition 3 : **Composition des polynômes**
Si $P(X) = \sum_{k=0}^{n} a_k X^k$ et $Q \in \mathbb{K}[X]$.
On définit $P \circ Q$, le polynôme composé par la formule suivante : $P \circ Q = \sum_{k=0}^{n} a_k Q^k$

Remarque 7. Cette loi $\circ$ n'est pas la loi de composition des applications dans la mesure où c'est une loi sur $\mathbb{K}[X]$

Proposition 7 : **Opérations**
Pour tout $\lambda \in \mathbb{K}$, P, Q, $R \in \mathbb{K}[X]$:

Distributivités à droite :
1. $(P + \lambda Q) \circ R = P \circ R + \lambda Q \circ R$
2. $(PQ) \circ R = (P \circ R).(Q \circ R)$
3. $(P \circ Q) \circ R = P \circ (Q \circ R)$
4. $X \circ P = P \circ X = P$

Preuve 7 : On s'en dispensera ...

Remarque 8. La loi $\circ$ n'est pas commutative et n'est pas distributive à gauche dans $\mathbb{K}[X]$. Chercher des C/ex !

Proposition 8 : Soient P et Q deux polynômes non nuls. On a alors :
$$\deg(P \circ Q) = \deg P \times \deg Q$$

Preuve 8 : On remplace P et Q par leur forme explicite.

Remarque 9. ⚠ Pour éviter des erreurs, on prendra soin de s'assurer que les polynômes sur lesquels on travaille sont non nuls avant d'utiliser cette formule sur le degré.

`Exemple 3.` (∗) Déterminer les polynômes $P \in \mathbb{R}[X]$ vérifiant $P \circ P = P$.

Exercice : 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 $P = Q \circ (X^2)$.

2 Arithmétique des polynômes

Théorème Fondamental 9 : **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 : $\begin{cases} A = BQ + R \\ \deg R < \deg B \end{cases}$

Preuve 9 :
On commence par démontrer l'existence de Q et R.

1. On peut commencer par remarquer que si $\deg B > \deg A$ alors $Q = 0$ et $R = A$ conviennent.
2. On fixe B et on procède par récurrence (forte) sur le degré de A.
   (a) Si $\deg A = 0$: facile
   (b) Soit $n \in \mathbb{N}$. Supposons l'existence de Q et R lorsque $\deg A \leq n$. Soit $A \in \mathbb{K}[X]$ de degré $n+1$.
   Notons $a_{n+1}X^{n+1}$ et b_pX^b les termes dominants respectifs de A et B.
   Pour se ramener à un polynôme de degré $\leq n$, on peut considérer le polynôme : $A - \frac{a_{n+1}}{b_p}.X^{n+1-p}B$.
   On applique alors l'hypothèse de récurrence à ce nouveau polynôme.

On démontre enfin l'unicité de cette décomposition.
La méthode est classique et utilise la fonction degré.

PROPOSITION 10 : **Factorisation dans $\mathbb{R}[X]$**

Soient $\begin{cases} A, B \in \mathbb{R}[X] \\ C, D \in \mathbb{C}[X] \end{cases}$ tels que $\begin{cases} A = BC + D \\ \deg D < \deg B \end{cases}$. Alors les polynômes $\begin{cases} C \\ D \end{cases}$ sont à coefficients réels.

Preuve 10 : Remarquons que $A = BC + D$ correspond à la division euclidienne de A par B dans $\mathbb{C}[X]$.
Notons $A = BQ + R$ la division euclidienne de A par B dans $\mathbb{R}[X]$.
Cette décomposition vérifie aussi les conditions de la division euclidienne dans $\mathbb{C}[X]$. D'après l'unicité de la division euclidienne, elle est donc identique à la décomposition $A = BC + D$. Par conséquent, $C = Q$ et $D = R$ et donc $C, D \in \mathbb{R}[X]$.

Remarque 10. Ce résultat s'applique en particulier lorsque $D = 0$.

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

`Exemple 4.` $(*)$ Entraînement !!
Montrer qu'en effectuant la division euclidienne de $A = X^5 + X^4 - X^3 + X - 1$ par $B = X^3 + X^2 + 2$ on obtient $Q = X^2 - 1$ et $R = -X^2 + X + 1$.

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

Remarque 11. On verra une méthode plus efficace dans le paragraphe sur les racines d'un polynôme.

Exercice : 4
$(**)$
Définition
On dit qu'une partie $\mathcal{I}$ de $\mathbb{K}[X]$ est un *idéal* de l'anneau $(\mathbb{K}[X], +, \times)$ lorsque :
1) $\mathcal{I}$ est un sous-groupe du groupe $(\mathbb{K}[X], +)$.
2) $\mathcal{I}$ 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, c'est à dire que :

$$\forall \mathcal{I} \text{ un idéal de } \mathbb{K}[X], \exists P \in \mathbb{K}[X] \text{ tel que } \mathcal{I} = \mathcal{I}(P) = \{Q \times P \ ; \ Q \in \mathbb{K}[X]\}$$

On dit alors que l'anneau $(\mathbb{K}[X], +, \times)$ est *principal*.

Définition 4 : **Divisibilité**
Soient A, B deux polynômes de $\mathbb{K}[X]$ avec $B \neq 0$.
On dit que B divise A ssi il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$. (On pourra écrire B/A)

Remarque 12. Dans ce cas, on dira aussi que A est *multiple* de B ou que l'on peut *mettre en facteur* le polynôme B dans le polynôme A. Lorsque $A \neq 0$, ceci n'est possible que si $\deg B \leq \deg A$.

Exercice : 5
(∗) Déterminer une CNS sur les réels λ et μ pour que X^2+2 divise $X^4+X^3+\lambda.X^2+\mu X+2$.

Exercice : 6
(∗∗) Soit un polynôme $P \in \mathbb{K}[X]$. Montrer que $(P-X)$ / $(P \circ P - X)$.

Théorème 11 : **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.*

Preuve 11 : On montre facilement que si P/Q et Q/P alors $\deg P = \deg Q$.
Comme il existe $R \in \mathbb{K}[X]$ tel que $Q = R.P$ alors on a $\deg R = 0$. CQFD !!

Théorème 12 : **Euclide**
Soient deux polynômes non nuls A et B de $\mathbb{K}[X]$. La division euclidienne donne : $\begin{cases} A = B.Q + R \\ \deg R < \deg B \end{cases}$.

Si $D \in \mathbb{K}[X]$, on a : $D \text{ divise } \begin{cases} A \\ B \end{cases} \iff D \text{ divise } \begin{cases} B \\ R \end{cases}$

Preuve 12 : Pas de difficulté.

Ce théorème permet, comme pour les entiers, de définir la notion de PGCD et de donner un algorithme pour le déterminer.

Algorithme d'Euclide
Soient deux polynômes non nuls A et B de $\mathbb{K}[X]$.
1. En effectuant des divisions euclidiennes successives, on construit une suite (R_k) de polynômes :
   (a) $R_0 = A$
   (b) $R_1 = B$
   (c) R_2 est le reste de la division euclidienne de R_0 par R_1.
   (d) et de façon générale : R_k est le reste de la division euclidienne de R_{k-2} par R_{k-1}.
2. (R_k) est une suite de polynômes de degré strictement décroissant.
   Il existe donc un premier entier n pour lequel $R_n = 0$.
3. Le polynôme R_{n-1} est un diviseur commun à A et B.
4. Or, d'après le théorème d'Euclide, si $D \in \mathbb{K}[X]$ divise A et B, alors D division tous les R_k. Donc les diviseurs communs à A et B sont exactement les diviseurs de R_{n-1}.

Définition 5 : **PGCD et PPCM**
Soient deux polynômes non nuls A et B de $\mathbb{K}[X]$. On appelle :
1. PGCD(A, B) le plus grand diviseur commun unitaire à A et B noté : $A \wedge B$
2. PPCM(A, B) le plus petit multiple commun unitaire à A et B noté : $A \vee B$

Attention : ici, *le plus grand* signifie *de degré maximal* et *le plus petit* signifie *de degré minimal.*

Remarque 13.
1. Le PGCD de deux polynômes est donc le dernier reste non nul normalisé obtenu dans l'algorithme d'Euclide.
2. Les lois $\wedge$ et $\vee$ sont associatives.
   On peut donc définir le PGCD et le PPCM de n polynômes où $n \in \mathbb{N}^*$.
3. Si $A \wedge B = 1$, on dit que les polynômes A et B sont *premiers entre eux.*

`Exemple 5.` (∗) Déterminer le PGCD de $\begin{cases} A(X) = X^3 + 2X^2 - X - 2 \\ B(X) = X^2 + 4X + 3 \end{cases}$ en vous inspirant de l'algorithme d'Euclide.

Exercice : 7

(∗∗) Soit a et b deux entiers naturels non nuls avec $a \geq b$. On note $\delta = a \wedge b$.
Montrer, en utilisant l'algorithme d'Euclide que : $(X^a - 1) \wedge (X^b - 1) = X^\delta - 1$.

THÉORÈME 13 : **Egalité de Bezout**
Soient deux polynômes non nuls A et B de $\mathbb{K}[X]$ et δ leur PGCD. Alors :

Il existe deux polynômes $(U, V) \in \mathbb{K}[X]$ tels que : $AU + BV = \delta$

Preuve 13 : Comme dans $\mathbb{Z}$, on détermine les polynômes U et V grâce à l'algorithme d'Euclide.

On pourra présenter les calculs intermédiaires dans un tableau de la forme :

$R_0 = A$	$R_1 = B$	R_2	...	R_k	...	D
	Q_1	Q_2	...	Q_k	...	
1	0	U_2	...	U_k	...	$U_n = U$
0	1	V_2	...	V_k	...	$V_n = V$

Remarque 14. Le couple de polynôme (U, V) n'est pas unique !

COROLLAIRE 14 : Soient deux polynômes non nuls A et B de $\mathbb{K}[X]$.
Les diviseurs communs à A et B sont les diviseurs de $A \wedge B$.

Preuve 14 : Immédiat d'après l'égalité de Bezout.

`Exemple 6.` (∗) Déterminer une égalité de Bezout pour les polynômes :

1. $\begin{cases} A = X^3 + X^2 + 2 \\ B = X^2 + 1 \end{cases}$ 2. $\begin{cases} A = X^4 + X^3 - 2X + 1 \\ B = X^2 + X + 1 \end{cases}$.

THÉORÈME 15 : **Théorème de Bezout (bis)**
Soient deux polynômes non nuls A et B de $\mathbb{K}[X]$. Alors :

$A \wedge B = 1 \iff$ il existe deux polynômes $(U, V) \in \mathbb{K}[X]$ tels que $AU + BV = 1$

Preuve 15 :
$\Rightarrow$ C'est une conséquence immédiate du théorème de Bezout
$\Leftarrow$ Un diviseur commun à A et B divise 1 ...

THÉORÈME 16 : **Théorème de Gauss**
Soient trois polynômes non nuls A, B et C de $\mathbb{K}[X]$.

Si $\begin{cases} A \text{ divise } BC \\ A \wedge B = 1 \end{cases}$ alors A divise C

Preuve 16 : Application immédiate du théorème de Bezout précédent.

Exercice : 8

(∗∗) Soit A, $B \in \mathbb{K}[X]$ non constants et premiers entre eux.
Montrer qu'il existe un unique couple $(U, V) \in \mathbb{K}[X]^2$ tel que : $\begin{cases} AU + BV = 1 \\ \deg U < \deg B \\ \deg V < \deg A \end{cases}$.

PROPOSITION 17 : **Propriétés diverses**
Soient A, B, $C \in \mathbb{K}[X]$.

1. $(C.A) \wedge (C.B) = C.(A \wedge B)$ (C unitaire)
2. $A \wedge (B \wedge C) = (A \wedge B) \wedge C$
3. $\left\{ \begin{array}{l} A \wedge B = 1 \\ A \wedge C = 1 \end{array} \right. \Rightarrow A \wedge (BC) = 1$
4. $A \wedge B = 1 \Longleftrightarrow A^p \wedge B^q = 1$
5. Si $D = A \wedge B$ alors $\left\{ \begin{array}{l} A = DA' \\ B = DB' \end{array} \right.$ avec $A' \wedge B' = 1$
6. $(A \wedge B)^k = A^k \wedge B^k$
7. Si $\left\{ \begin{array}{l} A \,/\, C \\ B \,/\, C \end{array} \right.$ avec $A \wedge B = 1$ alors AB divise C

Preuve 17 : On pourra procéder par analogie avec les propriétés équivalentes dans $\mathbb{Z}$.

`Exemple 7.` ($*$) Montrer que si a et b sont deux scalaires distincts, alors pour tout entiers :

$$(p,\, q) \in \mathbb{N}^*, \quad (X-a)^p \wedge (X-b)^q = 1$$

Exercice : 9
($*$) Soit $(A,\, B) \in \mathbb{K}[X]$ non constants. Montrer que :

$$A \wedge B = 1 \Longleftrightarrow AB \wedge (A+B) = 1$$

3 Fonctions polynômiales. Racines d'un polynôme

DÉFINITION 6 : **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 :

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

On pourra noter $\mathbb{K}[x]$ l'ensemble des fonctions polynomiales sur $\mathbb{K}$.

DÉFINITION 7 : **Equation Algébrique**
Soit $P \in \mathbb{C}[X]$.
Pour $x \in \mathbb{C}$, l'équation $\widetilde{P}(x) = 0$ est alors appelée *équation algébrique* associée au polynôme P.

THÉORÈME 18 : **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 :

1. $\widetilde{P \times Q} = \widetilde{P} \times \widetilde{Q}$;
2. $\widetilde{\lambda P + \mu Q} = \lambda \widetilde{P} + \mu \widetilde{Q}$;
3. $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$

Preuve 18 : Pas de difficulté ...

DÉFINITION 8 : **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 $\widetilde{P}(\alpha) = 0$.

Remarque 15. Les racines d'un polynôme de $\mathbb{K}[X]$ appartiennent au corps $\mathbb{K}$.

`Exemple 8.` ($*$) Soit $P \in \mathbb{C}[X]$ à coefficients réels et $\alpha \in \mathbb{C}$. Vérifier que : α racine de $P \Longleftrightarrow \bar{\alpha}$ racine de P.

THÉORÈME 19 : **Factorisation par $X - \alpha$**
Soit un polynôme $P \in \mathbb{K}[X]$ et un scalaire $\alpha \in \mathbb{K}$. Alors :

$$\alpha \text{ racine de } P \Longleftrightarrow (X-\alpha) \text{ divise } P$$

Preuve 19 : Dans le cas où $P \neq 0$, on effectue la division euclidienne de P par $(X-\alpha)$, et on exprime l'égalité obtenue en terme de fonctions polynômiales. On remplace alors x par α ...

COROLLAIRE 20 : **Factorisation par $(X-\alpha_1)\dots(X-\alpha_n)$**
Soit un polynôme $P \in \mathbb{K}[X]$, $n \in \mathbb{R}^*$ et $(\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n$. Alors :

$$\alpha_1, \dots, \alpha_n \text{ racines de } P \iff (X-\alpha_1)\dots(X-\alpha_n) \text{ divise } P$$

Preuve 20 : Par récurrence sur n.

`Exemple 9.` $(*)$ Soit un polynôme $P \in \mathbb{C}[X]$ à coefficients réels.

1. Montrer que si i est racine de P alors P peut se factoriser par X^2+1.
2. Montrer que, si j est racine de P alors P peut se factoriser par X^2+X+1.

Exercice : 10

$(*)$ Détermination du reste de la division euclienne d'un polynôme à l'aide des racines.

1. Soit $P \in \mathbb{C}[X]$ et $a \in \mathbb{C}$.
   Déterminer l'expression du reste de la division euclidienne de P par $(X-a)$.

2. Déterminer le reste de la division euclidienne de $A = X^{2000} - X^3 + X$ par $B = X^2+1$ à l'aide des racines.

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

THÉORÈME 21 : **Un polynôme non nul de degré inférieur à n admet au plus n racines distinctes**
Soit un polynôme $P \in \mathbb{K}_n[X]$.
Si le polynôme P admet au moins $(n+1)$ racines distinctes, alors il est nul.

Preuve 21 : C'est un corollaire du théorème précédent.

Remarque 16. Ce théorème est très utilisé pour montrer des unicités.

`Exemple 10.` $(**)$ Les polynômes de Lagrange : $P(x) = \sum_{i=1}^{n} \frac{\prod_{k\neq i}(X-x_k)}{\prod_{k\neq i}(x_i-x_k)}.y_i$ avec $\begin{cases} x_1 < x_2 < \dots < x_n \\ y_1, \dots, y_n \in \mathbb{R} \end{cases}$.

Nous savons que le graphe de la fonction polynômiale $\widetilde{P}$ passe par les n points du plan $M_1(x_1, y_1), \dots, M_n(x_n, y_n)$. Justifier qu'il n'existe pas d'autre fonction polynômiale de degré $n-1$ passant par ces n points.

Exercice : 11

$(**)$ Trouver les fonctions polynômiales périodiques de $\mathcal{F}(\mathbb{R},\mathbb{R})$.

THÉORÈME 22 : **Relation entre polynômes et fonctions polynômiales**
Si le corps $\mathbb{K}$ est infini (comme $\mathbb{R}$ ou $\mathbb{C}$), alors pour tout polynôme $P \in \mathbb{K}[X]$,

$$\left(\widetilde{P} = 0\right) \iff \left(P = 0\right)$$

Preuve 22 : Pas de difficulté en pensant à utiliser le théorème précédent.

`Exemple 11.` $(*)$ Contre-exemple :

Considérer le corps $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$ et trouver un polynôme $P \in \mathbb{K}[X]$ tel que $\begin{cases} P \neq 0 \\ \tilde{P} = 0 \end{cases}$.

THÉORÈME FONDAMENTAL 23 : **Identification d'un polynôme avec sa fonction polynômiale**
Si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, alors :

l'application $\begin{array}{rccc} \Phi : & \mathbb{K}[X] & \longrightarrow & \mathbb{K}[x] \\ & P & \mapsto & \widetilde{P} \end{array}$ est un isomorphisme d'algèbres.

Preuve 23 : Aucune difficulté !

Remarque 17. Ce théorème est très important car il permet de démontrer des propriétés sur les polynômes en utilisant les propriétés connues sur les fonctions polynômiales.
Ainsi, pour prouver que $P = Q$, on pourra prouver que $\varphi(P) = \varphi(Q)$.

Algorithme de Hörner : pour calculer $\widetilde{P}(\alpha)$

Soit le polynôme : $P = a_0 + a_1X + \cdots + a_nX^n$.
Si $\alpha \in \mathbb{K}$, l'idée de l'algorithme d'Hörner est de calculer $\widetilde{P}(\alpha)$ de la façon suivante :

1. a_n
2. $a_n \times \alpha + a_{n-1}$
3. $(a_n \times \alpha + a_{n-1}) \times \alpha + a_{n-2}$
4. ... etc ...

Après la ième itération on obtient $a_n\alpha^i + a_{n-1}\alpha^{i-1} + \cdots + a_{n-i}$.
Et à la nième itération on obtient finalement la valeur de $\widetilde{P}(\alpha)$.

Remarque 18. En algorithmique, on préfère utiliser l'algorithme de hörner plutôt qu'un calcul direct car cette algorithme fait appel à beaucoup moins d'opérations. Vérifier cette affirmation pour le calcul de $\widetilde{P}(\alpha)$ lorsque $\deg P = n \in \mathbb{N}^*$.

`Exemple 12.` (∗) Rédiger une procédure Maple mettant en oeuvre l'algorithme de hörner pour calculer l'image d'un scalaire par une fonction polynômiale.

4 Dérivation, formule de Taylor

DÉFINITION 9 : **Dérivée des polynômes**

Soit un polynôme $P = a_0 + a_1X + \cdots + a_pX^p \quad = \sum_{k=0}^{p} a_kX^k$.

On définit le *polynôme dérivé* de P par

$$P' = a_1 + 2a_2X + \cdots + pa_pX^{p-1} \quad = \sum_{k=0}^{p} k.a_kX^{k-1}$$

On définit ensuite les polynômes P'', ..., $P^{(k)}$ pour tout $k \in \mathbb{N}$.

Remarque 19.
1. La dérivée d'un polynôme constant ou nul est le polynôme nul.
2. Le terme $k.a_kX^{k-1}$ a bien un sens, même pour $k = 0$.

Remarque 20. La définition précédente est purement algébrique.
Elle ne correspond à la dérivée des fonctions polynômes que lorsque le corps de base $\mathbb{K}$ vaut $\mathbb{R}$.

PROPOSITION 24 : Soit $n \in \mathbb{N}$ et $P \in \mathbb{K}[X]$ de degré n. Alors :

1. $\deg(P') = n - 1$ si $n \in \mathbb{N}^*$
2. $\deg(P^{(k)}) = n - k$ si $k \leq n$
3. $P^{(k)} = 0$ si $k > n$

Preuve 24 : Petite récurrence sur k lorsque $k \leq n$. Pour le cas où $k > n$, on s'intéresse au polynôme $P^{(n)}$.

Remarque 21. Avant d'appliquer les formules précédentes, pensez à vérifier que le degré de P est bien adapté.

`Exemple 13.` (∗) Résoudre les équations suivantes :

1. $P'^2 = 4P$.
2. $(X^2 + 1)P'' - 6P = 0$.

Exercice : 12

(∗∗) Montrer que pour tout entier naturel $n \in \mathbb{N}^*$, il existe un unique polynôme $P_n \in \mathbb{Q}_n[X]$ tel que $P_n - P_n' = X^n$.
Exprimer les coefficients de P_n à l'aide de nombres factoriels.

Théorème 25 : **Dérivée d'une somme et d'un produit de polynômes**

L'application $D : \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ P & \mapsto & P' \end{array}$ est linéaire et vérifie : $(PQ)' = P'Q + PQ'$.

Preuve 25 :

1. Pour la linéarité, on utilise des polynômes sous leur forme explicite.
2. Pour la formule :
   (a) Méth 1 : Si $\mathbb{K} = \mathbb{R}$, on peut utiliser $\Phi : \mathbb{R}[X] \mapsto \{\text{f}^\circ \text{ polynomiales sur } \mathbb{R}\}$ et remarquer que $\widetilde{P'} = \left(\widetilde{P}\right)'$
   (b) Méth 2 : Sinon :
      i. on démontre que $(PQ)' = P'Q + PQ'$ pour $\left\{ \begin{array}{l} P = X^p \\ Q = X^q \end{array} \right.$, puis dans le cas où $\left\{ \begin{array}{l} P \in \mathbb{K}[X] \\ Q = X^q \end{array} \right.$
      ii. on utilise enfin la linéarité de la dérivation pour prouver le cas général.

Remarque 22. $\left\{ \begin{array}{l} \ker(D) = \mathbb{K}_0[X] \\ \text{Im}(D) = \mathbb{K}[X] \end{array} \right.$. D est donc un endomorphisme $\left\{ \begin{array}{l} \text{surjectif} \\ \text{pas injectif} \end{array} \right.$. Et $\ker(D^k) = \mathbb{K}_{k-1}[X]$.

Corollaire 26 : Si $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}^*$, alors : $\left(P^n\right)' = nP^{n-1}P'$

Preuve 26 : Par récurrence.

Théorème 27 : **Formule de Leibniz**
Soient deux polynômes $(P, Q) \in \mathbb{K}[X]^2$. On a la formule suivante pour la dérivée du polynôme produit :

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

Preuve 27 :

1. Dans le cas où $\mathbb{K} = \mathbb{R}$, il suffit d'utiliser l'isomorphisme Φ du théorème précédent.
2. Sinon, la démonstration est identique à la démonstration de la formule de Liebniz dans le cas de la dérivée nième d'un produit de fonctions de classe $\mathcal{C}^n$.

Proposition 28 : **Dérivée d'une composée**
Soient $P, Q \in \mathbb{K}[X]$. On a alors :

$$(P \circ Q)' = P' \circ Q.Q'$$

Preuve 28 : Pas de difficulté en prenant la forme explicite de P.

Lemme 29 : **Dérivées de** $(X-a)^n$
Soit $a \in \mathbb{K}$. On exprime pour $p \in \mathbb{N}$, la dérivée $p$ième du polynôme $(X-a)^n$:

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

Preuve 29 : Récurrence simple dans le cas où $p \leq n$. Le cas $p > n$ est alors immédiat.

Théorème Fondamental 30 : **Formule de Taylor**
Soit un polynôme $P \in \mathbb{K}[X]$ de degré $\leq n$ et un scalaire $a \in \mathbb{K}$.
On obtient la décomposition du polynôme P sur la base $\mathcal{B} = \left(1, (X-a), \ldots, (X-a)^n\right)$ de $\mathbb{K}_n[X]$:

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

Preuve 30 :
1. Dans le cas où $\mathbb{K} = \mathbb{R}$, on peut montrer cette formule dans le cas de la fonction polynômiale $\widetilde{P}$ à l'aide de la formule de Lagrange, puis utiliser l'isomorphisme Φ pour prouver l'égalité des polynômes associés.
2. Sinon, on peut constater que $\mathcal{B} = (1, (X-a), \ldots, (X-a)^n)$ est une base de $\mathbb{K}_n[X]$.
On commence alors par décomposer P sous la forme $P = \lambda_0.(X-a)^0 + \lambda_1.(X-a)^1 + \ldots \lambda_n.(X-a)^n$.
Puis, on détermine les coefficients λ_k en calculant la fonction polynôme $\widetilde{P}^{(k)}$ et en remplaçant x par a.

Remarque 23.
1. On dit alors que $(\widetilde{P}(a), \dfrac{\widetilde{P}'(a)}{1!}, \ldots, \dfrac{\widetilde{P}^{(n)}(a)}{n!})$ sont les coordonnées de P dans la base $\mathcal{B}$.
Cette décomposition est unique !
2. Dans le cas où $a = 0$, la formule s'appelle "formule de Mac Laurin".
Déterminer sans calculs les valeurs de $\widetilde{P}(0)$, $\widetilde{P}'(0)$, $\widetilde{P}''(0)$, et $\widetilde{P}^{(3)}(0)$, lorsque $P = 1 - 2X + 5X^2 - 3X^3$.

Exercice : 13

(∗∗) Déterminer les polynômes $P \in \mathbb{R}[X]$ tels que $\begin{cases} \widetilde{P}(1) = 1 \\ 4P(X) = (X-1)P'(X) + P''(X) \end{cases}$.

Corollaire 31 : Le reste de la divisition euclidienne de P par $(X-a)^k$ est :

$$R_k(X) = \widetilde{P}(a) + \widetilde{P}'(a)(X-a) + \cdots + \frac{\widetilde{P}^{(k-1)}(a)}{(k-1)!}(X-a)^{k-1}$$

Preuve 31 : Pas de difficulté en utilisant la formule de Taylor.

`Exemple 14.` (∗) Trouver le reste de la division euclidienne du polynôme $P = X^n + 1$ $(n \geq 3)$ par le polynôme $(X-1)^3$.

Théorème 32 : **Deuxième formule de Taylor**
Soit un polynôme $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}$ et un scalaire $a \in \mathbb{K}$.
On a alors la décomposition du polynôme $P \circ (X+a)$ sur la base canonique de $\mathbb{K}_n[X]$:

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

Preuve 32 : Conséquence immédiate de la première formule de Taylor.

`Exemple 15.` (∗ ∗ ∗) Soit $P \in \mathbb{K}[X]$. Montrer que $P(X+1) = \sum_{k=0}^{+\infty} \frac{1}{k!} P^{(k)}(X)$.

Définition 10 : **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.
On dit que α est *racine d'ordre au moins k* de P lorsque $(X-\alpha)^k$ divise P.

Remarque 24. Dans le cas où α est *racine d'ordre k exactement* de P, cela signifie que l'on peut mettre en facteur le polynôme $(X-\alpha)^k$ dans P, mais pas le polynôme $(X-\alpha)^{k+1}$.

Théorème Fondamental 33 : **Factorisation d'un polynôme**
Soit $P \in \mathbb{K}[X]$ de racines distinctes $\alpha_1, \ldots, \alpha_k$ d'ordre de multiplicité $p_1, \ldots, p_k$.
Il existe alors $Q \in \mathbb{K}[X]$ tel que le polynôme P se factorise sous la forme :

$$P = \prod_{i=1}^{k} (X-\alpha_i)^{p_i}.Q$$

Preuve 33 : Il suffit de démontrer que les polynômes $(X-\alpha_i)^{p_i}$ sont deux à deux premiers entre eux !

Remarque 25. Cela signifie en particulier que le degré du polynôme P est supérieur ou égal à la somme des ordres de multiplicité.

Théorème Fondamental 34 : **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. $P(\alpha) = P'(\alpha) = \ldots = P^{(k-1)}(\alpha) = 0_{\mathbb{K}}$.
  2. $P^{(k)}(\alpha) \neq 0_{\mathbb{K}}$.

Preuve 34 :
1. On utilise la formule de Taylor et le fait que la famille $\mathcal{B} = (1, (X-a), \ldots, (X-a)^{k-1})$ est libre.
2. Par l'absurde !

`Exemple 16.` (∗) Pour tout $n \in \mathbb{N}^*$, justifier les divisibilités suivantes :

1. $X^2 \mid (X+1)^n - nX - 1$.
2. $(X-1)^3 \mid nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$

Exercice : 14
(∗) Trouver une CNS sur $\lambda \in \mathbb{C}$ pour que $P = X^7 - X + \lambda$ admette une racine multiple.

5 Relations coefficients-racines pour les polynômes scindés

5.1 Le théorème de d'Alembert / Polynômes scindés

Définition 11 : **Polynôme scindé**
Soit $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}^*$. On dit que P est scindé si P s'écrit :

$$P = a_n \prod_{i=0}^{n} (X - \alpha_i) \qquad \text{où} \quad \begin{cases} \alpha_i \in \mathbb{K} \text{ sont les racines de } P \text{ (éventuellement identiques)} \\ a_n \neq 0 \text{ est le coefficient dominant du polynôme } P \end{cases}$$

Remarque 26. Un polynôme constant de $\mathbb{K}[X]$ ne peut donc être scindé.

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

Théorème Fondamental 35 : **Théorème de d'Alembert (admis)**
Soit un polynôme $P \in \mathbb{C}[X]$ tel que $\deg P \geq 1$.
Alors P possède au moins une racine complexe $\alpha \in \mathbb{C}$.

Corollaire 36 :
1. Tout polynôme de $\mathbb{C}[X]$ est scindé.
2. Tout polynôme de $\mathbb{C}[X]$ de degré $n \in \mathbb{N}^*$ admet n racines (éventuellement identiques).

Preuve 36 :
1. Par récurrence en utilisant le théorème de d'Alembert.
2. On distingue les deux cas : plus de n racines et moins de n racines.

Remarque 27. Ce résultat est faux pour $\mathbb{R}[X]$ comme le montre l'exemple $P(X) = X^2 + 1$.

Exercice : 15
(∗) Soit un polynôme $P \in \mathbb{R}[X]$.
Montrer que si P est scindé avec n racines distinctes, alors P' est également scindé dans $\mathbb{R}[X]$.

Remarque 28. Le résultat de l'exercice précédent est faux si $\mathbb{K}$ est 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' ($1/\sqrt{3}$ et $-1/\sqrt{3}$) ne sont pas rationnels.

5.2 Relations entre coefficients et racines d'un polynôme scindé

Pour déterminer ces relations, commençons par traiter le cas d'un polynôme de degré 2.

`Exemple 17.` Soit P un polynôme scindé de degré 3.
On a: $P(X) = a_3(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$ ou encore $P(X) = a_3X^3 + a_2X^2 + a_1X + a_0$.
Déterminer des relations entre les racines de P et ses coefficients.

DÉFINITION 12 : **Fonctions symétriques élémentaires des racines**
Considérons maintenant un polynôme **scindé** $P \in \mathbb{K}[X]$ de degré n, s'écrivant

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

Notons $\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n$ ses racines.

On définit les *fonctions symétriques élémentaires des racines* :

$$\sigma_k = \sum_{1\leq i_1<\cdots<i_k\leq n} \alpha_{i_1}\ldots\alpha_{i_k}$$

Remarque 29. Ainsi:

$$\begin{cases} \sigma_1 &= \alpha_1 + \cdots + \alpha_n \\ \sigma_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{p-1}\alpha_n \\ \sigma_3 &= \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \cdots + \alpha_{n-2}\alpha_{n-1}\alpha_n \\ & \cdots \\ \sigma_n &= \alpha_1\ldots\alpha_n \end{cases}$$

Remarque 30. Dans la formule, l'indice k de σ_k représente le nombre de racines dans chaque produit.

THÉORÈME FONDAMENTAL 37 : **Relations coefficients-racines**
Soit $P = a_n.X^n + a_{n-1}.X^{n-1} + \cdots + a_0$ un polynôme **scindé** de $\mathbb{K}[X]$ de racines $(\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n) \in \mathbb{K}^n$.
On a alors:

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

Preuve 37 : $\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n$ sont les racines de $P \Rightarrow P = a_n.\prod_{k=1}^{n}(X-\alpha_k) \Rightarrow$ "on développe P"
Il ne reste plus qu'à identifier les coefficients.

Remarque 31. Pour retrouver les formules du théorème, il pourra être utile de commencer par écrire:

$$P(X) = a_n(X^n + (-1)\sigma_1.X^{n-1} + (-1)^2\sigma_2.X^{n-2} + \cdots + (-1)^{n-1}\sigma_{n-1}.X + \sigma_n)$$

On pourra retrouver cette formule par analogie avec $P = a_2(X^2 - SX + P)$ où $S = \sigma_1$ et $P = \sigma_2$.

`Exemple 18.` Déterminer les valeurs de σ_1, σ_2, σ_3 et σ_4 lorsque $P = 3X^4 - 3X^3 + 8X^2 - 6 \in \mathbb{C}[X]$.

COROLLAIRE 38 : **Relations coefficients-racines**
Soient $(\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n) \in \mathbb{K}^n$ et $(\lambda_1,\ \lambda_2,\ \ldots,\ \lambda_n) \in \mathbb{K}^n$.
On a alors l'équivalence suivante:

$$\forall k \in [\![1,n]\!],\quad \sigma_k = \lambda_k$$

$$\Longleftrightarrow$$

$$\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n \text{ sont racines de } P = X^n - \lambda_1X^{n-1} + \lambda_2X^{n-2} + \cdots + (-1)^{n-1}\lambda_{n-1}X + (-1)^n\lambda_n$$

Preuve 38 : C'est la démonstration du théorème précédent en utilisant des équivalences.

Remarque 32. On utilise le théorème précédent pour résoudre des systèmes dont les équations permettent de calculer les fonctions symétriques des inconnues.

Exercice : 16

(∗) Trouver $(a,\ b,\ c) \in \mathbb{C}^3$ tels que $\begin{cases} a+b+c=1 \\ a^2+b^2+c^2=3 \\ a^3+b^3+c^3=1 \end{cases}$.

Exercice : 17

(∗∗) Donner une CNS sur $\lambda \in \mathbb{C}$ pour que le polynôme $X^3 - 7X + \lambda$ admette une racine qui soit le double d'une autre. Trouver alors toutes les racines.

Remarque 33.

1. Le théorème précédent montre que l'on peut exprimer les coefficients d'un polynôme scindé en fonction de ses racines. La réciproque est-elle vraie? OUI dans le cas où $\deg P \leq 2$ (résultat bien connu!) et NON dans le cas général! Un célèbre résultat de Galois (1811 - 1832) montre en effet, qu'il n'existe pas de formule qui permet d'exprimer les racines d'un polynôme quelconque à coefficients réels de degré supérieur à 5 à partir des coefficients du polynôme. Difficile dans ce cas de demander à un ordinateur de donner de façon exacte l'expression des racines d'un polynôme quelconque!!

   (a) On sait résoudre les équations algébriques de degré 2 depuis l'antiquité.
   (b) On sait résoudre les équations algébriques de degré 3 et 4 depuis le XVI ème siècle (Tartaglia - Cardan)
   (c) On sait qu'il est impossible de résoudre de façon générale les équations algébriques de degré 5 ou plus d'après les travaux d'Abel (1802 - 1829).

2. Par contre, on montre que toute expression polynômiale symétrique en les racines d'un polynôme (c'est à dire, qui reste invariante par permutations des racines) 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 : 18

(∗) Soit $P \in \mathbb{C}[X]$ défini par $P(X) = X^3 - 3X^2 - 10X + 24$, et α_1, α_2, α_3 ses racines dans $\mathbb{C}$.
Déterminer $\forall k \in [\![1,5]\!]$ $S_k = \alpha_1^k + \alpha_2^k + \alpha_3^k$.

Aide : Pour $k \geq 3$, vous pourrez effectuer la division euclidienne de X^k par P.

Exercice : 19

(∗) Soient x_1, x_2 et x_3 les racines du polynôme $P = X^3 + pX + q$ dans $\mathbb{C}[X]$. Calculer:

$$E = \sum_{k=1}^{3} \frac{1}{x_k^2}$$

Exercice : 20

(∗∗) Déterminer une CNS sur $\lambda \in \mathbb{C}$ pour que deux des racines x_1, x_2 et x_3 de $P = X^3 + 5X^2 - 8X + \lambda$ vérifient $x_1 + x_2 = -1$.

Remarque 34. Comme le montre l'excercice précédent, on pensera à utiliser les fonctions symétriques élémentaires des racines pour trouver les racines d'un polynômes, dès lors que l'on possède certaines informations sur les racines.

6 Décomposition d'un polynôme en produit de facteurs irréductibles

Nous avons vu dans une première partie sur l'arithmétique des polynômes que beaucoup de propriétés sont analogues à celles rencontrées en arithmétique des entiers. Dans cette partie, nous poursuivons l'analogie et introduisant la notion de *polynômes irréductibles* qui du fait de ses propriétes, peut-être considérée comme analogue à celle de *nombres premiers*.

6.1 Les polynômes irréductibles de $\mathrm{C}[X]$ et $\mathrm{R}[X]$

DÉFINITION 13 : **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 35. Les seuls diviseurs des polynômes P irréductibles sont donc les polynômes constants non nuls et les polynômes non nuls proportionnels à P.

LEMME 39 : **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 $\mathbb{K}[X]$.

Preuve 39 : Par l'absurde en utilisant la fonction degré.

`Exemple 19.` Exemples de polynômes irréductibles :

1. Dans $\mathbb{C}[X]$: $X-2$ et $X+i$ sont irréductibles
2. Dans $\mathbb{R}[X]$: $X-2$ et X^2+1 sont irréductibles
3. Dans $\mathbb{Q}[X]$: $X-2$, X^2+1 et X^2-2 sont irréductibles

THÉORÈME 40 : **Décomposition dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$**

1. Les polynômes irréductibles unitaires de $\mathbb{C}[X]$ sont les polynômes : $P_\alpha(X) = X-\alpha$ avec $\alpha \in \mathbb{C}$
2. Les polynômes irréductibles unitaires de $\mathbb{R}[X]$ sont :
   (a) Les polynômes de degré 1 de la forme $(X-\alpha)$ avec $\alpha \in \mathbb{R}$.
   (b) Les polynômes de degré 2 de la forme X^2+pX+q avec $p^2-4q<0$.

Preuve 40 :

1. C'est un corollaire immédiat du théorème de d'Alembert.
2. Pas de problème pour les polynômes de degré 1.
   Le cas des polynômes de degré 2 se traite à l'aide de la décomposition canonique.
   On montre enfin que les polynômes de degré ≥ 3 ne sont pas irréductibles en considérant une racine.

Remarque 36.

1. Dans $\mathbb{R}[X]$, tout polynôme de degré ≥ 3 est réductible !!
2. Dans $\mathbb{C}[X]$, tout polynôme de degré ≥ 2 est réductible !!

`Exemple 20.` $(*)$ 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 $p^2-4q<0$ (l'autre cas ne pose pas de problème), regrouper le terme en X^4 et le terme constant (forcément positif), faire apparaître un début de carré, puis utiliser l'identité $A^2-B^2=(A-B)(A+B)$.
Exemple : Factoriser les polynômes $P=X^4-3X^2+9$ et $Q=X^4+1$.

6.2 Un peu d'arithmétique ...

On retrouve des propriétés analogues aux propriétés bien connues sur les entiers :

PROPOSITION 41 :

1. Deux polynômes irréductibles sont premiers entre eux ou égaux à une constante multiplicative près.
2. Si $P_1, \dots, P_k$ sont irréductibles et $\forall i \in [\![1,k]\!]$, $P_i^{n_i}$ divise A alors $\prod_{i=1}^{k} P_i^{n_i}$ divise A.
3. Si P est irréductible et P ne divise pas A alors $P \wedge A = 1$.
4. Si P est irréductible et divise un produit de polynômes, alors P divise l'un des facteurs.

Preuve 41 :

1. Pas de difficulté.
2. On montre que $\forall i \neq j$, $P_i^{n_i} \wedge P_j^{n_j} = 1$ et on applique $\left\{ \begin{array}{l} A \ / \ C \\ B \ / \ C \\ A \wedge B = 1 \end{array} \right. \Rightarrow AB \ / \ C$.
3. Par l'absurde, on arrive à une contradiction avec P ne divise pas A.
4. Par l'absurde : si P ne divise aucun facteur, alors P est premier avec chaque facteur et donc avec le produit.

Remarque 37. En s'inspirant de la démonstration de l'infinité des nombres premiers, on démontre de même que le nombre de polynômes irréductibles de $\mathbb{K}[X]$ est infini. Ce résultat est cependant évident lorsque $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$.

THÉORÈME 42 : **Décomposition d'un polynôme en facteurs irréductibles**
Soit un polynôme $P \in \mathbb{K}[X]$ **unitaire**.
Alors P s'écrit de façon unique à l'ordre près comme produit de polynômes irréductibles **unitaires** et distincts de $\mathbb{K}[X]$:

$$P = P_1^{\alpha_1} \times \cdots \times P_n^{\alpha_n} \quad \text{avec} \quad \alpha_1, \dots, \alpha_n \in \mathbb{N}^*$$

Preuve 42 :
1. Pour l'existence de la décomposition, on pourra procéder par récurrence sur le degré n du polynôme.
2. Pour l'unicité de la décomposition, il suffit d'utiliser le théorème de Gauss pour les polynômes.

Remarque 38. Cette décomposition s'appelle la *décomposition primaire* de P.

6.3 Décomposition en polynômes irréductibles dans $\mathrm{C}[X]$ et $\mathrm{R}[X]$.

THÉORÈME 43 : **Décomposition dans $\mathbb{C}[X]$**

Tout polynôme de $\mathbb{C}[X]$ s'écrit donc de façon unique (à l'ordre près) sous la forme :

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

avec $\lambda \in \mathbb{R}$ le coefficient dominant de P.
Les complexes α_i ne sont pas forcément distincts.

Preuve 43 : Corollaire du théorème de décomposition d'un polynôme en produit de polynômes irréductibles.

`Exemple 21.` $(*)$ Décomposer le polynôme $P = X^n - 1$ dans $\mathbb{C}\ [X]$.

THÉORÈME 44 : **Décomposition dans $\mathbb{R}[X]$**

Tout polynôme de $\mathbb{R}[X]$ s'écrit de façon unique (à l'ordre près) sous la forme :

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

où tous les facteurs sont irréductibles unitaires et $\lambda \in \mathbb{R}$ est le coefficient dominant de P.

Preuve 44 : Corollaire du théorème de décomposition d'un polynôme en produit de polynômes irréductibles.

Méthode de décomposition de $P \in \mathbb{K}[X]$ en produit de polynômes irréductibles

1. Dans $\mathbb{C}[X]$, il suffit de déterminer les racines de P
2. Dans $\mathbb{R}[X]$:
   - On commence par effectuer une décomposition de $\mathbb{C}[X]$
   - On regroupe, puis on développe les facteurs correspondant à des racines conjuguées.

Exercice : 21
$(**)$ On considère les polynômes $P(X) = X^{2n} - 1$ et $Q(X) = X^{2n+1} - 1$.
Factoriser P et Q dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$.

THÉORÈME 45 : **Expression du PGCD et du PPCM**
Soient A et $B \in \mathbb{K}[X]$ non nuls de décompositions en facteurs irréductibles unitaires suivantes :

$$A = \lambda.\prod_{i\in\mathbb{N}} P_i^{n_i(A)} \quad \text{et} \quad B = \mu.\prod_{i\in\mathbb{N}} P_i^{n_i(B)} \quad \text{avec } \lambda,\ \mu \in \mathbb{K}$$

On a alors :

$$A \wedge B = \prod_{i\in\mathbb{N}} P_i^{\min(n_i(A),\ n_i(B))} \quad \text{et} \quad A \vee B = \prod_{i\in\mathbb{N}} P_i^{\max(n_i(A),\ n_i(B))}$$

Preuve 45 :

1. Il est évident que $\prod_{i\in\mathbb{N}} P_i^{\min(n_i(A),\ n_i(B))}$ est un diviseur commun à A et B.

   Soit D un diviseur commun à A et B et on démontre que celui-ci divise $\prod_{i\in\mathbb{N}} P_i^{\min(n_i(A),\ n_i(B))}$.

2. Il est évident que $\prod_{i\in\mathbb{N}} P_i^{\max(n_i(A),\ n_i(B))}$ est un multiple commun à A et B.

   Soit M un multiple commun à A et B et on démontre que celui-ci est multiple de $\prod_{i\in\mathbb{N}} P_i^{\max(n_i(A),\ n_i(B))}$.

`Exemple 22.` $(*)$ Déterminer le PGCD et le PPCM de $\begin{cases} A=(X-2)^3(X+1)^2 \\ B=(X-2)^2(X+1)^4(X+3) \end{cases}$.

COROLLAIRE 46 : **Formule reliant le PGCD et le PPCM**
Soient A et B deux polynômes de $\mathbb{K}[X]$ non nuls. On a alors :

Il existe $\lambda\in\mathbb{K}$ tel que : $\boxed{AB=\lambda.(A\wedge B).(A\vee B)}$

Preuve 46 : Pas de difficulté.

Remarque 39. λ est le produit des coefficients dominants de A et B.