Les Polynômes

MPSI Prytanée National Militaire

Pascal Delahaye

10 mai 2017

$$P_n(x) = \sum_{i=0}^{n} \left[f(x_i) \times \prod_{k=0,\, k\neq i}^{n} \frac{x - x_k}{x_i - x_k} \right]$$

Polynôme d'interpolation de Lagrange

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 :

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \quad \text{où} \quad \begin{cases} n \in \mathbb{N} \\ (a_0,\ a_1,\ \ldots,\ a_n) \in \mathbb{K}^n \quad \text{appelés "coefficients"} \end{cases}$$

1. X est appelée l'*indéterminée.*
2. P est aussi parfois noté $P(X)$.
3. 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 $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ est unique.
   Ainsi, on aura : $P = 0 \iff \forall k \in \mathbb{N},\ a_k = 0$.

Remarque 2. **Notation :**

On pourra noter un polynôme sous la forme $P = \displaystyle\sum_{i=0}^{+\infty} a_iX^i$ en sachant que les a_i sont nuls à partir d'un certain rang.

Définition 2 : **Lois de composition interne**

Soit $A = \displaystyle\sum_{i=0}^{+\infty} a_iX^i$ et $B = \displaystyle\sum_{i=0}^{+\infty} b_iX^i$. On définit sur $\mathbb{K}[X]$, les deux lci "+" et "$\times$" suivantes :

1. $A + B = \displaystyle\sum_{i=0}^{+\infty} (a_i + b_i)X^i$
2. $AB = \displaystyle\sum_{i=0}^{+\infty} c_iX^i \quad$ où $\quad c_i = \displaystyle\sum_{k=0}^{i} a_kb_{i-k}$

Remarque 3. Ces deux lci correspondent aux notions intuitives de l'addition et de la multiplication que nous avons.

Théorème Fondamental 1 : L'anneau des polynômes

$$\big(\mathbb{K}[X],+,\times\big) \quad \text{est un anneau commutatif}$$

L'élément neutre pour $+$ 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 de définition d'un anneau commutatif ...

Remarque 4. $(\mathbb{K}[X],+,\times)$ étant un anneau commutatif, on pourra utiliser la formule du binôme :

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

Définition 3 : Une autre lci : la composition des polynômes

Si $P(X)=\displaystyle\sum_{k=0}^{n}a_kX^k$ et $Q\in\mathbb{K}[X]$.

On définit $P\circ Q$, le polynôme composé par la formule suivante : $P\circ Q=\displaystyle\sum_{k=0}^{n}a_kQ^k$.

Notation : $P(X)=P\circ X$, $P(-X)=P\circ(-X)$, $P(X^2)=P\circ X^2$ ...etc...

Remarque 5. Même si elle lui ressemble fortement, $\circ$ n'est pas la loi de composition des applications puisque c'est une loi portant sur des polynômes.

Proposition 2 : Opérations

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

Distributivités $\boxed{\text{à droite}}$:

1. $(P+\lambda Q)\circ R=P\circ R+\lambda Q\circ R$
2. $(PQ)\circ R=(P\circ R).(Q\circ R)$

Autres :

3. $(P\circ Q)\circ R=P\circ(Q\circ R)$
4. $X\circ P=P\circ X=P$

Preuve 2 : On s'en dispensera ...

Remarque 6. La loi $\circ$ n'est pas commutative et n'est pas distributive à gauche dans $\mathbb{K}[X]$. Chercher des C/ex !

`Exemple 1.` Prouver qu'un polynôme pair $P\in\mathbb{R}[X]$ est de la forme $Q(X^2)$ avec $Q\in\mathbb{R}[X]$.
Un polynôme pair est un polynôme qui vérifie $P(X)=P(-X)$.

Définition 4 : Degré, valuation, terme dominant

Soit un polynôme $P=a_0+a_1X+\cdots+a_nX^n$ avec $a_n\neq 0$.

1. L'entier n est appelé le *degré* du polynôme P et est noté $\deg P$.
2. Par convention, le degré du polynôme nul vaut $-\infty$.
3. Le coefficient a_n est appelé le *coefficient dominant* du polynôme P.
4. Lorsque $a_n=1$, on dit que le polynôme P est *unitaire*.
5. Le monôme a_nX^n est appelé le *terme dominant* de P.

Théorème 3 : Degré d'un produit, d'une somme, d'une composée

1. $\deg\big(P+Q\big)\leq\max\big(\deg P,\ \deg Q\big)$
2. $\deg\big(PQ\big)=\deg P+\deg Q$ formule valable même si P et/ou Q est nul.
3. $\deg(P\circ Q)=\deg P\times\deg Q$ formule valable uniquement si $P\neq 0$ et $Q\neq 0$.

Preuve 3 :
On écrit P et Q sous leur forme générale et on s'intéresse aux termes dominants.

Remarque 7.

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. Pour montrer que $Q = \sum_{i=1}^{k} \lambda_i P_i$, où $(P_1,\ \dots,\ P_k)$ sont tous de degré n, est aussi 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 8. Le degré est un outil d'analyse performant dans la recherche de polynômes vérifiant une ou des conditions données (analyse / synthèse).

Avant d'utiliser la formule $\deg(P \circ Q) = \deg P \times \deg Q$, on prendra soin de s'assurer que les polynômes sur lesquels on travaille sont non nuls.

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

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

Exercice : 1

$(*)$ Soit (P_n) la suite de polynômes définie par la relation de récurrence : $\begin{cases} P_0 = 1 \\ P_{n+1} = 2XP_n + X \end{cases}$.

Déterminer pour tout n le degré et le coefficient dominant de P_n.
Aide : pour plus d'efficacité, on pourra travailler sur les termes dominants.

Théorème 4 : **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 4 :

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

Théorème 5 : **Polynômes inversibles**
Les éléments inversibles de l'anneau $\mathbb{K}[X]$ sont les polynômes constants non-nuls.

Preuve 5 : On utilise de nouveau la fonction degrée.

Définition 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.

Remarque 9. On montrera plus tard que cet ensemble est un sous-espace vectoriel de $\mathbb{K}[X]$ dont la famille $\left(1,\ X,\ X^2,\ \dots,\ X^n\right)$ forme une base appelée *base canonique* de $\mathbb{K}_n[X]$.

2 Arithmétique des polynômes

Théorème Fondamental 6 : **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 6 :
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^p les termes dominants respectifs de A et B.
   Pour se ramener à un polynôme de degré $\leq n$, on peut considérer le polynôme : $A - \dfrac{a_{n+1}}{b_p}.X^{n+1-p}B$.
   On applique alors l'hypothèse de récurrence à ce nouveau polynôme.

On démontre enfin l'unicité de cette décomposition de façon usuelle en utilisant la fonction degré.

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 $\left\{\begin{array}{l}\text{de } A = X^5 + X^4 - X^3 + X - 1 \\ \text{par } B = X^3 + X^2 + 2\end{array}\right.$ on obtient $\left\{\begin{array}{l} Q = X^2 - 1 \\ R = -X^2 + X + 1\end{array}\right.$.

Calcul de congruence

Comme pour les entiers, on pourra utiliser les règles de calcul de congruence pour :

- Rechercher le reste d'une division euclidienne
- Prouver une divisibilité

`Exemple 5.` $(*)$ Déterminer le reste de la division euclidienne de $A = X^{2000} - X^3 + X$ par $B = X^2 + 1$.

Remarque 10. On verra une méthode plus efficace dans le paragraphe sur les racines d'un polynôme.

Proposition 7 : **Factorisation dans $\mathbb{R}[X]$**

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

Preuve 7 : 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 11. Ce résultat s'applique en particulier lorsque $D = 0$.

Définition 6 : **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 : 2

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

Théorème 8 : **Polynômes associés**

Soient deux polynômes $(P,\ Q) \in \mathbb{K}[X]$ non-nuls.

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

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

Preuve 8 : 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 9 : **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 : $\boxed{D \text{ divise} \begin{cases} A \\ B \end{cases} \Longleftrightarrow D \text{ divise} \begin{cases} B \\ R \end{cases}}$

Preuve 9 : 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 7 : **PGCD et PPCM**

Soient deux polynômes A et B de $\mathbb{K}[X]$ dont l'un au moins est non nul. On appelle :

1. PGCD(A, B) tout diviseur commun à A et B de degré maximal.
   On notera $A \wedge B$ le seul PGCD de A et B unitaire (vu plus loin).
2. PPCM(A, B) tout multiple commun à A et B de degré minimal.
   On notera $A \vee B$ le seul PPCM de A et B unitaire (vu plus loin).

Remarque 13.

1. Le dernier reste non nul obtenu dans l'alg. d'Euclide appliqué à A et B est donc un PGCD de A et de B.
   On obtient alors LE PGCD en divisant ce polynôme par son coefficient dominant.
2. Si $A \wedge B = 1$, on dit que les polynômes A et B sont *premiers entre eux*.
3. On peut, de la même façon, définir le PGCD et le PPCM de n polynômes $A_1,\ \ldots,\ A_n$ où $n \in \mathbb{N}^*$.
   On note alors $A_1 \wedge \cdots \wedge A_n$ le PGCD unitaire.

COROLLAIRE 10 : **Ensemble des diviseurs et des multiples communs**

1. Les diviseurs communs à deux polynômes A et B (dont l'un est non nul) sont les diviseurs d'un PGCD.
2. Les multiples communs à deux polynômes A et B (dont l'un est non nul) sont les multiples d'un PPCM.

Preuve 10 :

1. Immédiat d'après l'algorithme d'Euclide.
2. A l'aide de la division euclidienne

COROLLAIRE 11 : Les PGCD et les PPCM de deux polynômes sont des polynômes associés.

Preuve 11 : Ceci provient du fait que les diviseurs communs sont les diviseurs d'un PGCD et que les multiples communs sont les multiples d'un PPCM

PROPOSITION 12 : Les lois $\wedge$ et $\vee$ sont associatives.

Preuve 12 : On compare les ensembles de diviseurs communs.

`Exemple 6.` $(*)$ Déterminer le PGCD de $\left\{\begin{array}{l} A(X) = X^3 + 2X^2 - X - 2 \\ B(X) = X^2 + 4X + 3 \end{array}\right.$ en vous inspirant de l'algorithme d'Euclide.

Exercice : 3

$(***)$ 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 : **Relation entre PGCD et PPCM**
Soient deux polynômes A et B de $\mathbb{K}[X]$ unitaires dont l'un est non nul.
Nous avons la relation suivante :

$$(A \wedge B)(A \vee B) = A.B$$

Preuve 13 : Voir la démonstration analogue dans le cas des entiers.

THÉORÈME 14 : **Egalité de Bezout**
Soient deux polynômes non nuls A et B de $\mathbb{K}[X]$ et δ un PGCD. Alors :

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

Preuve 14 : Comme dans $\mathbb{Z}$, on détermine les polynômes U et V grâce à l'algorithme d'Euclide.

Pour déterminer U et V, on pourra :

• Soit calculer les termes des suites (U_n) et (V_n) en présentant les calculs dans un tableau de la forme :

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

• Soit écrire les divisions euclidiennes successives et procéder par substitution pour déterminer la relation voulue.

Remarque 14. Le couple de polynômes $(U,\ V)$ n'est pas unique !
Pour déterminer tous les couples solutions, on utilise le théorème de Gauss, comme lors de la résolution des équations diophantiennes dans $\mathbb{Z}$.

`Exemple 7.` $(*)$ Déterminer une égalité de Bezout pour les polynômes :

1. $\left\{\begin{array}{l} A = X^3 + X^2 + 2 \\ B = X^2 + 1 \end{array}\right.$ 2. $\left\{\begin{array}{l} A = X^4 + X^3 - 2X + 1 \\ B = X^2 + X + 1 \end{array}\right.$.

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

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

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 $\mathbb{K}[X]$.

$$\text{Si} \quad \left\{\begin{array}{l} A \text{ divise } BC \\ A \wedge B = 1 \end{array}\right. \quad \text{alors} \quad A \text{ divise } C$$

Preuve 16 : Application immédiate du théorème de Bezout précédent.

Exercice : 4
$(**)$ 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 : $\left\{\begin{array}{l} AU + BV = 1 \\ \deg U < \deg B \\ \deg V < \deg A \end{array}\right.$.

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

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

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

`Exemple 8.` $(*)$ Montrer que si a et b sont deux scalaires distincts, alors pour tout entiers :

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

`Exemple 9.` $(*)$ Soient $A,\ B$ et C trois polynômes premiers deux à deux. Montrer que $(AB + BC + AC) \wedge ABC = 1$.

`Exemple 10.` $(*)$ Soit $(A,\ B) \in \mathbb{K}[X]$ non constants. Montrer que : $\quad A \wedge B = 1 \Longleftrightarrow AB \wedge (A+B) = 1$

THÉORÈME 18 : **Généralisation de l'égalité de Bezout**
Soient $n \in \mathbb{N}^*$ polynômes $A_1,\ \dots,\ A_n$ de $\mathbb{K}[X]$ dont l'un est non nul et δ un PGCD. Alors :

$$\text{Il existe } n \text{ polynômes } (U_1,\ \dots,\ U_n) \in \mathbb{K}[X]^n \text{ tels que :} \quad A_1U_1 + \cdots + A_nU_n = \delta$$

Preuve 18 : Par récurrence.

DÉFINITION 8 : **Polynômes premiers entre eux**
Soient $n \in \mathbb{N}^*$ polynômes $A_1,\ \dots,\ A_n$ de $\mathbb{K}[X]$.
On dira que :

1. $A_1,\ \dots,\ A_n$ sont *premiers entre eux dans leur ensemble* lorsque $A_1 \wedge \cdots \wedge A_n = 1$
2. $A_1,\ \dots,\ A_n$ sont *premiers entre eux deux à deux* lorsque $\forall i,\ j \in [\![1, n]\!]$ tels que $i \neq j$, on a $A_i \wedge A_j = 1$

3 Fonctions polynômiales. Racines d'un polynôme

Définition 9 : **Fonction polynômiale**
Soit un polynôme $P = a_0 + a_1X + \cdots + a_nX^n$ de $\mathbb{K}[X]$.
On définit à partir des coefficients de P, la *fonction polynômiale* associée :

$$P : \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \mapsto & a_0 + a_1x + \cdots + a_nx^n \end{array}$$

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

Remarque 15. On remarquera que cette définition utilise un "abus de notation" car la notation P désigne à la fois le polynôme P et la fonction polynomiale associée. Cet abus se justifie dans la mesure où l'on verra plus loin que dans $\mathbb{R}$ ou $\mathbb{C}$, l'égalité de deux fonctions polynômiales est équivalente à l'égalité des deux polynômes associés.

Définition 10 : **Equation algébrique - Nombre algébrique**

1. L'équation $P(x) = 0$ où $\begin{cases} P \in \mathbb{C}[X] \\ x \in \mathbb{C} \end{cases}$, est appelée *équation algébrique* associée au polynôme P.
2. On dit qu'un nombre complexe est un *nombre algébrique* lorsqu'il est solution d'une équation de la forme $P(x) = 0$ où $P \in \mathbb{Q}[X]$. Ainsi, les nombres, 4, $\frac{2}{5}$, $\sqrt{3}$, i et j sont des nombres algébriques.

   Les nombres non-algébriques sont dits *transcendants*. Par exemple : π, e...etc ...

`Exemple 11.` Justifiez que les rationnels sont des nombres algébriques ainsi que les nombres $\sqrt{n}$ où $n \in \mathbb{N}$.

Théorème 19 : **Les lois sur $\mathbb{K}[X]$ correspondent à celles sur $\mathcal{F}(\mathbb{K}, \mathbb{K})$**
Soient $(P, Q) \in \mathbb{K}[X]^2$.
Pour tout $x \in \mathbb{K}$, on a les propriétés suivantes :

1. $(P \times Q)(x) = P(x) \times Q(x)$
2. $(P + Q)(x) = P(x) + Q(x)$
3. $(P \circ Q)(x) = P \circ Q(x)$

Preuve 19 : Pas de difficulté ...

Définition 11 : **Racine d'un polynôme**
Soit un polynôme $P \in \mathbb{K}[X]$.
On dit qu'un scalaire $\alpha \in \mathbb{K}$ est une *racine* (ou un *zéro*) de P lorsque $P(\alpha) = 0$.

Remarque 16. Les racines d'un polynôme de $\mathbb{K}[X]$ appartiennent au corps $\mathbb{K}$.

`Exemple 12.` $(*)$ Soit $P \in \mathbb{C}[X]$ à coefficients réels et $\alpha \in \mathbb{C}$. Vérifier que : α racine de $P \iff \bar{\alpha}$ racine de P.

Théorème 20 : **Factorisation par $X - \alpha$**
Soit un polynôme $P \in \mathbb{K}[X]$ et un scalaire $\alpha \in \mathbb{K}$. Alors :

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

Preuve 20 : 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 21 : **Factorisation par $(X - \alpha_1)\dots(X - \alpha_n)$**
Soit un polynôme $P \in \mathbb{K}[X]$, $n \in \mathbb{R}^*$ et $(\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n$ deux à deux distincts.
Alors :

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

Preuve 21 : Par récurrence sur n.

`Exemple 13.` $(*)$ 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.
   En déduire que X^2+X+1 divise X^4+X^2+1.

Exercice : 5

$(*)$ 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.

Exercice : 6

$(**)$ Soit $p,\ q \in \mathbb{N}^*$ supérieurs à 2 et premiers entre eux. Montrer que $(X^p-1)(X^q-1) \mid (X-1)(X^{pq}-1)$

Corollaire 22 : **Polynôme ayant plus de racines que son degré**
Soient $P,\ Q \in \mathbb{K}_n[X]$.

1. Si P admet au moins $(n+1)$ racines distinctes, alors $P=0$.
2. Si P et Q coïncident en au moins $(n+1)$ valeurs distinctes, alors $P=Q$

Preuve 22 : C'est un corollaire du théorème précédent.

Remarque 17. Ce théorème est très utilisé pour montrer des unicités.
Il s'applique en particulier lorsqu'un polynôme admet une infinité de racines.

`Exemple 14.` $(*)$ Soit $P,\ Q \in \mathbb{C}[X]$. Justifier les affirmations suivantes :

1. Pour tout $n \in \mathbb{N}^*$ on a $P(2^n) = 0$ donc $P = 0$.
2. Pour tout $n \in \mathbb{N}^*$ on a $P(\cos(\dfrac{\pi}{2^n})) = Q(\cos(\dfrac{\pi}{2^n}))$ donc $P = Q$.
3. $P(X^2) = Q(X^2)$ implique $P = Q$.

Exercice : 7

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

Corollaire 23 : **Bijection canonique :**

L'application $\varphi : \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}\,[x] \\ P & \mapsto & (x \mapsto P(x)) \end{array}$ est une bijection.

Cela signifie en particulier que si deux applications polynômiales sont égales, alors leurs polynômes associés le sont aussi. Cette propriété justifie l'abus de notation utilisé pour désigner un polynôme et une fonction polynômiale de $\mathbb{R}[X]$ ou de $\mathbb{C}[X]$.

Preuve 23 : La surjectivité est vrai par définition d'une fonction polynômiale.
L'injectivité découle directement du théorème précédent.

Remarque 18. Le théorème est faux lorsque le corps $\mathbb{K}$ n'est pas fini. Donner un contre-exemple dans $\dfrac{\mathbb{Z}}{2\mathbb{Z}}\,[X]$.

COROLLAIRE 24 : **Les polynômes de Lagrange :**
Soient $n \in \mathbb{N}^*$, $x_1,\ x_2,\ \dots,\ x_{n+1} \in \mathbb{K}$ distincts deux à deux et $y_1,\ y_2,\ \dots,\ y_{n+1} \in \mathbb{K}$.
Il existe un unique polynôme de degré inférieur ou égal à n tel que : $\forall i \in [\![1, n+1]\!], \quad P(x_i) = y_i$.
Il s'agit du polynôme défini par la formule :

$$P(x) = \sum_{i=1}^{n+1} \frac{\prod_{k \neq i}(X - x_k)}{\prod_{k \neq i}(x_i - x_k)}.y_i$$

Preuve 24 : Le polynômes proposés convient bien.
On prouve alors qu'il est unique à l'aide du théorème précédent.

Remarque 19. Lorsque $\mathbb{K} = \mathbb{R}$, cela signifie qu'il existe une unique fonction polynômiale P dont le graphe passe par les $n+1$ points du plan $M_1(x_1,\ y_1),\ \dots,\ M_{n+1}(x_{n+1},\ y_{n+1})$.

Exercice : 8

(∗∗). Montrer qu'il existe $\alpha,\ \beta,\ \gamma \in \mathbb{R}$ tels que $\displaystyle\int_2^4 P(t)\ \mathrm{d}t = \alpha P(2) + \beta P(3) + \gamma P(4)$ pour tout $P \in \mathbb{R}_3[X]$.
Pouvez-vous généraliser cette propriété ?

PROPOSITION 25 : Soient $n \in \mathbb{N}^*$, $x_1,\ x_2,\ \dots,\ x_{n+1} \in \mathbb{K}$ distincts deux à deux et $y_1,\ y_2,\ \dots,\ y_{n+1} \in \mathbb{K}$.
Les polynômes $Q \in \mathbb{K}[X]$ tels que $\forall i \in [\![1, n+1]\!],\ Q(x_i) = y_i$ sont les polynômes de la forme :

$$Q = P + \prod_{k=1}^{n+1}(X - x_i)T \quad \text{où} \quad \begin{cases} P \text{ est le polynôme de lagrange associé à} \begin{cases} x_1,\ \dots,\ x_{n+1} \\ y_1,\ \dots,\ y_{n+1} \end{cases} \\ T \in \mathbb{K}[X] \end{cases}$$

Preuve 25 : On s'intéresse aux racines de $Q - P$.

DÉFINITION 12 : **Ordre de multiplicité d'une racine**
Soit un scalaire $\alpha \in \mathbb{K}$ et $k \in \mathbb{N}^*$.

On dit que α est *racine d'ordre au moins* k de P lorsque $(X - \alpha)^k$ divise P.
On dit que α est *racine d'ordre* k *exactement* de P lorsque $\begin{cases} (X-\alpha)^k \text{ divise } P \\ (X-\alpha)^{k+1} \text{ ne divise pas } P \end{cases}$.

Si $P(\alpha) \neq 0$, on dit qu'α est d'ordre de multiplicité 0.

Remarque 20.

1. On dira plus généralement que α est une racine multiple de P si son ordre de multiplicité est au moins 2.
2. 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 26 : **Factorisation d'un polynôme**
Soit $P \in \mathbb{K}[X]$ de racines distinctes $\alpha_1,\ \dots,\ \alpha_k$ d'ordre de multiplicité $p_1,\ \dots,\ p_k$.
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 26 : Il suffit de démontrer que les polynômes $(X - \alpha_i)^{p_i}$ sont deux à deux premiers entre eux !

Remarque 21. Cela signifie en particulier que le degré du polynôme P est supérieur ou égal à la somme des ordres de multiplicité.

4 Dérivation, formule de Taylor

DÉFINITION 13 : **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 22.

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 $k = 0$.

Attention

La définition précédente est purement algébrique.
Elle ne correspond à la dérivée des fonctions polynômiales que lorsque le corps de base est le corps des réels.

PROPOSITION 27 : Soit $P \in \mathbb{K}[X]$. On a alors :

- $\deg(P') = \deg P - 1$ si $\deg P \geq 1$
- $\deg(P^{(k)}) = \deg P - k$ si $\deg P \geq k$
- $P^{(k)} = 0$ si $\deg P < k$

Preuve 27 : Petite récurrence sur k lorsque $k \leq \deg P$.
Pour le cas où $k > \deg P$, on s'intéresse au polynôme $P^{(\deg P)}$.

Remarque 23. ⚠ Avant d'appliquer les formules précédentes, pensez à vérifier que le degré de P est bien adapté.

`Exemple 15.` $(*)$ Résoudre les équations suivantes :

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

THÉORÈME 28 : **Dérivée d'une combinaison linéaire, d'un produit et d'une composée de polynômes**
Pour tout $P,\ Q \in \mathbb{K}[X]$ et $\lambda,\ \mu \in \mathbb{K}$, on a :

1. $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$
2. $(PQ)' = P'Q + PQ'$.
3. $(P \circ Q)' = P' \circ Q.P'$.

Preuve 28 : Compte-tenu de ce que l'on sait sur la dérivée d'un produit de fonctions réelles ou complexes, on remarque que pour tout $x \in \mathbb{R}$, on a :

$$(\lambda P + \mu Q)'(x) = \lambda P'(x) + \mu Q'(x) \quad \text{et} \quad (PQ)'(x) = P'(x)Q(x) + P(x)'Q(x)$$

Or, deux polynômes qui coincident en un nombre infini de valeurs sont donc égaux.

COROLLAIRE 29 : Si $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}^*$, alors : $\big(P^n\big)' = nP^{n-1}P'$

Preuve 29 : Par récurrence.

THÉORÈME 30 : **Formule de Leibniz**
Soient deux polynômes $(P,\ Q) \in \mathbb{K}[X]^2$. On a la formule suivante pour la dérivée du polynôme produit :

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

Preuve 30 : 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 $\mathcal{C}^n$.
On peut aussi vérifier la relation pour les fonctions polynômiales complexes à variable réelle associées et en déduire l'égalité des polynômes.

LEMME 31 : **Dérivées de** $(X-a)^n$
Soit $a \in \mathbb{K}$. On exprime pour $p \in \mathbb{N}$, la dérivée $p$ième du polynôme $(X-a)^n$:

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

Preuve 31 : Récurrence simple dans le cas où $p \leq n$. Le cas $p > n$ est alors immédiat.

THÉORÈME FONDAMENTAL 32 : **Formule de Taylor**
Soit un polynôme $P \in \mathbb{K}_n[X]$ et un scalaire $a \in \mathbb{K}$.
On obtient la décomposition du polynôme P sur la base $\mathcal{B} = \Big(1,\ (X-a),\ \ldots,\ (X-a)^n\Big)$ de $\mathbb{K}_n[X]$:

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

Preuve 32 :

1. On montre en considérant $Q = P \circ (X+a)$ que P peut s'écrire sous la forme :
   $P = a_0 + a_1(X-a) + \cdots + a_n(X-a)^n$.
2. En dérivant k fois le polynôme P, on vérifie facilement que $a_k = \frac{P^{(k)}(a)}{k!}$

On peut également montrer que les 2 polynômes coïncident en toutes les valeurs réelles.

Remarque 24.

1. La notion de *base* sera vue dans un prochain chapitre.
2. Vous avez je pense, reconnu la forme de la formule de Taylor-Young sans le $o(x^n)$... qui ici, n'aurait aucun sens !

Remarque 25. On dit alors que $(P(a),\ \frac{P'(a)}{1!},\ \ldots,\ \frac{P^{(n)}(a)}{n!})$ sont les coordonnées de P dans la base $\mathcal{B}$.
Cette décomposition est unique !

COROLLAIRE 33 : **Formule de Mac Laurin**
Soit un polynôme $P \in \mathbb{K}_n[X]$.

$$P(X) = P(0) + P'(0)X + \cdots + \frac{P^{(n)}(0)}{n!}X^n$$

`Exemple 16.` Déterminer sans calculs les valeurs de $P(0)$, $P'(0)$, $P''(0)$, et $P^{(3)}(0)$, lorsque $P = 1 - 2X + 5X^2 - 3X^3$.

Exercice : 9
(∗∗) Déterminer les polynômes $P \in \mathbb{R}[X]$ de degré n tels que $nP(X) = XP'(X) + 2P''(X)$.

COROLLAIRE 34 : **Reste de la division euclidienne de** P **par** $(X-a)^k$

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

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

Preuve 34 : Pas de difficulté en utilisant la formule de Taylor.

`Exemple 17.` $(*)$ Trouver le reste de la division euclidienne du polynôme $P = X^n + 1$ $(n \geq 3)$ par le polynôme $(X-1)^3$.

LEMME 35 : Soit $k,\ r \in \mathbb{N}$ avec $\begin{cases} k \geq 2 \\ r \leq k \end{cases}$ et $P \in \mathbb{K}[X]$.

1. Si a est racine multiple d'ordre k de P alors a est racine multiple d'ordre $k-1$ de P'.
2. Si a est racine multiple d'ordre k de P alors a est racine multiple d'ordre $k-r$ de $P^{(r)}$.

Preuve 35 : On calcule P' et on généralise par récurrence.

THÉORÈME FONDAMENTAL 36 : **Caractérisation des racines multiples d'ordre k**
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 $\iff P(\alpha) = P'(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0_{\mathbb{K}}$.
- le scalaire α est racine de P d'ordre k exactement $\iff \begin{cases} P(\alpha) = P'(\alpha) = \ldots = P^{(k-1)}(\alpha) = 0_{\mathbb{K}} \\ P^{(k)}(\alpha) \neq 0_{\mathbb{K}} \end{cases}$.

Preuve 36 :

1. Avec la formule de Taylor.
2. Par l'absurde !

`Exemple 18.` $(*)$ Pour tout $n \in \mathbb{N}^*$, justifier les divisibilités suivantes :

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

Remarque 26. Lorsque $P \in \mathbb{C}[X]$ est à coefficients réels, on vérifie facilement que :
α est racine multiple d'ordre r de P si et seulement si $\bar{\alpha}$ est racine multiple d'ordre r de P.

COROLLAIRE 37 : Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$.
On a alors :

1. P admet une racine multiple $\iff$ $\begin{cases} P(x) = 0 \\ P'(x) = 0 \end{cases}$ admet une solution dans $\mathbb{K}$
2. α est une racine multiple de P $\iff$ $\begin{cases} P(\alpha) = 0 \\ P'(\alpha) = 0 \end{cases}$

Preuve 37 : Pas de difficulté.

`Exemple 19.` $(*)$ Montrer que le polynôme $P = 1 + X + \dfrac{X^2}{2!} + \cdots + \dfrac{X^n}{n!}$ admet n racines complexes distinctes.

Exercice : 10
$(*)$ 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 14 : **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 27. 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 38 : **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 39 :

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 39 :

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

Exercice : 11
($*$) 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 29. 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 rationnelles.

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 3.

`Exemple 20.` 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 15 : **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* : $\boxed{\sigma_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} \alpha_{i_1} \ldots \alpha_{i_k}}$

Remarque 30. Ainsi, par définition, nous avons : $\begin{cases} \sigma_1 &= \alpha_1 + \cdots + \alpha_n \\ \sigma_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{p-1}\alpha_n \\ \sigma_3 &= \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \cdots + \alpha_{n-2}\alpha_{n-1}\alpha_n \\ & \ldots \\ \sigma_n &= \alpha_1 \ldots \alpha_n \end{cases}$

Remarque 31. Dans la formule, l'indice k de σ_k représente le nombre de racines dans chaque produit.

THÉORÈME FONDAMENTAL 40 : **Relations coefficients-racines**
Si on connaît un polynôme scindé P, alors on connaît les valeurs des fonctions symétriques de ses 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 $(\alpha_1,\ \alpha_2,\ \dots,\ \alpha_n) \in \mathbb{K}^n$.
On a alors :

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

Preuve 40 : $\alpha_1,\ \alpha_2,\ \dots,\ \alpha_n$ 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 32.
Pour retrouver les formules du théorème, on pourra identifier les coefficients dans les deux expressions de P :

$$\begin{array}{lcllllllll}
P(X) & = & a_n(X^n & + & \dfrac{a_{n-1}}{a_n}.X^{n-1} & + & \dfrac{a_{n-2}}{a_n}.X^{n-2} & + \cdots + & \dfrac{a_1}{a_n}.X & + & \dfrac{a_0}{a_n}) \\
P(X) & = & a_n(X^n & + & (-1)\sigma_1.X^{n-1} & + & (-1)^2\sigma_2.X^{n-2} & + \cdots + & (-1)^{n-1}\sigma_{n-1}.X & + & \sigma_n)
\end{array}$$

On reconnaît en particulier la formule : $P = a_2(X^2 - SX + P)$ où $S = \sigma_1$ et $P = \sigma_2$.

`Exemple 21.` 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 41 : **Relations coefficients-racines**
Soient $(\alpha_1,\ \alpha_2,\ \dots,\ \alpha_n) \in \mathbb{K}^n$.
Si on connaît les valeurs des fonctions symétriques correspondantes, on connaît alors un polynôme dont les α_k sont racines. Soit $(\lambda_1,\ \lambda_2,\ \dots,\ \lambda_n) \in \mathbb{K}^n$.
On a en effet l'équivalence suivante :

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

$$\Longleftrightarrow$$

$$\alpha_1,\ \alpha_2,\ \dots,\ \alpha_n \text{ sont racines de } P = X^n - \lambda_1 X^{n-1} + \lambda_2 X^{n-2} + \cdots + (-1)^{n-1}\lambda_{n-1}X + (-1)^n\lambda_n$$

Preuve 41 : C'est la démonstration du théorème précédent en utilisant des équivalences.

Remarque 33. On utilise le théorème précédent pour résoudre des systèmes dont les équations permettent de calculer les fonctions symétriques des inconnues.

Exercice : 12
(∗) Trouver $(a,\ b,\ c) \in \mathbb{C}^3$ tels que $\begin{cases} a+b+c=1 \\ a^2+b^2+c^2=3 \\ a^3+b^3+c^3=1 \end{cases}$.

Remarque 34. Comme le montre les 2 exercices suivants, 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.

Exercice : 13
(∗∗) 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.

Exercice : 14
(∗∗) 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 $x_1 + x_2 = -1$. Trouver alors ces 3 racines.

Remarque 35.

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 lorsque $\deg P \geq 5$! 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 : 15

$(*)$ Soit $P \in \mathbb{C}[X]$ défini par $P(X) = X^3 - 3X^2 - 10X + 24$, et $\alpha_1, \ \alpha_2, \ \alpha_3$ 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 : 16

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

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

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 $\mathbb{C}[X]$ et $\mathbb{R}[X]$

Définition 16 : **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 36.

1. En d'autres termes, on dira qu'un polynôme est réductible lorsqu'on peut le factoriser sous la forme d'un produit de deux polynômes de degré au moins 1.
2. Les seuls diviseurs des polynômes P irréductibles sont donc les polynômes constants non nuls et les polynômes non nuls proportionnels à P. Nous verrons que les polynômes irréductibles jouent un rôle analogue à celui des nombres premiers en arithmétique.

Lemme 42 : **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 42 : Par l'absurde en utilisant la fonction degré.

Remarque 37. Comme le montre les exemples suivants, la notion de *polynôme irréductible* dépend du corps de base.

`Exemple 22.` 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 43 : **Les polynômes irréductibles de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$**

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 43 :

1. C'est un corollaire immédiat du théorème de d'Alembert-Gauss.
2. Pas de problème pour les polynômes de degré 1.
   Le cas des polynômes de degré 2 se traite par exemple 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 38.

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 23.` $(*)$ 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 44 :

1. Deux polynômes irréductibles sont premiers entre eux ou égaux à une constante multiplicative près.
2. Si P_1, …, 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 44 :

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 $\begin{cases} A \ / \ C \\ B \ / \ C \\ A \wedge B = 1 \end{cases} \Rightarrow AB \ / \ C$.
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 39. 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 45 : **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 45 :

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 40. Cette décomposition s'appelle la *décomposition primaire* de P.

Proposition 46 : **Caractérisation de la divisibilité dans** $\mathbb{K}[X]$
Soient deux polynômes A et B avec B non nul et $A = \lambda.P_1^{\alpha_1} \times \cdots \times P_n^{\alpha_n}$ sa décomposition primaire. On a :

$$B \mid A \quad \Longleftrightarrow \quad B = \mu.P_1^{\beta_1} \times \cdots \times P_n^{\beta_n} \quad \text{avec} \begin{cases} \mu \in \mathbb{K} \\ \forall k \in [\![1, n]\!], 0 \leq \beta_k \leq \alpha_k \end{cases}$$

Preuve 46 : Démonstration analogue à la démonstration du critère de divisibilité dans $\mathbb{Z}$.

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

Théorème 47 : **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 47 : Corollaire du théorème de décomposition d'un polynôme en produit de polynômes irréductibles.

Proposition 48 : Soit $n \in \mathbb{N}^*$.
Dans $\mathbb{C}$ $[X]$, le polynôme $P = X^n - 1$ se décompose sous la forme :

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

Preuve 48 : Aucune difficulté en recherchant les racines de P.

`Exemple 24.` $(*)$ Factoriser $P = (X - 1)^n - (X + 1)^n$ en produit de facteurs irréductibles dans $\mathbb{C}[X]$.

Corollaire 49 : **Caractérisation de la divisibilité dans** $\mathbb{C}[X]$
Soient deux polynômes A et B avec B non nul. On a :

$B \mid A \quad \Longleftrightarrow \quad$ les racines de B sont des racines de A d'ordre de multiplicité inférieur

Preuve 49 : Aucune difficulté en utilisant l'unicité de la décomposition en produit de polynômes irréductibles.

Théorème 50 : **Décomposition dans** $\mathbb{R}[X]$

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

$$P = \lambda(X - \alpha_1) \dots (X - \alpha_p)(X^2 + p_1 X + q_1) \dots (X^2 + p_r X + q_r)$$

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

Preuve 50 : 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 et leur ordre de multiplicité.
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 : 17

($**$) 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 $\mathbb{R}[X]$.

7 Connaissez-vous votre cours ?

	Questions	Réponses attendues
1.	Quelle est la structure de l'ensemble des polynômes à coefficients dans $\mathbb{K}$?	anneau
2.	Soit $P = a_nX^n + \cdots + a_1x + a_0$ de degré n. Que doit-on préciser ?	$a_n \neq 0$
3.	Pourquoi n'a-t-on pas toujours $\deg(P+Q) = \max(\deg P,\ \deg Q)$?	cf cours
4.	Dans quel type de raisonnement utilise-t-on souvent la fonction "degré" ? Si le degré n'apporte rien, à quoi peut-on aussi s'intéresser ?	Analyse/synthèse au terme dominant
5.	Quelles propriétés intéressantes possède l'anneau des polynômes ?	Intègre et commutatif
7.	Quelle différence faites-vous entre $\left\{\begin{array}{l} A = P \circ (X^2+X-1) \\ B = P(X^2+X-1) \\ C = P(X).(X^2+X-1) \end{array}\right.$?	$A = B \neq C$
8.	Les formules suivantes sont-elles toujours vraies ? $\left\{\begin{array}{l} \deg PQ = \deg P + \deg Q\ (1) \\ \deg P \circ Q = \deg P \times \deg Q\ (2) \end{array}\right.$	$\left\{\begin{array}{l} \text{(1) est toujours vraie} \\ \text{(2) slt si } P \text{ et } Q \neq 0 \end{array}\right.$
9.	Sur quelles idées repose la démonstration de la division euclidienne de polynômes ?	cf cours
10.	Effectuer la division euclidienne de $P = X^4 - X^2 + 1$ par $Q = X^2 + X + 1$	$P = (X^2 - X - 1)Q + 2 + 2X$
11.	Rappeler les résultats principaux d'arithmétique des Polynômes.	cf cours
13.	Comment prouve-t-on qu'un nombre α est une racine d'un polynôme P ?	On mq $P(\alpha) = 0$
14.	Que dire du nombre de racines complexes d'un polynôme non nul ? En déduire une méthode pour prouver qu'un polynôme est nul.	cf cours
15.	Que dire d'un polynôme à coefficient réel ayant une racine $\alpha \in \mathbb{C}\backslash\mathbb{R}$?	$\bar{\alpha}$ est aussi racine
16.	Que savez-vous des polynômes de Lagrange ? Définition, existence, unicité ?	cf cours
18.	Dans quel cas peut-on affirmer que $\deg P^{(k)} = \deg P - k$?	si $\deg P \geq k$
19.	Rappelez la formule de Leibniz et la formule de Taylor pour les polynômes.	cf cours

20.	Donnez la dérivée $k$ème de $(X-a)^n$.	$\dfrac{n!}{(n-k)!}(X-a)^{n-k}$ si $n \geq k$
21.	Quel est le reste de la division euclidienne de P par $(X-a)^k$	cf cours (Taylor)
22.	Définir la notion d'ordre de multiplicité d'une racine. Quelle est la caractérisation usuelle des racines multiples ?	cf cours
23.	Quand dit-on qu'un polynôme est scindé ?	cf cours
24.	Que dit le théorème de d'Alembert ? Que peut-on en déduire ?	cf cours
25.	Donnez la formule qui définit la f° symétrique des racines σ_k. Comment calculer sa valeur lorsqu'on connaît le polynôme associé ?	cf cours
26.	Savez-vous exprimer $x^2+y^2+z^2$ et $\frac{1}{x}+\frac{1}{y}+\frac{1}{z}$ en fonction de σ_1, σ_2 et σ_3. Peut-on faire de même avec $\frac{1}{xy}+\frac{1}{yz}+\frac{1}{zx}$?	cf cours OUI
27.	Donner les valeurs de σ_1, σ_2, σ_3 et σ_4 pour $P = 2X^4 - X^2 + X - 6$	$\sigma_1 = 0$, $\sigma_2 = -\frac{1}{2}$ $\sigma_3 = -\frac{1}{2}$, $\sigma_4 = -3$
28.	Quels sont les polynômes irréductibles de $\mathbb{C}[X]$? De $\mathbb{R}[X]$?	cf cours
29.	Décomposez $P = X^4 + X^3 + 2X^2 + X + 1$ en produit de polyn. irred. dans $\mathbb{C}[X]$?	...
30.	Savez-vous décomposer $P = X^{2n} - 1$ en produit de polyn. irred. dans $\mathbb{C}[X]$?	cf cours

8 Exercices de TD

Codage :

1. Les exercices avec des coeurs ♡ sont à traiter en priorité.
2. Le nombre d'étoiles $*$ ou de coeurs ♡ correspond à la difficulté des exercices.

I] Calculs algébriques sur les Polynômes

Pour répondre aux questions suivantes, on pourra envisager de :

1. utiliser les formules usuelles dans un anneau
2. faire des conjectures que l'on peut valider par récurrence

Exercice de TD : 1

(♡) Montrer que pour tout naturel $n \in \mathbb{N}^*$, on a : $\displaystyle\sum_{k=0}^{n} \binom{n}{k} 3^k (1-X)^{3n-2k} X^k = (1-X^3)^n$

Exercice de TD : 2

($*$) Montrer que pour tout naturel $n \in \mathbb{N}$, on a : $(X^3 + X^2 + X + 1).\sum_{k=0}^{2n}(-1)^k X^k = X^{2n+3} + X^{2n+1} + X^2 + 1$

Exercice de TD : 3

($\heartsuit$) Soit $n \in \mathbb{N}^*$. Développer le polynôme : $P_n = (1+X)(1+X^2)(1+X^{2^2})\dots(1+X^{2^n})$.

Exercice de TD : 4

($\heartsuit$) Soit $n \in \mathbb{N}^*$. Factoriser $P_n = 1 + \frac{1}{1!}X + \frac{1}{2!}X(X+1) + \cdots + \frac{1}{n!}X(X+1)(X+2)\dots(X+(n-1))$.

II] Arithmétique des Polynômes

Les notions et propriétés d'arithmétique sur les polynômes sont analogues à celles sur les entiers. Les raisonnements sont donc également très semblables.

Exercice de TD : 5

($\heartsuit\heartsuit$) On souhaite déterminer le PGCD de $A = X^n - a^n$ et de $B = X^p - a^p$ lorsque $n,\ p \in \mathbb{N}^*$ et $a \in \mathbb{R}$.

1. Déterminer le reste de la division euclidienne de X^n par B.
2. En déduire le reste de la division euclidienne de A par B.
3. En déduire $A \wedge B$.

Exercice de TD : 6

($*$) Résoudre dans $(\mathbb{R}[X])^2$ l'équation $P(X+1) + Q(X+2) = (X+3)$.

Exercice de TD : 7

($**$) Idéal principal dans l'anneau des polynômes.

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 :

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

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

Exercice de TD : 8

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

Exercice de TD : 9

($\heartsuit\heartsuit$) Relation de Bezout.

1. Montrer qu'il existe un unique couple $(S,\ T) \in \mathbb{R}_5[X]$ tels que $(1-X)^6 S + X^6 R = 1$ (*).
2. Détermination de R et S :
   (a) Montrer que $S(x) + o(x^5) = \dfrac{1}{(1-x)^6}$ au voisinage de 0. En déduire S.
   (b) En composant (*) par $(1-X)$, déterminer T

III] Fonctions polynômiales - Racines d'un polynôme

Plusieurs théorèmes sont ici essentiels :

1. Le fait de pouvoir factoriser par $X - x_0$ un polynôme dont x_0 est racine.
2. La caractérisation des racines d'ordre p à l'aide des dérivées kième.
3. La caractérisation des racines multiples.
4. La formule de Taylor sur les polynômes.
5. La formule de Liebniz.

Exercice de TD : 10

($**$) Trouver tous les polynômes de $\mathbb{R}_3[X]$ divisible par $(X-1)$ ayant le même reste dans les divisions euclidiennes par $(X-2)$, $(X-3)$ et $(X-4)$.

Exercice de TD : 11

($\heartsuit\heartsuit$) Soit $n \in \mathbb{N}^*$.
Factoriser en produit de facteurs de degré 1, le polynôme $P = (X+i)^n - (X-i)^n$.

Exercice de TD : 12

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

Exercice de TD : 13

($\heartsuit\heartsuit$) 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 de TD : 14

($\heartsuit$) On considère le polynôme $P(X) = aX^{n+1} + bX^n + 1 \in \mathbb{C}[X]$ où l'entier n est strictement positif.
Trouver une CNS pour que $(X-1)^2$ divise P.

Exercice de TD : 15

($*$) Soit $a,\ b$ et c trois complexes non nuls et distincts et $P = \dfrac{X(X-b)(X-c)}{a(a-b)(a-c)} + \dfrac{X(X-c)(X-a)}{b(b-c)(b-a)} + \dfrac{X(X-a)(X-b)}{c(c-a)(c-b)}$.

Démontrer que P peut s'écrire sous la forme $P = \lambda.(X-a)(X-b)(X-c) + 1$ où λ est une constante à déterminer.

Exercice de TD : 16

($**$) Déterminer les polynômes non constants de $\mathbb{R}[X]$ tels que P' divise P.
Indication : Vous commencerez par étudier le degré, puis vous pourrez utiliser la formule de Liebniz.

Exercice de TD : 17

($\heartsuit\heartsuit\heartsuit$) **Polynômes de Legendre (1752-1833) :**

Pour tout entier naturel n on pose $L_n = \dfrac{n!}{(2n)!}\big((X^2-1)^n\big)^{(n)}$.

1. Montrer que L_n est un polynôme unitaire de degré n.
2. Montrer que $\forall Q \in \mathbb{R}_{n-1}[X]$, on a $\displaystyle\int_{-1}^{1} L_n(t)Q(t)\,\mathrm{d}t = 0$
3. En déduire que L_n possède n racines simples toutes dans $]-1,\ 1[$.
   Indication : Considérer $Q = (X-x_1)(X-x_2)\dots(X-x_p)$ où $x_1,\ \dots,\ x_p$ sont les racines d'ordre impair de L_n

Exercice de TD : 18

($**$) Trouver tous les polynômes $P \in \mathbb{R}[X]$ de degré 7 tels que $(X-1)^4$ divise $P+1$ et $(X+1)^4$ divise $P-1$.
Indication : On commencera pas s'intéresser à P'.

Exercice de TD : 19

($\heartsuit\heartsuit$) Prouver que $a = \sqrt{3} + \sqrt{2}$ est un nombre algébrique, c'est à dire qu'il est racine d'un polynôme à coefficients entiers.
Indication : Chercher un polynôme dont les racines sont $a = \sqrt{3} + \sqrt{2}$ et $b = \sqrt{3} - \sqrt{2}$.

Exercice de TD : 20

($***$) Prouver que si $(a_k) \in \mathbb{R}^{\mathbb{N}}$, alors pour tout entier $r \geq 1$, on a :

$$\sum_{n=1}^{r}\sum_{m=1}^{r} \frac{a_n a_m}{m+n} \geq 0$$

Aide : on pourra introduire des fonctions polynômiales bien choisies et procéder à une intégration entre 0 et 1.

IV] Relations coefficients-racines

1. Il faut impérativement savoir déterminer les valeurs des fonctions symétriques élémentaires des racines d'un polynôme donné.
2. Lorsque l'énoncé nous donne une information sur les racines, il est souvent pertinent de rechercher ses racines en exprimant le système obtenu à l'aide des valeurs des fonctions symétriques élémentaires des racines.
3. Rappelez-vous que toute fonction symétrique (des racines) peut s'exprimer en fonction des fonctions symétriques élémentaires (des racines).

Exercice de TD : 21

($\heartsuit\heartsuit$) Soit $\alpha \in \mathbb{R}$.

En utilisant les racines de $P = (X+1)^n - e^{2in\alpha}$, calculer $\displaystyle\prod_{k=0}^{n-1} \sin(\frac{k\pi}{n} + \alpha)$.

Exercice de TD : 22

($\heartsuit\heartsuit$) Soit $(E) : x^4 + ax^3 + bx^2 + cx + d = 0$.
Déterminer une CNS pour que (E) admette deux racines opposées l'une de l'autre.

Exercice de TD : 23

($**$) Soit $P \in \mathbb{C}[X]$ de la forme $P(X) = X^3 + pX + q$.

1. Déterminer une CNS pour que ce polynôme admettent dans $\mathbb{C}$ trois racines a, b et c telles que $a = bc$.
2. Application : $p = -2$ et $q = -1$.

Exercice de TD : 24

($\heartsuit\heartsuit$) Factoriser $P = X^5 - 4X^4 + 9X^3 - 21X^2 + 20X - 5$ sachant que 2 de ces racines ont un produit égal à 5 et qu'une des racines est évidente.

Exercice de TD : 25

($\heartsuit\heartsuit$) On veut montrer qu'il n'existe pas de réels, $u,\ v$ et w vérifiant : $\left\{\begin{array}{l} u+v+w=3 \\ uv+vw+wu=6 \end{array}\right.$.
On suppose que $u,\ v,\ w$ existent.

1. Montrer alors qu'elles sont forcément distinctes.
2. Trouver un polynômes dont $u,\ v,\ w$ sont les racines
3. En utilisant le théorème de Rolle, prouver que $u,\ v,\ w$ ne peuvent pas exister.

V] Décomposition d'un polynôme en produit de facteurs irréductibles

1. La technique consiste à déterminer les racines du polynômes.
2. Lorsqu'on souhaite une décomposition des $\mathbb{R}[X]$, il faut alors regrouper les facteurs correspondants aux racines conjuguées.
3. Attention à bien vérifier que le nombre de racines trouvées correspond au degré du polynômes. Si ce n'est pas le cas, certaines racines sont multiples...

Exercice de TD : 26

($\heartsuit\heartsuit\heartsuit$) Soit $a \in]0,\ \pi[$ et $n \in \mathbb{N}^*$.
Factoriser en produit de facteurs irréductibles dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$ le polynôme $P = X^{2n} - 2\cos 2aX^n + 1$.

Exercice de TD : 27

($\heartsuit\heartsuit$) Factoriser $P = (X-1)^n - (X+1)^n$ en produit de facteurs irréductibles dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$.

Exercice de TD : 28

($***$) Soit $P \in \mathbb{R}[X]$ tel que pour tout $x \in \mathbb{R}$, on a $P(x) \geq 0$.
Prouver qu'il existe deux polynômes $A,\ B \in \mathbb{R}[X]$ tels que $P = A^2 + B^2$.

On pourra commencer par décomposer P dans $\mathbb{C}[X]$ puis s'intéresser à l'ordre de multiplicité des racines réelles

VI] Equations fonctionnelles polynômiales

Dans ce type de questions, il est très conseillé de commencer par une analyse.
En particulier, on pourra s'intéresser :

1. au degré
2. au terme dominant
3. aux racines : si l'on connaît une racine a du polynôme, on peut le factoriser par $(X-a)$.

La synthèse terminée, n'oubliez pas de faire la réciproque.

Exercice de TD : 29

(♡♡♡) Soit P un polynôme non nul de $\mathbb{C}[X]$ vérifiant la relation : $P(X^2)+P(X).P(X+1)=0$.

1. Montrer que si a est racine alors a^2 l'est aussi. Déterminer alors le module de a.
2. Montrer que si a est racine alors $(a-1)^2$ l'est aussi. Déterminer alors les racines possibles.
3. Montrer que seules 0 et 1 peuvent être racines. En déduire les polynômes P qui conviennent.

Exercice de TD : 30

(♡♡♡) Trouver tous les polynômes de $\mathbb{C}[X]$ vérifiant : $(X+3)P(X)=XP(X+1)$.