Chapitre 16

Polynômes

Objectifs

- Définir la notion de polynômes, étudier la structure de $\mathbb{K}[X]$.
- Définir la notion de degré d'un polynôme et étudier l'algorithme de la division euclidienne.
- Définir la notion de substitution dans un polynôme. Aborder la notion de racine, de polynômes scindés et le théorème de *D'Alembert*.
- Établir la formule de TAYLOR.

Sommaire

Dans tout ce chapitre, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$.

I) Définition d'un polynôme

1) Définition

DÉFINITION 16.1

On appelle polynôme à coefficients dans $\mathbb{K}$ toute suite d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang. Les termes d'une telle suite sont appelés : coefficients du polynôme, et la suite nulle est appelée polynôme nul. Si tous les termes sont nuls sauf un, le polynôme est appelé monôme. Si tous les termes sont nuls à partir de l'indice 1, on dit que le polynôme est constant.

L'ensemble des polynômes à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$, on a donc :

$$\mathbb{K}[X] = \{(u_n) \in \mathscr{F}(\mathbb{N},\mathbb{K}) \ / \ \exists\, N \in \mathbb{N}, n \geqslant N \Longrightarrow u_n = 0\}.$$

Deux polynômes sont égaux si et seulement si ils ont les mêmes coefficients (égalité de deux suites).

Polynômes particuliers :

a) Pour $k \in \mathbb{N}$, on note δ_k le polynôme défini par $\delta_k = (\delta_{k,n})$ où $\delta_{k,n} = \begin{cases} 1 & \text{si } n = k \\ 0 & \text{sinon} \end{cases}$ (symbole de *Krönecker* [1]). Par exemple, on a : $\delta_0 = (1,0,\ldots), \delta_1 = (0,1,0,\ldots)$.

b) On pose $X = \delta_1$, ce polynôme est appelé indéterminée de $\mathbb{K}[X]$, il peut être nommé par une autre lettre : $Y, Z, T, U, \ldots$, mais il s'agit toujours du polynôme δ_1.

2) Opérations sur les polynômes

Soient $P = (a_n)$ et $Q = (b_n)$ deux polynômes. Il existe deux entiers N et N' tels que : $n \geqslant N \Longrightarrow a_n = 0$, et $n \geqslant N' \Longrightarrow b_n = 0$, par conséquent si $n \geqslant \max(N, N')$, alors $a_n + b_n = 0$. Si $\lambda \in \mathbb{K}$, alors $n \geqslant N \Longrightarrow \lambda a_n = 0$.

DÉFINITION 16.2 (Somme et produit par un scalaire)

On pose : $P + Q = (a_n + b_n)$ (somme des deux suites), et pour $\lambda \in \mathbb{K}$, on pose $\lambda.P = (\lambda a_n)$. On définit ainsi une addition interne dans $\mathbb{K}[X]$ et un produit par les scalaires.

Propriétés : On a en fait repris l'addition de $\mathscr{F}(\mathbb{N},\mathbb{K})$ et le produit par un scalaire, on sait que pour ces opérations $\mathscr{F}(\mathbb{N},\mathbb{K})$ est un $\mathbb{K}$-e.v., or $\mathbb{K}[X] \subset \mathscr{F}(\mathbb{N},\mathbb{K})$, et la suite nulle est un polynôme, on en déduit que : $(\mathbb{K}[X], +, .)$ est un $\mathbb{K}$-e.v..

Avec les notations précédentes, pour $n \in \mathbb{N}$, on pose $c_n = \sum\limits_{k=0}^{n} a_k b_{n-k}$, si $n \geqslant N + N' - 1$, alors il est facile de voir que pour toute valeur de k dans $[\![0..n]\!]$, le produit $a_k b_{n-k}$ est nul, et donc c_n est nul. La suite (c_n) ainsi définie est donc un polynôme.

DÉFINITION 16.3 (Produit de deux polynômes)

On pose $P \times Q = (c_n)$ où la suite (c_n) est définie par : $c_n = \sum\limits_{k=0}^{n} a_k b_{n-k}$. On définit ainsi une multiplication interne dans $\mathbb{K}[X]$.

Remarques:
- Nous n'avons pas repris la multiplication des suites habituelle, nous verrons plus loin que l'intérêt de cette multiplication réside essentiellement dans le fait que le polynôme δ_k est égal à X^k (où $X = \delta_1$).
- Il y a d'autres expressions pour c_n : $c_n = \sum\limits_{k=0}^{n} a_{n-k} b_k = \sum\limits_{p+q=n} a_p b_q$.

Propriétés : on vérifie que cette multiplication :
- est commutative,
- est associative,
- possède un élément neutre qui est le polynôme δ_0,
- est distributive sur l'addition.

Par conséquent : $(\mathbb{K}[X], +, \times)$est un anneau.

On a également : $\forall P, Q \in \mathbb{K}[X], \forall \lambda \in \mathbb{K},\ \lambda.(P \times Q) = (\lambda.P) \times Q = P \times (\lambda.Q)$.

3) Écriture définitive des polynômes

Soit $P = (a_n)$ un polynôme, il existe un entier N tel que $n > N \Longrightarrow a_n = 0$, on peut donc écrire $P = (a_0, a_1, \ldots, a_N, 0, \ldots)$, ou encore, compte tenu de la définition de l'addition, $P = (a_0, 0, \ldots) + (0, a_1, 0, \ldots) +$

1. KRÖNECKER LEOPOLD (1823 – 1891) : mathématicien polonais qui a travaillé (entre autre) sur les équations algébriques.

$\cdots + (0,\ldots,0,a_N,0,\ldots)$, mais compte tenu de la définition du produit par un scalaire, on a encore $P = a_0\delta_0 + a_1\delta_1 + \cdots + a_N\delta_N$, c'est à dire : $P = \sum_{k=0}^{N} a_k\delta_k$.

Proposition : Pour $k \in \mathbb{N}$, on a $\delta_k = X^k$ où $X^k = \begin{cases} \delta_0 & \text{si } k = 0 \\ X \times X^{k-1} & \text{si } k \geqslant 1 \end{cases}$.

Preuve: Par récurrence sur k, pour $k = 0$ il n'y a rien à démontrer, supposons le résultat démontré pour un entier k, $X^{k+1} = X \times X^k = \delta_1 \times \delta_k = (c_n)$ où $c_n = \sum_{p=0}^{n} \delta_{1,p}\delta_{k,n-p} = \delta_{k,n-1} = \delta_{k+1,n}$, on en déduit que $X^{k+1} = \delta_{k+1}$ (égalité des coefficients). □

En reprenant les notations précédentes, on a ainsi l'écriture définitive des polynômes : $P = \sum_{k=0}^{N} a_kX^k$. Ce que l'on écrit parfois plus simplement : $P = \sum_{k\in\mathbb{N}} a_kX^k$, étant entendu qu'il s'agit là d'une somme finie puisque les coefficients sont nuls à partir d'un certain rang.

Plongement de $\mathbb{K}$ dans $\mathbb{K}[X]$: L'application $\phi : \mathbb{K} \to \mathbb{K}[X]$ définie par $\phi(\lambda) = \lambda.\delta_0 = (\lambda,0,\ldots)$, est une application injective qui vérifie pour $\lambda,\mu \in \mathbb{K}$:

- $\phi(\lambda+\mu) = \phi(\lambda)+\phi(\mu)$
- $\phi(\lambda\mu) = \phi(\lambda)\phi(\mu)$
- $\phi(1) = \delta_0$ $(=1_{\mathbb{K}[X]})$.

Par conséquent, chaque polynôme constant $(\lambda,0,\ldots)$ peut être identifié avec le scalaire λ, autrement dit, on pose $\lambda = (\lambda,0,\ldots)$. En particulier, le polynôme nul est noté simplement 0, et le polynôme δ_0 est simplement noté 1. On peut donc considérer désormais : $\mathbb{K} \subset \mathbb{K}[X]$, $\mathbb{K}$ étant l'ensemble des polynômes constants.

Finalement : si $P = (a_n) = (a_0,\ldots,a_N,0,\ldots)$, alors : $P = \sum_{k=0}^{N} a_kX^k = a_0 + a_1X + \cdots + a_NX^N$, et :

$$\sum_{n\in\mathbb{N}} a_nX^n = \sum_{n\in\mathbb{N}} b_nX^n \iff \forall\, n\in\mathbb{N}, a_n = b_n.$$

$$(\sum_{n\in\mathbb{N}} a_nX^n) + (\sum_{n\in\mathbb{N}} b_nX^n) = \sum_{n\in\mathbb{N}} (a_n+b_n)X^n.$$

$$(\sum_{n\in\mathbb{N}} a_nX^n) \times (\sum_{n\in\mathbb{N}} b_nX^n) = \sum_{n\in\mathbb{N}} \left(\sum_{p+q=n} a_pb_q\right)X^n.$$

$$\sum_{n\in\mathbb{N}} a_nX^n \in \mathbb{K} \iff \forall\, n \geqslant 1, a_n = 0.$$

II) Division euclidienne

1) Degré d'un polynôme

Soit $P \in \mathbb{K}[X]$, si $P = 0$ alors tous les coefficients de P sont nuls, si $P \neq 0$, alors l'ensemble des indices des coefficients non nuls de P n'est pas vide, et il est majoré (les coefficients sont nuls à partir d'un certain rang), donc cet ensemble admet un plus grand élément.

DÉFINITION 16.4

Soit $P \in \mathbb{K}[X]$, si $P = 0$ alors on pose $\deg(P) = -\infty$, *sinon on pose* $\deg(P) = \max\{k \in \mathbb{N} \;/\; a_k \neq 0\}$. *Si P est non nul de degré n, alors le coefficient a_n est appelé coefficient dominant de P, si ce coefficient vaut 1, alors on dit que le polynôme P est unitaire (ou normalisé).*

Caractérisations du polynôme nul et des polynômes constants non nuls

- $P = 0 \iff \deg(P) = -\infty$.
- $P \in \mathbb{K}^* \iff \deg(P) = 0$.

THÉORÈME 16.1

Soient $P, Q \in \mathbb{K}[X]$, $\deg(P+Q) \leqslant \max(\deg(P), \deg(Q))$, *et* $\deg(P \times Q) = \deg(P) + \deg(Q)$.

Preuve: Si l'un des deux polynômes est nul, alors le théorème est évident. Supposons les deux polynômes non nuls : $P = \sum\limits_n a_n X^n$ et $Q = \sum\limits_n b_n X^n$, si $a_n + b_n \neq 0$ alors $a_n \neq 0$ ou $b_n \neq 0$, donc $n \leqslant \deg(P)$ ou $n \leqslant \deg(Q)$ *i.e.* $n \leqslant \max(\deg(P), \deg(Q))$, ce qui prouve le premier résultat.

$P \times Q = \sum\limits_n c_n X^n$ où $c_n = \sum\limits_{p+q=n} a_p b_q$. Posons $N = \deg(P)$ et $N' = \deg(Q)$, il est clair que $c_{N+N'} = a_N b_{N'} \neq 0$, d'autre part si $n > N + N'$, alors si $p + q = n$ on a $p > N$ ou $q > N'$ donc $a_p b_q = 0$ ce qui entraîne $c_n = 0$. Par conséquent, $\deg(P \times Q) = N + N' = \deg(P) + \deg(Q)$. □

Lorsque P et Q ont des degrés distincts, ou bien lorsque P et Q ont même degré mais des coefficients dominants non opposés, alors $\deg(P+Q) = \max(\deg(P), \deg(Q))$.

THÉORÈME 16.2

L'anneau $(\mathbb{K}[X], +, \times)$ *est un anneau intègre. Le groupe des inversibles est* $\mathbb{K}^*$ *l'ensemble des polynômes constants non nuls.*

Preuve: Si P et Q sont deux polynômes non nuls, alors $\deg(P \times Q) = \deg(P) + \deg(Q) \in \mathbb{N}$, donc $P \times Q \neq 0$, ce qui prouve que $\mathbb{K}[X]$ est intègre.

Si P est inversible dans $\mathbb{K}[X]$, alors il existe un polynôme Q tel que $P \times Q = 1$, d'où $\deg(P) + \deg(Q) = 0$, ce qui entraîne $\deg(P) = \deg(Q) = 0$ et donc $P \in \mathbb{K}^*$. La réciproque est évidente. □

Notation : Soit $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n :

$$\mathbb{K}_n[X] = \{P \in \mathbb{K}[X] \;/\; \deg(P) \leqslant n\}$$

Il est facile de vérifier que $\mathbb{K}_n[X] = \mathrm{Vect}\,[1, X, \ldots, X^n]$, c'est donc un s.e.v. de $\mathbb{K}[X]$.

2) Algorithme de la division euclidienne

THÉORÈME 16.3 (de la division euclidienne)

Soient A et B deux polynômes avec $B \neq 0$, alors il existe deux polynômes Q et R ***uniques*** *tels que :*

$$A = B \times Q + R \text{ avec } \deg(R) < \deg(B)$$

Preuve: Pour l'existence : si $\deg(A) < \deg(B)$, alors on peut prendre $Q = 0$ et $R = A$; si $\deg(A) = \deg(B) = d$: soit a_d le coefficient dominant de A, et b_d celui de B, posons $Q = \frac{a_d}{b_d}$, alors le coefficient dominant de $B \times Q$ est a_d, donc $\deg(A - B \times Q) < d = \deg(B)$, on peut donc prendre $R = A - B \times Q$. Supposons maintenant l'existence démontrée pour $\deg(A) \leqslant n$ avec $n \geqslant d$, et soit A de degré $n+1$, notons a_{n+1} son coefficient dominant, soit $Q' = \frac{a_{n+1}}{b_d} X^{n+1-d}$, alors $\deg(B \times Q') = n+1$ et le coefficient dominant de $B \times Q'$ est a_{n+1}, donc $\deg(A - B \times Q') \leqslant n$, d'après l'hypothèse de récurrence, il existe deux polynômes Q'' et R tels que $A - B \times Q' = B \times Q" + R$ avec $\deg(R) < \deg(B)$, mais alors $A = B \times (Q' + Q'') + R$, ce qui prouve l'existence au rang $n+1$.

Pour l'unicité : supposons que $A = B \times Q + R = B \times Q' + R'$ avec $\deg(R) < \deg(B)$ et $\deg(R') < \deg(B)$, alors $B \times (Q - Q') = R' - R$, d'où $\deg(B) + \deg(Q - Q') = \deg(R' - R) < \deg(B)$, comme $\deg(B) \geqslant 0$, on a nécessairement $\deg(Q - Q') = -\infty = \deg(R' - R)$, et donc $Q = Q', R = R'$. □

La démonstration est constructive, en ce sens qu'elle donne un algorithme de calcul du quotient (Q) et du reste (R).

Exemple: Avec $A = X^4 + aX^2 + bX + c$ et $B = X^2 + X + 1$, on obtient le quotient $Q = X^2 - X + a$ et le reste $R = (b - a + 1)X + c - a$. On peut vérifier que $A = B \times (X^2 - X + a) + (b - a + 1)X + c - a$.

3) Divisibilité

Définition 16.5

Soient $A,B \in \mathbb{K}[X]$, on dit que B divise A lorsqu'il existe un polynôme Q tel que $A = Q \times B$, notation $B|A$.

Remarque: On définit ainsi une relation dans $\mathbb{K}[X]$, on peut vérifier que celle - ci est réflexive, transitive, mais elle n'est ni symétrique, ni antisymétrique. Plus précisément, $B|A$ et $A|B$ ssi il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$ (on dit que A et B sont **associés**).

Théorème 16.4

- *Si $B \neq 0$, alors $B|A$ ssi le reste de la division euclidienne de A par B est nul.*
- *Si $A \neq 0$ et $B|A$, alors $\deg(B) \leqslant \deg(A)$.*
- *Si $B|A$ et $B|C$, alors $\forall\, U,V \in \mathbb{K}[X], B|A \times U + C \times V$.*

Preuve: Celle - ci est simple et laissée en exercice. □

Remarque: Il découle du dernier point que si $B|A-C$ et $B|D-E$, alors $B|(A+D)-(C+E)$ et $B|AD-EC$, en particulier, si $B|A-C$ alors $\forall\, n \in \mathbb{N}, B|A^n - C^n$.

III) Fonctions polynomiales, racines

1) Substitution

Théorème 16.5

Soit $\mathscr{A}$ une $\mathbb{K}$-algèbre et soit $a \in \mathscr{A}$, l'application : $S_a : \begin{array}{ccc} \mathbb{K}[X] & \to & \mathscr{A} \\ \sum\limits_{k=0}^{n} \alpha_k X^k & \mapsto & \sum\limits_{k=0}^{n} \alpha_k a^k \end{array}$, est un morphisme de $\mathbb{K}$-algèbres, c'est à dire : $\forall\, P,Q \in \mathbb{K}[X], \forall\, \lambda \in \mathbb{K}$

- $S_a(P+Q) = S_a(P) + S_a(Q)$.
- $S_a(P \times Q) = S_a(P) \times S_a(Q)$.
- $S_a(\lambda P) = \lambda S_a(P)$.
- $S_a(1) = 1$.

Preuve: Celle - ci repose sur les règles de calculs dans une algèbre. □

Remarque: L'application S_a est appelée substitution par a. Concrètement, le théorème ci - dessus dit que la substitution par a consiste simplement à remplacer l'indéterminée X par a. Par exemple, si on a $P = Q \times B + R$, alors $S_a(P) = S_a(Q) \times S_a(B) + S_a(R)$.

2) Fonctions polynomiales

Définition 16.6

L'application : $\widetilde{P} : \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & S_x(P) \end{array}$, est appelée fonction polynomiale associée au polynôme P. Si $P = \sum\limits_{k=0}^{n} a_k X^k$, alors $\widetilde{P} : x \mapsto \sum\limits_{k=0}^{n} a_k x^k$ où x est une variable qui décrit $\mathbb{K}$.

On prendra garde à ne pas confondre la variable x, qui est un élément de $\mathbb{K}$, avec l'indéterminée X (qui n'appartient pas à $\mathbb{K}$).

Remarque: On a $\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}$, $\widetilde{P \times Q} = \widetilde{P} \times \widetilde{Q}$, $\widetilde{\lambda.P} = \lambda.\widetilde{P}$.

3) Racines d'un polynôme

DÉFINITION 16.7

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$, on appelle racine de P dans $\mathbb{K}$ tout élément $a \in \mathbb{K}$ tel que $\widetilde{P}(a) = 0$, c'est à dire toute solution dans $\mathbb{K}$ à l'équation $\sum_{k=0}^{n} a_k x^k = 0$.

THÉORÈME 16.6

Soit $P \in \mathbb{K}[X]$:
- *Soit $a \in \mathbb{K}$, a est racine de P ssi $X - a | P$.*
- *Si $\deg(P) \leqslant n$ et si P admet au moins $(n+1)$ racines dans $\mathbb{K}$, alors $P = 0$.*

Preuve: Soit $a \in \mathbb{K}$, on effectue la division euclidienne de P par $X - a$: $P = Q \times (X - a) + R$ avec $\deg(R) < 1$, donc R est un polynôme constant $R = \lambda$, finalement $P = Q \times (X - a) + \lambda$. Substituons a à X : $\widetilde{P}(a) = \widetilde{Q}(a) \times (a - a) + \lambda$, c'est à dire : $\lambda = \widetilde{P}(a)$, ce qui prouve la première assertion.

La deuxième assertion se démontre par récurrence sur n : pour $n = 0$, l'hypothèse dit que P est une constante et que P a au moins une racine, donc cette constante est nulle, *i.e.* $P = 0$. Supposons le résultat démontré au rang n, et soit $\deg(P) \leqslant n + 1$ avec P ayant au moins $n + 2$ racines, soit a l'une d'elles, alors il existe $Q \in \mathbb{K}[X]$, tel que $P = Q \times (X - a)$, mais alors $\deg(Q) \leqslant n$ et Q a au moins $n + 1$ racines dans $\mathbb{K}$, donc $Q = 0$ (HR) et par conséquent, $P = 0$ □

Conséquences :

a) Si $a_1, \ldots, a_n$ sont des racines distinctes de P alors $(X - a_1) \cdots (X - a_n) | P$.

b) Si P est non nul de degré n, alors P admet au plus n racines distinctes.

c) L'application $\phi : \mathbb{K}[X] \to \mathscr{F}(\mathbb{K}, \mathbb{K})$ définie par $\phi(P) = \widetilde{P}$ est injective. On pourrait donc identifier P et $\widetilde{P}$ la fonction polynomiale associée à P.

Exercice: Soit P un polynôme de degré 2, on pose :

$$Q = (1 - X^2)\widetilde{P}(0) + \frac{X(X-1)}{2}\widetilde{P}(-1) + \frac{X(X+1)}{2}\widetilde{P}(1).$$

Montrer que $P = Q$.

Pour montrer qu'un polynôme P est nul on dispose de trois méthodes :
- *Montrer que tous les coefficients de P sont nuls.*
- *Montrer que le degré de P est $-\infty$.*
- *Montrer que P a une infinité de racines.*

Soit P un polynôme non nul et soit $a \in \mathbb{K}$, on sait que que si $(X - a)^k | P$ alors $k \leqslant \deg(P)$ (car $P \neq 0$). Par conséquent l'ensemble $\{k \in \mathbb{N} \ / \ (X - a)^k | P\}$ est un ensemble non vide (contient 0) et majoré par $\deg(P)$, comme c'est une partie de $\mathbb{N}$, cet ensemble admet un plus grand élément.

DÉFINITION 16.8 (multiplicité d'une racine)

Soit $P \in \mathbb{K}[X]$ un polynôme non nul et soit $a \in \mathbb{K}$, on appelle multiplicité de a dans P le plus grand des entiers k tels que $(X - a)^k | P$. Notation : $m_P(a)$. Une racine de multiplicité 1 est appelée racine simple, une racine de multiplicité 2 est appelée racine double...etc

Remarques:
- a est racine de P équivaut à $m_P(a) \geqslant 1$.
- Il est facile de vérifier que si $q \in \{k \in \mathbb{N} \ / \ (X - a)^k | P\}$, alors tout entier inférieur ou égal à q est également dans l'ensemble, cela signifie que l'ensemble $\{k \in \mathbb{N} \ / \ (X - a)^k | P\}$ est un intervalle d'entiers, on peut donc énoncer :

$$m = m_P(a) \iff (X - a)^m \text{ divise } P \text{ et } (X - a)^{m+1} \text{ ne divise pas } P.$$

Exercice: Calculer la multiplicité de 1 dans les polynômes $P = X^3 - 3X^2 + 2$ et $Q = X^3 - 4X^2 + 5X - 2$.

THÉORÈME 16.7

Soit P un polynôme non nul, soit $a \in \mathbb{K}$, et soit $m \in \mathbb{N}$, on a alors :

$$m = m_P(a) \iff \exists\, Q \in \mathbb{K}[X], P = (X-a)^m \times Q \text{ et } \widetilde{Q}(a) \neq 0.$$

Preuve: Si on a $P = (X-a)^m \times Q$ et $\widetilde{Q}(a) \neq 0$, alors $m_P(a) \geqslant m$, mais si $(X-a)^{m+1}|P$, il est facile de voir que $X-a|Q$ ce qui est absurde, donc $m_P(a) = m$.

Réciproquement, si $m = m_P(a)$, alors il existe Q tel que $P = (X-a)^m \times Q$, si $\widetilde{Q}(a) = 0$ alors $X-a|Q$ et donc $(X-a)^{m+1}|P$ ce qui contradictoire, donc $\widetilde{Q}(a) \neq 0$. □

THÉORÈME 16.8

Soient $P, Q \in \mathbb{K}[X]$, non nuls, et $a \in \mathbb{K}$

a) $m_{P\times Q}(a) = m_P(a) + m_Q(a)$.

b) *si $P+Q \neq 0$, alors $m_{P+Q}(a) \geqslant \min(m_P(a); m_Q(a))$.*

Preuve: Laissée en exercice. □

4) Corps algébriquement clos

Soit P un polynôme non nul ayant des racines dans $\mathbb{K}$, soient $a_1, \ldots, a_n$ **toutes** les racines distinctes de P de multiplicités respectives : $m_1, \ldots, m_n$. D'après ce qui précède il existe un polynôme Q tel que $P = (X-a_1)^{m_1} \times Q$ avec $\widetilde{Q}(a_1) \neq 0$, comme $a_2 \neq a_1$ on peut affirmer que a_2 est racine de Q : $Q = (X-a_2)^m \times T$ avec $\widetilde{T}(a_2) \neq 0$, mais alors $P = (X-a_2)^m \times (X-a_1)^{m_1} \times T$, on en déduit que $m = m_2$, par conséquent on a $P = (X-a_1)^{m_1}(X-a_2)^{m_2} \times T$ avec a_1 et a_2 qui ne sont pas racines de T. De proche en proche (récurrence sur n) on a arrive à : il existe un polynôme S tel que

$$P = (X-a_1)^{m_1} \cdots (X-a_n)^{m_n} \times S,$$

avec $a_1, \ldots, a_n$ qui ne sont pas racines de S, mais comme P n'a pas d'autres racines on peut en déduire que S est **sans racine** dans $\mathbb{K}$.

THÉORÈME 16.9 (factorisation d'un polynôme connaissant toutes ses racines)

Si $a_1, \ldots, a_n$ sont les racines distinctes de P de multiplicités respectives $m_1, \ldots, m_n$, alors il existe un polynôme Q sans racine dans $\mathbb{K}$ tel que : $P = Q \times \prod_{k=1}^{n} (X-a_k)^{m_k}$.

DÉFINITION 16.9 (polynôme scindé)

*Si $a_1, \ldots, a_n$ sont les racines distinctes de P de multiplicités respectives $m_1, \ldots, m_n$, alors d'après le théorème précédent : $\sum_{k=1}^{n} m_k \leqslant \deg(P)$. La quantité : $\sum_{k=1}^{n} m_k$ (somme des multiplicités des racines) est appelée **nombre de racines de P comptées avec leur multiplicité**. On dira que le polynôme P est scindé sur $\mathbb{K}$ lorsque cette quantité est égale au degré de P, on dit aussi que P admet toutes ses racines dans $\mathbb{K}$ (toutes : signifie que le nombre de racines comptées avec leur multiplicité, est égal au degré)*

En reprenant la factorisation précédente : $P = Q \times \prod_{k=1}^{n} (X-a_k)^{m_k}$, on voit que lorsque P est scindé, alors $\deg(Q) = 0$, le polynôme Q est donc une constante non nulle, en comparant les coefficients dominants de chaque coté, on voit que Q est égal au coefficient dominant de P, d'où l'énoncé :

THÉORÈME 16.10

Si P est scindé et si $a_1, \ldots, a_n$ sont les racines distinctes de P de multiplicités respectives $m_1, \ldots, m_n$, alors : $P = \lambda \prod_{k=1}^{n} (X-a_k)^{m_k}$, où λ est le coefficient dominant de P.

Exemples:
- $X^2 - 2$ est scindé sur $\mathbb{R}$, mais pas sur $\mathbb{Q}$.
- $X^2 + 1$ est scindé sur $\mathbb{C}$, mais pas sur $\mathbb{R}$.

DÉFINITION 16.10
On dit que le corps $\mathbb{K}$ est algébriquement clos lorsque tout polynôme non constant de $\mathbb{K}[X]$ admet au moins une racine dans $\mathbb{K}$.

D'après les exemples précédents, les corps $\mathbb{Q}$ et $\mathbb{R}$ ne sont pas algébriquement clos.

THÉORÈME 16.11
Si $\mathbb{K}$ est un corps algébriquement clos, alors tout polynôme non constant de $\mathbb{K}[X]$ est scindé sur $\mathbb{K}$.

Preuve: On montre par récurrence sur n que si $\deg(P) = n$ alors P admet n racines dans $\mathbb{K}$. Pour $n = 1$, $P = aX + b = a(X + b/a)$, une racine $-b/a$. Supposons le résultat démontré au rang n, et soit P de degré $n+1$: P est non constant, donc P admet au moins une racine a, d'où $P = (X - a) \times Q$, mais $\deg(Q) = n$, il suffit alors d'appliquer l'hypothèse de récurrence à Q pour terminer. □

THÉORÈME 16.12 (de D'Alembert [2])
$\mathbb{C}$ est un corps algébriquement clos.

Exemples:
- Factoriser $X^{2n} - 1$ dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$.

$$\begin{aligned}
X^{2n} - 1 &= \prod_{k=0}^{2n-1} (X - \exp(ik\frac{\pi}{n})) \\
&= (X-1)(X+1)\prod_{k=1}^{n-1}(X - \exp(ik\frac{\pi}{n}))(X - \exp(-ik\frac{\pi}{n})) \\
&= (X-1)(X+1)\prod_{k=1}^{n-1}(X^2 - 2\cos(k\frac{\pi}{n})X + 1).
\end{aligned}$$

- Factoriser dans $\mathbb{R}[X]$: $X^4 + X^2 + 1$ et $X^4 + X^2 - 1$.

$$\begin{aligned}
X^4 + X^2 + 1 &= (X^2+1)^2 - X^2 = (X^2 - X + 1)(X^2 + X + 1) \\
X^4 + X^2 - 1 &= (X^2 + \frac{1}{2})^2 - \frac{5}{4} = (X^2 + \frac{1+\sqrt{5}}{2})(X^2 - \frac{\sqrt{5}-1}{2}) \\
&= (X^2 + \frac{1+\sqrt{5}}{2})(X - \sqrt{\frac{\sqrt{5}-1}{2}})(X + \sqrt{\frac{\sqrt{5}-1}{2}})
\end{aligned}$$

5) Relations racines coefficients

Soit P un polynôme scindé sur $\mathbb{K}$, si $\deg(P) = n$ et si λ est le coefficient dominant de P, alors il existe $a_1, \ldots, a_n \in \mathbb{K}$ (racines de P) tels que $P = \lambda(X - a_1)\cdots(X - a_n)$, si on développe ensuite cette expression, on va obtenir les coefficients de P en fonction des a_k. Par exemple :
- $P = \lambda(X - a_1)(X - a_2) = \lambda X^2 - \lambda(a_1 + a_2)X + \lambda a_1 a_2$.
- $P = \lambda(X - a_1)(X - a_2)(X - a_3) = \lambda X^3 - \lambda(a_1 + a_2 + a_3)X^2 + \lambda(a_1a_2 + a_1a_3 + a_2a_3)X - \lambda a_1a_2a_3$.

Notation : On pose $\sigma_0 = 1$, et pour k compris entre 1 et n : $\sigma_k = \sum\limits_{1 \leqslant i_1 < \cdots < i_k \leqslant n} a_{i_1} \cdots a_{i_k}$.

σ_k est la somme des produits des racines (de P) par paquets de longueur k, par exemple : σ_1 est la somme des racines, σ_2 est la somme des produits deux à deux, $\cdots$, σ_n est le produit des racines.

Par récurrence on peut alors établir que :

2. D'ALEMBERT JEAN Le Rond (1717 – 1783) : mathématicien français qui contribua notamment à l'étude des nombres complexes, l'analyse et les probabilités.

$$(X-a_1)\cdots(X-a_n)=X^n-\sigma_1X^{n-1}+\sigma_2X^{n-2}-\cdots+(-1)^n\sigma_n=\sum_{k=0}^{n}(-1)^k\sigma_kX^{n-k}$$

On en déduit :

THÉORÈME 16.13

Soient $a_1,\ldots,a_n\in\mathbb{K}$, si $P=\sum\limits_{k=0}^{n}\alpha_kX^k=\alpha_n(X-a_1)\cdots(X-a_n)$, alors on a les relations racines - coefficients suivantes :

$$\alpha_{n-k}=(-1)^k\alpha_n\sigma_k,$$

En particulier, la somme des racines est $-\frac{\alpha_{n-1}}{\alpha_n}$ et le produit des racines est $(-1)^n\frac{\alpha_0}{\alpha_n}$.

Exercice: Calculer la somme et le produit des racines n-ièmes de l'unité.

IV) Formule de Taylor des polynômes

1) Dérivation des polynômes

On reprend la dérivation usuelle des fonctions polynomiales :

DÉFINITION 16.11

Soit $P=\sum\limits_{k}a_kX^k$, on appelle polynôme dérivé de P, le polynôme noté P' ou $\frac{dP}{dX}$, et défini par :

$$P'=\sum_{k\geqslant 1}ka_kX^{k-1}.$$

Par récurrence, la dérivée n-ième de P, notée $P^{(n)}$, est : $P^{(n)}=\begin{cases}P & \text{si } n=0\\ \left[P^{(n-1)}\right]' & \text{si } n\geqslant 1\end{cases}$

THÉORÈME 16.14 (propriétés)

Soient, $P,Q\in\mathbb{K}[X]$ et soit $\lambda\in\mathbb{K}$:

- *$(P+Q)'=P'+Q'$ et $(\lambda P)'=\lambda P'$.*
- *$(P\times Q)'=P'\times Q+P\times Q'$, plus généralement, on a la formule de* LEIBNIZ [3] *:*

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

- *$P(Q)'=Q'\times P'(Q)$ (dérivée d'une composée).*

Preuve: La première propriété est simple à vérifier. Pour la deuxième propriété, on commence par montrer que $(X^n\times Q)'=nX^{n-1}\times Q+X^n\times Q'$, puis on applique la première propriété. La formule de LEIBNIZ se montre ensuite par récurrence sur n (exactement comme la formule du binôme de NEWTON). Quant à la troisième, on commence par le cas où $P=X^n$, c'est à dire on commence par montrer que $[Q^n]'=nQ'\times Q^{n-1}$, ce qui se fait par récurrence sur n, on utilise ensuite la première propriété pour le cas général. □

THÉORÈME 16.15

Si $P=X^n$, alors $P^{(k)}=\begin{cases}\frac{n!}{(n-k)!}X^{n-k} & \text{si } k\leqslant n\\ 0 & \text{si } k>n\end{cases}$. On en déduit que si $P=\sum\limits_{n}a_nX^n$, alors

$$P^{(k)}=\sum_{n\geqslant k}\frac{n!}{(n-k)!}a_nX^{n-k}$$

3. *LEIBNIZ Gottfried* (1646 – 1716) : philosophe et mathématicien allemand.

En particulier si $\deg(P) = n$ *alors* $P^{(n)} = a_n n!$ *et si* $k > \deg(P)$*, alors* $P^{(k)} = 0$*. D'autre part, lorsque* $k \leqslant \deg(P)$*, alors* $\deg(P^{(k)}) = \deg(P) - k$*.*

Preuve: Celle - ci est simple et laissée en exercice. □

2) Formule de Taylor

Soit $P = \sum_{k=0}^{n} a_k X^k$, soit r un entier compris entre 0 et n, alors $P^{(r)} = \sum_{k=r}^{n} \mathrm{A}_k^r a_k X^{k-r}$, substituons 0 à X, on obtient alors $\widetilde{P^{(r)}}(0) = r! a_r$, on en déduit donc que :

$$\forall r \in [\![0..n]\!], a_r = \frac{\widetilde{P^{(r)}}(0)}{r!}.$$

Remarquons que la formule reste vraie pour $r > n$, finalement on obtient la formule de Taylor[4] en 0 :

$$P = \sum_k \frac{\widetilde{P^{(k)}}(0)}{k!} X^k.$$

Soit $a \in \mathbb{K}$, posons $Q = P(X + a)$ (composée de P avec le polynôme $X + a$), d'après ce qui précède, on a :

$$Q = \sum_k \frac{\widetilde{Q^{(k)}}(0)}{k!} X^k.$$

Or, il est facile de montrer que $Q^{(k)} = P^{(k)}(X+a)$, par conséquent $\widetilde{Q^{(k)}}(0) = \widetilde{P^{(k)}}(a)$, et comme $P = Q(X-a)$, on obtient :

$$P = \sum_k \frac{\widetilde{P^{(k)}}(a)}{k!}(X - a)^k.$$

THÉORÈME 16.16

Si $P \in \mathbb{K}[X]$ *et* $a \in \mathbb{K}$*, alors :* $P = \sum_k \frac{\widetilde{P^{(k)}}(a)}{k!}(X - a)^k$*. C'est la formule de* Taylor *pour le polynôme* P *en* a*.*

Applications:

– Division euclidienne d'un polynôme P par $(X - a)^n$: d'après la formule de Taylor en a appliquée à P, on a :

$$\begin{aligned} P &= \sum_k \frac{\widetilde{P^{(k)}}(a)}{k!}(X - a)^k \\ &= \sum_{k \geqslant n} \frac{\widetilde{P^{(k)}}(a)}{k!}(X - a)^k + \sum_{k<n} \frac{\widetilde{P^{(k)}}(a)}{k!}(X - a)^k \\ &= (X - a)^n \times \sum_{k \geqslant n} \frac{\widetilde{P^{(k)}}(a)}{k!}(X - a)^{k-n} + \sum_{k<n} \frac{\widetilde{P^{(k)}}(a)}{k!}(X - a)^k, \end{aligned}$$

comme $\deg(\sum_{k<n} \frac{\widetilde{P^{(k)}}(a)}{k!}(X - a)^k) < n$, on en déduit que le quotient Q et le reste R dans la division euclidienne par $(X - a)^n$ sont :

$$Q = \sum_{k \geqslant n} \frac{\widetilde{P^{(k)}}(a)}{k!}(X - a)^{k-n} \quad \text{et} \quad R = \sum_{k<n} \frac{\widetilde{P^{(k)}}(a)}{k!}(X - a)^k.$$

4. Taylor Brook (1685 – 1731) : mathématicien anglais qui a énoncé sa célèbre formule en 1715.

– Calcul de la multiplicité d'une racine : $a \in \mathbb{K}$ est une racine de P de multiplicité $n \geqslant 1$ si et seulement si :

$$\forall\ k \in [\![0..n-1]\!], \widetilde{P^{(k)}}(a) = 0 \text{ et } \widetilde{P^{(m)}}(a) \neq 0.$$

En effet, d'après ce qui précède,

$$\begin{aligned} n = m_P(a) &\iff R = 0 \text{ et } Q(a) \neq 0 \\ &\iff R(X+a) = 0 \text{ et } Q(a) \neq 0 \\ &\iff \forall k \in [\![0..n-1]\!], \widetilde{P^{(k)}}(a) = 0, \text{ et } \widetilde{P^{(n)}}(a) \neq 0 \end{aligned}$$

V) Exercices

★Exercice 16.1

Factoriser dans $\mathbb{R}[X]$ les polynômes suivants :

$$X^6+1;\ \ X^4+1;\ \ X^4-2X^2+3;\ \ X^4+5X^2+3;\ \ X^8+X^4+1;\ \ X^9+X^6+X^3+1.$$

★Exercice 16.2

Soit $P = X^5 - 2X^4 - X^3 + 2X^2 + X - 2$ et $Q = X^3 - 2X^2 - 3X + 6$. Factoriser P et Q sachant qu'ils ont une racine commune.

★Exercice 16.3

Soit $P = X^3 + pX + q \in \mathbb{C}[X]$, montrer que l'on peut trouver $u, v \in \mathbb{C}$ tels que $a = u + v$ soit racine de P avec $uv = -\frac{p}{3}$. Application : déterminer les racines de $X^3 - 3X + 1$.

★Exercice 16.4

On considère le polynôme P_n défini par $P_n = \prod\limits_{k=0}^{n}(1+X^{2^k})$. Simplifier $(1-X) \times P_n$, en déduire l'expression développée de P_n.

★Exercice 16.5

Soit $P \in \mathbb{K}[X]$, montrer que P est pair (*i.e.* $P(-X) = P$) ssi les coefficients de P d'indices impairs sont nuls. Montrer que P est impair (*i.e.* $P(-X) = -P$) ssi les coefficients d'indices pairs sont nuls.

★Exercice 16.6

a) Soient $\alpha, \beta \in \mathbb{K}$, distincts, soit $P \in \mathbb{K}[X]$, calculer le reste dans la division euclidienne de P par $(X-\alpha)(X-\beta)$, puis par $(X-\alpha)^2$.

b) Calculer le quotient et le reste dans la division euclidienne de $(X-1)^{n+2} - (X+2)^n - 2$ par $(X-1)^n$.

★Exercice 16.7

Soient $a_0, \ldots, a_n$ $n+1$ éléments distincts de $\mathbb{K}$, et $P \in \mathbb{K}[X]$:

a) Montrer qu'il existe un unique polynôme R de degré $\leqslant n$ tel que $\widetilde{R}(a_k) = \widetilde{P}(a_k)$ pour $k \in [\![0..n]\!]$. Calculer R lorsque $\deg(P) < n+1$ et lorsque $P = X^{n+1}$.

b) Pour k compris entre 0 et n, on pose : $L_k = \prod\limits_{i=0, i\neq k}^{n} \dfrac{X - a_i}{a_k - a_i}$. Calculer $\deg(L_k)$ et montrer que $L_k(a_j) = \delta_{k,j}$. En déduire le polynôme R pour P quelconque. Calculer $\sum\limits_{k=0}^{n} L_k$.

★Exercice 16.8

a) Montrer que dans $\mathbb{R}[X], X^2 - X + 1 | (X-1)^{n+2} + X^{2n+1}$.

b) Montrer que dans $\mathbb{R}[X], X^3 - 3X^2 + 3X - 1 | X^{2n+1} - (2n+1)X^{n+1} + (2n+1)X^n - 1$.

c) Soient n et m deux entiers positifs, montrer que si $n|m$ alors $X^n - 1 | X^m - 1$.

d) Montrer que $X^2 - 2\cos(\theta)X + 1 | \cos((n-1)\theta)X^{n+1} - \cos(n\theta)X^n - \cos(\theta)X + 1$, dans $\mathbb{R}[X]$.

e) Soient $P, Q \in \mathbb{R}[X]$, montrer que si $P|Q$ dans $\mathbb{C}[X]$, alors $P|Q$ dans $\mathbb{R}[X]$.

f) Soit $P \in \mathbb{K}[X]$, montrer que $P - X | P(P) - P$, en déduire que $P - X | P(P) - X$.

★Exercice 16.9
Calculer la multiplicité de 1 dans les polynômes $P = X^{2n} - nX^{n+1} + nX^{n-1} - 1$ et $Q = X^{2n+1} - (2n+1)X^{n+1} + (2n+1)X^n - 1$.

★Exercice 16.10
Soit $P \in \mathbb{R}[X]$, soit $z \in \mathbb{C}$ une racine complexe non réelle de P de multiplicité m. Montrer que $\overline{z}$ est également racine de P de multiplicité m. En déduire que tout polynôme non constant de $\mathbb{R}[X]$ se factorise en produit de facteurs de degré 1 ou 2, les facteurs de degré 2 étant sans racine réelle.

★Exercice 16.11

a) Déterminer tous les polynômes P de degré n tels que $P(X^2) = P^2$ (poser $P = a_nX^n + Q$ où $\deg(Q) < n$).

b) Déterminer tous les polynômes P, Q, R de $\mathbb{R}[X]$ qui vérifient : $P^2 - XQ^2 = XR^2$.

c) Déterminer les polynômes $P \in \mathbb{C}[X]$ qui vérifient : $P'|P$.

★Exercice 16.12
Soient $a_1, \ldots, a_n$ des entiers distincts, soit $P = (X - a_1)\cdots(X - a_n) - 1$. On suppose qu'il existe deux polynômes Q et R à coefficients entiers, tels que $P = Q \times R$. Montrer que si Q est non constant, alors $\deg(Q) = \deg(P)$ et $R = \pm 1$.

★Exercice 16.13
Soit $s, p \in \mathbb{C}$ avec $p \neq 0$. A quelle(s) condition(s) les racines de $X^2 - sX + p$ ont-elles le même argument ?

★Exercice 16.14

a) Montrer qu'il existe un unique polynôme $T_n \in \mathbb{R}[X]$ de degré au plus n tel que :

$$\forall\ x \in \mathbb{R}, T_n(\cos(x)) = \cos(nx).$$

b) Calculer T_0, T_1, T_2, T_3. Calculer $T_n(0)$ et le coefficient dominant de T_n.

c) Étudier la parité de T_n. Montrer que T_n admet n racines dans $[-1;1]$. Calculer leur produit.

d) Démontrer la relation : $\forall\ n \geqslant 1, T_{n+1} = XT_n + \frac{1}{n}(X^2 - 1)T_n'$. Calculer T_4.

e) Démontrer la relation : $\forall\ n \in \mathbb{N}, T_{n+2} = 2XT_{n+1} - T_n$.

f) Montrer que $T_n(T_m(X)) = T_m(T_n(X)) = T_{nm}(X)$.

★Exercice 16.15

a) Soit $S_n = \sum_{k=0}^{n}(-1)^k \left(\mathrm{C}_n^k\right)^2$, soit $P = (1 - X)^n$ et $Q = (1 + X)^n$. Calculer le coefficient de X^n dans le produit $P \times Q$, en déduire une simplification de S_n.

b) En s'inspirant d'une même démarche, simplifier : $\sum_{k=0}^{n} \left(\mathrm{C}_n^k\right)^2 \quad ; \quad \sum_{k=0}^{p} \mathrm{C}_n^k \mathrm{C}_m^{p-k}$.

★Exercice 16.16
Soit $P \in \mathbb{R}[X]$ tel que $\forall\ x \in \mathbb{R}, P(x) \geqslant 0$. Soit $n = \deg(P)$, et $Q = P + P' + \cdots + P^{(n)}$. Montrer que $\forall\ x \in \mathbb{R}, Q(x) \geqslant 0$.

★Exercice 16.17
Soit $f : \mathbb{R}_3[X] \to \mathbb{R}_3[X]$ définie par $\forall P \in \mathbb{R}_3[X], f(P) = Q + R$ où Q et R sont respectivement le quotient et le reste de la division de P par $(X - 1)^2$.

a) Montrer que f est un endomorphisme de $\mathbb{R}_3[X]$.

b) Déterminer $\ker(f)$ et $\mathrm{Im}(f)$.

c) Résoudre l'équation $f(P) = 2X + 1$ dans $\mathbb{R}_3[X]$.