Polynômes

Dans tout le chapitre, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

I L'ensemble $\mathbb{K}[X]$

1) Généralités

a) Définition

Définition :

On appelle **polynôme** toute expression de la forme

$$P = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n = \sum_{k=0}^{n} a_kX^k$$

où $n \in \mathbb{N}$, $a_0, a_1, \ldots, a_n$ des éléments de $\mathbb{K}$, et où X est appelé **l'indéterminée**.

On appelle **fonction polynômiale** associée à P la fonction suivante, notée P également définie sur $\mathbb{K}$ par :

$$P : x \mapsto= a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = \sum_{k=0}^{n} a_kx^k$$

A noter : C'est une inconnue X ?

La lettre X ne doit pas être vue comme une inconnue. Ce X n'est pas un nombre et X pourra être remplacé par divers objets, dans des contextes particuliers.

Pour simplifier, on peut dire que X est l'application identité : $x \mapsto x$, et donc que X^k est l'application $x \mapsto x^k$.

Comme en pratique, on utilisera les polynômes plus comme un cas particulier de fonctions que comme des objets à part entière, cette notation X^k vue comme la fonction "puissance k" prend tout son sens.
Notons enfin que pour insister sur l'aspect polynôme "formel", on pourra utiliser la notation $P(X)$ plutôt que P tout court... ce qui est également souvent plus clair !

Définition :

Soit P un polynôme et $x \in \mathbb{K}$. Quand on calcule $P(x)$, on dit qu'on **évalue** le polynôme en x. Ainsi, on dit que $P(x)$ est **l'évaluation de P en x**.

Exemple :
Soit la fonction

$$P : x \mapsto 2x^3 - 4x + 2$$

est une fonction polynomiale, associée au polynôme

$$P = 2X^3 - 4X + 2$$

que l'on peut aussi noter $P(X) = 2X^3 - 4X + 2$.

L'évaluation de P en 2 est $P(2) = 10$.

Définition :

- On appelle **monôme de degré** k tout polynôme de la forme aX^k avec $a \neq 0$.
- Soit $P = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$. Pour tout i, le nombre a_i est appelé **coefficient d'indice** i du polynôme.
- L'ensemble des polynômes à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$.

Exemples :

- $P = 1 + 2X + 4X^4$ est un polynôme. Son coefficient d'indice 0 est , celui d'indice 4 est et son coefficient d'indice 5 est .
- $P = 3X^5$ est un monôme degré 5.

b) Egalités de polynomes

Proposition 1 :

Aux coefficients nuls prêts, l'écriture d'un polynôme, rangé par degrés des monômes, est unique.
Autrement dit : deux polynômes P est Q sont égaux si et seulement si ils ont les mêmes coefficients.

Remarque :

"Aux coefficients nuls prêts" signifie que l'on peut avoir des coefficients a_k nuls dans l'écriture $P = \sum_{k=0}^{n} a_k X^k$.

Ainsi : $X^4 + X + 1 = X^4 + 0X^3 + X + 1 = 0X^{42} + X^4 + X + 1$.

▷ *Preuve :*

◁

2) Opérations élémentaires sur les polynômes

On définit sur les polynômes les mêmes opérations que sur les fonctions classiques.

a) Somme

Définition :

Soient $(P,Q) \in (\mathbb{K}[X])^2$, $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{p} b_k X^k$, avec n et p deux entiers. Quitte à compléter P ou Q par des 0, on peut supposer $n = p$ et écrire $Q = \sum_{k=0}^{n} b_k X^k$. On définit alors le polynôme $P+Q$ par :

$$P + Q = \sum_{k=0}^{n} (a_k + b_k) X^k$$

Ainsi, pour additionner des polynômes, on additionne les coefficients de même indice.

Exemple :
soient $P = 3X^2 + 4X + 1$ et $Q = 5X^3 + 2X$ alors $P + Q =$

Remarque :

- La somme est commutative : on a $P + Q = Q + P$, quels que soient les polynômes.
- Si $P, Q \in \mathbb{K}[X]$, alors $P + Q \in \mathbb{K}[X]$: on a donc stabilité de $\mathbb{K}[X]$ pour l'opération d'addition.

b) Produit

On pose sur $\mathbb{K}[X]$ une opération de multiplication, héritée à nouveau du produit naturel sur les fonctions polynômiale, où après avoir développé le produit, on regroupe par puissance :

Définition :

Soient $(P,Q) \in (\mathbb{K}[X])^2$, $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{p} b_k X^k$, avec n et p deux entiers. On définit le polynôme PQ par

$$PQ = \sum_{k=0}^{n+p} c_k X^k \qquad \text{avec } c_k = \sum_{i+j=k} a_i b_j$$

Remarques :

1. $\sum_{i+j=k}$ sous entend que l'on fait la somme pour tous les i et tous les j tels que $0 \leq i \leq n$ et $0 \leq j \leq p$ avec $i + j = k$. Par exemple,

$$c_1 = a_0 b_1 + a_1 b_0,$$

$$c_2 = \qquad ,$$

$$c_3 =$$

2. On peut aussi écrire $c_k = \sum_{i=0}^{n} a_i b_{k-i}$ avec la convention que si $k - i < 0$ ou si $k - i > p$, le coefficient b_{k-i} est nul.

Exemple

- $(2X^2 + 3X + 1)(X - 2) \quad =$

Remarques :

- Pour tout scalaire $\lambda \in \mathbb{K}$ et pour tout $P \in \mathbb{K}[X]$, on peut calculer λP qui est également un polynôme : on peut voir le scalaire comme un polynôme et appliquer la proposition précédente. Il suffit alors de multiplier tous les coefficients de P par λ.
- A nouveau, on remarque la stabilité de $\mathbb{K}[X]$, cette fois par le produit...

Proposition 2 :

Soient P et Q deux polynômes. Alors $PQ = QP$.
Le produit de polynôme est donc commutatif.

▷ *Preuve* : Avec les notations de la définition, on a pour tout k, $c_k = \sum_{i+j=k} a_i b_j = \sum_{i+j=k} b_j a_i$.
Les variables i et j jouent des rôles symétriques, donc calculer PQ ou QP donne bien la même formule. ◁

Corolaire 1 :

Soit $n \in \mathbb{N}$ et $P \in \mathbb{K}[X]$. On définit la puissance n-ème de P, notée P^n, par

$$P^0 = 1 \quad \text{et} \quad ,\forall n \geq 1, P^n = P.P^{n-1}$$

Alors pour tout $n \in \mathbb{N}$, P^n est un polynôme.

▷ *Preuve* :

◁

c) Composition

Définition :

Soient $(P, Q) \in \mathbb{K}[X]$ avec $P = \sum_{k=0}^{n} a_k X^k$.

On définit le polynôme composé de Q par P, noté $P \circ Q$ ou $P(Q)$ par,

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

On remarque que par puissance et somme de polynôme, $P \circ Q$ est bien un polynôme.

Exemple
$P = X^2 + X + 1$ et $Q = 3X + 1$, alors

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

Principe : on remplace X par Q et on développe si besoin.

3) Degré d'un polynôme

a) Définitions

Définition :

Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme.

On appelle degré de P, noté $deg(P)$, le plus grand p tel que $a_p \neq 0$.

Par convention, $\deg(0) = -\infty$.

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

Exemple :

- $P(X) = 5X^2 - 1$ est de degré . Ainsi $P \in$
- $Q(X) = \sin(\pi)X^5 + 3X^2 + 3$ est de degré .

Définition : Vocabulaire

Soit P un polynôme non nul, $P = \sum_{k=0}^{n} a_k X^k$. On définit les notions suivantes :

- **Terme dominant** : le monôme non nul de plus haut degré (pas forcément n...).
- **Coefficient dominant** : le coefficient du terme dominant.
- **Terme constant** : le coefficient du terme de degré 0 (le coefficient a_0).
- **Polynôme unitaire** : un polynome dont le coefficient dominant est 1.

Exemple :
Soit $P = 3X^5 + 2X + 1$. Son terme dominant est

Son coefficient dominant est

Son terme constant est

b) Opérations et degré

Proposition 3 :

Soient P et Q deux polynômes.

1. $\deg(P + Q)$
2. si $\deg(P) \neq \deg(Q)$, $\deg(P + Q)$
3. $\deg(PQ)$
4. $\deg(P \circ Q)$

Remarque :
si P et Q sont deux polynômes de $\mathbb{K}_n[X]$, alors la première propriété donne $deg(P+Q) \leq n$.
Ainsi $P+Q = \mathbb{K}_n[X]$.
De plus, pour tout $\lambda \in \mathbb{K}$, $deg(\lambda P) = n$ si $\lambda \neq 0$, où $-\infty$ si $\lambda = 0$.
Dans tous les cas $deg(\lambda P) \leq n$, donc $\lambda P \in \mathbb{K}[X]$
On dit alors, comme pour les matrices, que $\mathbb{K}_n[X]$ est un espace vectoriel.

c) "Intégrité" de $\mathbb{K}[X]$

Theorème 1 :

Soient P et Q deux polynômes de $\mathbb{K}[X]$.
Alors $PQ = 0$ si seulement si $P = 0$ ou $Q = 0$ En particulier, le produit de deux polynômes non nul est non nul.

▷ *Preuve :*

◁

Attention : On parle ici de polynômes nuls, pas de polynômes qui s'annulent...

II Division et racines dans $\mathbb{K}[X]$

1) Division

a) Division euclidienne

Proposition 4 :

Soient A et B deux polynômes de $\mathbb{K}[X]$ avec B non nul. Alors il existe un unique couple de polynômes (Q, R) de $\mathbb{K}[X]$ avec $deg(R) < deg(B)$ tels que

$$A = BQ + R$$

On dit qu'on a effectué la **division euclidienne de A par B**, que Q est le **quotient** et R le **reste** de la division.

▷ *Preuve :*

◁

Remarque :
A noter que la division euclidienne dans $\mathbb{K}[X]$ donne des polynômes de $\mathbb{K}[X]$: en particulier, si on est au départ dans $\mathbb{R}[X]$, il n'y a pas de polynôme à coefficient complexes qui vont apparaitre...

En pratique
On pose la division euclidienne un peu comme on le fait pour les nombres entiers, en ne se concentrant successivement sur les termes dominants :
Exemple : division de $X^5 + 2X^4 + 3X^2 - 4X + 1$ par $X^2 + X + 1$

b) Divisibilité

Définition :

Soient A et B deux polynômes de $\mathbb{K}[X]$.
On dit que B divise A (et on note $B|A$) si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$ (autrement dit, le reste par la division euclidienne est nul).
On dit alors que B est un diviseur de A, ou que A est un multiple de B.

Exemple :
soit $A = X^4 - 1$ et $B = X^2 - 1$. On a $A = (X^2 - 1)(X^2 + 1)$ donc

Proposition 5 :

(i) $\forall A \in \mathbb{K}[X], A|A$
(ii) $\forall A \in \mathbb{K}[X], A|0$
(iii) $\forall A, B, C \in \mathbb{K}[X]$,si $A|B$ et $B|C$, alors $A|C$
(iv) si $B|A$ avec $A \neq 0$, alors $deg(B) \leq deg(A)$ (attention : faux avec $A = 0$)

▷ *Preuve :*

◁

2) Racines

Dans cette section, on confondra souvent le polynôme P et sa fonction polynômiale associée, notée P également.

a) Racines et divisibilité

Définition :

On appelle racine du polynôme $P \in \mathbb{K}[X]$ tout nombre $\alpha \in \mathbb{K}$ tel que $P(\alpha) = 0$

Remarquons déjà un premier résultat qu'on a déjà observé pour les polynômes du second degré dans le premier chapitre sur les complexes, et qu'on généralise ici :

Propriété 1 :

Soit $P \in \mathbb{R}[X]$. Si P admet une racine complexe non réelle λ, alors $\overline{\lambda}$ est racine également.

▷ *Preuve :*

◁

On peut donner une autre preuve d'un résultat déjà énoncé dans le premier chapitre sur les complexes :

Theorème 2 :

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$, alors

α est racine de P si et seulement si $(X - \alpha)$ divise P.

▷ *Preuve :*

◁

Corolaire 2 :

Soit $p \in \mathbb{N}$, $p \neq 0$. Si $\alpha_1, \alpha_2, \ldots, \alpha_p$ sont p racines distinctes d'un polynôme $P \in \mathbb{K}[X]$, alors le polynôme P est divisible par $(X - \alpha_1)(X - \alpha_2)\ldots(X - \alpha_p)$

▷ *Preuve :* Intuitivement assez clair. Se démontre par récurrence. ◁

b) Nombre de racines d'un polynôme

Theorème 3 :

Soit $n \in \mathbb{N}^*$ et $P \in \mathbb{K}_n[X]$. Si P admet au moins $n+1$ racines distinctes, alors P est nul.

▷ *Preuve :*

◁

Corolaire 3 :

Le théorème donne immédiatement les résultats suivants :

- Le nombre de racines d'un polynôme non nul est majoré par son degré.
- Un polynôme qui admet une infinité de racines distinctes est nul.

Exemple :
La fonction sin n'est pas un polynôme puisque tous les nombres de la forme $x_k =$ avec $k \in \mathbb{Z}$ vérifient $\sin(x_k) = 0$: il y aurait une infinité de racines alors que sin n'est pas nulle...

c) Racines multiples

Définition :

Soit P un polynôme non nul et $\alpha \in \mathbb{K}$.
On dit que α est racine d'ordre de multiplicité k si et seulement si on peut écrire

$$P = (X - \alpha)^k Q$$

où Q est un polynôme tel que $Q(\alpha) \neq 0$.

Autrement dit, l'ordre de multiplicité d'une racine α est la plus grande puissance possible de $(X - \alpha)$ qui divise P.

Définition :

α est dit "racine multiple" d'un polynôme P si la racine α est d'ordre au moins 2.
Si α est racine d'ordre 1, on dit que c'est une racine simple.
Si α est racine d'ordre 2, on parle de racine double.

Exemple :
2 est racine double de $P = (X - 2)^2(X + 1)$
Soit $P(X) = X^3 - 3X + 2$. Quel est l'ordre de 1 ?

Remarques :

- Si α est tel que $P(\alpha) \neq 0$, alors α n'est pas racine.
  On peut quand même écrire $P = (X - \alpha)^0 P$, donc d'après la définition, α est une racine d'ordre 0... sans être une vraie racine. En pratique, on parlera rarement de racine d'ordre 0...
- Si $P = 0$ alors tout $\alpha \in \mathbb{K}$ est racine. Mais pour tout $k \in \mathbb{N}$, on a $0 = (X - a)^k O$: il n'y pas de puissance maximale. Dans ce cas là, on ne donne pas d'ordre pour les racines du polynôme nul.

3) Polynômes scindés :

a) Définitions et exemples :

Définition :

Un polynôme $P \in \mathbb{K}[X]$ non nul est dit scindé sur $\mathbb{K}$ si et seulement si il est constant ou si il existe $n \in \mathbb{N}^*$, $\lambda \in \mathbb{K}^*$ et $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ (pas nécessairement distincts) tels que

$$P = \lambda \prod_{k=1}^{n} (X - \alpha_k)$$

On a alors $\lambda = a_n$ où a_n est le coefficient dominant de P.

Exemples :

- $P = 2X^2 - 2$ est un polynôme scindé sur $\mathbb{R}$ car $P =$
- $Q = X^2 + 2X + 1$
- $R = X^2 + 1$

- Si P est un polynôme de degré n admettant n racines distinctes, il est nécessairement scindé.

b) Relations entre racines et coefficients

Theorème 4 :

Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme scindé.
Ainsi $\exists \alpha_1, \dots, \alpha_n \in \mathbb{K}$ tels que $P = a_n(X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_n)$
Alors

- $\sum_{k=1}^{n} \alpha_k = -\frac{a_{n-1}}{a_n}$
- $\prod_{k=1}^{n} \alpha_k = (-1)^n \frac{a_0}{a_n}$

▷ *Preuve :*

◁

Exemples :

- Soit $P =$
- Soit $P = X^n - 1$

Remarques :

- C'est une généralisation du résultat qu'on connaissait déjà sur les équations algébriques du second degré.
- Attention, en cas de racines multiples, on compte les racines autant de fois que leur ordre de multiplicité.

III Dérivation

1) Dérivation

a) Définition et propriétés immédiates

Définition :

Soit $P \in \mathbb{K}[X]$, $P = \sum_{k=0}^{n} a_k X^k$. On appelle **polynôme dérivé de** P le polynôme $P' \in \mathbb{K}[X]$ défini par

$$P' = \sum_{k=1}^{n} k a_k X^{k-1}$$

Exemple :
$P = 4X^3 + 2X + 1$ a pour polynôme dérivé $P' =$

Remarque
Il s'agit d'une définition, mais elle provient naturellement de la dérivée d'une fonction polynomiale...
Ainsi, la dérivée, formelle, sur l'ensemble des polynômes coïncide avec la dérivée (en tant que limite du taux d'accroissement) sur les fonctions polynomiales réelles.

Propriété 2 :
Pour tous polynômes $P, Q \in \mathbb{K}[X]$ et pour tout $\lambda, \mu \in \mathbb{K}$, on a

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

▷ *Preuve* : Avant tout technique : on manipule les expressions pour les vérifier. On admet. ◁

b) Dérivées successives :

Définition :

Soit P un polynôme et $n \in \mathbb{N}$. On définit la dérivée d'ordre n de P, notée $P^{(n)}$ par

$$\begin{cases} P^{(0)} &= P \\ \forall n \geq 1,\ P^{(n)} &= \left(P^{(n-1)}\right)' \end{cases}$$

Exemple
Soit $P(X) = 2X^3 + 2X^2 - X + 1$ alors

$P' =$

$P^{(2)} =$

$P^{(3)} =$

$P^{(4)} =$

Propriété 3 :
Soit $P \in \mathbb{K}[X]$ et $k \in \mathbb{N}$. On a

- Si $deg(P) \geq k$, $deg(P^{(k)}) = deg(P) - k$.
- si $deg(P) < k$, $P^{(k)} = 0$ et $deg(P^{(k)}) = -\infty$

▷ *Preuve* : Ce résultat se montre par récurrence : chaque dérivation fait perdre un degré... ◁

Proposition 6 : Formule de Leibniz

Soit A et B deux polynômes, alors pour tout $n \in \mathbb{N}$,

$$(AB)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} A^{(k)} B^{(n-k)}$$

▷ *Preuve :*
La preuve est évidemment très proche de celle du binôme de Newton. Dans l'hérédité, la clef est que

$$(A^{(k)}B^{(n-k)})' = (A^{(k)})'B^{(n-k)} + A^{(k)}(B^{(n-k)})' = A^{(k+1)}B^{(n-k)} + A^{(k)}B^{(n-k+1)}$$

On obtient alors $(AB)^{(n+1)} = \left((AB)^{(n)}\right)' = \sum_{k=0}^{n} \binom{n}{k} A^{(k+1)}B^{(n-k)} + A^{(k)}B^{(n-k+1)}$ et la preuve se poursuit comme dans le cas réel ou complexe, avec un glissement d'indice et la formule triangulaire de Pascal.

◁

c) Formule de Taylor

Lemme 1

Soit $n \in \mathbb{N}$ et $P = X^n$
Alors si $k \leq n$,

$$P^{(k)} = n(n-1)\dots(n-k+1)X^{n-k} = \frac{n!}{(n-k)!}X^{n-k}$$

et si $k > n$,

$$P^{(k)} = 0$$

▷ *Preuve :*

◁

Theorème 5 : Formule de Taylor pour les polynômes

Soient $n \in \mathbb{N}$ et $P \in \mathbb{K}_n[X]$ et $\alpha \in \mathbb{K}$.
Alors

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

En particulier :

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

▷ *Preuve :*

◁

2) Racine multiple et dérivation

a) caractérisation :

Proposition 7 :

Soit α une racine d'ordre $m > 0$ d'un polynôme $P \in \mathbb{K}[X]$. Alors α est racine d'ordre $m-1$ de P'.

▷ *Preuve :*

◁

Remarque :
On généralise facilement par récurrence cette baisse d'ordre : si α est d'ordre m pour P, alors α est d'ordre $m-2$ pour P'', $m-3$ pour $P^{(3)}$, etc. Ainsi pour tout $k \leq m$, α est racine d'ordre $m-k$ de $P^{(k)}$.
Cela fourni donc une caractérisation pratique l'ordre de multiplicité :

Proposition 8 :

Soit un polynôme P, $\alpha \in \mathbb{R}$ et $m \in \mathbb{N}^*$.
Alors α est racine d'ordre m si et seulement si $P^{(k)}(\alpha) = 0$ pour tout $k \in \{0, 1, \ldots, m-1\}$ et $P^{(m)}(\alpha) \neq 0$.

▷ *Preuve :*
Le sens direct provient de la remarque : arrivée à dérivée m-ième, α est d'ordre $m - m = 0$: ce n'est plus une racine, alors que jusque là c'était le cas.
Réciproquement,

◁

Exemple
On veut l'ordre de la racine 2 dans $P(X) = X^3 - X^2 + X - 6$:

b) Cas particulier des polynômes de $\mathbb{R}[X]$

Proposition 9 :

Soit $P \in \mathbb{R}[X]$ et $\alpha \in \mathbb{C}$ une racine non réelle, d'ordre de multiplicité m.
Alors $\bar{\alpha}$ est aussi une racine de P, de même ordre de multiplicité que α.

▷ *Preuve :*

◁

IV Factorisation des polynômes - décomposition en éléments simples

1) Polynômes irréductibles

Définition :

Un polynôme $P \in \mathbb{K}[X]$ est dit **irréductible** si il est non constant et si

$$\forall A, B \in \mathbb{K}[X], P = AB \Longrightarrow A \text{ ou } B \text{ est constant}$$

Autrement dit, un polynôme non constant est irréductible si et seulement si aucune factorisation par autre chose que des scalaires n'est possible.

Exemples :

- Si P est de degré 1, alors $P = \lambda(X - a)$ avec $\lambda, a \in \mathbb{K}$: les polynômes de degré 1 sont irréductibles
- Si P admet une racine α avec $deg(P) > 1$ alors $P = (X - \alpha)Q$, avec $deg(Q) \geq 1$. Ainsi P **n'est pas irréductible.**
- $P = X^2 + X + 1$ est irréductible en tant que polynôme de $\mathbb{R}[X]$, mais pas en tant que polynôme de $\mathbb{C}[X]$

Remarque :
La notion est à rapprocher des nombres premiers : un nombre $p \geq 2$ est premier si et seulement si il n'a que deux diviseurs, 1 et lui même.
Autrement dit : $p = ab \Longrightarrow a = 1$ ou $b = 1$

2) Factorisation

a) Théorème de d'Alembert-Gauss

Theorème 6 : de d'Alembert-Gauss

Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine dans $\mathbb{C}$.

▷ *Preuve :* Admis ◁

Corolaire 4 :

Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

▷ *Preuve :*

◁

Corolaire 5 :

Tout polynôme non nul de $\mathbb{C}[X]$ est scindé

▷ *Preuve :*

◁

Corolaire 6 :

Les polynômes irréductibles de $\mathbb{R}[X]$ sont :

- Les polynômes de degré 1
- Les polynômes de degré 2 dont le discriminant est strictement négatif.

▷ *Preuve :*

◁

Le saviez-vous ? — Le théorème fondamental de l'algèbre

Le théorème de d'Alembert-Gauss et ses corolaires ont des conséquences tellement importantes sur la résolution des équations et la structure des polynômes qu'on le surnomme **théorème fondamental de l'algèbre**.

Nous sommes au XVIIIe siècle, au lendemain (c'est à dire un siècle après...) de la découverte des nombres complexes. La plupart des scientifiques de l'époque sont maintenant convaincu de l'importance de cet ensemble, on les manipule enfin sous la forme algébrique pendant qu'Euler introduit la notation $e^{i\theta}$ et montre que $e^{i\pi} + 1 = 0$.

On "sent" alors qu'un résultat est tout proche : tout polynôme non constant admet au moins une racine !

Jean le Rond d'Alembert propose une première preuve, en 1746, preuve qu'il incluera dans un article de la célèbre *Encyclopédie*, en 1751.

La preuve se révèle incomplète, et pour cause : on manque de nombreux résultats, dont le théorème des valeurs intermédiaires.

Plusieurs mathématiciens se succèderont pour montrer rigoureusement ce résultat : Euler, Lagrange, Laplace, Argand....

Cependant l'histoire retient la preuve de Carl Friedrich Gauss... ou plutôt les preuves !

De 1799 à 1849, quatre preuves sont publiées, chacune avec des arguments de nature différente. Si la première était encore incomplète, dès la seconde, en 1815, on a enfin une preuve rigoureuse...

b) Décomposition primaire d'un polynôme de $\mathbb{C}[X]$

On a montré que tout polynôme de $\mathbb{C}[X]$ est scindé, c'est à dire s'écrit sous la forme

$$P = \lambda \prod_{k=1}^{n} (X - \alpha_k)$$

où $n = deg(P)$ et $\alpha_1, \ldots, \alpha_n$ des complexes.
Ce sont donc les racines de P, eventuellement répétée (selon leur ordre de multiplicité), ce qui donne le résultat ci dessous :

Theorème 7 :

Tout polynôme de $\mathbb{C}[X]$ se factorise sous la forme

$$P = a(X - \alpha_1)^{m_1}(X - \alpha_2)^{m_2} \ldots (X - \alpha_n)^{m_n} = a \prod_{k=1}^{n} (X - \alpha_k)^{m_k}$$

où $\alpha_1, \alpha_2, \ldots, \alpha_n$ sont les racines complexes distinctes de P, d'ordres de multiplicité respectifs $m_1, m_2, \ldots, m_p$, (donc $m_1 + m_2 + \ldots + m_p = deg(P)$) et $a \in \mathbb{R}$ est le coefficient dominant.

Exemple :
Pour $n \geq 2$, décomposons $X^n - 1$ en produit d'irréductibles dans $\mathbb{C}[X]$:

Une application de la décomposition primaire est la divisibilité :

Méthode : Montrer la divisibilité à l'aide de la factorisation

Soient P et Q deux polynômes de $\mathbb{C}[X]$. Pour montrer que $P|Q$, on peut déterminer les décompositions primaire de P et de Q et vérifier que tout facteur irréductible de P apparait dans celle de Q avec des puissances supérieures.

Exemple :
Soient les polynômes $P = (X-2)^2(X+i)(X-i)$, $Q = (X+3)^2(X-2)^3(X+i)^2(X-i)$, $R = (X+3)^2(X-2)(X+i)^2(X-i)$ et $S = (X+3)^3(X+i)(X-i)$.

c) Décomposition primaire dans $\mathbb{R}[X]$

Theorème 8 :

Tout polynôme de $\mathbb{R}[X]$ se factorise de façon unique, à l'ordre des facteurs près, sous la forme

$$P = a\prod_{k=1}^{n}(X-\alpha_k)^{m_k}\prod_{j=1}^{p}(X^2+\beta_k X+\gamma_k)^{n_k}$$

où $\alpha_1, \alpha_2, \ldots, \alpha_n$ sont les racines réelles distinctes de P, d'ordres de multiplicité respectifs $m_1, m_2, \ldots, m_p$, et les polynômes $X^2+\beta_k X+\gamma_k$ ont un discriminant strictement négatifs. De plus, $m_1+m_2+\ldots+m_p+2(n_1+\ldots+n_p) = deg(P)$.

▷ *Preuve :*

◁

Méthode : OBTENIR LA DÉCOMPOSITION PRIMAIRE DANS

La preuve précédente contient en fait une méthode pour factoriser un polynôme $P \in \mathbb{R}[X]$:

1. On décompose P en tant que polynôme de $\mathbb{C}[X]$: P est un produit de facteur de la forme $(X-x_i)^{m_i}$ où les x_i sont les racines de P dans $\mathbb{C}$, m_i leur ordre de multiplicité.
2. Les racines complexes non réelles de P sont deux à deux conjuguées, avec même ordre de multiplicité. On les regroupe.
3. On termine en identifiant bien le coefficient dominant.

Exemple :
Décomposition de $P = X^4+X^2+1$ dans $\mathbb{R}[X]$:

3) Décomposition en éléments simples

a) Fraction rationnelle :

Définition :

On appelle **fraction rationnelle** à coefficients dans $\mathbb{K}$ toute expression de la forme

$$F = \frac{P}{Q}, \quad \text{avec } P, Q \in \mathbb{K}[X], Q \text{ non nul.}$$

Exemple :

l'expression $F = \dfrac{X^3 - 3X + 2}{X^3 - X^2 - 8X + 12}$ est une fraction rationnelle, avec $P = X^3 - 3X + 2$ et $Q = X^3 - X^2 - 8X + 12$...

Définition :

Soit $F = \dfrac{P}{Q}$ une fraction rationnelle et $\alpha \in \mathbb{K}$.

- On dit que α est un **zero** de F de multiplicité m si α est une racine de P d'ordre de multiplicité m.
- On dit que α est un **pôle** de F de multiplicité m si α est racine de Q d'ordre de multiplicité m.

Exemple :

Reprenons $F = \dfrac{X^3 - 3X + 2}{X^3 - X^2 - 8X + 12}$:

b) Décomposition dans le cas à pôles simples :

Theorème 9 :

Soit F une fraction rationnelle, $F = \dfrac{P}{Q}$ avec Q scindé à racines simples.

Ainsi $Q = a\prod_{k=1}^{n}(X-\alpha_i)$ où les α_i sont les racines de Q.

Alors il existe un n-uplet $(a_1, a_2, \ldots, a_n) \in \mathbb{K}^n$ et $E \in \mathbb{K}[X]$, uniques, tels que

$$F(X) = E(X) + \sum_{i=1}^{n} \frac{a_i}{X-\alpha_i}$$

Le polynôme $E[X]$ est alors appelé **partie entière** de F.

▷ *Preuve* : On admet. ◁

Remarque :
Si le polynôme Q n'est pas scindé à racines simples, l'énoncé indiquera toujours la forme à rechercher.

Méthode : Trouver les coefficients et $E[X]$ (cas pôles simples) :

1. On effectue la division euclidienne de P par Q : on obtient $P = EQ + R$ avec $deg(R) < deg(Q)$.
   Ainsi $\dfrac{P}{Q} = \dfrac{EQ+R}{Q} = E + \dfrac{R}{Q}$
2. On décompose Q sous la forme $Q = a\prod(X-\alpha_i)$
3. On détermine les coefficients a_i, en multipliant l'expression par $(X-a_i)$ où via un système

Exemple :
Soit $F(X) = \dfrac{X^2+2X+5}{X^2-3X+2}$