Lycée du Parc
842

Polynômes

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

1 Généralités sur $\mathbb{K}[X]$

1.1 Définitions

Définition 1. Un polynôme à coefficients dans $\mathbb{K}$ est une suite $P = (a_k)_{k\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ qui est nulle à partir d'un certain rang que l'on note plutôt à l'aide d'une indéterminée sous la forme :

$$P(X) = \sum_{k\geqslant 0} a_k X^k = a_0 + a_1 X + a_2 X^2 + a_3 X^3 + \cdots$$

(cette somme est nécessairement finie)
Les nombres $a_0, a_1, a_2, \ldots$ sont appelés les coefficients du polynôme.

On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$. Comme $\mathbb{R} \subset \mathbb{C}$, on a l'inclusion $\mathbb{R}[X] \subset \mathbb{C}[X]$.

Exemple 1. *Le polynôme* $1 - 2X + 4X^3 - X^5$ *est défini par le suite* $(1, -2, 0, 4, 0, -1, 0, 0, 0, 0, \ldots)$.

Polynômes remarquables :
• le polynôme nul est défini par la suite nulle. Il est noté 0 ou $0_{\mathbb{K}[X]}$.
• les polynômes constants sont définis par les suites nulles à partir du rang 1. Ils sont notés a (au lieu de aX^0), avec $a \in \mathbb{K}$.
• les monômes sont les polynômes de la forme aX^n, avec $a \in \mathbb{K}^*$ et $n \in \mathbb{N}$, et sont définis par les suites dont tous les termes sont nuls sauf un.

Définition 2. Soit $P(X) = \sum_{k\geqslant 0} a_k X^k \in \mathbb{K}[X]$, $P(X) \neq 0$. On appelle degré du polynôme $P(X)$ le plus grand élément de l'ensemble $\{k \in \mathbb{N} \text{ tel que } a_k \neq 0\}$ et on le note $\deg(P(X))$ ou $\deg(P)$

Convention: Si $P(X) = 0$, par convention, le degré de $P(X)$ est $-\infty$.

Exemples 1.
1. *Le degré du polynôme* $1 - 2X + 4X^3 - X^5$ *est égal à* 5.
2. *On dit que* $2X^3$ *est un monôme de degré* 3.

Proposition 1.
$\deg(P) = 0 \Leftrightarrow P$ est une constante non nulle

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

Exemples 2.

1. *$\mathbb{K}_0[X]$ est l'ensemble des polynômes constants,*
2. *$\mathbb{K}_1[X] = \{a_0 + a_1 X$ avec $a_0, a_1 \in \mathbb{K}\}$*
3. *Pour tout $n \in \mathbb{N}$, $\mathbb{K}_n[X] = \{\sum_{k=0}^{n} a_k X^k$ avec $a_0, a_1, \dots, a_n \in K\}$.*

Remarque:$\mathbb{K}[X] = \bigcup_{n\in\mathbb{N}} K_n[X]$. On a

$$\mathbb{K}_0[X] \subset \mathbb{K}_1[X] \subset \mathbb{K}_2[X] \subset \mathbb{K}_3[X] \subset \dots \mathbb{K}[X]$$

Définition 3. Soit $P(X) = \sum_{k\geqslant 0} a_k X^k \in \mathbb{K}[X]$.
• Pour tout $k \in \mathbb{N}$, on dit que $a_k X^k$ est le terme de degré k du polynôme $P(X)$ et a_k est le coefficient d'indice k de $P(X)$.
• Si $P(X) \neq 0$, en notant $n = \deg(P(X))$ on dit que $a_n X^n$ est le terme dominant du polynôme $P(X)$ et a_n est son coefficient dominant.
• Le polynôme $P(X)$ est dit unitaire si son coefficient dominant vaut 1.
• Le coefficient a_0 est appelé le coefficient constant du polynôme $P(X)$.

Remarque. *Les coefficients d'un polynôme sont uniques : deux polynômes P et Q sont égaux si et seulement si leurs coefficients sont égaux.*

Définition 4. Soient $P(X) = \sum_{k\geqslant 0} a_k X^k \in \mathbb{K}[X]$. On appelle fonction polynomiale associée au polynôme $P(X)$ la fonction suivante :

$$\begin{array}{rccl} \tilde{P}: & \mathbb{K} & \to & \mathbb{K} \\ & x & \mapsto & \sum_{k\geqslant 0} a_k x^k \quad \textit{(cette somme est finie)} \end{array}$$

Selon $\mathbb{K}$, c'est une fonction de la variable réelle à valeurs réelles ou une fonction de la variable complexe à valeurs complexes.

Remarque importante : Soient $P(X) = \sum_{k\geqslant 0} a_k X^k$, $Q(X) = \sum_{k\geqslant 0} b_k X^k \in K[X]$ et soient $\tilde{P}$ et $\tilde{Q}$ leurs fonctions polynomiales associées.
• On rappelle que les polynômes $P(X)$ et $Q(X)$ sont égaux si et seulement si $\forall k \in \mathbb{N}$, $a_k = b_k$, c'est-à-dire si et seulement si tous leurs coefficients sont égaux.
• Tandis que par définition de l'égalité de deux fonctions, les fonctions polynomiales $\tilde{P}$ et $\tilde{Q}$ sont égales si et seulement si $\forall x \in K$, $\sum_{k\geqslant 0} a_k x^k = \sum_{k\geqslant 0} b_k x^k$, c'est-à-dire si et seulement si toutes leurs évaluations sont égales.
Ces deux définitions sont fondamentalement différentes !
$*$ *On obtient facilement que si les polynômes $P(X)$ et $Q(X)$ sont égaux, alors leurs fonctions polynomiales associées sont égales. En effet, si $\forall k \in \mathbb{N}$, $a_k = b_k$ alors $\forall x \in K$, $\sum_{k\geqslant 0} a_k x^k = \sum_{k\geqslant 0} b_k x^k$.*
$*$ *Par contre, la réciproque est difficile. C'est un théorème qui a été admis jusqu'à présent sous le nom de " théorème d'identification des coefficients de deux fonctions polynomiales " et qui sera démontré en toute généralité dans ce chapitre. Pour se convaincre de la difficulté de ce théorème, on peut déjà le démontrer " à la main " pour des polynômes de degrés inférieurs ou égaux à 2 . C'est l'exercice suivant :*

Exemple 2. *Soient* $a_0, a_1, a_2, b_0, b_1, b_2 \in K$. *On suppose que* $\forall x \in K$, *on a* $a_0 + a_1 x + a_2 x^2 = b_0 + b_1 x + b_2 x^2$. *Démontrer que* $(a_0, a_1, a_2) = (b_0, b_1, b_2)$.

Proposition 2.

Soit $b \in \mathbb{K}$ et $P(X) = \sum_{k=0}^{n} a_k (X-b)^k$. Alors $P = 0 \Leftrightarrow \forall k \in [\![0, n]\!]$, $a_k = 0$.

remarque: Cela signifie que l'on a aussi l'unicité de l'écriture lorsque P est écrit sous cette forme (et pas seulement dans le cas particulier où $b = 0$).

Preuve: *On écrit*

$$P = \sum_{k=0}^{n} a_k \sum_{j=0}^{k} \binom{k}{j} X^j (-b)^{k-j} = \sum_{j=0}^{n} \left(\sum_{k=j}^{n} \binom{k}{j} a_k (-b)^{k-j} \right) X^j = 0$$

donc pour tout $j \in [\![0, n]\!]$,

$$\sum_{k=j}^{n} a_k \binom{k}{j} (-b)^{k-j} = 0.$$

On obtient un système d'équation $(a_n, a_{n-1}, \ldots, a_0)$ *qui est triangulaire, il admet donc la solution nulle pour unique solution donc* $(a_n, a_{n-1}, \ldots, a_0) = (0, \ldots, 0)$ *et le polynôme* P *est bien nul. On a bien le résultat souhaité.*

1.2 Structure de $\mathbb{K}[X]$

Les polynômes peuvent s'ajouter et se multiplier entre eux. Les lois $+$ et $\times$ sont commutatives, associatives et $\times$ est distributive sur $+$.

Proposition 3.

Soit $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{p} b_k X^k$, alors $PQ = \sum_{k=0}^{n+p} c_k X^k$ avec $c_k = \sum_{j=0}^{k} a_j b_{k-j}$

Remarque. *Ici, on admet que les* a_i *sont nuls pour* $i > n$ *et les* b_j *sont nuls pour* $j > p$. *Cela permet d'éviter la notation suivante, qui est beaucoup plus lourde:*

$$c_k = \sum_{\substack{0 \leqslant i \leqslant n \\ 0 \leqslant j \leqslant p \\ i+j=k}} a_i b_j.$$

Exemples 3.

1. $P = b_0 + b_1 X + b_2 X^2 + b_3 X^3$ *et* $Q = a_0 + a_1 X + a_2 X^2$. *PQ=?*
2. $(aX^2 + bX + c)^2 =?$
3. $(X-a)(X-b)(X-c) =$
4. $(X-a)(X-b)(X-c)(X-d) =$.

Tout polynôme P a un opposé $(-P)$, mais pas d'inverse pour $\times$. En effet, sauf dans le cas où P est un polynôme constant non nul, on peut former $\dfrac{1}{P}$ mais ce n'est pas un élément de $\mathbb{K}[X]$. On dit que $\mathbb{K}[X]$ est un anneau commutatif.

Théorème 4.
Soit $(P, Q) \in \mathbb{K}[X]^2$ tel $PQ = 0$, alors nécessairement soit $P = 0$, soit $Q = 0$.
On dit que l'anneau $\mathbb{K}[X]$ est intègre.

Preuve: *On va montrer la contraposée. On suppose donc P ET Q non nuls, montrons que PQ est non nul. On note a_nX^n et b_mX^m les termes dominants de P et Q, alors le terme de degré $n+m$ de PQ vaut $a_nb_mX^{n+m}$, il est donc non nul*

Remarque. *L'ensemble des fonctions continues n'est pas intègre.*

On peut aussi multiplier un polynôme $\mathbb{K}[X]$ par un scalaire $\lambda \in \mathbb{K}$. On dit que $\mathbb{K}[X]$ est un $\mathbb{K}$-espace vectoriel. Il est également possible de définir la composée de deux polynômes. On utilise la même notation $\circ$ que pour les fonctions.

Proposition 5.
Soit $P, Q \in \mathbb{K}[X]$ non nuls tels que $\deg(P) = n$ et $\deg(Q) = p$. Alors :

- $\deg(P+Q) \leqslant \max\left(\deg(P), \deg(Q)\right)$.
- Si $\deg(P) \neq \deg(Q)$ alors $\deg(P+Q) = \max\left(\deg(P), \deg(Q)\right)$.
- $\forall \lambda \in \mathbb{K}^\star$, $\deg(\lambda P) = \deg(P)$.
- $\deg(PQ) = \deg(P) + \deg(Q)$
- $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

Preuve: ***Preuve:*** *On note $P = \sum_{j=0}^{n} a_jX^j$ et $Q = \sum_{j=0}^{p} b_jX^j$. On ne va montrer que le troisième point. On suppose* $\deg(Q) \neq \deg(P)$. *Quitte à les permuter, on peut supposer $n > p$. On a alors*

$$P + Q = \sum_{j=0}^{p} (a_j + b_j)X^j + \sum_{j=p+1}^{n} a_jX^j.$$

Le terme dominant de $P+Q$ est donc a_nX^n, il est non nul (puisque c'est le terme dominant de P) donc $P+Q$ et P ont bien même degré.

1.3 Dérivation

Définition 5. Soit $P = \sum_{k=0}^{n} a_kX^k$. On appelle dérivée de P le polynôme $P' = \sum_{k=1}^{n} ka_kX^{k-1}$.

Remarques :
Cette notion algébrique de dérivation provient de la dérivation des fonctions polynomiales. Pour tout $P(X) \in K[X]$, on a $(\tilde{P'}) = (\tilde{P})'$ c'est-à-dire que la fonction polynomiale associée à un polynôme dérivé est égale à la fonction dérivée de la fonction polynomiale associée.

Par contre, cette définition algébrique ne fait intervenir aucun taux d'accroissement ni aucun passage à la limite. Elle est toujours applicable. La question de dérivabilité qui existe en analyse n'a pas lieu d'être avec un point de vue uniquement algébrique.

Notations : Pour tout $P(X) \in K[X]$ et tout $n \in \mathbb{N}$, on définit par récurrence la dérivée n-ième de P par $P^{(0)}(X) = P(X)$ et pour tout $n \in \mathbb{N}$, $P^{(n+1)}(X) = (P^{(n)})'(X)$.

Exemples 4.

1. $(1 - 2X + 4X^3 - X^5)' = -2 + 12X^2 - 5X^4$
2. *Soit* $n \in \mathbb{N}^*$ *et soit* $a \in \mathbb{K}$. *On pose* $P(X) = \frac{1}{n!}(X-a)^n$. *On veut calculer le polynôme dérivé de* $P(X)$. *On a* $P'(X) = \dfrac{1}{(n-1)!}(X-a)^{n-1}$, $P^{(k)}(X) = \dfrac{1}{(n-k)!}(X-a)^{n-k}$ *si* $k \leqslant n$, 0 *si* $k > n$.

Plus généralement, les formules de compatibilité entre opérations sur les fonctions (polynomiales) et dérivation restent vraies pour les polynômes. Plus précisément, on la propriété suivante :

Proposition 6.
Pour tout $P(X), Q(X) \in \mathbb{K}[X]$, $\lambda \in K$, on a :

- $(P+Q)' = P' + Q'$
- $(\lambda.P)' = \lambda.P'$
- $(PQ)' = P'Q + PQ'$ et plus généralement $\forall n \in \mathbb{N}^*$, $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$

Preuve: *Cela découle de la linéarité de la somme.*

Proposition 7.
Pour tout $P(X) \in \mathbb{K}[X]$, $\deg(P') = \begin{cases} \deg(P) - 1 & \text{si} \quad \deg(P) \geqslant 1 \\ -\infty & \text{si} \quad \deg(P) \leqslant 0 \end{cases}$

Théorème 8 (Formule de Taylor pour les polynômes)**.**
Soit $P(X) \in \mathbb{K}[X]$ non nul et soit $b \in K$. On a $P(X) = \sum_{j \geqslant 0} \dfrac{P^{(j)}(b)}{j!}(X-b)^j$ ce qui se réécrit, en notant $N \in \mathbb{N}$ tel que $\deg(P) \leqslant N$,

$$P(X) = \sum_{j=0}^{N} \frac{P^{(j)}(b)}{j!}(X-b)^j$$

Preuve: *Soit* P *de degré* $n \neq 0$. *On a déjà vu que le résultat est vrai pour* $b = 0$. *Soit* $b \in \mathbb{K}$ *quelconque. On pose* $R(X) = P(X+b)$. *On a* $R^{(k)}(0) = P^{(k)}(b)$. *On sait que* $R(X) =$

$\sum_{k=0}^{n} \frac{R^{(k)}(0)X^k}{k!}$ *donc*

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

On en déduit que

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

2 Divisibilité

2.1 Diviseurs et facteurs irréductibles

Définition 6. Soit $D, M \in \mathbb{K}[X]$. On dit que M est un multiple de D (ou bien que D est un diviseur de M) s'il existe $Q \in \mathbb{K}[X]$ tel que $M = Q \times D$.

Remarques. *1. toute constante non nul divise tout polynôme*

2. tout multiple d'un polynôme par une cste $k \in \mathbb{K}^\star$ est à la fois un diviseur et un multiple de ce polynôme.

Exemple 3. $2X+6$ *divise* $X+3$ *et* $2X+6$ *est un multiple de* $X+3$.

Théorème 9.
la divisibilité est transitive : si P divise Q et Q divise R alors P divise R.

Théorème 10.
Soit P et Q non nuls. Si P divise Q et $\deg(P) = \deg(Q)$ alors $Q = kP$ où $k \in \mathbb{K}^\star$.

Théorème 11 (Division euclidienne des polynômes)**.**
Soient $A, B \in \mathbb{K}[X]$ tels que $B \neq 0$. Alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $A(X) = B(X) \times Q(X) + R(X)$ et $\deg(R) < \deg(B)$.

Preuve: *On se donne* $A(X) = \sum_{k=0}^{n} \alpha_k X^k$ *et* $B(X) = \sum_{k=0}^{m} \beta_k X^k$*. Si* $m > n$*, alors les polynômes* 0 *et* A *donnent l'égalité souhaité. On suppose donc* $n \geqslant m$*. Le polynôme*

$$A_1(X) = A(X) - \frac{\alpha_n}{\beta_m} X^{n-m} B(X),$$

est alors de degré strictement inférieur à n*.*

- *S'il est nul, on a la division euclidienne avec un reste nul.*
- *Sinon, on note* d_1 *son degré.*
  - *Si* $d_1 < m$*, alors* $A = \frac{\alpha_n}{\beta_m} X^{n-m} B(X) + A_1(X)$ *est la division euclidienne.*

– *Sinon, et on va soustraire à* A_1 *un polynôme de la forme* $k_1 X^{d_1-m}B(X)$ *de façon à obtenir un polynôme* A_2 *de degré strictement inférieur à* d_2.

La suite des degrés d_i *étant une suite d'entiers positifs strictement décroissante, il va exister un rang* r *où* $d_r < m$ *et on aura fini. On aura donc des polynômes* A_j *de degré* d_j *et des constantes* k_j *tels que*

$$A_{j+1} = A_j - k_j X^{d_j-m}B(X) \text{ donc } A_j - A_{j+1} = k_j X^{d_j-m}B(X).$$

En posant $A_0 = A$ *et* $d_0 = n$, *on peut sommer ces égalités pour* j *allant de* 0 *à* $r-1$, *on obtient*

$$A - A_r = \sum_{j=0}^{r} k_j X^{d_j-m}B(X) \text{ d'où } A = \left(\sum_{j=0}^{r} k_j X^{d_j-m}\right) B(X) + A_r,$$

avec $\deg(A_r) < m$.

On a montré l'existence. Reste à montrer l'unicité.

On suppose par l'absurde qu'il existe $(Q_1, R_1) \neq (Q_2, R_2)$ *tels que*

$$A = Q_1 B + R_1 = Q_2 B + R_2 \text{ avec } \deg(R_i) < \deg(B).$$

On a donc

$$B \times (Q_1 - Q_2) + (R_1 - R_2).$$

Le polynôme $R_1 - R_2$ *est non nul donc l'un des deux* R_i *au moins est non nul, le degré de la différence vaut donc au plus* $\deg(B)$. *Par ailleurs,* $\deg(B \times (Q_1 - Q_2)) = \deg(B) + \deg(Q_1 - Q_2) \geqslant \deg(B)$. *On obtient une contradiction puisque* $B \times (Q_1 - Q_2) = -(R_1 - R_2)$.

Définition 7. Avec les notations du théorème précédent, Q est appelé quotient et R est le reste de la division euclidienne de A par B.

Exemples 5.

1. *Calculer le quotient et le reste de la division euclidienne de* $2X^4 + 5X^3 + 3X^2 + 2X - 6$ *par* $X^2 + X - 1$.
   En posant la division euclidienne, on trouve $Q(X) = 2X^2 + 3X + 2)$ *et* $R(X) = 3X - 4$.
2. *Calculer le reste de la division euclidienne de* $X^{17} + 5X^8 - 4$ *par* $X^2 - 1$.
   On sait que le reste est de la forme $aX + b$, *on a* $a + b = 2$ *et* $0 = -a + b$ *d'où* $a = b = 1$.

Définition 8. Polynômes irréductibles de $\mathbb{K}[X]$: Un polynôme $P \in \mathbb{K}[X]$ est dit irréductible lorsqu'il est non constant et lorsque ses seuls diviseurs sont les kP avec $k \in \mathbb{K}^\star$, ainsi que les polynômes constants non nuls.

Remarque. *Les polynômes irréductibles dans* $\mathbb{K}[X]$ *sont analogues des nombres premiers dans* $\mathbb{Z}$. *Pourquoi alors ne peut-on dire d'un polynôme irréductible que "ses seuls diviseurs sont lui même et 1" ? Parce que toutes les constantes non nulles divisent un polynôme, et tous ses multiples par un scalaire non nul aussi.*

⚠ la propriété "d'être irréductible ", pour un polynôme, dépend du corps $\mathbb{K}$ considéré.

Exemple 4. $X^2 + 1$ *est irréductible dans* $\mathbb{R}[X]$ *mais pas dans* $\mathbb{C}[X]$.

2.2 Racines et diviseurs

Proposition 12.
Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors :
a est une racine de P ssi $P(a) = 0$, ssi $(X - a)$ divise P, ssi il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - a)Q$.

Preuve: *On suppose $P(a) = 0$, on écrit $P(X) = (X - a)Q(X) + R(X)$ avec $\deg(R) < 1$, R est donc une constante. En évaluant l'égalité en a, on montre que R est nul, on a donc bien $X - a|P$. Réciproquement, si $(X - a)$ divise P alors $P(X) = (X - a)Q(X)$ donc on a bien $P(a) = 0$.*

Proposition 13.
Soit $P \in \mathbb{K}[X]$. Si a et b sont deux racines distinctes de P, alors $(X - a)(X - b)$ divise P.

Preuve: *On suppose que a et b sont deux racines distinctes, alors*

$$P(X) = (X - a)(X - b)Q(X) + R(X)$$

avec $\deg(R) < 2$. On a donc $R(X) = \alpha X + \beta$. En évaluant en a et b, on obtient

$$\begin{cases} \alpha a + \beta & = 0 \\ \alpha b + \beta & = 0 \end{cases}$$

donc

$$\begin{cases} \alpha a + \beta & = 0 \\ \alpha(a - b) & = 0 \end{cases}$$

Le système d'inconnues (α, β) est triangulaire avec des pivots non nuls donc il admet seulement la solution nulle, on a bien $R = 0$.

Exemples 6.

1. *Montrer que $\forall n \in \mathbb{N}$, le polynôme $A = X^2 - X + 1$ divise le polynôme $P_n = (X-1)^{n+2} + X^{2n+1}$.*
2. *Décomposer $Q = 15X^4 + 2X^2 - 1$ en produit de polynômes irréductibles.*
3. *Montrer que $X^3 + 2X^2 + X$ divise $X^5 + 3X^4 + 4X^3 + 3X^2 + X$*

Définition 9. Si $(X - a)^m$ divise P et $(X - a)^{m+1}$ ne divise pas P alors on dit que a est racine de multiplicité m de P.

Théorème 14.
Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors :
a est racine de P de multiplicité m ssi $P = (X - a)^m Q$ avec $Q \in \mathbb{K}[X]$ et $Q(a) \neq 0$.

Preuve: *On suppose tout d'abord a racine de multiplicité m, on a donc $(X - a)^m|P$ et $(X - a)^{m+1}$ ne divise pas P. On en déduit qu'il existe Q_1 tel que*

$$P(X) = (X - a)^m Q(X),$$

puis Q_1, r tel que $Q(X) = (X - a)Q_1(X) + r$ avec r une constante. On a donc

$$P(X) = (X - a)^{m+1} Q_1(X) + r(X - a)^m.$$

Par unicité de la division euclidienne, $r(X-a)^m$ est le reste de la division euclidienne de P par $(X-a)^{m+1}$, il est donc non nulle, par hypothèse. On en déduit que $r \neq 0$ donc $Q(a) = r \neq 0$, on a bien la première implication.

Réciproquement, on suppose que $P(X) = (X-a)^m Q(X)$ avec $Q(a) \neq 0$. Il est clair que $(X-a)^m | P$. Par ailleurs, $Q(a) \neq 0$ implique $Q(X) = (X-a)Q_1(X) + r$ avec $r \neq 0$. En remplaçant $Q(X)$ par son expression, on obtient

$$P(X) = (X-a)^{m+1}Q_1(X) + r(X-a)^m,$$

donc le reste de la division euclidienne de P par $(X-a)^{m+1}$ n'est pas nul ce qui montre que $(X-a)^{m+1}$ ne divise pas P.

Définition 10. Une racine de multiplicité 1 d'un polynôme est appelée racine simple ; de multiplicité 2, racine double, En général si multiplicité>1, racine multiple.

Théorème 15.
Si $P, Q \in \mathbb{K}[X]$ et P divise Q, alors les racines de P sont aussi racines de Q.

Preuve: *On suppose que P divise Q, alors il existe A tel que $P(X)A(X) = Q(X)$. Soit α une racine de P, alors $P(\alpha)A(\alpha) = 0$ donc α est racine de Q.*

La réciproque n'est pas vraie en général :
que P divise Q.

Exemple 5. *$P(X) = (X-1)^2$ et $Q(X) = (X-1)(X-2)$.*

2.3 Racines et dérivées

Théorème 16.
Soit $P \in \mathbb{K}[X]$ non constant et $a \in \mathbb{K}$. Alors a est une racine de P de multiplicité m si et seulement si

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

Exemple 6. *Montrer que $X^3 + 2X^2 + X$ divise $X^5 + 3X^4 + 4X^3 + 3X^2 + X$*

Preuve: *Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On écrit $P(X) = \displaystyle\sum_{k=0}^{n} \frac{P^{(k)}(a)(X-a)^k}{k!}$.*

On suppose a racine de P de multiplicité m. On a

$$P(X) = (X-a)^m Q(X) \text{ avec } Q(a) \neq 0$$

On écrit

$$\begin{aligned}
(X-a)^m Q(X) &= (X-a)^m \sum_{j=0}^{n-m} \frac{Q^{(j)}(a)(X-a)^j}{j!} \\
&= \sum_{j=0}^{n-m} \frac{Q^{(j)}(a)(X-a)^{j+m}}{j!} \\
&= \sum_{k=m}^{n} \frac{Q^{(k-m)}(a)(X-a)^k}{(k-m)!}
\end{aligned}$$

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

Par unicité de l'écriture, on a $P^{(k)}(a) = 0$, $\forall k \in [\![0, m-1]\!]$ *et* $\frac{P^{(m)}(a)}{m!} = Q^{(0)}(a) \neq 0$.

Réciproquement, supposons que $\forall k \in [\![0, m-1]\!]$, $P^{(k)}(a) = 0$ *et* $P^{(m)}(a) \neq 0$. *On a alors*

$$\begin{aligned} P(X) &= \sum_{k=0}^{n} \frac{P^{(k)}(a)(X-a)^k}{k!} \\ &= \sum_{k=m}^{n} \frac{P^{(k)}(a)(X-a)^k}{k!} \\ &= (X-a)^m \sum_{k=m}^{n} \frac{P^{(k)}(a)(X-a)^{k-m}}{k!} \end{aligned}$$

On pose $Q(X) = \sum_{k=m}^{n} \frac{P^{(k)}(a)(X-a)^{k-m}}{k!}$. *On a* $Q(a) = \frac{P^{(m)}(a)}{m!} \neq 0$, *a est bien racine de P de multiplicité m.*

3 Thm de d'Alembert-Gauss et conséquences

3.1 Théorème de d'Alembert-Gauss

Théorème 17 (Théorème de d'Alembert-Gauss (admis))**.** *Soit* $P \in \mathbb{C}[X]$ *un polynôme non constant. Alors il admet au moins une racine sur* $\mathbb{C}$.

Proposition 18.
Soit $P \in \mathbb{R}[X]$. Si $\alpha \in \mathbb{C}$ est racine de P, alors $\overline{\alpha}$ est aussi racine de P.

3.2 Polynômes irréductibles

Proposition 19.
Les polynômes irréductibles sur $\mathbb{C}[X]$ sont les polynômes de degré 1.

Preuve: *Les polynômes de degré 1 sont irréductibles sur* $\mathbb{C}$, *montrons que ce sont les seuls. Soit P un polynôme de degré au moins 2. Alors, d'après d'Alembert Gauss, il existe* $\alpha \in \mathbb{C}$ *racine de P. Donc* $(X-\alpha)$ *divise P. Comme P est de degré au moins 2, P s'écrit comme le produit de deux polynômes non constants, il n'est donc pas irréductible.*

Proposition 20.
Les polynômes irréductible sur $\mathbb{R}[X]$ sont :

- Les polynômes de degré 1
- Les polynômes de degré 2 de discriminant strictement négatifs.

Preuve: *Les polynômes de degré 1 sont clairement irréductibles sur* $\mathbb{R}[X]$. *Soit maintenant P un polynôme de degré 2 de discriminant strictement négatif. S'il n'est pas irréductible, il s'écrit*

$P+AB$ avec A et B de degré au moins 1 donc de degré 1. Mais A et B sont à coefficients réels, ils admettent donc des racines réelles ce qui contredit le discriminant strictement négatif. Montrons que ce sont les seuls polynômes irréductibles sur $\mathbb{R}[X]$. Soit d'abord P de degré 2. Alors, si le discriminant est positif ou nul, P admet une racine réelle, il n'est donc pas irréductible sur $\mathbb{R}[X]$. Soit maintenant P de degré supérieur ou égal à 3. D'après d'Alembert Gauss, il admet une racine α. Si α est réelle, alors P n'est pas irréductible. Si α est strictement complexe, alors $\overline{\alpha}$ est aussi racine de P donc $(X-\alpha)(X-\overline{\alpha})$ divise P et comme $(X-\alpha)(X-\overline{\alpha}) = X^2 - 2\mathcal{R}e(\alpha)X + |\alpha|^2 \in \mathbb{R}[X]$, cela signifie qu'il existe $Q \in \mathbb{R}[X]$ tel que $P(X) = \left(X^2 - 2\mathcal{R}e(\alpha)X + |\alpha|^2\right) Q(X)$. On sait que $\deg(P) \geqslant 3$ donc $\deg(Q) \geqslant 1$ ce qui montre que P n'est pas irréductible.

Un polynôme peut n'avoir aucune racine réelle mais ne pas être irréductible.

Exemple 7. $P(X) = (X^2+1)^2$.

3.3 Factorisation

3.3.1 Définition

Théorème 21.
Tout polynôme de $\mathbb{K}[X]$ se décompose en produit de polynômes irréductibles de $\mathbb{K}[X]$ et cette décomposition est unique à un facteur constant près et à l'ordre des facteurs. $\forall P \in \mathbb{K}[X], \exists Q_1, Q_2, \dots, Q_p$ irréductibles dans $\mathbb{K}[X]$ tels que $P = Q_1 \times Q_2 \times \dots \times Q_p$. En rassemblant les facteurs identiques :

$$P = \prod_{i=1}^{s} Q_i^{m_i},$$

m_i est appelé ordre de multiplicité de Q_i dans la décomposition de P en facteurs irréductibles.

3.3.2 Décomposition sur $\mathbb{C}[X]$

Théorème 22.
Soit $P \in \mathbb{C}[X]$, alors P s'écrit sous la forme $P = \lambda \displaystyle\prod_{i=1}^{r} (X-a_i)^{m_i}$ avec $m_i > 0$. Cette écriture est unique à l'ordre des facteurs près. Le scalaire λ est le coefficient dominant de P.

Les facteurs irréductibles de P sont les $(X-a_i)$, et non les les $(X-a_i)^{m_i}$.

Remarque. *Si $a_1, a_2, \dots, a_n$ sont racines de P de multiplicités respectives $m_1, m_2, \dots, m_n$ alors $(X-a_k)^{m_k}$ divise P, les $(X-a_k)$ sont les facteurs unitaires de degré 1 de la décomposition de P en facteurs irréductibles. Déterminer les racines d'un polynôme permet de déterminer les facteurs de degré 1 de sa décomposition en facteurs irréductibles.*

Exemples 7.

1. *Décomposer $X^n - 1$.*

2. *Décomposer $P = 2X^3 - (5+6i)X^2 + 9iX + 1 - 3i$ dans $\mathbb{C}[X]$ sachant qu'il possède une racine réelle.*

3.3.3 Décomposition sur $\mathbb{R}[X]$

Théorème 23.
Soit $P \in \mathbb{R}[X]$, alors il existe $(a_1, \dots, a_r) \in \mathbb{R}^r$, $(m_1, \dots, m_r) \in (\mathbb{N}^\star)^r$, $(Q_1, \dots, Q_s) \in \mathbb{R}[X]^s$ et $(\alpha_1, \dots, \alpha_s) \in (\mathbb{N}^\star)^s$, où les Q_i sont des polynômes de degré 2, de discriminant strictement négatif, tels que

$$P(X) = \prod_{i=1}^{r} (X - a_i)^{m_i} \times \prod_{j=1}^{s} Q_j^{\alpha_j}.$$

3.3.4 Polynômes scindés

Définition 11. Un polynôme est dit scindé sur $\mathbb{K}[X]$ si tous ses facteurs irréductibles, dans sa décomposition sur $\mathbb{K}[X]$, sont de degré 1.

Proposition 24.
Tout polynôme est scindé sur $\mathbb{C}[X]$.

Preuve: *On a déjà vu que les polynômes irréductibles sur $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.*

Proposition 25.
Un polynôme de $\mathbb{R}[X]$ est scindé sur $\mathbb{R}$ si et seulement si toutes ses racines sont réelles.

Preuve: Si P est scindé, toutes ses racines réelles. Pour montrer l'autre implication, montrons la contraposée. On suppose que P n'est pas scindé, alors un de ses facteurs irréductibles est de degré 2, il admet donc deux racines complexes conjuguées.

Exemples 8.

1. $(X - i)(X + i)^2$ *scindé*

2. $(X + 2)(X - 1 - i)$ *simplement scindé*

Proposition 26.
Soit $P \in \mathbb{K}[X]$ un polynôme scindé sur $\mathbb{K}$ et $\alpha_1, \dots, \alpha_n$ ses racines comptées avec multiplicité.

Alors si $P = \sum_{k=0}^{n} a_k X^k$, on a

- $a_0 = a_n(-1)^n \prod_{i=1}^{n} \alpha_i$
- $a_{n-1} = -a_n \sum_{i=1}^{n} \alpha_i$

3.4 Nombre de racines

Théorème 27.
Un polynôme de $\mathbb{C}[X]$ de degré $n \in \mathbb{N}$ admet exactement n racines (comptées avec leur ordre de multiplicité).
Un polynôme de $\mathbb{R}[X]$ de degré $n \in \mathbb{N}$ admet au plus n racines (comptées avec leur ordre de multiplicité).

Preuve: *On reprend la décomposition en facteurs premiers.*

- *Si* $P \in \mathbb{C}[X]$, *alors* $\deg(P) = \sum_{i=1}^{r} m_i$.
- *Si* $P \in \mathbb{C}[X]$, *alors* $\deg(P) \geqslant \sum_{i=1}^{r} m_i$

Théorème 28.
Si un polynôme supposé de degré $n \in \mathbb{N}$ admet strictement plus de n racines (comptées avec leur ordre de multiplicité), alors il est le polynôme nul.

Preuve: *On suppose, par l'absurde, qu'il est non nul. Alors il admet au plus n racines comptées avec multiplicité. On a une contradiction.*

Exemple 8. *Soit* $f : x \mapsto \sum_{k \geqslant 0} a_k x^k$ *et* $g : x \mapsto \sum_{k \geqslant 0} b_k x^k$ *deux fonctions polynomiales telles que* $\forall x \in \mathbb{R}, f(x) = g(x)$. *Montrer que pour tout* k, $a_k = b_k$.

Méthode : Pour démontrer qu'un polynôme P est nul, on peut prouver, au choix :

- que tous ses coefficients sont nuls
- que $\forall x \in \mathbb{R}, P(x) = 0$
- que le nombre de racines de P, comptées avec leur ordre de multiplicité, est strictement plus grand que le degré supposé de P (voire est infini)
- que $deg(P) < 0$

Remarque: Pour montrer que $P = Q$, on montre que $P - Q$ est le polynôme nul.

4 Décomposition en éléments simple

Définition 12. On appelle fraction rationnelle un quotient de deux polynômes dont le dénominateur est non nul : $\dfrac{P(X)}{Q(X)}$ avec $Q \neq 0$.

Les zéros de la fraction rationnelle $\dfrac{P}{Q}$ sont les racines de P. Les pôles de la fraction rationnelle $\dfrac{P}{Q}$ sont les racines de Q.

Remarque: On ne rentrera pas dans les détails formels des fractions rationnelles, l'objectif étant uniquement calculatoire.

Théorème 29 (décomposition en éléments simples d'une fraction rationnelle à pôles simples)**.**

Soit $(P, Q) \in \mathbb{K}[X] \times \mathbb{K}[X] \setminus \{0\}$ tel que $Q(X) = \lambda \prod_{i=1}^{r} (X - a_i)$ avec les a_i deux à deux distincts. Alors si on note A le quotient de la division euclidienne de P par Q, il existe un unique $(\alpha_1, \ldots, \alpha_r) \in \mathbb{K}^r$ tel que

$$\frac{P}{Q} = A + \sum_{i=1}^{r} \frac{\alpha_i}{X - a_i}.$$

Remarque: La décomposition en éléments simples pour des fractions rationnelles admettant des pôles multiples ou pour laquelle Q n'est pas scindé existe mais sa forme doit vous être donnée.

Exemples 9.

1. *Déterminer la décomposition en éléments simples de* $\dfrac{X^2 + 2X + 5}{X^2 - 3X + 2}$.
2. *Déterminer la décomposition en éléments simples de* $\dfrac{4X^3}{X^4 - 1}$.
3. (a) *Déterminer la décomposition en éléments simples de* $\dfrac{1}{X(X+1)(X+2)}$
   (b) *Soit* $f : \begin{cases} \mathbb{R} \setminus \{-2, -1, 0\} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \dfrac{1}{x(x+1)(x+2)} \end{cases}$.
      i. *Déterminer une primitive de* f.
      ii. *Calculer les dérivées* n*-ièmes de* f *pour* $n \in \mathbb{N}$.
   (c) *Soit* $n \in \mathbb{N}^\star$*, calculer* $\displaystyle\sum_{k=1}^{n} \frac{1}{k(k+1)(k+2)}$.