Chapitre XVI : Les polynômes

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

Introduction

Formellement, on définit un polynôme comme une suite $(a_0, a_1, a_2, a_3, \dots, a_n, \dots) \in \mathbb{K}^{\mathbb{N}}$ à valeurs dans $\mathbb{K}$, dont tous les termes sont nuls à partir d'un certain rang.
Par exemple, le polynôme $4X^7 + 2X^6 - X^5 + 2X^3 - 8X - 12$ s'écrit comme la suite

$$(-12, -8, 0, 2, 0, -1, 2, 4, 0, 0, 0, 0, \dots).$$

Il est assez facile de vérifier que la somme de deux suites ayant un nombre fini de termes non nuls (donc de deux polynômes) est encore une suite ayant un nombre fini de termes non nuls : pour $n, m \in \mathbb{N}$ avec $n \geqslant m$,

$$(a_0, a_1, \dots, a_m, \dots, a_n, 0, 0, \dots) + (b_0, b_1, , \dots, b_m, 0, 0, \dots) = (a_0 + b_0, a_1 + b_1, \dots, a_m + b_m, a_{m+1}, \dots, a_n, 0, 0, \dots).$$

On peut multiplier également une suite ayant un nombre fini de termes non nul par un scalaire $\lambda \in \mathbb{K}$ et obtenir une suite ayant un nombre fini de termes non nuls : pour $n \in \mathbb{N}$,

$$\lambda\,(a_0, a_1, \dots, a_m, \dots, a_n, 0, 0, \dots) = (\lambda\, a_0, \lambda\, a_1, \dots, \lambda\, a_n, 0, 0, \dots).$$

On appelle maintenant 1 la suite $(1, 0, 0, \dots)$, qui est bien un polynôme, X la suite $(0, 1, 0, 0, \dots)$ qui est aussi un polynôme, X^2 la suite $(0, 0, 1, 0, \dots)$ et ainsi de suite : pour tout $k \in \mathbb{N}$,

$$X^k = (0, 0, \dots, 0, \underbrace{1}_{\text{position } k}, 0, \dots).$$

On s'aperçoit alors que

$$(a_0, a_1, a_2, \dots, a_n, 0, 0, \dots) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n.$$

Le grand X désigne l'inconnu des polynômes et n'est donc pas un réel. L'utilité des polynômes est de définir des opérations algébriques sans donner la nature explicite de X puis de transposer ces résultats à tout ensemble d'objets mathématiques pourvu qu'il soit compatible avec quelques règles élémentaires d'addition et de multiplication (les réels, les matrices, les fonctions,...).

I Définition

Définition I.1

- On appelle **polynôme** P tout $n+1$-uplet, $n \in \mathbb{N}$, de $\mathbb{K}$: $(a_0, a_1, \dots, a_n)$ que l'on écrit
$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n.$$
- Le scalaire a_k est appelé le k-ième **coefficient** de P.
- On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$.

Remarque 1 :

- De la même façon que $i = (0, 1)$ est un complexe que l'on ne présente pas à chaque raisonnement, *l'indéterminée* X n'est pas une *variable*. On dira donc : soit $P \in \mathbb{K}[X]$ le polynôme définit par $P = 1 + X + X^2$ et non soit P le polynôme défini par $X \mapsto 1 + X + X^2$ ou encore défini pour tout $X \in \mathbb{K}$, par $P(X) = 1 + X + X^2$.
- L'étude des polynômes de façon formelle (en gardant l'indéterminée X) peut par la suite s'appliquer à obtenir des résultats sur les réelles par exemple en s'intéressant à $x \mapsto x^2 + x + 1$, sur les fonctions en regardant $f \circ f + f + \mathrm{Id}$, sur les matrices en regardant $A^2 + A + I_n$. On peut même appliquer les polynômes... à des polynômes ! en regardant $1 + P + P^2$ (cf plus loin pour le produit de polynômes).

- Les polynômes constants s'écrivent simplement $P = a_0 \in \mathbb{K}$ et donc on injecte $\mathbb{K} \subseteq \mathbb{K}[X]$.
- On note parfois $P = \sum_{k=0}^{+\infty} a_k X^K$, avec la convention $X^0 = 1$, le polynôme P. Cela implique que les coefficients a_k sont tous nuls à partir d'un certain rang.
- On appelle polynôme nulle le polynôme dont tous les coefficients sont nuls.
- Deux polynômes sont égaux si et seulement si leurs coefficients coïncident :

$$P = \sum_{k=0}^{+\infty} a_k X^k = \sum_{k=0}^{+\infty} b_k X^k = Q \qquad \Leftrightarrow \qquad \forall k \in \mathbb{N},\ a_k = b_k.$$

Définition I.2

Soient $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$ deux polynômes de $\mathbb{K}[X]$.

- *(Addition).* On pose $P + Q$ le polynôme défini par

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

- *(Multiplication).* On pose PQ le polynôme défini par

$$PQ = \sum_{k=0}^{+\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k.$$

- *(Multiplication par un scalaire).* On pose λP le polynôme défini par

$$\lambda P = \sum_{k=0}^{+\infty} \lambda a_k X^k.$$

Exemple 2 :

1. On pose $P = 1 + 2X - 3X^2 + X^3$ et $Q = X - X^2$. Calculer $2P$, PQ et $P + Q$ avec les formules et montrer que cela correspond à aux calculs classiques.

Définition I.3

Soient P et Q deux polynômes de $\mathbb{K}[X]$, $n \in \mathbb{N}$. On pose $P = \sum_{k=0}^{n} a_k X^k$. On définit alors la composée $P \circ Q$ par

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

Exemple 3 : Soient $P = 1 + X + X^2$ et $Q = 1 + X$. Calculer $Q \circ P$ et $P \circ Q$.

Exemple 4 : Pour tout $P \in \mathbb{K}[X]$, on a $P \circ X = P$. On note alors souvent $P(X) = P \circ X = P$.

Définition I.4

- Soit $P = \sum_{k=0}^{+\infty} a_k X^k$ un polynôme, on définit le **degré** de P par

$$P = \begin{cases} \max\{k \in \mathbb{N} \mid a_k \neq 0\} \text{ si } P \neq 0 \\ -\infty \text{ si } P = 0 \end{cases}$$

- Un polynôme ayant un seul coefficient non nul $R = a_n X^n$ est appelé un monôme.
- Si $P = \sum_{k=0}^{+\infty} \neq 0$ et $n = \deg(P) \in \mathbb{N}$, alors le coefficient a_n est appelé **le coefficient dominant** de P et le monôme $a_n X^n$ **le terme dominant de** P. Le polynôme P s'écrit alors $P = \sum_{k=0}^{n} a_k X^k = a_n X^n + \cdots + a_1 X + a_0$.
- Si le coefficient dominant du polynôme P est égal à 1, on dit que le polynôme P est **unitaire** ou normalisé.

Proposition I.5

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

1. $\deg(P+Q) \leqslant \max(\deg(P), \deg(Q))$, avec égalité si $\deg(P) \neq \deg(Q)$.
2. $\deg(PQ) = \deg(P) + \deg(Q)$.
3. $\deg(\lambda P) = \begin{cases} \deg(P) & \text{si } \lambda \neq 0 \\ -\infty & \text{si } \lambda = 0 \end{cases}$.
4. $\deg(P \circ Q) = \deg(P) \times \deg(Q)$ si $P \neq 0$ et $Q \neq 0$.

Exemple 5 : A connaître.
L'anneau $\mathbb{K}[X]$ est intègre. Soit $(P, Q) \in \mathbb{K}[X]^2$, montrer que $PQ = 0 \Rightarrow P = 0$ OU $Q = 0$.

Définition I.6

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

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

Proposition I.7

Soit $n \in \mathbb{N}$. L'ensemble $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$.

1. L'ensemble $\mathbb{K}_n[X]$ est inclus dans $\mathbb{K}[X]$: $\mathbb{K}_n[X] \subseteq \mathbb{K}[X]$.
2. Le polynôme nul est dans $\mathbb{K}_n[X]$: $0 \in \mathbb{K}_n[X]$.
3. L'ensemble $\mathbb{K}_n[X]$ est stable par combinaison linéaire : $\forall (\lambda, \mu) \in \mathbb{K}$, $\forall (P, Q) \in \mathbb{K}_n[X]$, on a
$$\lambda P + \mu Q \in \mathbb{K}_n[X].$$

Définition I.8

Soient $n \in \mathbb{N}$ et $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$.

1. Pour tout $\alpha \in \mathbb{K}$, on définit le scalaire $P(\alpha)$ par $P(\alpha) = \sum_{k=0}^{n} a_k \alpha^k$.
2. Pour toute fonction $f \in \mathscr{F}(\mathbb{K}, \mathbb{K})$, on définit la fonction $P(f)$ par $P(f) = \sum_{k=0}^{n} a_k f^k$, où $f^0 = \mathrm{Id}$.
3. Pour tout $A \in \mathscr{M}_p(\mathbb{K})$, on définit la matrice $P(A)$ par $P(A) = \sum_{k=0}^{n} a_k A^k$, où $A^0 = I_p$.

Exemple 6 : Si $P = 1 + X^2 - 2X^3$. Pour $\alpha = 2$, calculer $P(\alpha)$. Pour $f : x \mapsto x+1$, calculer $P(f)$. Pour $A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$, calculer $P(A)$.

Définition I.9

Soient $n \in \mathbb{N}$ et $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$. On appelle **fonction polynomiale** associée à P la fonction

$$\begin{aligned} \tilde{P} \quad : \quad & \mathbb{R} \to \mathbb{K} \\ & x \mapsto P(x). \end{aligned}$$

Exemple 7 : Si $P = 4 + 2X - X^3 + 12X^4 + X^9$, alors la fonction polynomiale associée à P est $\tilde{P} : x \mapsto 4 + 2x - x^3 + 12x^4 + x^9$.

II Dérivation

Définition II.1

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

$$P' = \sum_{k=1}^{n} k a_k X^{k-1} = \sum_{k=0}^{n-1} (k+1)\, a_{k+1} X^k.$$

Remarque 8 :

- La définition ci-dessus est formelle et fonctionne pour tous les polynômes. De même qu'il est maladroit et même erroné de présenter X comme une variable, on ne justifie pas que P est dérivable, car on ne parle pas dans cette définition de taux d'accroissement.
- Bien entendu cette définition de dérivée pour les *polynôme* est cohérente avec la définition de la dérivée pour les *fonctions* polynomiales : si $\tilde{P} \in \mathscr{F}(\mathbb{R}, \mathbb{K})$ est une fonction polynomiale, alors $\tilde{P}$ est dérivable sur $\mathbb{R}$ (au sens fonction) et de plus sa dérivée $\left(\tilde{P}\right)'$ est la fonction polynomiale $(\tilde{P'})$ associée à P' (dérivée de P au sens polynôme).

Proposition II.2

Soient P, $Q \in \mathbb{K}[X]$ deux polynômes et λ, $\mu \in \mathbb{K}$ deux scalaires.

1. Si $\deg(P) \geqslant 1$, alors $\deg(P') = \deg(P) - 1$.
2. Le polynôme P est constant si et seulement si $P' = 0$.
3. *(Linéarité).* $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$.
4. *(Produit).* $(PQ)' = P'Q + PQ'$
5. *(Composition).* $(P \circ Q)' = Q' (P' \circ Q)$.

Proposition II.3

On définit par récurrence pour tout $r \in \mathbb{N}$, la dérivée r-ième de P par

$$P^{(0)} = P \qquad \text{et} \qquad P^{(r+1)} = \left(P^{(r)}\right)'.$$

Exemple 9 :

$$\forall n \in \mathbb{N},\ \forall r \in \mathbb{N}, \qquad (X^n)^{(r)} = \begin{cases} X^n & \text{si } r = 0 \\ n(n-1)\dots(n-r+1)X^{n-r} = \frac{n!}{(n-r)!} X^{n-r} & \text{si } 0 < r \leqslant n \\ 0 & \text{si } r > n. \end{cases}$$

Proposition II.4

Soient P, $Q \in \mathbb{K}[X]$ deux polynômes, λ, $\mu \in \mathbb{K}$ deux scalaires et n et $r \in \mathbb{N}$ deux entiers.

1. Si P est non nul de degré n et si $r \leqslant n$ alors $P^{(r)}$ est de degré $n - r$.
2. Si $r > n$, alors $P^{(r)} = 0$.
3. *(Linéarité).* $(\lambda P + \mu Q)^{(r)} = \lambda P^{(r)} + \mu Q^{(r)}$.
4. *(Formule de Leibniz)* $(PQ)^{(r)} = \sum_{k=0}^{r} \binom{k}{r} P^{(k)} Q^{(r-k)}$.

Proposition II.5 (Formule de Taylor pour les polynômes)

Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n \in \mathbb{N}$ (P non nul), alors pour tout $h \in \mathbb{K}$,

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

ou encore

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

Démonstration. Soit $n \in \mathbb{N}$, $P \in \mathbb{K}_n[X]$ et $h \in \mathbb{K}$. On note $Q = P(X+h) = P \circ (X+h)$. On a $\deg(Q) = \deg(P) \times \deg(X+h) = n \times 1 = n$. On pose alors $(b_0, \dots, b_n) \in \mathbb{K}^n$ les coefficients de Q :

$$Q = \sum_{k=0}^{n} b_k X^k.$$

En calculant les dérivées successives de Q, on obtient pour tout $r \in \{1, \dots, n\}$

$$\begin{aligned}
Q &= b_0 + b_1 X + b_2 X^2 + b_3 X^3 + \cdots + b_n X^n \\
Q' &= b_1 + 2b_2 X + 3b_3 X^2 + 4b_4 X^3 + \cdots + n b_n X^{n-1} \\
Q'' &= 2b_2 + 6b_3 X + 4 \times 3 b_4 X^2 + 5 \times 4 b_5 X^3 + \cdots + n(n-1) b_n X^{n-2} \\
&\vdots \\
Q^{(r)} &= r! b_r + \frac{(r+1)!}{1!} b_{r+1} X + \cdots + \frac{n!}{(n-r)!} X^{n-r}.
\end{aligned}$$

Notamment $Q^{(r)}(0) = r! b_r$.
D'autre part, par dérivée de la composée, on a

$$\begin{aligned}
Q' &= (P \circ (X+h))' = P' \circ (X+h) \\
Q'' &= P'' \circ (X+h) \\
&\vdots \\
Q^{(r)} &= P^{(r)} \circ (X+h).
\end{aligned}$$

Par conséquent, $Q^{(r)}(0) = P^{(r)}(h)$. Conclusion, pour tout $r \in \{1, \dots, n\}$

$$b_r = \frac{P^{(r)}(h)}{r!}.$$

Autrement dit,

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

Enfin, on observe que $Q \circ (X-h) = P \circ (X+h) \circ (X-h) = P$ et donc

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

□

Remarque 10 : En particulier si $h = 0$ alors $P = \sum_{k=0}^{n} a_k X^k = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!} X^k$ et donc

$$\forall k \in \mathbb{N}, \quad a_k = \frac{P^{(k)}(0)}{k!}.$$

(la formule est facilement vérifiable pour $k > n = \deg(P)$ car alors $a_k = 0$ et $P^{(k)} = 0$)

III Division dans $\mathbb{K}[X]$

Définition III.1

Soit $(P,Q)\in\mathbb{K}[X]^2$ deux polynômes. On dit que Q **divise** Q ou P est un **multiple** de Q si et seulement s'il existe $R\in\mathbb{K}[X]$ tel que $P=QR$. On note alors $P|Q$.

Exemple 11 :

1. Le polynôme $(X-1)(X+2)$ divise $(X-1)^2(X+2)(X^2+1)$.
2. Tous les polynômes divisent 0 mais 0 ne divise que lui-même.
3. Le polynôme X divise X^5-3X^3+X.
4. Le polynôme $X-1$ divise X^n-1 pour $n\in\mathbb{N}^*$ car $X^n-1=(X-1)\sum_{k=0}^{n-1}X^k$.

Proposition III.2

Soient $P,Q,R,U,V\in\mathbb{K}[X]$.

1. Si $Q|P$ et si $P\neq 0$ alors $\deg(Q)\leqslant\deg(P)$.
2. La divisibilité est réflexive $P|P$.
3. La divisibilité est transitive si $R|Q$ et si $Q|P$ alors $R|P$.
4. Si $U|P$ et si $V|Q$ alors $UV|PQ$.
5. Si $R|P$ et si $R|Q$ alors $R|UP+VQ$.

Attention, la divisibilité n'est ni anti-symétrique et encore moins symétrique.

Proposition III.3

Soient $(P,Q)\in\mathbb{K}[X]$. Les propositions suivantes sont équivalentes.

1. $Q|P$ et $P|Q$.
2. Il existe $\lambda\in\mathbb{K}^*$ tel que $P=\lambda Q$

Démonstration. (1) $\Rightarrow$ (2). Si $Q|P$ et $P|Q$, alors $\deg(Q)\leqslant\deg(P)\leqslant\deg(Q)$ et donc $\deg(P)=\deg(Q)$. On sait également qu'il existe $R\in\mathbb{K}[X]$ tel que $P=QR$ et donc $\deg(P)=\deg(Q)+\deg(R)=\deg(P)+\deg(R)$. Si $P=0$ alors $P|Q$ implique $Q=0$ et donc (2) est vrai. Supposons $P\neq 0$ i.e. $\deg(P)\in\mathbb{N}$. Alors $\deg(R)=0$ c'est-à-dire R est constant et non nul, $R=\lambda\in\mathbb{K}^*$ et donc $P=\lambda Q$.
(2) $\Rightarrow$ (1) est évident.

□

Théorème III.4 (Division euclidienne)

Soient $(A,B)\in\mathbb{K}[X]^2$ avec $B\neq 0$. Il existe un unique couple $(Q,R)\in\mathbb{K}[X]^2$ tel que

$$\begin{aligned}&A=BQ+R,\\&\deg(R)<\deg(B).\end{aligned}$$

Le polynôme R est appelé le reste et Q le quotient de la division euclidienne de A par B.

Démonstration. Existence. On fixe un polynôme $B=\sum_{k=0}^{m}b_kX^k$. On pose alors pour tout $n\in\mathbb{N}$, la proposition

$$\mathscr{P}(n)\quad:\quad\text{« }\forall A\in\mathbb{K}_n[X],\ \exists(Q,R)\in\mathbb{K}[X],\ A=BQ+R\quad\text{ET}\quad\deg(R)<m.\text{ »}$$

Démontrons par récurrence que $\mathscr{P}(n)$ est vraie.
Initialisation. Supposons $n=0$ et fixons $A=a\in\mathbb{K}_0[X]=\mathbb{K}$. Premier cas, $m=0$ alors $B=b\in\mathbb{K}^*$. Donc le couple $(Q,R)=\left(\frac{a}{b},0\right)$ est solution :

$$a=\frac{a}{b}b+0\qquad\text{ET}\qquad\deg(0)=-\infty<0=\deg(B)=m.$$

Second cas, $m>0$ alors, le couple $(0,a)$ est solution :

$$a=0\times B+a\qquad\text{ET}\qquad\deg(a)=0<m.$$

Par conséquent, $\mathscr{P}(0)$ est vraie.
Hérédité. Soit $n \in \mathbb{N}$. Supposons $\mathscr{P}(n)$ vraie et montrons que $\mathscr{P}(n+1)$ est vraie. Fixons $A \in \mathbb{K}_{n+1}[X]$.
Premier cas, $\deg(A) < m$, alors $(0, A)$ est une solution car

$$A = 0 \times B + A \qquad \text{ET} \qquad \deg(A) < m.$$

Second cas $p = \deg(A) \geqslant m$ alors $A = \sum_{k=0}^{p} a_k X^k$. Posons

$$\begin{aligned} A_1 = A - \frac{a_p}{b_p} X^{p-m} B &= \sum_{k=0}^{p} a_k X^k - \sum_{k=0}^{m} \frac{a_p}{b_p} b_k X^{p-m+k} \\ &= a_p X^p + \sum_{k=0}^{p-1} a_k X^k - a_p X^p - \sum_{k=0}^{m-1} \frac{a_p}{b_p} b_k X^{p-m+k} \\ &= \sum_{k=0}^{p-1} a_k X^k - \sum_{k=p-m}^{p-1} \frac{a_p}{b_p} b_{k-p+m} X^k. \end{aligned}$$

Donc $\deg(A_1) \leqslant p-1 < \deg(A) \leqslant n+1$. Ainsi, $A_1 \in \mathbb{K}_n[X]$. Donc par hypothèse de récurrence, il existe $(Q_1, R_1) \in \mathbb{K}[X]^2$ tel que

$$A_1 = Q_1 B + R_1 \qquad \text{ET} \qquad \deg(R_1) < m.$$

Dès lors,

$$A = \frac{a_p}{b_p} X^{p-m} B + Q_1 B + R_1 = \underbrace{\left(\frac{a_p}{b_p} X^{p-m} + Q_1 \right)}_{=:Q} B + R_1.$$

En posant $R = R_1$, on obtient que le couple $(Q, R) \in \mathbb{K}[X]$ est solution :

$$A = QB + R \qquad \text{ET} \qquad \deg(R) < m.$$

Ceci étant vrai pour tout $A \in \mathbb{K}_{n+1}[X]$, on en déduit que $\mathscr{P}(n+1)$ est vraie.
Conclusion. La propriété $\mathscr{P}(n)$ est vraie pour tout $n \in \mathbb{N}$.

Unicité. Soient $(Q_1, R_1) \in \mathbb{K}[X]^2$ et $(Q_2, R_2) \in \mathbb{K}[X]^2$ tels que

$$\begin{aligned} A &= Q_1 B + R_1 \qquad \text{ET} \qquad \deg(R_1) < \deg(B) \\ A &= Q_2 B + R_2 \qquad \text{ET} \qquad \deg(R_2) < \deg(B) \end{aligned}$$

Par soustraction, $0 = (Q_1 - Q_2) B + R_1 - R_2$ donc $R_1 - R_2 = -(Q_1 - Q_2) B$. Par conséquent, $\deg(R_1 - R_2) = \deg(Q_1 - Q_2) + \deg(B)$. Si $Q_1 \neq Q_2$, alors $\deg(Q_1 - Q_2) \geqslant 0$ et donc

$$\deg(B) \leqslant \deg(R_1 - R_2) \leqslant \max(R_1, R_2) < \deg(B),$$

ce qui est absurde. On en déduit que $Q_1 = Q_2$ puis que $R_1 = R_2$.

□

Remarque 12 : $B|A$ si et seulement si le reste de la division euclidienne de A par B est nul.

Exemple 13 : Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Calculer le reste de la division euclidienne de P par $X - \alpha$.
Algorithme de la division euclidienne.

Exemple 14 : La division de $X^3 + X^2$ par $X - 1$ donne :

$$\begin{array}{rr|l} X^3 & +X^2 & X - 1 \\ \cline{3-3} -(X^3 & -X^2) & X^2 + 2X + 2 \\ \cline{1-2} 2X^2 & & \\ -(2X^2 & -2X) & \\ \cline{1-2} 2X & & \\ -(2X & -2) & \\ \cline{1-2} +2 & & \end{array}$$

Donc $X^3 + X^2 = (X^2 + 2X + 2) \times (X - 1) + 2$.

Exemple 15 : Calculer la division euclidienne de $X^3 + 2X^2 - X - 2$ par $X^2 + 1$.

IV Racine d'un polynôme

Définition IV.1

Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. On dit α est **une racine** de P si $P(\alpha) = 0$.

Proposition IV.2

Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Les propositions suivantes sont équivalentes.

1. α est une racine de P
2. Le polynôme $X - \alpha$ divise P.

Démonstration. D'après l'exemple 13, pour tout $\alpha \in \mathbb{K}$, il existe $Q \in \mathbb{K}[X]$, on a $P = Q(X - \alpha) + P(\alpha)$. Donc α est une racine si et seulement si $P(\alpha) = 0$ si et seulement si $P = Q(X - \alpha)$ si et seulement si $X - \alpha$ divise P. □

Proposition IV.3

Soient $P \in \mathbb{K}[X]$. Si $\alpha_1, \dots, \alpha_p$ sont des racines **distinctes** de P alors $\prod_{k=1}^{p}(X - \alpha_i)$ divise P.

Démonstration. On fixe $\alpha_1, \dots, \alpha_p$, p scalaires distincts. On pose pour tout $k \in [\![1; p]\!]$ la propriété suivante :

$$\mathscr{P}(k) \quad : \quad \text{« } \forall P \in \mathbb{K}[X],\ \text{si } \alpha_1, \dots \alpha_k \text{ sont racines de } P \text{ alors } \prod_{l=1}^{k}(X - \alpha_i) \,|P \text{ ».}$$

Initialisation. Si $k = 1$, d'après la proposition précédente, $\mathscr{P}(1)$ est vraie.
Hérédité. Soit $k \in [\![1; p-1]\!]$. Supposons que $\mathscr{P}(k)$ est vraie. Montrons que $\mathscr{P}(k+1)$ est vraie. Soit $P \in \mathbb{K}[X]$ tel que $\alpha_1, \dots, \alpha_{k+1}$ soient des racines de P. Alors puisque a_{k+1} est une racine de P, d'après la proposition précédente, il existe $Q \in \mathbb{K}[X]$ tel que

$$P = (X - \alpha_{k+1})\, Q.$$

Pour tout $i \in [\![1; k]\!]$, $\alpha_i \neq \alpha_{k+1}$ donc $P(\alpha_i) = 0 \ \Rightarrow\ Q(\alpha_i) = 0$. On a donc montré que $\alpha_1, \dots, \alpha_k$ sont des racines de Q. Donc d'après l'hypothèse de récurrence, on sait que $\prod_{l=1}^{k}(X - \alpha_i) \,|P$:

$$\exists Q_1 \in \mathbb{K}[X], \quad P = (X - \alpha_{k+1})\, Q = (X - \alpha_{k+1}) \prod_{i=1}^{k}(X - \alpha_i)\, Q_1 = \prod_{i=1}^{k+1}(X - \alpha_i)\, Q_1.$$

Autrement dit, $\prod_{i=1}^{k+1}(X - \alpha_i) \,|P$ et donc $\mathscr{P}(k+1)$ est vraie.
Conclusion : pour tout $k \in [\![1; p]\!]$, $\mathscr{P}(k)$ est vraie et notamment $\mathscr{P}(p)$ est vraie ce qui démontre la proposition. □

Corollaire IV.4

1. Tout polynôme de degré $n \in \mathbb{N}$ admet au plus n racines distinctes.
2. Tout polynôme non nul admet un nombre fini de racines.
3. Soit $P \in \mathbb{K}[X]$ et A une partie infinie de $\mathbb{K}$. Alors
$$(\forall x \in A,\ P(x) = 0) \ \Rightarrow\ P = 0.$$
4. Soit $(P, Q) \in \mathbb{K}[X]^2$ et A une partie infinie de $\mathbb{K}$. Alors
$$(\forall x \in A,\ P(x) = Q(x)) \ \Rightarrow\ P = Q.$$

Démonstration. Soit $n \in \mathbb{N}$ et $P \in \mathbb{K}_n[X]$. Si P admet strictement plus de n racines, alors d'après la proposition précédente, il existe $\alpha_1, \dots, \alpha_{n+1} \in \mathbb{K}$, $n+1$ scalaires distincts tels que $\prod_{k=1}^{n+1}(X - \alpha_k) \,|P$. Par conséquent, si $P \neq 0$, alors $n + 1 = \deg\left(\prod_{k=1}^{n+1}(X - \alpha_k)\right) \leqslant \deg(P) = n$ ce qui est absurde. Donc $P = 0$. Nous avons démontré le premier point. Les autre points découlent directement de ce premier point. □

Remarque 16 : Ce résultat est souvent utile pour montrer qu'un polynôme est nul en montrant qu'il est de degré n et possède au moins $n+1$ racines ou en montrant qu'il possède une infinité de racines.

Exemple 17 :

- Montrer que la fonction sinus n'est pas une fonction polynomiale.
- Montrer que l'exponentielle complexe n'est pas une fonction (complexe) polynomiale.

Définition IV.5

Soient $P \in \mathbb{K}[X]$, $P \neq 0$ et $\alpha \in \mathbb{K}$, une racine de P. On appelle **ordre de multiplicité** de α l'entier $m \in \mathbb{N}^*$ tel que

$$(X-\alpha)^m \mid P \qquad \text{ET} \qquad (X-\alpha)^{m+1} \text{ en divise pas } P$$

Une racine de multiplicité 1 est dite **simple** et une racine de multiplicité 2 est dite **double**.

Remarque 18 :

- Cette définition est cohérente. Posons $\mathscr{N} = \{p \in \mathbb{N}^* (X-\alpha)^p \mid P\}$. Si α est une racine on sait que $(X-\alpha) \mid P$ et donc $1 \in \mathscr{N}$. Donc $\mathscr{N} \neq \emptyset$. De plus, puisque $P \neq 0$, pour tout $p > \deg(P)$, on a par considération sur le degré que $(X-\alpha)^p$ qui ne divise pas P. Donc $\mathscr{N}$ est majorée par $\deg(P)$. Donc $\mathscr{N}$ est une partie non vide et majorée de $\mathbb{N}$ et admet une maximum qui est m.
- Le scalaire α est une racine de multiplicité $m \in \mathbb{N}$ de P si et seulement s'il existe $Q \in \mathbb{K}[X]$ tel que

$$P = (X-\alpha)^m Q \qquad \text{ET} \qquad Q(\alpha) \neq 0.$$

- $(X-\alpha)^m \mid P$ si et seulement si α est une racine de P de multiplicité d'au moins m.

Proposition IV.6

Soit $P \in \mathbb{K}[X]$, $P \neq 0$. Si $\alpha_1, \ldots, \alpha_p$ sont des racines distinctes de P de multiplicité $m_1, \ldots, m_p$ respectivement alors

$$\prod_{k=1}^{p} (X-\alpha_k)^{m_k} = (X-\alpha_1)^{m_1} (X-\alpha_2)^{m_2} \times \cdots \times (X-\alpha_p)^{m_p} \mid P.$$

Corollaire IV.7

Un polynôme de degré $n \in \mathbb{N}$ possède au plus n racines comptées avec leur ordre de multiplicité.

Proposition IV.8

Soient $P \in \mathbb{K}[X]$, $P \neq 0$ et $\alpha \in \mathbb{K}$. Les propositions suivantes sont équivalentes.

1. α est une racine de P de multiplicité m.
2. $P(\alpha) = P'(\alpha) = P''(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0$ et $P^{(m)}(\alpha) \neq 0$.

Démonstration. (1) $\Rightarrow$ (2). Soient $P \in \mathbb{K}[X]$, $P \neq 0$ et α une racine de P de multiplicité $m \in \mathbb{N}^*$. Alors il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-\alpha)^m Q$ et $Q(\alpha) \neq 0$. Par la formule de Leibniz, pour tout $p \in \mathbb{N}$,

$$P^{(p)} = \sum_{k=0}^{p} \binom{p}{k} \left((X-\alpha)^m\right)^{(k)} Q^{(p-k)}.$$

Or pour tout $k \in [\![1; m]\!]$, $\left((X-\alpha)^m\right)^{(k)} = \frac{m!}{(m-k)!}(X-\alpha)^{m-k}$. Donc si $p \leqslant m-1$, pour tout $k \leqslant p \leqslant m-1$, $m-k \geqslant 1$ et donc $\left((X-\alpha)^m\right)^{(k)}(\alpha) = 0$. Ainsi $P^{(p)}(\alpha) = 0$. Si $p = m$, alors

$$P^{(m)}(\alpha) = \sum_{k=0}^{m} \binom{m}{k} \left((X-\alpha)^m\right)^{(k)}(\alpha) Q^{(p-k)}(\alpha) = m! Q(\alpha) \neq 0.$$

(2) $\Rightarrow$ (1). Soient $P \in \mathbb{K}[X]$, $P \neq 0$ et $\alpha \in \mathbb{K}$ tel que $P(\alpha) = P'(\alpha) = P''(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0$ et $P^{(m)}(\alpha) \neq 0$. Puisque $P^{(m)} \neq 0$, on en déduit que $n = \deg(P) \geqslant m-1$. Alors par la formule de Taylor,

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k = \sum_{k=m}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k = (X-\alpha)^m \underbrace{\sum_{k=m}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^{m-k}}_{=Q}.$$

On en déduit donc que α est une racine de P de multiplicité d'au moins m. De plus $Q(\alpha) = \frac{P^{(m)}(\alpha)}{m!} + 0 \neq 0$. Donc α est de multiplicité m exactement.

□

Exemple 19 : Soit $P = -2 + 5X - 2X^2 - 4X^3 + 4X^4 - X^5$. Vérifier que 1 est une racine de P et calculer son ordre de multiplicité.

V Factorisation

Définition V.1

Soit $P \in \mathbb{K}[X]$. On dit que P est un polynôme **irréductible** dans $\mathbb{K}[X]$ si et seulement si

1. P est non constant : $\deg(P) \geqslant 1$.
2. Les seuls diviseurs de P sont les polynômes constants (non nuls) et les polynômes λP avec $\lambda \in \mathbb{K}^*$. Autrement dit

$$P = AB \quad \Rightarrow \quad (\deg(A) = 0 \quad \text{OU} \quad \deg(B) = 0).$$

Exemple 20 :

- Tous les polynômes de degré 1 sont irréductibles.
- Tous les polynômes de degré strictement plus grand que 1 ne sont pas irréductibles.
- La réciproque du point précédent est fausse : $\left(X^2+1\right)\left(X^2+2\right)$ n'a pas de racine réelle mais n'est pas irréductible.

Exemple 21 : Le polynôme $P = X^2 + 1$ est-il irréductible dans $\mathbb{C}[X]$? dans $\mathbb{R}[X]$?

Définition V.2

Soit $P \in \mathbb{K}[X]$. On dit que P est un polynôme **scindé** dans $\mathbb{K}[X]$ si et seulement s'il est constant ou s'écrit comme un produit de polynôme de de degré 1

Remarque 22 :

- Si P est un polynômes non constant, alors il existe $a_1, \ldots, a_k$, non nuls et $b_1, \ldots, b_k$ tels que

$$P = (a_1X + b_1)(a_2X + b_2)\cdots(a_kX + b_k) = a_1a_2\ldots a_k\left(X + \frac{b_1}{a_1}\right)\left(X + \frac{b_2}{a_2}\right)\cdots\left(X + \frac{b_k}{a_k}\right).$$

  Posons $a = a_1a_2\ldots a_k$ et $x_1 = -\frac{b_1}{a_1}, \ldots, x_k = -\frac{b_k}{a_k}$. Alors

$$P = a(X - x_1)(X - x_2)\cdots(X - x_k),$$

  où les x_i sont les racines de P (éventuellement se confondant). En regroupant les facteurs identiques, on écrit

$$P = a(X - \alpha_1)^{m_1}\cdots(X - \alpha_r)^{m_r},$$

  où les α_i sont les racines de P de multiplicité m_i.
- Le fait que P soit scindé ou non dépend du corps $\mathbb{K}$. Le polynôme $X^2 + 1$ est scindé dans $\mathbb{C}[X]$ mais pas dans $\mathbb{R}[X]$.

Théorème V.3 (Théorème de d'Alembert-Gauss)

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

Corollaire V.4

- Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes constants.
- Tous les polynômes de $\mathbb{C}[X]$ sont scindés.
- Tout polynôme de degré $n \in \mathbb{N}^*$ admet exactement n racines comptées avec leur multiplicité.

Théorème V.5 (Théorème de décomposition en produit de facteurs irréductibles dans $\mathbb{C}[X]$)

Pour tout $P \in \mathbb{C}[X]$ il existe $a, \alpha_1, \dots, \alpha_p \in \mathbb{C}$ et $m_1, \dots, m_p \in \mathbb{N}^*$ tels que

$$P = a\left(X-\alpha_1\right)^{m_1} \dots \left(X-\alpha_p\right)^{m_p}.$$

Exemple 23 : Rappel, à connaitre : Dans $\mathbb{C}[X]$, pour tout $n \in \mathbb{N}^*$

$$X^n - 1 = \prod_{k=0}^{n-1}\left(X - \mathrm{e}^{\frac{2ik\pi}{n}}\right) \qquad \text{et} \qquad \sum_{k=0}^{n-1} X^k = 1 + X + \cdots + X^{n-1} = \prod_{k=1}^{n-1}\left(X - \mathrm{e}^{\frac{2ik\pi}{n}}\right).$$

Théorème V.6 (Théorème de décomposition en produit de facteurs irréductibles dans $\mathbb{R}[X]$)

Pour tout $P \in \mathbb{R}[X]$ il existe $a, \alpha_1, \dots, \alpha_p, \beta_1, \dots, \beta_q, \gamma_1, \dots, \gamma_q \in \mathbb{R}$ et $m_1, \dots, m_p, s_1, \dots, s_q \in \mathbb{N}^*$ tels que

$$P = a\left(X-\alpha_1\right)^{m_1} \dots \left(X-\alpha_p\right)^{m_p}\left(X^2+\beta_1 X+\gamma_1\right)^{s_1} \dots \left(X^2+\beta_q X+\gamma_q\right)^{s_q},$$

avec pour tout $k \in [\![1;q]\!]$, $\beta_q^2 - 4\gamma_q < 0$.

Démonstration. Soit $P \in \mathbb{R}[X]$. Par le théorème V.5, il existe $a, \alpha_1, \dots, \alpha_r \in \mathbb{C}$ et $m_1, \dots, m_r \in \mathbb{N}^*$ tels que

$$P = a\left(X-\alpha_1\right)^{m_1} \dots \left(X-\alpha_r\right)^{m_r}.$$

Quitte à les réindexer, on suppose que $\alpha_1, \dots, \alpha_p$ sont réels tandis que $\alpha_{p+1}, \dots, \alpha_r$ sont complexes (non réels). Puisque P est réelle, il est facile de vérifier que si ω est une racine de P alors $\overline{\omega}$ est aussi une racine de P. Donc pour tout $i \in [\![p+1;r]\!]$, $\overline{\alpha_i} \in \{\alpha_1, \dots, \alpha_{i-1}, \alpha_{i+1}, \alpha_r\}$. Par conséquent, il existe $q(=(r-p)/2) \in \mathbb{N}$ et $\omega_1, \dots, \omega_q \in \mathbb{C}\setminus\mathbb{R}$ tels que

$$\{\omega_1, \dots, \omega_q, \overline{\omega_1}, \dots, \overline{\omega_q}\} = \{\alpha_{p+1}, \dots, \alpha_r\}.$$

De plus si ω_i est une racine de multiplicité $s \in \mathbb{N}^*$, alors ω est une racine de $P, P', \dots, P^{(s-1)}$ mais pas de $P^{(s)}$. Donc par passage au conjugué, on en déduit également que $\overline{\omega}$ est une racine de $P, P', \dots, P^{(s-1)}$ mais pas de $P^{(s)}$. Autrement dit $\overline{\omega}$ est une racine de multiplicité s également. De par ces considérations, on peut écrire

$$\begin{aligned} P &= a\left(X-\alpha_1\right)^{m_1} \dots \left(X-\alpha_p\right)^{m_p}\left(X-\omega_1\right)^{s_1}\left(X-\overline{\omega_1}\right)^{s_1} \dots \left(X-\omega_q\right)^{s_q}\left(X-\overline{\omega_1}\right)^{s_q} \\ &= a\left(X-\alpha_1\right)^{m_1} \dots \left(X-\alpha_p\right)^{m_p}\left(X^2-2\mathrm{Re}\left(\omega_1\right)X+\left|\omega_1\right|\right)^{s_1} \dots \left(X^2-2\mathrm{Re}\left(\omega_q\right)X+\left|\omega_q\right|^2\right)^{s_q}. \end{aligned}$$

On pose $\beta_i = -2\mathrm{Re}\left(\omega_i\right)$ et $\gamma_i = \left|\omega_i\right|^2$ qui sont des réels tels que $\beta_i^2 - 4\gamma_i = 4\mathrm{Re}\left(\omega\right)^2 - 4\left|\omega_i\right|^2 < 0$ car $\omega_i \notin \mathbb{R}$. On a alors bien

$$P = a\left(X-\alpha_1\right)^{m_1} \dots \left(X-\alpha_p\right)^{m_p}\left(X^2+\beta_1 X+\gamma_1\right)^{s_1} \dots \left(X^2+\beta_q X+\gamma_q\right)^{s_q}.$$

□

Proposition V.7

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

1. Les polynômes de degré 1.
2. Les polynômes de degré 2 ayant un discriminant strictement négatif.

Exemple 24 : Calculer la décomposition dans $\mathbb{R}[X]$ des polynômes suivants.

1. X^4+1 2. X^8-1 3. X^5+1

Soient $n \in \mathbb{N}^*$ et $P \in \mathbb{K}[X]$ un polynôme scindé de degré n. On note d'une part

$$P = a_n X^n + \cdots + a_1 X + a_0$$

et d'autre part

$$P = a\left(X-x_1\right) \dots \left(X-x_n\right),$$

où des x_i sont éventuellement égaux entre eux. En développant, on obtient

$$P = a\left(X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} + \cdots + (-1)^p \sigma_p X^{n-p} + \cdots + (-1)^n \sigma_n\right).$$

où pour tout $p \in [\![1;n]\!]$,

$$\sigma_p = \sum_{1 \leqslant i_1 < \cdots < i_p \leqslant n} x_{i_1} \dots x_{i_p}.$$

Ces formules permettent de relier les coefficients de P à ses racines. Notamment

$$\sigma_1 = x_1 + \cdots + x_p = -\frac{a_{n-1}}{a_n} \qquad \text{et} \qquad \sigma_n = x_1 x_2 \dots x_n = (-1)^n \frac{a_0}{a_n}.$$

Proposition V.8

Soient $n \in \mathbb{N}^*$ et $P \in \mathbb{K}[X]$ un polynôme scindé de degré n. On note $a_0, \dots, a_n$ les coefficients de P et $x_1, \dots, x_n$ ses racines avec multiplicité. Alors

$$x_1 + \cdots + x_p = -\frac{a_{n-1}}{a_n} \qquad \text{et} \qquad x_1 x_2 \dots x_n = (-1)^n \frac{a_0}{a_n}.$$

Exemple 25 : Déterminer les racines de $P = 3X^3 + 9X^2 - 12$.

Exemple 26 : Soient $P = X^2 + pX + q \in \mathbb{K}_3[X]$. On suppose P scindé dans $\mathbb{K}$ et on note x_1, x_2 et x_3 les racines de P. Exprimer $x_1^2 + x_2^2 + x_3^2$ en fonction de p et q.