Polynômes

Table des matières

I – Construction de l'ensemble des polynômes à une indéterminée 3
1– Anneaux et algèbres . . . 3
2– Algèbre des suites à support fini . . . 4
3– Algèbre et espaces vectoriels de polynômes . . . 5
4– Exercices . . . 6

II – Substitution et fonction polynômiale 7
1– Substitution par un polynôme . . . 7
2– Fonction polynômiale . . . 7
3– Exercices . . . 8

III – Dérivation 8
1– Définition . . . 8
2– Propriétés . . . 8
3– Dérivée n-ième . . . 8
4– Formule de Taylor . . . 9
5– Exercices . . . 10

IV – Divisibilité 10
1– Polynômes diviseurs et multiples . . . 10
2– Division euclidienne de polynômes . . . 10
3– Exercices . . . 11

V – Racines d'un polynôme 12
1– Racine . . . 12
2– Racine multiple . . . 12
3– Nombre de racines . . . 13
4– Exercices . . . 13

VI – Polynômes scindés 14
1– Définition . . . 14
2– Relations entre coeffciets et racines . . . 14
3– Exercices . . . 16

VII – Polynômes irréductibles réels et complexes 16
1– Théorème de D'Alembert–Gauss . . . 16
2– Polynômes irréductibles . . . 17
3– Polynômes premiers entre eux . . . 19
4– Exercices . . . 19

VIII – Exercices 20

Introduction

On reconnaît un arbre par ses feuilles, et un polynôme par ses racines...

Les polynômes sont un outil des mathématiques à la fois simples (formés uniquement par produits et sommes de constantes et d'indéterminées), mais extrêmement expressifs et riches. Leur manipulation, et d'une manière générale les opérations qu'ils permettent sont relativement simples. On les retrouve dans presques toutes les branches des mathématiques, leur histoire étant profondément liée à celle de l'algèbre, et de l'analyse.

En mathématiques appliquées, ils permettent d'approcher localement toute fonction suffisamment dérivable, par les développements limités, et permettent de représenter des formes lisses par les courbes de Bézier, largement utilisées dans l'industrie.
En algèbre linéaire, ils donnent accès à des décomposition de matrices très pratiques. Plus généralement, ces résultats se retrouvent par exemple dans l'étude de systèmes d'équations différentielles, ou de suites linéaires récurrentes.
Enfin, ils apparaissent également dans des branches plus avancées de mathématiques. Il serait illusoire de toutes les nommer, mais on y trouve, entre autres, la théorie de la complexité, la théorie des nœuds, la théorie de Galois, l'étude des équations diophantiennes, ...

L'objet de ce chapitre est de donner des bases algébriques à l'étude des polynômes, notamment par la construction formelle de *l'anneau des polynômes à une indéterminée sur un corps donné*. Cela nous permettra de donner un cadre précis et rigoureux à l'étude de ces objets, afin d'en exploiter au mieux l'expressivité dans la suite de votre cursus.

I – Construction de $\mathbb{K}[X]$

1– Anneaux et algèbres

Définition 1. *Anneau*
Soit A un ensemble possédant au moins deux éléments. Soient $\perp$ et $*$ deux *loi de composition internes* sur A. On dit que $(A, \perp, *)$ est un **anneau** sitôt que :

1– $(A, \perp)$ est un *groupe abélien* ;

2– $\perp$ est distributive par rapport à $*$, c'est-à-dire :

$$\forall (a,b,c) \in A^3,\ a*(b\perp c) = (a*b)\perp(a*c) \text{ et } (a\perp b)*c = (a*c)\perp(b*c)$$

3– A possède un *élément neutre* pour la loi $*$.

De plus, on dira que :

- $(A, \perp, *)$ est un **anneau commutatif** sitôt que la loi $*$ est commutative.
- $(A, \perp, *)$ est un **anneau intègre** sitôt que :

$$\forall (a,b) \in A^2,\ a*b = 0 \implies a = 0 \text{ ou } b = 0 \text{ avec } 0 \text{ l'élément neutre du groupe } (A, \perp)$$

Remarque 1. Si l'anneau $(A, \perp, *)$ n'est pas intègre, il existe (au moins) deux élément a et b tels que $a * b = 0$ avec $a \neq 0$ et $b \neq 0$. On dit alors que a et b sont des **diviseurs de** 0.

Remarque 2. En quelques sortes, un anneau est un groupe, sur lequel on rajoute une « multiplication », sans forcément exiger que tous les éléments soient inversibles pour cette multiplication (on obtient alors un corps), ou qu'il n'y ait pas de diviseurs de 0 (sauf pour les anneau intègres).

Exemple 1. *Quelques anneaux classiques*

- $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, sont des anneaux commutatifs intègres
- $(\mathcal{C}(I, \mathbb{R}), +, \times)$ est un anneau commutatif, non-intègre (par exemple, les fonctions indicatrices $\mathbb{1}_{x<0}$ et $\mathbb{1}_{x>0}$ sont des diviseurs de 0).
- $(\mathcal{M}_n(\mathbb{K}), +, \times)$ est un anneau non-commutatif, non-intègre.

Remarque 3. Soit $a \in A$, et soit $n \in \mathbb{N}$. On note :

- $na = \underbrace{a + a + \cdots + a}_{n \text{ fois}}$ avec $0a = 0_A$
- $(-n)a = -(na)$
- $a^n = \underbrace{a \times a \times \cdots \times a}_{n \text{ fois}}$ avec $a^0 = 1_A$.

Ce sont les même conventions que pour un corps.

Proposition 1. *Calcul dans un anneau*
Soit $(A, +, \times)$ un anneau, soient 0_A l'élément neutre pour $+$, et 1_A l'élément neutre pour $\times$. Pour $a \in A$, on notera $-a$ son symétrique pour $+$. On a les propriétés suivantes :

- 0_A est **absorbant** pour la loi $\times$: $\forall a \in A,\ 0_A \times a = a \times 0_A = 0_A$
- Soient $(a, b) \in A^2$ **qui commutent** pour $\times$ ($a \times b = b \times a$), et $n \in \mathbb{N}^*$ alors :

$$a^n - b^n = (a-b) \times \sum_{k=0}^{n-1} a^{n-1-k} \times b^k = (a-b) \times (a^{n-1} + a^{n-2} \times b + a^{n-3} \times b^2 + \cdots + a \times b^{n-2} + b^{n-1})$$

et on a également la **formule de** Newton :

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \times b^{n-k}$$

Remarque 4. Comme on l'a vu avec les matrices, dans le cas des anneaux, il **faut** que les deux éléments commutent pour que la factorisation précédente et la formule de Newton soient vraies !

Remarque 5. *Groupe des inversibles*
Soit $(A, \perp, *)$ un anneau. L'ensemble des éléments de A possédant un inverse pour la loi $*$ forme un groupe, que l'on appelle *groupe des inversibles de l'anneau* A, et que l'on note généralement $(A^\times, *)$, ou $(U(A), *)$. Démontrer qu'il s'agit bien d'un groupe est un bon exercice de remise en forme en algèbre...
Par exemple, le groupe des inversibles de $(\mathbb{Z}, +, \times)$ est $\{-1; +1\}$. Celui de $(\mathbb{C}, +, \times)$ est $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Rappelez-vous, le groupe des inversible de l'ensemble des matrices carrées de taille n à même un nom spécifique...

Définition 2. $\mathbb{K}$*-algèbre*
Soit $\mathbb{K}$ un corps. On appelle $\mathbb{K}$-algèbre tout quadruplet $(A, +, \times, \cdot)$ tel que :

1– $(A, +, \times)$ est un anneau ;

2– $(A, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel ;

3– Les lois $\times$ et $\cdot$ vérifient :

$$\forall \lambda \in \mathbb{K}, \forall (a, b) \in A^2,\ \lambda \cdot (a \times b) = (\lambda \cdot x) \times y = x \times (\lambda \cdot y)$$

Remarque 6. Une algèbre, c'est donc à la fois un anneau (donc, possédant une multiplication *interne* notée $\times$), **et** un espace-vectoriel (donc, possédant une multiplication externe notée $\cdot$), avec les deux multiplications qui sont « compatibles ».

Exemple 2. *Quelques algèbres classiques*

- $(\mathbb{R}, +, \times, \cdot)$ et $(\mathbb{C}, +, \times, \cdot)$ sont des $\mathbb{R}$-algèbres.
- $(\mathbb{C}, +, \times, \cdot)$ est également une $\mathbb{C}$-algèbre.
- $(\mathcal{M}_n(\mathbb{R}), +, \times, \cdot)$ et $(\mathcal{C}(I, \mathbb{R}), +, \times, \cdot)$ sont des $\mathbb{R}$-algèbres.

2– Algèbre des suites à support fini

Définition 3. *Suite à support fini*
Soit $\mathbb{K}$ un corps commutatif (typiquement, $\mathbb{R}$ ou $\mathbb{C}$). On dit qu'une suite d'élément de $\mathbb{K}$, $(a_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ est **à support fini** sitôt que :

$$\exists N \in \mathbb{N} \,/\, \forall n \in \mathbb{N},\ n > N \implies a_n = 0$$

C'est-à-dire qu'elle est *nulle à partir d'un certain rang*, ou encore, que sont support (l'ensemble des valeurs pour lesquelles la suite est non-nulle) est *fini*.
On note $\mathbb{K}^{(\mathbb{N})}$ l'ensemble des suites à support fini d'éléments de $\mathbb{K}$.

Remarque 7. $\mathbb{K}^{(\mathbb{N})}$ est, naturellement, un sous-espace vectoriel de l'ensemble des suites d'éléments de $\mathbb{K}$: $\mathbb{K}^{\mathbb{N}}$. On peut donc le munir des lois $+$ et $\cdot$ de ce dernier pour en faire un espace vectoriel.
On pourrait le munir d'une multiplication « naïve » comme $(a_n)_{n\in\mathbb{N}} \odot (b_n)_{n\in\mathbb{N}} = (a_n \times b_n)_{n\in\mathbb{N}}$. Cependant, un peu pour le mêmes raisons qu'avec les matrices (gardons en tête que l'on veut construire un ensemble de polynôme, dans lequel $(1 + x) \times (2 + x) = 2 + 3x + x^2$ et pas $2 + x^2$, par exemple...), on va privilégier une autre forme de multiplication interne ; le **produit de** Cauchy.

Définition 4. *Produit de* Cauchy
Soient $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ deux suites à support finis d'éléments de $\mathbb{K}$. On définit sur $\mathbb{K}^{(\mathbb{N})}$ l'opération suivante, notée $\times$ et appelée **produit de** Cauchy de $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$:

$$(a_n)_{n\in\mathbb{N}} \times (b_n)_{n\in\mathbb{N}} = (c_n)_{n\in\mathbb{N}}$$

avec

$$c_n \overset{\text{def}}{=} \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k+l=n} a_k b_l$$

Remarque 8. Notons qu'ainsi définit, $\times$ est bien une loi *interne* sur $\mathbb{K}^{(\mathbb{N})}$, puisque la suite obtenue est bien de support fini. De plus, cette loi est **commutative**.

Théorème 1. $(\mathbb{K}^{(\mathbb{N})}, +, \times, \cdot)$ *est une* $\mathbb{K}$*-algèbre, avec pour éléments neutres :*

- $(0, 0, 0, \dots)$ *pour* $+$ *et*
- $(1, 0, 0, \dots)$ *pour* $\times$.

De plus, l'anneau $(\mathbb{K}^{(\mathbb{N})}, +, \times)$ *est intègre et commutatif.*

Définition 5. Dans la $\mathbb{K}$-algèbre $(\mathbb{K}^{(\mathbb{N})}, +, \times, \cdot)$, on note X la suite définie par :

$$X \overset{\text{def}}{=} (\delta_{1,n})_{n\in\mathbb{N}} = (0, 1, 0, 0, \dots)$$

Proposition 2. Soit $k \in \mathbb{N}^*$. La suite définie par :

$$X^k \overset{\text{def}}{=} \underbrace{X \times X \times \cdots \times X}_{k \text{ fois}}$$

est égale à la suite :

$$X^k = (\delta_{k,n})_{n\in\mathbb{N}} = (0, \dots, 0, \underbrace{1}_{k\text{-ième position}}, 0, \dots)$$

Remarque 9. C'est là tout l'intérêt d'avoir choisi comme multiplication interne le produit de Cauchy...

3– Algèbres $\mathbb{K}[X]$ et espace vectoriel $\mathbb{K}_n[X]$

Définition 6. *Polynôme à une indéterminée*
On appelle **polynôme à une indéterminée** tout élément de $(\mathbb{K}^{(\mathbb{N})}, +, \times, \cdot)$. Avec les notation introduites précédemment, et en utilisant la structure d'espace vectoriel de $\mathbb{K}^{(\mathbb{N})}$, on peut écrire toute suite $(a_n)_{n\in\mathbb{N}}$ de $\mathbb{K}^{(\mathbb{N})}$ comme combinaison linéaire (finie, mais arbitrairement grande) des suites X^k :

$$(a_0, a_1, a_2, \dots, a_n, \dots, 0, 0, \dots) = a_0X^0 + a_1X^1 + a_2X^2 + \cdots + a_nX^n + \cdots + 0 + \cdots = \sum_{n\in\mathbb{N}} a_nX^n$$

La somme est finie, bien que portant sur $\mathbb{N}$ entier, car la suite est à support fini. On appelle alors X **l'indéterminée**, et dans ce contexte on choisit la notation $\mathbb{K}[X]$ à la place de $\mathbb{K}^{(\mathbb{N})}$ pour les **polynômes à une indéterminée à coefficient dans** $\mathbb{K}$.
Les lois internes et externe sont les mêmes, mais prennent dans ce contexte une nouvelle notation : si $P = (a_n)_{n\in\mathbb{N}} = \sum_{n\in\mathbb{N}} a_nX^n$ et $Q = (b_n)_{n\in\mathbb{N}} = \sum_{n\in\mathbb{N}} b_nX^n$, et $\lambda \in \mathbb{K}$

1– $P + Q = \sum_{n\in\mathbb{N}} (a_n + b_n)X^n$

2– $\lambda P = \sum_{n\in\mathbb{N}} \lambda a_n X^n$

3– $P \times Q = PQ = \sum_{n\in\mathbb{N}} c_n X^n$ avec $c_n = \sum_{k+l=n} a_k b_l$

Exemple 3. *Polynômes*

- $P = 1 + 3X - 2X^3 + 12X^5 \in \mathbb{R}[X]$
- $Q = \mathrm{i}X - (5 + \mathrm{i})X^7 \in \mathbb{C}[X]$
- $(3X + 4X^4)(-2X + X^3) = -6X^2 + 3X^4 - 8X^5 + 4X^7$

Définition 7. *Degré et valuation d'un polynôme*
Soit $P \in \mathbb{K}[X] \setminus \{0\}$, avec $P = \sum_{n\in\mathbb{N}} a_n X^n$.

- On appelle **degré** de P, noté $\deg(P)$ le nombre

$$\deg(P) \stackrel{\text{def}}{=} \max\{n \in \mathbb{N} \,/\, a_n \neq 0\}$$

  Quand $\deg(P) = n$, on appelle a_n le **coefficient dominant** de P, et $a_n X^n$ le **terme dominant**.
- On appelle **valuation** de P, noté $\text{val}(P)$ le nombre

$$\text{val}(P) \stackrel{\text{def}}{=} \min\{n \in \mathbb{N} \,/\, a_n \neq 0\}$$

- Par convention, pour $P = 0$, on prend $\deg(P) = -\infty$ et $\text{val}(P) = +\infty$.

Exemple 4. *Degré et valuation*
- Pour $P = 1 + X^3$, $\deg(P) = 3$, et $\text{val}(P) = 0$.
- Pour $P = -X^2 + 3X^5$, $\deg(P) = 5$, et $\text{val}(P) = 2$.
- Pour $P = X^n - (X+1)^n$, $\deg(P) = n-1$, et $\text{val}(P) = 0$.
- Pour $P = 3$, $\deg(P) = 0$, et $\text{val}(P) = 0$.

Remarque 10. On a $\deg(P) = 0 \Leftrightarrow P = a_0,\ a_0 \in \mathbb{K}^*$. On identifie donc l'ensemble des polnyômes constants à $\mathbb{K}^*$.

Définition 8. *Espace vectoriel de polynômes de degré inférieur ou égal à n*
On définit $\mathbb{K}_n[X] \stackrel{\text{def}}{=} \{P \in \mathbb{K}[X] \,/\, \deg(P) \leqslant n\}$. C'est un $\mathbb{K}$-espace vectoriel de dimension $n+1$ et de base canonique $(1, X, \ldots, X^n)$.

Proposition 3. Soit $(P, Q) \in \mathbb{K}[X]^2$, alors :
- $\deg(PQ) = \deg(P) + \deg(Q)$.
- $\deg(P+Q) \leqslant \max(\deg(P), \deg(Q))$.
- $\text{val}(PQ) = \text{val}(P) + \text{val}(Q)$.
- $\text{val}(P+Q) \geqslant \min(\text{val}(P), \text{val}(Q))$.

Proposition 4. Le groupe des inversibles de $\mathbb{K}[X]$ est l'ensemble des polynômes constants non-nuls :

$$U(\mathbb{K}[X]) = \mathbb{K}[X]^\times = \mathbb{K}^*$$

4– Exercices

Exercice I-1. Démontrer la **Proposition 3**.

Exercice I-2. Démontrer la **Proposition 4**.

Exercice I-3. Peut-on trouver des polynômes $P, Q \in \mathbb{K}[X]$ tels que $Q^2 = XP^2$?

II – Substitution et fonction polynômiale

1– Substitution par un polynôme

Remarque 11. Soit P un polynôme de $\mathbb{K}[X]$ de degré n, on peut donc écrire $P = \sum_{k=0}^{n} a_k X^k$. Soit $Q \in \mathbb{K}[X]$. Les termes de la forme Q^k sont également des polynômes, et toute combinaison linéaire de ces termes l'est aussi. Notamment :

$$\sum_{k=0}^{n} a_k Q^k \in \mathbb{K}[X]$$

Définition 9. *Substitution*
Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$, et soit $Q \in \mathbb{K}[X]$. Suite à la remarque précédente, on pose :

$$P \circ Q \overset{\text{def}}{=} P(Q) \overset{\text{def}}{=} \sum_{k=0}^{n} a_k Q^k$$

On dit que ce polynôme est obtenu par **substitution** de Q à l'indeterminée X.

Exemple 5. Soit $P = 1 + X + X^2$.
1– $Q = X^2,\ P(Q) = 1 + X^2 + X^4$.
2– $P(1+X) = 1 + (1+X) + (1+X)^2 = 3 + 3X + X^2$.
3– $P(X-a) = 1 + (X-a) + (X-a)^2$, avec $a \in \mathbb{K}$.

Proposition 5. *Degré d'une substitution*
Soit $(P, Q) \in \mathbb{K}[X]^2$, non nuls, alors $\deg(P \circ Q) = \deg(P) \times \deg(Q)$, et $\text{val}(P \circ Q) \geqslant \text{val}(P) \times \text{val}(Q)$ avec égalité si $\text{val}(Q) \neq 0$

2– Fonction polynômiale

Définition 10. *Fonction polynômiale associée à un élément de* $\mathbb{K}[X]$
Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$, on appelle **fonction polynômiale associée à** P la fonction :

$$\left\{ \begin{array}{rcl} \tilde{P} : \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & \tilde{P}(x) \overset{\text{def}}{=} \sum_{k=0}^{n} a_k x^k \end{array} \right.$$

Par abus de notation, on notera cette fonction P également, et l'image de x, $P(x)$.

Remarque 12. L'application

$$\left\{ \begin{array}{rcl} \phi : \mathbb{K}[X] & \to & \mathbb{K}^{\mathbb{K}} \\ P & \mapsto & \tilde{P} \end{array} \right.$$

est compatible avec les opération $+$, $\times$, $\cdot$ (on dit que c'est un *morphisme de* $\mathbb{K}$-algèbre). Elle est également compatible avec $\circ$, et avec la dérivation (que l'on verra dans la partie suivante). Enfin, elle est injective quand $\mathbb{K}$ est infini, c'est notamment le cas de $\mathbb{R}$ et $\mathbb{C}$; en conséquence, on pourra souvent travailler sur la fonction polynômiale associée à P (et ainsi utiliser des résultats issus de l'analyse réelle ou complexe), et transposer les informations obtenues sur le polynôme P.

3– Exercices

Exercice II-4. Trouver les polynômes $P \in \mathbb{R}[X]$ tels que :

1– $P \circ P = P$.

2– $P(X^2) = (X^2+1)P$.

Exercice II-5. Démontrer la **Proposition 5**.

III – Dérivation dans $\mathbb{K}[X]$

1– Définition

Définition 11. *Dérivée d'un polynôme*

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

$$\begin{cases} P' \overset{\text{def}}{=} 0 & \text{si } \deg(P) \leqslant 0 \ (P \text{ est constant, ou nul}) \\ P' \overset{\text{def}}{=} \sum_{k=1}^{n} k a_k X^{k-1} & \text{sinon (on a } \deg(P) \geqslant 1) \end{cases}$$

Exemple 6. Pour $P = 1 + 2X^3 - 6X^7$, on a $P' = 6X^2 - 42X^6$.

2– Propriétés

Théorème 2. *Propriétés de la dérivation des polynômes*

*1– La dérivation des polynômes est **linéaire**, c'est-à-dire :*

$$\forall (P,Q) \in \mathbb{K}[X]^2,\ \forall \lambda \in \mathbb{K},\ (\lambda P + Q)' = \lambda P' + Q'$$

*2– La dérivation d'un produit de deux polynômes s'obtient par la **règle de** Leibniz :*

$$\forall (P,Q) \in \mathbb{K}[X]^2,\ (PQ)' = P'Q + PQ'$$

3– La dérivation d'une composée de deux polynômes s'obtient avec une règle analogue au théorème de dérivation des fonctions composées *:*

$$\forall (P,Q) \in \mathbb{K}[X]^2,\ (P \circ Q)' = (P' \circ Q)Q'$$

3– Dérivée n-ième

Définition 12. *Dérivée n-ième d'un polynôme*

Soient $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$. On définit la **dérivé n-ième** de P, $P^{(n)}$, par :

$$\begin{cases} P^{(n)} \overset{\text{def}}{=} P & \text{si } n = 0 \\ P^{(n)} \overset{\text{def}}{=} \left(P^{(n-1)}\right)' & \text{sinon} \end{cases}$$

Remarque 13. On note parfois les dérivées secondes et troisièmes par $''$ et $'''$ au lieu de $^{(2)}$ et $^{(3)}$.

Théorème 3. *Formule de* Leibniz

Soient $(P,Q) \in \mathbb{K}[X]^2$, $n \in \mathbb{N}$. Alors :

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

Exemple 7. Soit $P \in \mathbb{K}[X]$, et soient $Q = (1+X^2)P$ et $n \in \mathbb{N},\ n \leqslant 2$. Alors :

$$\begin{aligned} Q^{(n)} &= ((1+X^2)P)^{(n)} \\ &= \sum_{k=0}^{n} \binom{n}{k} (1+X^2)^{(k)} P^{(n-k)} \end{aligned}$$

Or, $(1+X^2)' = 2X$, $(1+X^2)'' = 2$, $(1+X^2)''' = 0$ et $\forall k \in \mathbb{N},\ k \geqslant 3 \implies (1+X^2)^{(k)} = 0$. Donc :

$$\begin{aligned} Q^{(n)} &= \sum_{k=0}^{2} \binom{n}{k} (1+X^2)^{(k)} P^{(n-k)} \\ &= \binom{n}{0}(1+X^2)P^{(n)} + \binom{n}{1} 2XP^{(n-1)} + \binom{n}{2} 2P^{(n-2)} \\ &= (1+X^2)P^{(n)} + 2nXP^{(n-1)} + n(n-1)P^{(n-2)} \end{aligned}$$

Proposition 6. Si $P \in \mathbb{K}[X]$ est un polynôme de degré p, alors $P^{(k)}$ est un polynôme de degré $p-k$ si $p \geqslant k$, et $-\infty$ si $p < k$ (polynôme nul).

Remarque 14. Ce résultat se démontre facilement sur les mônomes (termes de la forme $a_k X^k$), par récurrence sur k, puis s'étend naturellement au polynômes en remarquant que, par la dérivation, le terme dominant reste dominant.

4– Formule de Taylor

Théorème 4. *Formule de* Taylor
Soit $P \in \mathbb{K}[X]$, avec $\deg(P) = n$, et soit $a \in \mathbb{K}$. On peut écrire P sous la forme suivante :

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

Démonstration 1. Soit $P \in \mathbb{K}[X]$, avec $\deg(P) = n$, et soit $a \in \mathbb{K}$. On peut écrire P sous sa forme développée :

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

Alors, pour tout $h \in \mathbb{K}$, on a :

$$P(X+h) = \sum_{k=0}^{n} a_k (X+h)^k \overset{\text{def}}{=} Q(h)$$

Remarquons que Q est également un polynôme, de degré $n \times 1 = n$. Donc, on peut l'écrire sous la forme

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

Par une récurrence simple, on obtient que $k \leqslant n-1 \implies Q^{(k)}(X) = k!b_k + XQ_k$, avec Q_k un polynôme de degré $n-k-1$. En prenant la valeur en 0 des fonctions polynomiales associée, on a donc :

$$P^{(k)}(h) = Q^{(k)}(0) = k!b_k + 0 \times Q_k(0) = k!b_k$$

Et donc, $b_k = \dfrac{P^{(k)}(h)}{k!}$, ce qui permet d'écrire :

$$\forall h \in \mathbb{K}, P(X+h) = \sum_{k=0}^{n} \frac{P^{(k)}(h)}{k!} X^k$$

Enfin, en prenant $h = a$ et en subsituant $X - a$ à X, on obtient :

$$\forall h \in \mathbb{K}, P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(h)}{k!} (X-a)^k$$ □

5– Exercices

Exercice III-6. En posant $P = \sum_{k=0}^{p} a_k X^k$ et $Q = \sum_{k=0}^{q} b_k X^k$, démontrer le **Théorème 2**.

Exercice III-7. Par récurrence sur n, démontrer le **Théorème 3**.

Exercice III-8. Trouver dans $\mathbb{R}[X]$ les polynômes P tels que :

1– $(P')^2 = 4P$

2– $(X^2+1)P'' = 6P$

Exercice III-9. Montrer que $\forall n \in \mathbb{N},\ \exists! P_n \in \mathbb{R}[X]\ /\ P_n - P_n' = X^n$. On raisonnera par analyse/synthèse.

Exercice III-10. Soit $P \in \mathbb{K}[X]$. Montrer que $P(X+1) = \sum_{n\in\mathbb{N}} \frac{1}{n!} P^{(n)}(X)$.
(On pourra, par exemple, utiliser la formule de Talyor en 0 pour trouver les valeurs des dérivées de P en 1 en fonction de celles en 0, puis une nouvelle fois pour formuler $P(X+1)\ldots$)

IV – Divisibilité

1– Diviseurs et multiples dans $\mathbb{K}[X]$

Définition 13. *Divisibilité des polynômes*
Soit $(A,B) \in \mathbb{K}[X]^2$. On dit que B **divise** A, ou également que A est **un multiple** de B, que l'on note $B|A$, lorsque :

$$\exists Q \in \mathbb{K}[X]\ /\ A = BQ$$

Exemple 8. *Quelques multiples*

- (X^2-1) est un multiple de $2X+2$ dans $\mathbb{R}[X]$ car $X^2-1 = (2X+2)\times\frac{1}{2}(X-1)$.
- $(X-\mathrm{i})|(X^2+1)$ dans $\mathbb{C}[X]$ car $X^2+1 = (X-\mathrm{i})(X+\mathrm{i})$

Remarque 15. La divisibilité est en fait une notion valable dans tous les anneaux (donc, dès qu'on a une multiplication interne) : pensez à l'arithmétique dans $\mathbb{Z}$ par exemple. Cela explique pourquoi nous auront dans cette partie plusieurs résultats similaires à ce que l'on connaître déjà pour les entiers relatifs. D'ailleurs, quand $a|b$, on dit aussi que a est *un diviseurs* de b. C'est pourquoi, dans un anneau, quand on a un couple d'élément $(u,v)\ /\ u\times v = 0$, on dit que ce sont des *diviseurs de* 0.

2– Division euclidienne dans $\mathbb{K}[X]$

Théorème 5. *Division euclidienne dans* $\mathbb{K}[X]$.
Soit $(A,B) \in \mathbb{K}[X]^2$*, avec* $B \neq 0$*. Alors il existe un* ***unique*** *couple* $(Q,R) \in \mathbb{K}[X]^2$ *tel que :*

$$\begin{cases} A = BQ + R \\ \deg(R) < \deg(B) \end{cases}$$

Q est alors appelé le ***quotient*** *de la division euclidienne de A par B, et R est appelé le* ***reste****.*

Remarque 16. C'est, en somme, la même chose de la division euclidienne dans $\mathbb{Z}$, sauf que la condition sur le reste n'est plus $r < |b|$, mais $\deg(R) < \deg(B)\ldots$
D'ailleurs, pour calculer effectivement cette division euclidienne, on va poser l'opération et effectuer le même algorithme que dans $\mathbb{Z}$.

Méthode 1. *Division euclidienne de polynômes*
Effectuons la division euclidienne de $6+6X-4X^2+10X^3-6X^4+12X^5$ par $1-X+2X^2$.

$$\begin{array}{rrrrrrrrrrrrrrr|lllll}
 & 12X^5 & - & 6X^4 & + & 10X^3 & - & 4X^2 & + & 6X & + & 6 & 2X^2 & - & X & + & 1 \\
\hline
- & (12X^5 & - & 6X^4 & + & 6X^3) & & & & & & & 6X^3 & & & & \\
\hline
 & \emptyset & + & \emptyset & + & 4X^3 & - & 4X^2 & + & 6X & + & 6 & & & & & \\
 & & & & - & (4X^3 & - & 2X^2 & + & 2X) & & & & + & 2X & & \\
\hline
 & & & & & & - & 2X^2 & + & 4X & + & 6 & & & & & \\
 & & & & & & - & (-2X^2 & + & X & - & 1) & & & & - & 1 \\
\hline
 & & & & & & & & & 3X & + & 7 & 6X^3 & + & 2X & - & 1
\end{array}$$

On obtient donc le quotient, à droite, $Q=(6X^3+2X-1)$, et le reste, à gauche, $R=3X+7$. On peut alors écrire : $12X^5-6X^4+10X^3-4X^2+6X+6=(2X^2-X+1)(6X^3+2X-1)+(3X+7)$.

Exemple 9. On peut, pour s'entraîner, détailler le calcul des division euclidiennes suivantes :

1– $(-3)+7X+7X^2-3X^3=(3X^2+2X-1)(-X+3)$

2– $(-\mathrm{i})+(2-2\mathrm{i})X-(1+\mathrm{i})X^2+(4+2\mathrm{i})X^3+(2-2\mathrm{i})X^4+(1/2-\mathrm{i})X^5+(1/2+(5\mathrm{i})/2)X^6+2X^7=((\mathrm{i}+1)X^5-\mathrm{i}/2X^4+2X^2-\mathrm{i})((1-\mathrm{i})X^2+(2+\mathrm{i})X)+X-\mathrm{i}$

3– Exercices

Exercice IV -11. *Démonstration*

1– Démontrer, par l'absurde, le résultat d'**unicité** du **Théorème 5**.

2– Montrer que si S et T sont deux polynômes de $\mathbb{K}[X]$ non-nuls, avec S de degré n et de coefficient dominant a, et T de degré p et de coefficient dominant b, et $n\geqslant p$, alors

$$\deg\left(S-\frac{a}{b}X^{n-p}T\right)<\deg S$$

3– Par récurrence sur le degré du polynôme A, montrer le résultat d'**existence** du **Théorème 5**.

Exercice IV -12. Effectuer les divisions euclidiennes de polynômes suivantes :

1– $(-1)-3X^2-X^4+6X^5$ par $(2X^2+X)$

2– $(-2)+X+5X^4-6X^5+X^6+4X^7-2X^8$ par X^3-2X^2+1

3– $2+4\mathrm{i}X-4X^2+3\mathrm{i}X^3+2\mathrm{i}X^4+(1-\mathrm{i})X^5+(1+\mathrm{i})X^6$ par $X^2-\mathrm{i}X+2$

Exercice IV -13. Dans cet exercice, on prendra $n\in\mathbb{N}$, $n\geqslant 2$

1– Soit $(a,b)\in\mathbb{K}^2$ tels que $a\neq b$, soit $P\in\mathbb{K}[X]$. Exprimer le reste de la division euclidienne de P par $(X-a)(X-b)$ en fonction de $P(a)$ et $P(b)$.

(Notons qu'on peut commencer par écrire $P=BQ+R$ avec $B=(X-a)(X-b)$, puis faire les substitution nécessaires)

2– En déduire le reste de la division euclidienne de $X^{n+2}-2X^{n+1}-X+1$ par X^2-5X+6.

3– Soit $a\in\mathbb{K}$, soit $P\in\mathbb{K}$. Exprimer le reste de la division euclidienne de P par $(X-a)^2$ en fonction de $P(a)$ et $P'(a)$.

(Notons la similitude avec la question 1– ...)

4– En déduire le reste de la division euclidienne de X^n+X-1 par X^2-2X+1.

5– Soit $t \in \mathbb{R}$. Donner le reste de la division euclidienne de $(X\sin(t)+\cos(t))^n$ par X^2+1 en fonction de t.

(Notons qu'une division euclidienne vraie dans $\mathbb{R}$ reste vraie dans $\mathbb{C}$, et donc permet une substitution de X par i*...)*

Exercice IV -14. Soit $(a,b) \in \mathbb{N}^{*2}$, et soit r le reste de la division euclidienne de a par b. Montrer que le reste de la division euclidienne de X^a par X^b-1 est X^r.

V – Racines d'un polynôme

1– Racine

Définition 14. *Racine d'un polynôme*
Soient $P \in \mathbb{K}[X]$, et $a \in \mathbb{K}$. On dit que a est une **racine** de P sitôt que :

$$P(a) = 0$$

Proposition 7. Soient $P \in \mathbb{K}[X]$, et $a \in \mathbb{K}$. On a :

$$P(a) = 0 \Leftrightarrow (X-a)|P$$

Pour que a soit une racine de P, il faut et il suffit que $(X-a)$ divise P.

Démonstration 2. Soient $P \in \mathbb{K}[X]$, et $a \in \mathbb{K}$ une racine de P. On peut effectuer la division euclidienne de P par $(X-a)$:

$$\exists!(Q,R) \in \mathbb{K}[X]^2 \ / \ P = (X-a)Q + R \text{ et } \deg(R) < 1$$

Autrement dit, R est une constante (polynôme de degré 0), que l'on notera r. On peut alors substituer a à X :

$$P(a) = \underbrace{(a-a)}_{=0} Q(a) + R(a) = 0 + r = 0 \text{ (car } P(a) = 0)$$

Donc $r = 0$, et donc $\exists Q \in \mathbb{K}[X] \ / \ P = (X-a)Q$, c'est-à-dire, $(X-a)|P$.
Réciproquement, si $(X-a)|P$, alors $\exists B \in \mathbb{K}[X] \ / \ P = (X-a)B$, et en substituant a à X, on obtient :

$$P(a) = \underbrace{(a-a)}_{=0} B(a) = 0$$

Donc a est bien une racine de P. □

Exemple 10. On peut ainsi affirmer que $\forall n \in \mathbb{N},\ X^{n+2} - 2X^n + X^3 + X^2 - 1$ est divisible par $(X-1)$.

2– Racine multiple

Définition 15. *Racine multiple d'un polynôme*
Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$. Soit $r \in \mathbb{N}^*$. On dit que a est une **racine de P (d'ordre) de multiplicité r** sitôt que :

1– $(X-a)^r | \ P$

2– $(X-a)^{r+1} \nmid P$

Pour $r = 1$, on dira que a est racine *simple*. Pour $r = 2$, double, et pour $r = 3$, triple, *etc...*

Remarque 17. En somme, r est « le plus grand nombre » de fois qu'on peut diviser P par $(X-a)$, sans faire de « fractions » de polynômes. Si ici, c'est la propriété de divisibilité qui sert de base à la définition (contrairement au cas $r = 1$, on retrouve cependant une propriété d'annulation similaire à la précédente...

Proposition 8. Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$, et $r \in \mathbb{N}^*$. Alors :

$$a \text{ est une racine de } P \text{ d'ordre } r \Leftrightarrow \exists Q \in \mathbb{K}[X] \ / \ P = (X-a)^r Q \text{ et } Q(a) \neq 0$$

Proposition 9. Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$, et $r \in \mathbb{N}^*$. Alors :

$$a \text{ est une racine de } P \text{ d'ordre } r \Leftrightarrow \forall k \in [\![0; r-1]\!],\ P^{(k)}(a) = 0 \text{ et } P^{(r)}(a) \neq 0$$

De plus,

$$a \text{ est une racine de } P \text{ d'ordre } \textbf{au moins } r \Leftrightarrow \forall k \in [\![0; r-1]\!],\ P^{(k)}(a) = 0$$

Remarque 18. Une racine de P d'ordre r est donc un nombre qui annule les r premières dérivées (de la 0-ième à la $(r-1)$-ième) de P.

Exemple 11. On peut montrer que, pour $n \leqslant 2$, $X^n - X + 1$ n'as jamais de racines doubles dans $\mathbb{C}$, voir exercice **V-15**.

Proposition 10. Soit $P \in \mathbb{K}[X]$, ayant (entre autre) pour racines $(a_1, a_2, \ldots, a_k)$, de multiplicités respectives $(\alpha_1, \alpha_2, \ldots, \alpha_k)$. Alors :

$$\exists Q \in \mathbb{K}[X] \ / \ P = \left(\prod_{i=1}^{k} (X - a_i)^{\alpha_i} \right) Q \text{ et } \forall i \in [\![1; k]\!],\ Q(a_i) \neq 0$$

3– Nombre de racines

Théorème 6. *Soit $P \in \mathbb{K}$, avec $\deg(P) = n$. Si P admet au moins $n+1$ racines (comptées avec leurs multiplicités) dans $\mathbb{K}$, alors P est le polynôme nul.*

Autrement dit, « un polynôme dont le nombre de racines dépasse strictement le degré est nul ».

Notamment, un polynôme de $\mathbb{K}_n[X]$ non-nul admet au plus n racines.

Théorème 7. *Soient $(A, B) \in \mathbb{K}[X]^2$ et S une partie infinie de $\mathbb{K}$, telle que $\forall x \in S,\ A(x) = B(x)$. Alors*

$$A = B$$

Autrement dit, deux polynômes qui coïncident sur une partie infinie sont égaux

Remarque 19. C'est ce résultat qui permet de montrer le résultat d'injectivité de la **Remarque 12**, à savoir que l'application

$$\left\{ \begin{array}{rcl} \phi : \mathbb{K}[X] & \to & \mathbb{K}^{\mathbb{K}} \\ P & \mapsto & \tilde{P} \end{array} \right.$$

est injective.

4– Exercices

Exercice V-15. L'objectif de cet exercice est de montrer que le polynôme $X^n - X + 1$ n'as que des racines simples dans $\mathbb{C}$.

1– Pour $n = 0$ et $n = 1$, donnez les racines de ce polynôme.

2– Pour $n \geqslant 2$ montrer qu'une racine double z s'écrit nécessairement de la forme $\dfrac{n}{n-1}$.

3– En déduire qu'alors $P'(z) > 0$

4– Conclure

Exercice V -16. L'objectif de cet exercice est de démontrer la **Proposition 10**. Soit donc $P \in \mathbb{K}[X]$, ayant pour racines $(a_1, a_2, \ldots, a_k)$, de multiplicités respectives $(\alpha_1, \alpha_2, \ldots, \alpha_k)$.

1– Justifier que
$$\exists Q_1 \in \mathbb{K}[X] \ / \ P = (X - a_1)^{\alpha_1} Q_1 \text{ et } Q_1(a_1) \neq 0$$

2– Montrer que $(a_2, a_3 \ldots, a_k)$ sont racines de Q_1 de multiplicités respectives $(\alpha_2, \alpha_3 \ldots, \alpha_k)$.

3– Par récurrence (finie), montrer la **Proposition 10**.

Exercice V -17. *Théorèmes*

1– Avec l'aide de la **Proposition 10** et d'une réflexion sur le degrés des polynômes, montrer le **Théorème 6**.

2– En étudiant le polynôme $P = A - B$ (avec les notations de l'énoncé), démontrer de **Théorème 7**.

VI – Polynômes scindés

1– Définition

Définition 16. *Polynôme scindé*
Soit $P \in \mathbb{K}[X]$. On dit que P est **scindé** sitôt que :
$$\exists \lambda \in \mathbb{K},\ \exists (a_1, a_2, \ldots, a_n) \in \mathbb{K}^n \ / \ P = \lambda \prod_{k=1}^{n} (X - a_k)$$
C'est-à-dire qu'il se décompose en produit de facteurs de degré 1.

Remarque 20. Dans la définition précédente, on a alors forcément $\deg(P) = n$. Par ailleurs, les $(a_k)_{k \in [\![1;n]\!]}$, qui sont les racines de P ne sont pas nécessairement distincts (on peut avoir des racines doubles, triples, etc...).
Si on prend uniquement les racines distinctes $(a_1, a_2, \ldots, a_m)$, avec leurs ordres de multiplicité respectifs $(\alpha_1, \alpha_2, \ldots, \alpha_m)$, alors on peut écrire :
$$P = \lambda \prod_{i=1}^{m} (X - a_i)^{\alpha_i}$$
Et on a $\deg(P) = \sum_{i=1}^{m} \alpha_i$.

Exemple 12. Attention, le caractère scindé d'un polynôme dépend parfois du corps où on se place.
- $X^2 - 1 = (X - 1)(X + 1)$ est scindé dans $\mathbb{R}[X]$, et dans $\mathbb{C}[X]$.
- $P = (X - 1)(X + 2)^2$ également.
- $X^2 + 1$ n'est pas scindé dans $\mathbb{R}[X]$, mais il l'est dans $\mathbb{C}[X]$ (par $(X - \mathrm{i})(X + \mathrm{i})$).
- $X^n - 1 = \prod_{k=1}^{n} (X - \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}})$ n'est scindé dans $\mathbb{R}[X]$ que pour $n \leqslant 2$. Il est toujours scindé dans $\mathbb{C}[X]$.

2– Relations entre coeffciets et racines

Remarque 21. Soit $P \in \mathbb{K}[X]$ un polynôme scindé. Ce polynôme peut donc s'écrire sous deux formes :
$$\underbrace{P = \sum_{k=0}^{n} c_k X^k}_{\text{sommes et coefficients}} \quad \text{et} \quad \underbrace{P = \lambda \prod_{i=1}^{n} (X - r_i)}_{\text{produit et racines}}$$
Ces deux formes représentant le même polynôme P, il est naturel de se poser la question du lien entre les coefficients (c_k) et les racines (r_i). Notons que ce n'est valide que pour les polyômes scindés, et qu'on a pris la forme avec des racines non-nécessairement distinctes.

Prenons le cas $n = 2$. On a alors :

$$P = c_0 + c_1X + c_2X^2 \text{ et } P = \lambda(X - r_1)(X - r_2)$$

On peut développer le produit, ce qui nous donne alors les équations suivantes :

$$\left\{\begin{array}{ccc} \lambda & = & c_2 \\ -\lambda(r_1 + r_2) & = & c_1 \\ \lambda r_1 r_2 & = & c_0 \end{array}\right. \Longrightarrow \left\{\begin{array}{ccc} \lambda & = & c_2 \\ r_1 + r_2 & = & -\dfrac{c_1}{c_2} \\ r_1 r_2 & = & \dfrac{c_0}{c_2} \end{array}\right.$$

Une étude analogue dans le cas $n = 3$ donnera :

$$\left\{\begin{array}{ccc} \lambda & = & c_3 \\ r_1 + r_2 + r_3 & = & -\dfrac{c_2}{c_3} \\ r_1r_2 + r_2r_3 + r_1r_3 & = & \dfrac{c_1}{c_3} \\ r_1r_2r_3 & = & -\dfrac{c_0}{c_3} \end{array}\right.$$

On voit apparaître des sommes que l'on appelle les **fonctions symétriques de** Newton : dans le cas général, on pose :

$$\sigma_k = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} r_{i_1} r_{i_2} \dots r_{i_k}$$

Ainsi, $\sigma_1 = r_1 + r_2 + \cdots + r_n$ est la somme de tous les termes (ou, de produits à 1 terme). De même $\sigma_2 = r_1r_2 + r_1r_3 + \cdots + r_1r_n + r_2r_3 + \cdots + r_{n-1}r_n$ est la somme de tous les doubles produits, et $\sigma_3 = r_1r_2r_3 + \cdots + r_1r_{n-1}r_n + \cdots + r_{n-2}r_{n-1}r_n$ est la somme de tous les triples produits, etc ... enfin, $\sigma_n = r_1r_2 \dots r_n$ est le produit de tous les termes.
Le développement d'un polynôme scindé de degré n donne alors :

$$\left\{\begin{array}{ccc} \lambda & = & c_n \\ \sigma_k & = & (-1)^k \dfrac{c_{n-k}}{c_n} \quad \forall k \in [\![1; n]\!] \end{array}\right.$$

On peut synthétiser cette remarque dans le théorème suivant.

Théorème 8. *Formules symmétriques de* Newton
Soit $P \in \mathbb{K}[X]$ un polynôme scindé, non-nul, de degré n, que l'on écrit sous les formes suivantes :

$$P = \sum_{k=1}^{n} c_k X^k \text{ et } P = \lambda \prod_{i=1}^{n} (X - r_i)$$

avec $(c_k)_{k \in [\![0;n]\!]} \in \mathbb{K}^n$, $c_n \in \mathbb{K}^*$, $(r_i)_{i \in [\![1;n]\!]} \in \mathbb{K}^n$, $\lambda \in \mathbb{K}^*$. Alors

$$\left\{\begin{array}{ccll} \lambda & = & c_n & \\ \sigma_1 & = & r_1 + \cdots + r_n = -\dfrac{c_{n-1}}{c_n} & \\ \sigma_k & = & (-1)^k \dfrac{c_{n-k}}{c_n} & \forall k \in [\![2; n-1]\!] \\ \sigma_n & = & r_1r_2 \cdots r_n = (-1)^n \dfrac{c_0}{c_n} & \end{array}\right.$$

avec

$$\sigma_k = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} r_{i_1} r_{i_2} \dots r_{i_k} \qquad \forall k \in [\![1; n]\!]$$

Exemple 13. Résolvons le système (non-linéaire) de 3 inconnues complexes x, y et z suivant :

$$\left\{\begin{array}{ccc} x + y + z & = & 1 \\ \dfrac{1}{x} + \dfrac{1}{y} + \dfrac{1}{z} & = & 1 \\ xyz & = & -4 \end{array}\right.$$

Soit (x, y, z) un triplet solution. On a alors :

$$\left\{\begin{array}{lcccl} \sigma_1 & = & x+y+z & = & 1 \\ \sigma_2 & = & xy+yz+zx & & \\ \sigma_3 & = & xyz & = & -4 \end{array}\right.$$

Notons que $\sigma_2 = xyz\left(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\right) = -4$, et donc x, y et z sont les racines du polynôme :

$$X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3 = X^3 - X^2 - 4X + 4 \stackrel{\text{def}}{=} P$$

On observe que 1 est une racine évidente de P, que l'on peut donc factoriser par $(X-1)$ avec une division euclidienne (dont le reste sera nul car $(X-1)|P$). On obtient alors :

$$P = (X-1)(X^2-4) = (X-1)(X-2)(X+2)$$

qui est un polynôme scindé de racines $\{1; 2; -2\}$. Inversement, de tels triplets (obtenus en permutant les valeurs de x, y, et z) sont bien solutions du système.

3– Exercices

Exercice VI-18. Résoudre les système suivants, d'inconnues complexes x, y, z :

1– $\left\{\begin{array}{lcccl} x+y+z & = & 1 \\ xyz & = & 1 \\ |x| = |y| & = & |z| \end{array}\right.$ 2– $\left\{\begin{array}{lcl} x+y+z & = & 2 \\ x^2+y^2+z^2 & = & 14 \\ x^3+y^3+z^3 & = & 20 \end{array}\right.$

Exercice VI-19. Trouver les racines de $X^3 - 8X^2 + 23X - 28$, sachant que la somme de deux des racines est égale à la troisième.

VII – Polynômes irréductibles de $\mathbb{R}[X]$ et $\mathbb{C}[X]$

1– Théorème de D'Alembert–Gauss

Théorème 9. *de* D'Alembert–Gauss

$$\forall P \in \mathbb{C}[X],\ \deg(P) \geqslant 1 \implies \exists x \in \mathbb{C} \ /\ P(x) = 0$$

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

Remarque 22. Ce théorème est également appelé **théorème fondamental de l'algèbre**. Paradoxalement, il n'existe aucune démonstration *algébrique* de ce théorème (on peut le démontrer à l'aide de la topologie ou de l'analyse complexe), c'est pourquoi nous le considérerons admis dans la suite du cours.

Corollaire 1. *Tout polynôme complexe est scindé*
Soit $P \in \mathbb{C}[X]$, non-constant. Alors, nécessairement P est **scindé**, donc s'écrit :

$$P = \lambda \prod_{i=1}^{n} (X - a_i), \quad \text{avec } n = \deg(P),\ (a_i)_{i \in [\![1;n]\!]} \in \mathbb{C}^n,\ \lambda \in \mathbb{C}^*$$

Exemple 14. *Polynômes complexes courants sous forme scindée*

- $(X^2+1) = (X-\mathrm{i})(X+\mathrm{i})$
- $(X^2+X+1) = (X-j)(X-j^2)$ avec $j = \mathrm{e}^{\frac{2\mathrm{i}\pi}{3}}$
- $(X^n-1) = \prod_{k=1}^{n} (X - \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}})$
- $X^2 - 2\cos(\theta)X + 1 = (X - \mathrm{e}^{\mathrm{i}\theta})(X - \mathrm{e}^{-\mathrm{i}\theta})$

2– Polynômes irréductibles

Définition 17. *Polynôme irréductible*
Soit $P \in \mathbb{K}[X]$ un polynôme *non-constant*. On dit que P est **irréductible** sitôt que *ses seuls diviseurs sont :*

- Les constantes non-nulles, $\alpha \in \mathbb{K}^*$
- Les produits de P et d'une constante non-nulle : $\alpha P,\ \alpha \in \mathbb{K}^*$

Remarque 23. Notez la similitude avec les nombres premiers, dans l'anneau $\mathbb{Z}$, qui n'ont pour seuls diviseurs que ± 1 et $\pm p$. Le terme multiplicatif ± 1 est ici remplacé par $\alpha \in \mathbb{K}^*$, car le *groupe des inversibles* de $\mathbb{K}[X]$ est $\mathbb{K}^*$, contre $\{-1; +1\}$ pour $\mathbb{Z}\ldots$
Remarquez également que l'on exclue les polynômes constants de la définition, tout comme on a exclu 1 et -1 de la définition des nombres premiers. En somme, les polynômes irréductibles sont les « nombre premiers de l'ensemble des polynômes ». Notamment, tout comme il est possible de décomposer un entier en produit de facteurs premiers, nous allons voir qu'on peut décomposer un polynôme en produits de facteurs irréductibles. Cependant, il convient au préalable de décrire plus précisément ces facteurs.

Théorème 10. *Les polynômes irréductibles de* $\mathbb{C}[X]$ *sont les polynômes de degré* 1.

Remarque 24. C'est une conséquence directe du théorème de D'Alembert–Gauss. La démonstration fera l'objet d'un exercice.

Théorème 11. *Les polynômes irréductibles de* $\mathbb{R}[X]$ *sont :*

1– Les polynômes de degré 1, ainsi que

2– Les polynômes de degré 2 n'ayant pas de racines réelles.

Démonstration 3. Soit $P \in \mathbb{K}[X]$ un polynôme.

- Si $\deg(P) = 0$ ou $P = 0$, par définition, P n'est pas irréductible.
- Si $\deg(P) = 1$, alors P est irréductible.
  En effet, prenons A un diviseur de P, on a donc $P = AB,\ (A, B) \in \mathbb{R}[X]^2$. Alors $\deg(P) = 1 = \deg(A) + \deg(B)$. C'est à dire que soit $\deg(A)$, soit $\deg(B)$ est nul, mais on est alors nécessairement dans l'un des deux cas de la définition.
- Si $\deg(P) = 2$ et P admet une racine réelle a, alors $(X - a)$ est un diviseur de P, et P n'est pas irréductible.
- Si $\deg(P) = 2$ et P n'admet pas de racines réelles, alors P est irréductible.
  En effet, prenons A un diviseur de P, on a donc $P = AB,\ (A, B) \in \mathbb{R}[X]^2$. Alors $\deg(P) = 2 = \deg(A) + \deg(B)$. Si $\deg(A) = 0$ ou 2, on est dans l'un des deux cas de la définition. Le cas $\deg(A) = 1$ est exclus, en effet, si $\deg(A) = 1$, alors $A = aX + b,\ (a, b) \in \mathbb{R}^* \times \mathbb{R}$ et A admet pour racine $\dfrac{-b}{a}$, et donc P également, ce qui est absurde.
- Si $\deg(P) = n > 2$, alors P n'est pas irréductible. En effet
  - Si P admet au moins une racine réelle $a \in \mathbb{R}$, il est divisible par $(X - a)$, et donc n'est pas irréductible.
  - Si P n'admet pas de racines réelles, écrivons alors P sous sa forme développée :

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

    Soit z une racine complexe de P (qui existe nécessairement, par le théorème de D'Alembert–Gauss). Alors

    $$P(z) = \sum_{k=1}^{n} a_k z^k = 0,\ (a_k)_{k \in [\![0;n]\!]} \in \mathbb{R}^{n+1}$$

En notant $\bar{z}$ son complexe conjugué, on a alors :

$$\begin{aligned} P(\bar{z}) &= \sum_{k=1}^{n} a_k (\bar{z})^k \\ &= \sum_{k=1}^{n} a_k \overline{z^k} \\ &= \sum_{k=1}^{n} \overline{a_k z^k} \text{ car } a_k \in \mathbb{R} \\ &= \overline{\sum_{k=1}^{n} a_k z^k} \\ &= \bar{0} = 0 \end{aligned}$$

donc $\bar{z}$ est également une racine (complexe) de P. Par division successive, on peut écrire :

$$\exists Q \in \mathbb{C}[X] \ / \ P = (X - z)(X - \bar{z})Q, \ \deg Q \geqslant 1$$

Notons alors que $F \stackrel{\text{def}}{=} (X - z)(X - \bar{z}) = X^2 - (z + \bar{z})X + z\bar{z} = X^2 - 2\Re(z)X + |z|^2 \in \mathbb{R}[X]$ (au passage, il s'agit d'un polynôme sans racines réelles...) De plus, puisque $P \in \mathbb{R}[X]$ et $F \in \mathbb{R}[X]$ et $P = FQ$, alors nécessairement $Q \in \mathbb{R}[X]$ (il suffit de prendre la partie imaginaire pour s'en convaincre...), et donc

$$\exists (F, Q) \in \mathbb{R}[X] \ / \ P = FQ \text{ avec } \deg(F) = 2 \text{ et } \deg(Q) \geqslant 1$$

Donc P n'est pas irréductible.

En conclusion de tous ces cas, les seuls polynômes réels irréductibles sont les polynômes de degré 1 et les polynômes de degré 2 sans racines réelles. □

Remarque 25. Un point essentiel a été vu dans cette démonstration : si α est une racine d'un polynôme à coefficients réels, alors son conjugué $\bar{\alpha}$ l'est également, et le produit des termes $(X - \alpha)(X - \bar{\alpha})$ est un polynôme à coefficients réels, de degré 2, sans racines réelles (donc irréductible dans $\mathbb{R}[X]$).

Exemple 15. *polynôme irréductibles de* $\mathbb{R}[X]$

- $X^2 + X + 1$ est irréductible dans $\mathbb{R}[X]$ (mais pas dans $\mathbb{C}[X]$).
- $X^2 - X + 1$ est irréductible dans $\mathbb{R}[X]$ (mais pas dans $\mathbb{C}[X]$).
- $X - 1$ est irréductible dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$.

Théorème 12. *Soit $P \in \mathbb{K}[X]$ un polynôme non-constant. Alors on peut décomposer P en produit d'une constante $\alpha \in \mathbb{K}^*$ et de facteurs irréductibles de $\mathbb{K}[X]$:*

$$\exists \alpha \in \mathbb{K}^*, (Q_1, \ldots, Q_m) \in \mathbb{K}[X]^m \ / \ P = \alpha \prod_{i=1}^{m} Q_i, \quad \text{avec } \forall i \in [\![1; m]\!], \ Q_i \text{ irréductible dans } \mathbb{K}[X]$$

De plus, cette décomposition est unique (à l'ordre des facteurs près) si on impose que le coefficient dominant des polynômes Q_i soit 1.

Exemple 16. *Décomposition en produits de facteurs irréductibles*

- $X^4 + X^2 + 1 = (1 - X + X^2)(1 + X + X^2)$ dans $\mathbb{R}[X]$

  On peut obtenir cette factorisation grâce aux identités remarquables : $X^4 + X^2 + 1 = (X^2 + 1)^2 - X^2 = \ldots$
- $X^4 - X^2 + 1 = (X^2 - \sqrt{3}X + 1)(X^2 + \sqrt{3}X + 1)$ dans $\mathbb{R}[X]$

  Cette décomposition peut être obtenue en calculant toutes les racines complexes du polynômes, puis en développant dans le polynôme scindé les termes deux par deux, avec à chaque fois une racine et son conjugué.

– $X^{12}-1=(X-1)(X+1)(X^2+1)(X^2-X+1)(X^2+X+1)(X^2-\sqrt{3}X+1)(X^2+\sqrt{3}X+1)$.

On peut obtenir cette décomposition en remarquant au préalable que $1,-1,\mathrm{i},-\mathrm{i},j,\bar{j},-j,-\bar{j}$ sont racines (avec $j=\mathrm{e}^{\frac{2\mathrm{i}\pi}{3}}$), donc $X^{12}-1$ est divisible par

$$\underbrace{(X-1)(X+1)}_{1,-1\text{ racines}}\underbrace{(X^2+1)}_{\mathrm{i},-\mathrm{i}\text{ racines}}\underbrace{(X^2+X+1)}_{j,\bar{j}\text{ racines}}\underbrace{(X^2-X+1)}_{-j,-\bar{j}\text{ racines}}$$

La division euclidienne par ce polynôme laisse alors comme quotient X^4-X^2+1, que l'on a déjà factorisé.

Proposition 11. Un polynôme de $\mathbb{R}[X]$ à toujours un nombre pair de racines complexes, et deux racines complexes conjuguées ont toujours le même ordre de multiplicité.

Remarque 26. On a donc plusieurs méthodes pour décomposer un polynôme en produits de facteurs irréductibles dans $\mathbb{R}[X]$ ou $\mathbb{C}[X]$:

1– Trouver des racines par les méthodes habituelles (racines évidentes, changement de variable, résolution par radicaux,...), puis faire la division euclidienne par le polynôme $(X-a)(X-b)\dots$ ainsi obtenu

2– Utiliser une identité remarquable $A^n-B^n=(A-B)(A^{n-1}+A^{n-2}B+\cdots+B^{n-1})$, $(A+B)^n$, etc ...

3– Écriture du polynôme sous forme développée et résolution de système ;

4– ...

3– Polynômes premiers entre eux

Définition 18. *Polynômes premier entre eux* Soit $(P,Q)\in\ \mathbb{K}[X]$. On dit que P et Q sont **premiers entre eux** sitôt que :

$$\forall D\in\mathbb{K}[X],\ (D|P\text{ et }D|Q)\implies D\in\mathbb{K}^*$$

c'est-à-dire que *leurs seuls facteurs commun sont les polynômes constants non-nuls.*

Exemple 17. *Polynômes premier entre eux*

1– X^2-1 et X^2+1 sont premiers entre eux.

2– X^3+X^2+X+1 et X^2-1 ne sont pas premiers entre eux.

3– X^3+1 et X^2+1 sont premiers entre eux.

Proposition 12. Deux polynômes de $\mathbb{C}[X]$ sont premiers entre eux si et seulement si il n'ont aucune racine en commun.

Remarque 27. Cela vient naturellement du fait que tout polynôme de $\mathbb{C}[X]$ est scindé. Une question qu'on peut alors se poser est : peut-on avoir deux polynômes P et Q à coefficients réels qui soient premiers entre eux si on les considère comme des polynômes de $\mathbb{C}[X]$, mais ne le sont plus quand on les considère comme des polynômes de $\mathbb{R}[X]$? Évidemment, ce n'est pas possible. Et réciproquement, peut-on avoir deux polynômes P et Q à coefficients réels qui soient premiers entre eux si on les considère comme des polynômes de $\mathbb{R}[X]$, mais ne le sont plus quand on les considère comme des polynômes de $\mathbb{C}[X]$? Là encore, c'est impossible, mais la démonstration mérite d'être écrite...

4– Exercices

Exercice VII-20. *Démonstrations*

1– À l'aide d'une récurrence et du théorème de D'Alembert–Gauss, démontrer le **Corollaire 1**.

2– Démontrer le **Théorème 10**.

3– En déduire le **Théorème 12** dans le cas $\mathbb{K}=\mathbb{C}$.

4– À l'aide de la **Proposition 11** et des questions précédentes, démontrer le **Théorème 12** dans le cas $\mathbb{K} = \mathbb{R}$.

Exercice VII-21. *Décomposition en produits de facteurs irréductibles*
Décomposer les polynômes suivants dans $\mathbb{R}[X]$ (éventuellement en passant par $\mathbb{C}[X]$) :

1– $X^4 - 1$
2– $X^5 - 1$
3– $(X^2 - 2X + 1)^2 - 1$
4– $X^4 + X^2 + 1$
5– $X^4 + X^2 - 6$
6– $X^8 + X^4 + 1$
7– $X^{2n+1} - 1$ avec $n \in \mathbb{N}^*$
8– $X^{2n} - 2\cos(\alpha n)X^n + 1$ avec $n \in \mathbb{N}^*$ et $\alpha \in]0; \pi[$.

VIII – Exercices

Exercice VIII-22. Soit P un polynôme complexe, non-constant. Existe-t'il $\lambda \in \mathbb{C}$ tel que $P - \lambda$ soit un polynôme scindé à racines simples ?

Exercice VIII-23. *Les polynômes dérivés de polynômes scindés sont scindés*

1– Soit $f : \mathbb{R} \mapsto \mathbb{R}$ une fonction dérivable, dont on suppose qu'elle s'annule au moins $n \geqslant 2$ fois. Montrer que f' s'annule au moins $n - 1$ fois.
2– Soit $P \in \mathbb{R}[X]$ un polynôme scindé à racines simples, de degré $n \geqslant 2$. Montrer que P' est scindé
3– En déduire que $\forall P \in \mathbb{R}[X]$, P scindé $\implies$ P' scindé sur $\mathbb{R}$ ou constant.
4– Soit $(a, b, c) \in \mathbb{R}^3$. Montrer que $X^{10} + aX^9 + bX^8 + cX^6 + X + 1$ n'est pas scindé sur $\mathbb{R}$.

Exercice VIII-24. À quelle condition sur $(\lambda, \mu) \in \mathbb{R}$ a-t'on $(X^2 + 2) | (X^4 + X^3 + \lambda X^2 + \mu X + 2)$?

Exercice VIII-25. Montrer que :

1– $\forall n \in \mathbb{N}^*,\ X^2 | (X + 1)^n - nX - 1$
2– $\forall n \in \mathbb{N}^*,\ (X - 1)^3 | nX^{n+2} - (n + 2)X^{n+1} + (n + 2)X - n$
3– $\forall (n, p, q) \in \mathbb{N}^3,\ X^2 + X + 1 | X^{3q+2} + X^{3p+1} + X^{3n}$

Exercice VIII-26. Trouver les polynômes $P \in \mathbb{C}[X]$ vérifiant :

1– $P(X^2) = P(X)P(X - 1)$
2– $P(X^2) = P(X)P(X + 1)$

Exercice VIII-27. *Polynômes de* Lagrange
Soit $(a_i)_{i \in [\![0;n]\!]} \in \mathbb{K}^{n+1}$ une famille d'éléments deux-à-deux distincts ($i \neq j \implies a_i \neq a_j$). Pour $i \in [\![0; n]\!]$, on pose :

$$L_i \stackrel{\text{def}}{=} \prod_{\substack{0 \leqslant j \leqslant n \\ j \neq i}} (X - a_j) \frac{1}{\prod_{\substack{0 \leqslant j \leqslant n \\ j \neq i}} (a_i - a_j)}$$

1– Calculer $L_i(a_j)$ pour $i \neq j$, avec $(i, j) \in [\![0; n]\!]^2$
2– Calculer $L_i(a_i)$ pour $i \in [\![0; n]\!]$
3– Quel est le degré de L_i ?
4– Montrer que $\forall P \in \mathbb{K}[X],\ \deg(P) \leqslant n \implies P = \sum_{i=0}^{n} P(a_i) L_i$
5– **Application :** donner un polynôme P tel que : $P(0) = 1$, $P(1) = 6$, $P(2) = 4$, $P(-1) = 2$, et $P(-2) = -1$.