Table des matières

1 L'algèbre $\mathbb{K}[X]$

1.1 Définition

Définition 1. *Soit $\mathbb{K}$ un corps. Alors il existe une algèbre commutative $\mathbb{K}[X]$ et un élément $X \in \mathbb{K}[X]$ appelé indéterminée tels que :*
— *Pour tout $P \in \mathbb{K}[X]$, il existe $n \in \mathbb{N}$ et $a_0, \dots, a_n \in \mathbb{K}$ tels que*

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

où, par abus de notation, $a_0 = a_0 \cdot 1_{\mathbb{K}[X]} = a_0 X^0$.
— *Pour tout $n \in \mathbb{N}$ et $a_0, \dots, a_n \in \mathbb{K}$*

$$a_0 + a_1 X + \cdots + a_n X^n = 0 \quad \Longrightarrow \quad a_0 = \cdots = a_n = 0$$

On l'appelle algèbre des polynômes à coefficients dans $\mathbb{K}$.

Remarques :

⇨ Soit $P \in \mathbb{K}[X]$, $a_0, \dots, a_n \in \mathbb{K}$ et $b_0, \dots, b_m \in \mathbb{K}$ tels que $P = a_0 + a_1 X + \cdots + a_n X^n$ et $P = b_0 + b_1 X + \cdots + b_m X^m$. Si on prolonge les définitions des suites a et b en posant $a_k = 0$ pour $k > n$ et $b_k = 0$ pour $k > m$, alors les suites (a_k) et (b_k) sont égales. On dit que les a_k sont les coefficients du polynôme P.

⇨ Deux polynômes sont égaux si et seulement si ils ont les mêmes coefficients.

⇨ Les coefficients d'un produit de deux polynômes se calculent par la formule

$$\left[\sum_{k=0}^{n} a_k X^k\right] \cdot \left[\sum_{k=0}^{m} b_k X^k\right] = \sum_{k=0}^{n+m} \left(\sum_{l=0}^{k} a_{k-l} b_l\right) X^k$$

Exercice :

⇨ Soit $n \in \mathbb{N}$. Montrer que

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$$

1.2 Substitution

Définition 2. *Soit $\mathcal{A}$ une $\mathbb{K}$-algèbre, $x \in \mathcal{A}$ et $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$. On définit $P(x)$ par :*

$$P(x) = a_0 1_{\mathcal{A}} + a_1 x + \cdots + a_n x^n \in \mathcal{A}$$

On dit que l'on a substitué l'élément $x \in \mathcal{A}$ à l'indéterminée X.

Remarques :

⇨ Si $\mathcal{A}$ une $\mathbb{K}$-algèbre et $x \in \mathcal{A}$, l'application φ de $\mathbb{K}[X]$ dans $\mathcal{A}$ qui à P associe $P(x)$ vérifie

$$\begin{aligned} \forall P, Q \in \mathbb{K}[X] \quad \forall \lambda, \mu \in \mathbb{K} \qquad & (\lambda P + \mu Q)(x) = \lambda P(x) + \mu Q(x) \\ \forall P, Q \in \mathbb{K}[X] \qquad & (PQ)(x) = P(x)\, Q(x) \\ & 1_{\mathbb{K}[X]}(x) = 1_{\mathcal{A}} \end{aligned}$$

On dit que c'est un morphisme d'algèbre.

⇨ Si $x \in \mathcal{A}$ et $n \in \mathbb{N}^*$, le calcul naïf de x^n nécessite $n-1$ multiplications dans $\mathcal{A}$. Si $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$, le calcul de $P(x)$ nécessite donc $n(n-1)/2$ multiplications dans $\mathcal{A}$. Cependant, si on écrit

$$P(x) = ((\cdots((a_n x + a_{n-1})\, x + a_{n-2})\, x + \cdots + a_2)\, x + a_1)\, x + a_0$$

le calcul de $P(x)$ nécessite $n-1$ multiplications dans $\mathcal{A}$. Cette méthode de calcul est connue sous le nom d'algorithme de Hörner.

⇨ On dit qu'un polynôme P est un polynôme annulateur de $x \in \mathcal{A}$ lorsque $P(x) = 0$. Par exemple, si $\mathbb{K} = \mathbb{Q}$ et $\mathcal{A} = \mathbb{R}$, $P = X^2 - 2$ est un polynôme annulateur de $\sqrt{2}$. Si E est un $\mathbb{K}$-espace vectoriel et si $s \in \mathcal{L}(E)$ est une symétrie, alors $P = X^2 - 1$ est un polynôme annulateur de s.

⇨ On dit qu'un élément $z \in \mathbb{C}$ est algébrique lorsqu'il existe un polynôme non nul $P \in \mathbb{Q}[X]$ tel que $P(z) = 0$. Par exemple $z_1 = \left(1+\sqrt{5}\right)/2$ est algèbrique car $P_1 = X^2 - X - 1 \in \mathbb{Q}[X]$ est un polynôme annulateur de z_1. De même, j est algèbrique car $P_2 = X^3 - 1 \in \mathbb{Q}[X]$ est un polynôme annulateur de j.
Lorsqu'on effectue des calculs avec un nombre algébrique z, il est souvent plus économe en calculs d'exploiter le fait que $P(z) = 0$ plutôt que de remplacer z par sa valeur. Par exemple, si $x = \left(1+\sqrt{5}\right)/2$, en exploitant le fait que $x^2 = x + 1$, on a

$$\left(\frac{1+\sqrt{5}}{2}\right)^3 = x^3 = x \cdot x^2 = x(x+1) = x^2 + x = 2x + 1 = 2 + \sqrt{5}$$

Comme $x^2 - x - 1 = 0$, on a $x(x-1) = 1$, donc $1/x = (x-1)$, donc

$$\frac{1}{\left(\frac{1+\sqrt{5}}{2}\right)} = \frac{1}{x} = x - 1 = \frac{-1+\sqrt{5}}{2}$$

⇨ On dit qu'un élément de $\mathbb{C}$ est transcendant lorsqu'il n'est pas algébrique. On peut montrer (mais c'est difficile) que e et π sont transcendants.

Exercice :

⇨ Montrer que $1 + \sqrt{7}$ et $\sqrt{2} + \sqrt{5}$ sont algébriques.

Définition 3. *Soit $P, Q \in \mathbb{K}[X]$. On définit le polynôme $P \circ Q$ par :*

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

Remarque :

⇨ Si $P \in \mathbb{K}[X]$, $P(X) = P$. Un polynôme peut donc indifféremment être noté P ou $P(X)$.

Définition 4. *Soit $P \in \mathbb{K}[X]$. On dit que :*
- *P est pair lorsque $P(-X) = P(X)$*
- *P est impair lorsque $P(-X) = -P(X)$*

Proposition 1. *Soit $P \in \mathbb{K}[X]$. Alors :*
- *P est pair si et seulement si ses coefficients d'indices impairs sont nuls.*
- *P est impair si et seulement si ses coefficients d'indices pairs sont nuls.*

1.3 Degré d'un polynôme

Définition 5. *Soit $P \in \mathbb{K}[X]$. On définit le degré de P que l'on note $\deg P$ par :*
- *Si $P = 0$, on pose $\deg P = -\infty$.*
- *Sinon, il existe $n \in \mathbb{N}$ et $a_0, \dots, a_n \in \mathbb{K}$ tels que :*

$$P = a_0 + a_1 X + \cdots + a_n X^n \quad et \quad a_n \neq 0$$

De plus n et les $a_0, \dots, a_n$ sont uniques ; on pose alors $\deg P = n$. Le coefficient a_n est appelé coefficient dominant de P.

Remarques :

⇨ Un polynôme $P \in \mathbb{K}[X]$ est de degré inférieur ou égal à $n \in \mathbb{N}$ si et seulement si il existe $a_0, \dots, a_n \in \mathbb{K}$ tels que :

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

⇨ On dit qu'un polynôme P est constant lorsqu'il existe $\lambda \in \mathbb{K}$ tel que $P = \lambda$, c'est-à-dire lorsque son degré est inférieur ou égal à 0.

Proposition 2. *Soit $P, Q \in \mathbb{K}[X]$ et $n \in \mathbb{N}$.*
- *Soit $\lambda, \mu \in \mathbb{K}$. Si $\deg P \leqslant n$ et $\deg Q \leqslant n$, alors :*

$$\deg(\lambda P + \mu Q) \leqslant n$$

- *Soit $\lambda \in \mathbb{K}^*$ et $\mu \in \mathbb{K}$. Si $\deg P = n$ et $\deg Q < n$, alors :*

$$\deg(\lambda P + \mu Q) = n$$

Remarque :

⇨ Lorsque P et Q sont des polynômes de degré n, il est possible que $P + Q$ soit de degré strictement inférieur à n. Par exemple $P = X + 1$ et $Q = -X$ sont de degré 1 mais $P + Q = 1$ est de degré 0.

Exercice :

⇨ Soit $P \in \mathbb{K}[X]$. Calculer le degré de $P(X+1) - P(X)$.

Définition 6. *Soit $n \in \mathbb{N}$. On note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n.*

Remarques :

⇨ Si $n \in \mathbb{N}$, $\mathbb{K}_n[X]$ est stable par combinaison linéaire.

⇨ Si $n \geqslant 1$, $\mathbb{K}_n[X]$ n'est pas stable par produit. En effet, $X^n \in \mathbb{K}_n[X]$ mais $X^{2n} = X^n \cdot X^n \notin \mathbb{K}_n[X]$.

Proposition 3. *Soit $P, Q \in \mathbb{K}[X]$. Alors :*

$$\deg(PQ) = \deg P + \deg Q$$

Remarques :

⇨ Si $P \in \mathbb{K}[X]$ est non nul et si $n \in \mathbb{N}$, alors $\deg(P^n) = n \deg P$.

⇨ Si $P \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$ n'est pas constant, alors $\deg(P \circ Q) = \deg(P) \deg(Q)$.

Proposition 4. *$\mathbb{K}[X]$ est une algèbre intègre :*

$$\forall P, Q \in \mathbb{K}[X] \quad PQ = 0 \quad \Longrightarrow \quad [P = 0 \quad ou \quad Q = 0]$$

Proposition 5. *Les éléments inversibles de $\mathbb{K}[X]$ sont les polynômes de degré 0, c'est-à-dire les polynômes constants non nuls.*

Définition 7. *On dit qu'un polynôme non nul U est unitaire lorsque son coefficient dominant est égal à 1. Tout polynôme P non nul s'écrit de manière unique sous la forme $P = \lambda P_u$ où $\lambda \neq 0$ et P_u est unitaire. Lorsque $P = 0$, on pose par convention $P_u = 0$.*

1.4 Racines, fonctions polynomiales

Définition 8. *Soit $P \in \mathbb{K}[X]$. On appelle racine de P tout élément $\alpha \in \mathbb{K}$ tel que $P(\alpha) = 0$.*

Remarques :

- La notion de racine dépend du corps considéré. En effet, si on le considère comme élément de $\mathbb{C}[X]$, les racines de $(X^2-2)(X^2+1)$ sont $\sqrt{2}, -\sqrt{2}, i, -i$. Considéré comme élément de $\mathbb{R}[X]$, ses racines sont $\sqrt{2}, -\sqrt{2}$. Enfin il n'a aucune racine si on le considère comme un élément de $\mathbb{Q}[X]$.
- Si $\mathbb{K}$ est un sous-corps de $\mathbb{L}$, $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{L}$, on dit que α est une racine de P sur $\mathbb{L}$ lorsque $P(\alpha) = 0$.
- Les polynômes de degré 1 admettent une unique racine.
- D'après le théorème des valeurs intermédiaires, tout polynôme réel de degré impair admet (au moins) une racine réelle.

Proposition 6. *Si $n \in \mathbb{N}$, tout polynôme de degré n admet au plus n racines.*

Remarques :

- On en déduit qu'un polynôme de degré inférieur ou égal à n admettant $n+1$ racines deux à deux distinctes est nul. De même, si deux polynômes de degrés inférieurs ou égaux à n prennent la même valeur en $n+1$ points deux à deux distincts, alors ils sont égaux.
- Un polynôme admettant une infinité de racines est donc nul. De même, deux polynômes prenant la même valeur sur un ensemble infini sont égaux.

Exercices :

- Montrer que les polynômes de $\mathbb{K}[X]$ tels que $P(X) = P(X+1)$ sont les polynômes constants.
- Montrer qu'il n'existe pas de polynôme $P \in \mathbb{C}[X]$ tel que, pour tout $z \in \mathbb{C}$, $P(z) = \overline{z}$.
- On se donne $n+1$ éléments de $\mathbb{K}$ deux à deux distincts $x_0, x_1, \ldots, x_n$ et $y_0, \ldots, y_n \in \mathbb{K}$. Montrer qu'il existe un unique polynôme P de degré inférieur ou égal à n tel que

$$\forall k \in [\![0, n]\!] \quad P(x_k) = y_k$$

On dit que P est le polynôme interpolateur de Lagrange associé aux familles (x_k) et (y_k).

Définition 9. *On dit qu'une application $f : \mathbb{K} \to \mathbb{K}$ est une fonction polynomiale lorsqu'il existe $P \in \mathbb{K}[X]$ tel que :*

$$\forall x \in \mathbb{K} \quad f(x) = P(x)$$

Proposition 7. *Si $\mathbb{K}$ est infini, l'application de l'algèbre $\mathbb{K}[X]$ dans l'algèbre $\mathcal{F}(\mathbb{K}, \mathbb{K})$, qui au polynôme P associe la fonction polynomiale $\tilde{P}$, est injective.*

Remarques :

- Cette proposition permet, lorsque $\mathbb{K}$ est infini, d'identifier polynômes et fonctions polynomiales. C'est pourquoi certains énoncés se permettent de confondre polynômes et fonctions polynomiales, identification que nous ne ferons que lorsque l'énoncé le demande explicitement.
- Cette proposition est fausse lorsque le corps $\mathbb{K}$ est fini. En effet, si $\mathbb{K} = \{a_1, \ldots, a_n\}$, le polynôme

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

est non nul car $\deg P = n$, mais la fonction polynomiale associée est nulle.

1.5 Polynôme dérivé

Définition 10. *Soit $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$. On définit le polynôme dérivé de P par :*

$$\begin{aligned} P' &= a_1 + 2a_2 X + \cdots + n a_n X^{n-1} \\ &= \sum_{k=1}^{n} k a_k X^{k-1} \end{aligned}$$

Remarque :

- Dans le cas où $\mathbb{K} = \mathbb{R}$, la fonction polynomiale associée à P' est la dérivée de la fonction polynomiale associée à P.

Proposition 8. *Soit $P, Q \in \mathbb{K}[X]$ et $\lambda, \mu \in \mathbb{K}$. Alors :*

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

Définition 11. *Soit $P \in \mathbb{K}[X]$. On définit par récurrence la dérivée n-ième de P par :*

- $P^{(0)} = P$
- $\forall n \in \mathbb{N} \quad P^{(n+1)} = \left[P^{(n)}\right]'$

Remarque :

⇨ Soit $n \in \mathbb{N}$. Alors

$$\forall k \in \mathbb{N} \quad (X^n)^{(k)} = \begin{cases} \frac{n!}{(n-k)!} X^{n-k} & \text{si } k \leqslant n \\ 0 & \text{sinon} \end{cases}$$

En particulier, si $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$, alors

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

Proposition 9. *Soit $P, Q \in \mathbb{K}[X]$ et $n \in \mathbb{N}$*

— *Soit $\lambda, \mu \in \mathbb{K}$. Alors :*

$$(\lambda P + \mu Q)^{(n)} = \lambda P^{(n)} + \mu Q^{(n)}$$

— *On a :*

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

Cette formule est appelée formule de Leibnitz.

Exercice :

⇨ Calculer $(X^2 P)^{(n)}$ en fonction des dérivées successives de P.

Proposition 10. *Soit $P \in \mathbb{K}[X]$. Alors :*

— $\deg P' = \deg(P) - 1$ *si* $\deg P \geqslant 1$.

— $\deg P' = -\infty$ *sinon.*

Remarques :

⇨ $P' = 0$ si et seulement si P est constant.

⇨ Pour tout $P \in \mathbb{K}[X]$, $\deg P' \leqslant \deg(P) - 1$.

⇨ Soit $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$. Alors le degré de $P^{(n)}$ est égal à $\deg(P) - n$ si $\deg P \geqslant n$ et à $-\infty$ sinon. En particulier, quel que soit $P \in \mathbb{K}[X]$, $\deg P^{(n)} \leqslant \deg(P) - n$.

Proposition 11. *Soit P un polynôme de degré inférieur ou égal à n et $\alpha \in \mathbb{K}$. Alors :*

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

2 Arithmétique dans $\mathbb{K}[X]$

2.1 Relation de divisibilité, division euclidienne

Définition 12. *Soit $A, B \in \mathbb{K}[X]$. On dit que A divise B lorsqu'il existe $P \in \mathbb{K}[X]$ tel que $B = PA$.*

Remarque :

⇨ Si $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$, $X - \alpha$ divise P si et seulement si α est une racine de P.

Proposition 12. *La relation de divisibilité*

— *est réflexive :* $\forall A \in \mathbb{K}[X] \quad A|A$

— *est transitive :* $\forall A, B, C \in \mathbb{K}[X] \quad [A|B \quad et \quad B|C] \Longrightarrow A|C$

— *n'est pas antisymétrique. Cependant :*

$$\forall A, B \in \mathbb{K}[X] \quad [A|B \quad et \quad B|A] \quad \Longleftrightarrow \quad [\exists \lambda \in \mathbb{K}^* \quad A = \lambda B]$$

Si tel est le cas, on dit que A et B sont associés.

Proposition 13. *Soit $A, B, C \in \mathbb{K}[X]$ et $P, Q \in \mathbb{K}[X]$, alors :*

$$[A|B \quad et \quad A|C] \quad \Longrightarrow \quad A|(PB + QC)$$

Proposition 14. *Soit $A, B \in \mathbb{K}[X]$.*

— *Si $B \neq 0$, alors :*

$$A|B \quad \Longrightarrow \quad \deg A \leqslant \deg B$$

— *Si $A|B$ et $\deg A = \deg B$, alors A et B sont associés.*

Définition 13. *Soit $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Alors, il existe un unique couple $(Q, R) \in \mathbb{K}[X]$ tel que :*

$$A = QB + R \quad et \quad \deg R < \deg B$$

Q est appelé quotient de la division euclidienne de A par B, R son reste.

Remarques :

⇨ Si $A, B \in \mathbb{K}[X]$ et $B \neq 0$, alors B divise A si et seulement si le reste de la division euclidienne de A par B est nul.

⇨ Si B est un polynôme annulateur non nul de x et $A \in \mathbb{K}[X]$, alors $A(x) = R(x)$ où R est le reste de la division euclidienne de A par B. En effet

$$A(x) = Q(x) \underbrace{B(x)}_{=0} + R(x)$$

⇨ Il est parfois utile de connaître le reste de la division euclidienne de A par B sans calculer son quotient.
Par exemple, si $A = X^n$ et $B = (X-1)(X-2)$, le reste R de la division euclidienne de A par B est de degré inférieur ou égal à 1 donc il existe $a, b \in \mathbb{R}$ tels que $R = aX + b$. Comme $A = QB + R$, on en déduit que $A(1) = Q(1) B(1) + R(1)$. Comme $B(1) = 0$, on a $A(1) = R(1)$. De même $A(2) = R(2)$. Donc

$$\begin{cases} a + b = 1 \\ 2a + b = 2^n \end{cases}$$

on en déduit que $a = 2^n - 1$ et $b = 2 - 2^n$. Donc $R = (2^n - 1)X + (2 - 2^n)$. Cette méthode fonctionne dès que le polynôme B, de degré n, admet n racines deux à deux distinctes.
Si $A = X^n$ et $B = (X-1)^2$, le reste R de la division euclidienne de A par B est de degré inférieur ou égal à 1 donc il existe $a, b \in \mathbb{R}$ tels que $R = aX + b$. Comme plus haut, $A(1) = R(1)$. En dérivant la relation $A = QB + R$, on obtient $A' = B'Q + BQ' + R'$. Puisque 1 est racine de B et de B', on en déduit que $A'(1) = R'(1)$. Donc

$$\begin{cases} a + b = 1 \\ a \quad\;\; = n \end{cases}$$

On en déduit que $a = n$ et $b = 1 - n$, donc $R = nX + (1 - n)$.

Exercices :

⇨ Calculer $x^5 + x^4 - 1$ où $x = (1 + \sqrt{5})/2$.

⇨ Montrer que le polynôme $P = X^3 + pX + q \in \mathbb{R}[X]$ admet 3 racines réelles deux à deux distinctes si et seulement si $4p^3 + 27q^2 < 0$.

2.2 Plus grand commun diviseur

Définition 14. *Soit $A, B \in \mathbb{K}[X]$. Il existe un unique polynôme unitaire ou nul P tel que :*
- *$P|A$ et $P|B$*
- *$\forall Q \in \mathbb{K}[X] \quad [Q|A \text{ et } Q|B] \Longrightarrow Q|P$*

On l'appelle pgcd *(plus grand commun diviseur) de A et de B et on le note* $\text{pgcd}(A, B)$, *(A, B) ou $A \wedge B$.*

Remarque :

⇨ Soit $A, B \in \mathbb{K}[X]$. Si l'un des deux polynômes est non nul, le pgcd de A et B est le polynôme unitaire de plus grand degré qui divise A et B.

⇨ Si $\alpha, \beta \in \mathbb{K}$ sont distincts, alors $(X - \alpha) \wedge (X - \beta) = 1$.

Proposition 15. *On a :*

$$\begin{aligned} \forall A \in \mathbb{K}[X] \quad & A \wedge 0 = A_u \\ \forall A \in \mathbb{K}[X] \quad & A \wedge 1 = 1 \\ \forall A, B \in \mathbb{K}[X] \quad & A \wedge B = 0 \Longleftrightarrow [A = 0 \quad et \quad B = 0] \end{aligned}$$

Proposition 16. *On a :*

$$\begin{aligned} \forall A, B \in \mathbb{K}[X] \quad & A \wedge B = B \wedge A \\ \forall A, B \in \mathbb{K}[X] \quad \forall \lambda, \mu \in \mathbb{K}^* \quad & A \wedge B = (\lambda A) \wedge (\mu B) = A_u \wedge B_u \\ \forall A, B, P \in \mathbb{K}[X] \quad & (PA) \wedge (PB) = P_u (A \wedge B) \end{aligned}$$

Définition 15. *Soit $A_1, \ldots, A_n \in \mathbb{K}[X]$. Il existe un unique polynôme unitaire ou nul P tel que :*
- *$\forall i \in [\![1, n]\!] \quad P|A_i$*
- *$\forall Q \in \mathbb{K}[X] \quad [\forall i \in [\![1, n]\!] \quad Q|A_i] \Longrightarrow Q|P$*

On l'appelle pgcd *(plus grand commun diviseur) de la famille $(A_1, \ldots, A_n)$ et on le note* $\text{pgcd}(A_1, \ldots, A_n)$, *ou $A_1 \wedge \cdots \wedge A_n$.*

Remarque :

⇨ Le pgcd d'une famille $(A_1, \ldots, A_n)$ de polynômes ne dépend pas de l'ordre de ces derniers.

Proposition 17. *Soit $A_1, \ldots, A_n \in \mathbb{K}[X]$ et $p \in [\![1, n-1]\!]$. Alors*

$$A_1 \wedge \cdots \wedge A_n = (A_1 \wedge \cdots \wedge A_p) \wedge (A_{p+1} \wedge \cdots \wedge A_n)$$

2.3 Algorithme d'Euclide

Proposition 18. *Soit $A, B, P \in \mathbb{K}[X]$. Alors :*

$$A \wedge B = A \wedge (B + PA) = (A + PB) \wedge B$$

En particulier, si $B \neq 0$ et R est le reste de la division euclidienne de A par B, on a :

$$A \wedge B = B \wedge R$$

Exercice :

⇨ Calculer $A \wedge B$ où $A = X^4 - X^3 + X^2 + X - 2$ et $B = X^3 + X^2 - X - 1$.

Proposition 19. *Soit $\mathbb{L}$ un corps, $\mathbb{K}$ un sous-corps de $\mathbb{L}$ et P et $Q \in \mathbb{K}[X]$. Alors :*
- *P divise Q dans $\mathbb{K}[X]$ si et seulement si P divise Q dans $\mathbb{L}[X]$.*
- *Les* pgcd *et* ppcm *de P et de Q dans $\mathbb{K}[X]$ sont les mêmes que ceux dans $\mathbb{L}[X]$.*

2.4 Relation de Bézout

Proposition 20. *Si $A, B \in \mathbb{K}[X]$, il existe $U, V \in \mathbb{K}[X]$ tels que :*

$$UA + VB = A \wedge B$$

Remarques :

⇨ Les polynômes U et V sont appelés polynômes de Bézout.

⇨ Le couple (U, V) n'est pas unique. En effet, si $(U_0, V_0) \in \mathbb{K}[X]^2$ est un couple de polynômes de Bézout, alors pour tout $P \in \mathbb{K}[X]$, $(U_0 + PB, V_0 - PA)$ en est un autre.

Exercice :

⇨ Calcul d'un couple de polynômes de Bezout pour $A = (X-1)^2$ et $B = (X+2)^2$.

Définition 16. *Soit $A, B \in \mathbb{K}[X]$. On dit que A et B sont premiers entre eux lorsque $A \wedge B = 1$.*

Remarques :

⇨ Deux polynômes premiers entre eux n'admettent aucune racine commune. Cependant, la réciproque est fausse. En effet, si $\mathbb{K} = \mathbb{R}$, $P = X^2 + 1$ n'admet aucune racine réelle, donc aucune racine commune avec lui-même. Pourtant $P \wedge P = P \neq 1$.

Exercice :

⇨ Montrer que si A et B sont premiers entre eux, il en est de même pour $A - B$ et $A + B$.

Proposition 21. *Soit $A, B \in \mathbb{K}[X]$. Alors A et B sont premiers entre eux si et seulement si il existe $U, V \in \mathbb{K}[X]$ tels que :*

$$UA + VB = 1$$

Remarque :

⇨ Nous avons déjà vu que le couple $(U, V) \in \mathbb{K}[X]^2$ n'est pas unique. Cependant, si A et B sont premiers entre eux et non constants, il existe un unique couple $(U, V) \in \mathbb{K}[X]^2$ de polynômes de Bézout tel que $\deg U < \deg B$ et $\deg V < \deg A$. On peut vérifier que c'est le couple donné par l'algorithme d'Euclide.

Proposition 22.
- *Soit $A, B, C \in \mathbb{K}[X]$ tels que $A \wedge B = 1$ et $A \wedge C = 1$. Alors $A \wedge (BC) = 1$.*
- *Plus généralement, si $A \in \mathbb{K}[X]$ est premier avec chaque élément d'une famille de polynômes $B_1, \dots, B_n \in \mathbb{K}[X]$, alors A est premier avec leur produit.*
- *Soit $A, B \in \mathbb{K}[X]$ deux polynômes premiers entre eux et $m, n \in \mathbb{N}$. Alors $A^m \wedge B^n = 1$.*

Définition 17. *Soit $A_1, \dots, A_n \in \mathbb{K}[X]$.*
- *On dit que $A_1, \dots, A_n$ sont deux à deux premiers entre eux lorsque*

$$\forall i, j \in [\![1, n]\!] \quad i \neq j \Longrightarrow A_i \wedge A_j = 1$$

- *On dit que $A_1, \dots, A_n$ sont premiers entre eux dans leur ensemble lorsque*

$$A_1 \wedge \cdots \wedge A_n = 1$$

Remarques :

⇨ Si les polynômes $A_1, \dots, A_n$ sont deux à deux premiers entre eux, alors ils sont premiers entre eux dans leur ensemble. Cependant, la réciproque est fausse. Par exemple, les polynômes $A_1 = (X-2)(X-3)$, $A_2 = (X-1)(X-3)$ et $A_3 = (X-1)(X-2)$ sont premiers entre eux dans leur ensemble mais ne sont pas deux à deux premiers entre eux.

Proposition 23. *Soit $A_1, \dots, A_n \in \mathbb{K}[X]$. Alors $A_1, \dots, A_n$ sont premiers entre eux dans leur ensemble si et seulement si il existe $U_1, \dots, U_n \in \mathbb{K}[X]$ tels que*

$$U_1 A_1 + \cdots + U_n A_n = 1$$

2.5 Lemme de Gauss

Proposition 24. *Soit $A, B, C \in \mathbb{K}[X]$. Alors :*

$$[A|BC \quad et \quad A \wedge B = 1] \quad \Longrightarrow \quad A|C$$

Remarque :

⇨ Si $A, B \in \mathbb{K}[X]$ sont premiers entre eux et le couple $(U_0, V_0) \in \mathbb{K}[X]^2$ est tel que $U_0 A + V_0 B = 1$, l'ensemble des couples de polynômes de Bézout pour A et B est

$$\{(U_0 + PB, V_0 - PA) : P \in \mathbb{K}[X]\}$$

Proposition 25.
- *Soit $A, B, C \in \mathbb{K}[X]$. On suppose que $A|C$, $B|C$ et $A \wedge B = 1$. Alors $AB|C$.*
- *Plus généralement si $A \in \mathbb{K}[X]$ est divisé par chaque élément d'une famille $B_1, \dots, B_n \in \mathbb{K}[X]$ de polynômes deux à deux premiers entre eux, alors il est divisé par leur produit.*

2.6 Plus petit commun multiple

Définition 18. *Soit $A, B \in \mathbb{K}[X]$. Il existe un unique polynôme unitaire ou nul P tel que :*
- *$A|P$ et $B|P$*
- *$\forall Q \in \mathbb{K}[X] \quad [A|Q \quad et \quad B|Q] \Longrightarrow P|Q$*

On l'appelle ppcm *(plus petit commun multiple) de A et de B et on le note* $\text{ppcm}(A, B)$*, ou $A \vee B$.*

Proposition 26. *On a :*

$$\begin{aligned} \forall A \in \mathbb{K}[X] \quad & A \vee 0 = 0 \\ \forall A \in \mathbb{K}[X] \quad & A \vee 1 = A_u \\ \forall A, B \in \mathbb{K}[X] \quad & A \vee B = 0 \Longleftrightarrow [A = 0 \quad ou \quad B = 0] \end{aligned}$$

Proposition 27. *On a :*

$$\begin{aligned} \forall A, B \in \mathbb{K}[X] \quad & A \vee B = B \vee A \\ \forall A, B \in \mathbb{K}[X] \quad \forall \lambda, \mu \in \mathbb{K}^* \quad & A \vee B = (\lambda A) \vee (\mu B) = A_u \vee B_u \\ \forall A, B, P \in \mathbb{K}[X] \quad & (PA) \vee (PB) = P_u (A \vee B) \end{aligned}$$

Proposition 28. *Soit $A, B \in \mathbb{K}[X]$.*
- *Si $A \wedge B = 1$, alors :*

$$A \vee B = (AB)_u$$

- *De manière générale :*

$$(A \wedge B)(B \vee A) = (AB)_u$$

2.7 Polynômes irréductibles

Définition 19. *On dit qu'un polynôme $P \in \mathbb{K}[X]$ de degré supérieur ou égal à 1 est irréductible lorsque ses seuls diviseurs sont les polynômes associés à 1 ou à P.*

Remarques :

- Un polynôme P de degré supérieur ou égal à 1 est irréductible si et seulement si ses diviseurs sont de degré 0 ou de même degré que P.
- Si $\alpha \in \mathbb{K}$, $P = X - \alpha$ est irréductible.
- Un polynôme $P \in \mathbb{K}[X]$ de degré inférieur ou égal à 3 n'admettant aucune racine dans $\mathbb{K}$ est irréductible. En particulier, les polynômes de $\mathbb{R}[X]$ de degré 2 dont le discriminant est strictement négatif sont irréductibles.
- Cependant, il existe des polynômes $P \in \mathbb{K}[X]$ n'admettant aucune racine dans $\mathbb{K}$ et qui ne sont pas irréductibles. Par exemple le polynôme $P = (X^2+1)^2$ n'admet aucune racine dans $\mathbb{R}$ sans être irréductible.

Proposition 29. *Soit P un polynôme irréductible et $A \in \mathbb{K}[X]$. Alors $P|A$ ou $P \wedge A = 1$.*

Proposition 30. *Soit $P \in \mathbb{K}[X]$ un polynôme irréductible.*
- *Si $A, B \in \mathbb{K}[X]$:*
$$P|AB \iff [P|A \quad ou \quad P|B]$$
- *Plus généralement, P divise un produit si et seulement si il divise un de ses facteurs.*

Proposition 31. *Tout polynôme non constant admet un diviseur irréductible.*

Remarque :

- En particulier, un polynôme est associé à 1 si et seulement si il n'admet aucun diviseur irréductible.

Proposition 32. *Soit $A \in \mathbb{K}[X] \setminus \{0\}$. Alors, il existe $\lambda \in \mathbb{K}^*$, $P_1, \dots, P_r$ des polynômes unitaires irréductibles deux à deux distincts et $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$ tels que :*
$$A = \lambda \prod_{k=1}^{r} P_k^{\alpha_k}$$
De plus, à permutation près des P_k, cette décomposition est unique.

Définition 20. *Lorsque $A \in \mathbb{K}[X] \setminus \{0\}$ et P est polynôme unitaire irréductible, on appelle valuation de P relativement à A et on note $\mathrm{Val}_P(A)$ le plus grand $\alpha \in \mathbb{N}$ tel que $P^\alpha | A$.*

Remarques :

- Si $A \in \mathbb{K}[X] \setminus \{0\}$, il n'existe qu'un nombre fini de polynômes unitaires irréductibles P tels que $\mathrm{Val}_P(A) \neq 0$. Ce sont les polynômes unitaires irréductibles apparaissant dans la décomposition de A en polynômes irréductibles.
- Si $\lambda \in \mathbb{K}^*$ est le coefficient dominant de A, la décomposition de n en polynômes unitaires irréductibles s'écrit
$$A = \lambda \prod_{P \in \mathcal{I}} P^{\mathrm{Val}_P(A)}$$
où $\mathcal{I}$ désigne l'ensemble des polynômes unitaires irréductibles de $\mathbb{K}[X]$.

Proposition 33. *Soit $A, B \in \mathbb{K}[X] \setminus \{0\}$. Alors*
- *$A|B$ si et seulement si*
$$\forall P \in \mathcal{I} \quad \mathrm{Val}_P(A) \leqslant \mathrm{Val}_P(B)$$
- *Le* pgcd *et le* ppcm *de A et B est donné par les relations*
$$\begin{aligned} \forall P \in \mathcal{I} \quad \mathrm{Val}_P(A \wedge B) &= \min(\mathrm{Val}_P(A), \mathrm{Val}_P(B)) \\ \mathrm{Val}_P(A \vee B) &= \max(\mathrm{Val}_P(A), \mathrm{Val}_P(B)) \end{aligned}$$

Exercice :

- Soit A et $B \in \mathbb{C}[X]$ deux polynômes premiers entre eux. Montrer que si AB est un carré, alors il en est de même pour A et B.

3 Racines d'un polynôme

3.1 Racines multiples

Proposition 34. *Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Alors α est une racine de P si et seulement si $X - \alpha$ divise P.*

Remarque :

- Si $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$ et $x = p/q$ est une racine rationnelle de P mise sous forme irréductible, alors $q|a_n$ et $p|a_0$. Cette relation nous permet de trouver les racines rationnelles de P. Par exemple, si $P = 2X^3 + 5X^2 + X - 3$ et p/q est une racine rationnelle de P mise sous forme irréductible, alors $q|2$ et $p|3$ donc $p \in \{-3, -1, 1, 3\}$ et $q \in \{1, 2\}$. Réciproquement, on constate que seul $-3/2$ est une racine de P. On peut donc factoriser P par $2X+3$. On obtient $P = (2X+3)\left(X^2 + X - 1\right)$, ce qui permet d'obtenir toutes les racines de P.

Définition 21. *Soit $\alpha \in \mathbb{K}$ une racine du polynôme non nul $P \in \mathbb{K}[X]$. On appelle ordre de α relativement à P le plus grand entier $\omega \in \mathbb{N}^*$ tel que $(X-\alpha)^\omega | P$. Les racines d'ordre 1 sont appelées racines simples et celles d'ordre $\omega \geqslant 2$ sont appelées racines multiples.*

Remarques :

⇨ Pour simplifier l'énoncé des théorèmes suivants, on dira qu'un élément $\alpha \in \mathbb{K}$ est une racine d'ordre nul de P lorsqu'il n'est pas racine de P. Avec cette extension de définition, l'ordre de α relativement à P n'est rien d'autre que la valuation de $X - \alpha$ relativement à P.

⇨ Le scalaire $\alpha \in \mathbb{K}$ est une racine d'ordre $\omega \in \mathbb{N}$ de P si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - \alpha)^{\omega} Q$ et $Q(\alpha) \neq 0$.

Proposition 35. *Soit $P \in \mathbb{K}[X]$ un polynôme non nul et $\alpha \in \mathbb{K}$. Si α est racine d'ordre $\omega \in \mathbb{N}^*$ de P, α est racine d'ordre $\omega - 1$ de P'.*

Proposition 36. *Soit $P \in \mathbb{K}[X]$ un polynôme non nul, $\alpha \in \mathbb{K}$ et $\omega \in \mathbb{N}$. Alors les deux assertions suivantes sont équivalentes :*
- *α est racine d'ordre ω de P.*
- *$P(\alpha) = 0, P'(\alpha) = 0, \ldots, P^{(\omega-1)}(\alpha) = 0$ et $P^{(\omega)}(\alpha) \neq 0$.*

Exercice :

⇨ Calculer l'ordre de 1 relativement à $P = X^4 - 2X^3 + 2X^2 - 2X + 1$.

Proposition 37. *Soit $P \in \mathbb{R}[X]$ et $\alpha \in \mathbb{C}$. Alors, lorsqu'on considère P comme élément de $\mathbb{C}[X]$:*
- *α est racine de P si et seulement si $\overline{\alpha}$ est racine de P.*
- *Si tel est le cas, α et $\overline{\alpha}$ ont même ordre relativement à P.*

Proposition 38. *Soit $P \in \mathbb{K}[X]$ un polynôme non nul et $\alpha_1, \ldots, \alpha_r$ des racines de P deux à deux distinctes d'ordres respectifs $\omega_1, \ldots, \omega_r \in \mathbb{N}^*$. Alors, il existe $Q \in \mathbb{K}[X]$ tel que :*

$$P = (X - \alpha_1)^{\omega_1} \cdots (X - \alpha_r)^{\omega_r} Q$$

En particulier $\omega_1 + \cdots + \omega_r \leqslant n$. On dit que P admet au plus n racines comptées avec leur ordre de multiplicité.

Définition 22. *Soit $P \in \mathbb{K}[X]$ un polynôme non nul de degré $n \in \mathbb{N}$. On suppose que P admet r racines $\alpha_1, \ldots, \alpha_r$ deux à deux distinctes d'ordres respectifs $\omega_1, \ldots, \omega_r \in \mathbb{N}^*$ avec $\omega_1 + \cdots + \omega_r = n$. Alors, en notant $\lambda \in \mathbb{K}^*$ le coefficient dominant de P, on a*

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

On dit alors que P est scindé.

Remarque :

⇨ La notion de polynôme scindé dépend du corps considéré. Par exemple le polynôme $P = (X^2 + 1)^2$ est scindé sur $\mathbb{C}$ alors qu'il ne l'est pas sur $\mathbb{R}$.

Définition 23. *Soit $P \in \mathbb{K}[X]$ un polynôme non nul de degré $n \in \mathbb{N}$. On suppose que P admet n racines $\alpha_1, \ldots, \alpha_n$ deux à deux distinctes. Alors, elles sont simples et en notant $\lambda \in \mathbb{K}^*$ le coefficient dominant de P, on a*

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

On dit alors que P est scindé simple.

Exercice :

⇨ Soit $n \in \mathbb{N}^*$. Factoriser $X^n - 1$ sur $\mathbb{C}[X]$.

Définition 24. *Soit $x_1, \ldots, x_{n+1} \in \mathbb{K}$ deux à deux distincts et $y_1, \ldots, y_n, y_{n+1} \in \mathbb{K}$. Alors, il existe un unique polynôme P de degré inférieur où égal à n tel que*

$$\forall i \in [\![1, n+1]\!] \quad P(x_i) = y_i$$

On l'appelle polynôme interpolateur de Lagrange associé aux familles $(x_1, \ldots, x_{n+1})$ et $(y_1, \ldots, y_{n+1})$.

Proposition 39. *Soit $x_1, \ldots, x_{n+1} \in \mathbb{K}$ deux à deux distincts. Pour tout $i \in [\![1, n+1]\!]$, on note L_i le polynôme définit par*

$$L_i = \prod_{\substack{k=1 \\ k \neq i}}^{n+1} \frac{X - x_k}{x_i - x_k}$$

Si $y_1, \ldots, y_{n+1} \in \mathbb{K}$, alors le polynôme interpolateur de Lagrange P associé aux familles $(x_1, \ldots, x_{n+1})$ et $(y_1, \ldots, y_{n+1})$ est donné par

$$P = \sum_{i=1}^{n+1} y_k L_k$$

Remarque :

⇨ Soit $x_1, \ldots, x_{n+1} \in \mathbb{K}$ deux à deux distincts, $y_1, \ldots, y_{n+1} \in \mathbb{K}$ et $P \in \mathbb{K}[X]$. Alors

$$\forall i \in [\![1, n+1]\!] \quad P(x_k) = y_k$$

si et seulement si il existe un polynôme $Q \in \mathbb{K}[X]$ tel que

$$P = \sum_{i=1}^{n+1} y_k L_k + Q \prod_{k=1}^{n+1} (X - x_k)$$

3.2 Théorème fondamental de l'algèbre

Théorème 1. *Tout polynôme de $\mathbb{C}[X]$ de degré supérieur ou égal à 1 admet (au moins) une racine dans $\mathbb{C}$.*

Exercice :

⇨ Soit $P \in \mathbb{C}[X]$ est de degré supérieur ou égal à 1. Montrer que l'application $\tilde{P}$ de $\mathbb{C}$ dans $\mathbb{C}$ qui à z associe $P(z)$ est surjective.

Proposition 40. *Les polynôme unitaires irréductibles de $\mathbb{C}[X]$ sont les $X-\alpha$ avec $\alpha \in \mathbb{C}$.*

Remarques :

⇨ Soit P et Q deux polynômes non nuls de $\mathbb{C}[X]$. Alors P divise Q si et seulement si pour toute racine α de P, α est racine de Q et son ordre relativement à P est inférieur ou égal à son ordre relativement à Q.

⇨ Deux polynômes non nuls de $\mathbb{C}[X]$ sont égaux si et seulement si ils ont le même coefficient dominant et les mêmes racines avec les mêmes ordres de multiplicité.

⇨ Dans $\mathbb{C}[X]$, deux polynômes sont premiers entre eux si et seulement si ils n'admettent aucune racine commune. En particulier, deux polynômes de $\mathbb{R}[X]$ sont premiers entre eux si et seulement si ils n'admettent aucune racine complexe en commun.

Exercices :

⇨ Montrer que X^2+1 divise X^n+X si et seulement si $n \equiv 3$ [4].

⇨ Soit $n, m \in \mathbb{N}$. Montrer que $(X^n-1) \wedge (X^m-1) = X^{n \wedge m} - 1$.

Proposition 41. *Soit $P \in \mathbb{C}[X]$ un polynôme non nul. Alors, il existe $\alpha_1, \ldots, \alpha_r \in \mathbb{C}$ deux à deux distincts, $\omega_1, \ldots, \omega_r \in \mathbb{N}^*$ et $\lambda \in \mathbb{C}^*$ tels que :*

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

De plus, à permutation près de α_k, cette décomposition est unique. En particulier, les polynômes non nuls de $\mathbb{C}[X]$ sont scindés.

Remarques :

⇨ En pratique, cette décomposition est équivalente à la recherche du coefficient dominant de P, de ses racines et de leur ordre de multiplicité.

⇨ Sur $\mathbb{C}$, un polynôme de degré $n \in \mathbb{N}$ admet exactement n racines comptées avec leur ordre de multiplicité.

⇨ Un polynôme non nul $P \in \mathbb{C}[X]$ est scindé simple si et seulement si P et P' sont premiers entre eux.

Proposition 42. *Les polynômes unitaires irréductibles de $\mathbb{R}[X]$ sont les :*
- *$X-\alpha$ avec $\alpha \in \mathbb{R}$*
- *X^2+bX+c avec $\Delta = b^2-4c < 0$*

Proposition 43. *Soit $P \in \mathbb{R}[X]$ un polynôme non nul. Alors, il existe $\alpha_1, \ldots, \alpha_r \in \mathbb{R}$ deux à deux distincts, $\omega_1, \ldots, \omega_r \in \mathbb{N}^*$, $(b_1, c_1), \ldots, (b_s, c_s) \in \mathbb{R}^2$ deux à deux distincts tels que $\Delta_l = b_l^2 - 4c_l < 0$ pour tout $l \in [\![1, s]\!]$, $\omega'_1, \ldots, \omega'_s \in \mathbb{N}^*$ et $\lambda \in \mathbb{R}^*$ tels que :*

$$P = \lambda \prod_{k=1}^{r} (X-\alpha_k)^{\omega_k} \prod_{l=1}^{s} \left(X^2+b_lX+c_l\right)^{\omega'_l}$$

De plus, à permutation près des α_k et des (b_l, c_l), cette décomposition est unique.

Remarque :

⇨ En pratique, si on a effectué la décomposition de $P \in \mathbb{R}[X]$ en produit de polynômes unitaires irréductibles dans $\mathbb{C}[X]$, il suffit de regrouper les racines conjuguées et de développer ces produits pour obtenir la décomposition dans $\mathbb{R}[X]$. En effet, si $\alpha \in \mathbb{C}$

$$(X-\alpha)(X-\overline{\alpha}) = X^2 - 2\operatorname{Re}(\alpha) X + |\alpha|^2 \in \mathbb{R}[X]$$

Cependant, il est parfois possible d'aboutir plus rapidement à la décomposition dans $\mathbb{R}[X]$ en utilisant les identités algébriques.

Exercices :

⇨ Factoriser X^6-1 et X^4+1 sur $\mathbb{R}[X]$.

⇨ Soit $n \in \mathbb{N}^*$. Factoriser X^n-1 sur $\mathbb{R}[X]$.

3.3 Fonctions symétriques élémentaires

Remarque :

⇨ Soit $\alpha, \beta, \gamma \in \mathbb{K}$. Alors

$$(X-\alpha)(X-\beta)(X-\gamma) = X^3 - (\alpha+\beta+\gamma)X^2 + (\alpha\beta+\alpha\gamma+\beta\gamma)X - \alpha\beta\gamma$$

On introduit donc les quantités $\sigma_1 = \alpha+\beta+\gamma$, $\sigma_2 = \alpha\beta+\alpha\gamma+\beta\gamma$ et $\sigma_3 = \alpha\beta\gamma$. Remarquons que ces expressions sont symétriques en α, β, γ, c'est-à-dire qu'elles sont invariantes par permutation de ces 3 variables. On peut montrer que réciproquement toute expression polynomiale symétrique en α, β, γ peut s'exprimer comme un polynôme en ces 3 quantités. Par exemple $x = \alpha^2+\beta^2+\gamma^2$ est symétrique en α, β, γ et on remarque que

$$\begin{aligned} \sigma_1^2 &= (\alpha+\beta+\gamma)^2 \\ &= \alpha^2+\beta^2+\gamma^2+2(\alpha\beta+\alpha\gamma+\beta\gamma) \\ &= x+2\sigma_2 \end{aligned}$$

donc $x = \sigma_1^2 - 2\sigma_2$.

Définition 25. *Soit $\alpha_1, \dots, \alpha_n \in \mathbb{K}$. On définit les polynômes symétriques élémentaires en les variables $\alpha_1, \dots, \alpha_n$ par :*

$$\begin{aligned} \sigma_1 &= \alpha_1 + \cdots + \alpha_n \\ \sigma_2 &= \sum_{i_1 < i_2} \alpha_{i_1} \alpha_{i_2} \\ &\vdots \\ \sigma_n &= \alpha_1 \cdots \alpha_n \end{aligned}$$

Plus précisément, pour tout $k \in [\![1, n]\!]$

$$\sigma_k = \sum_{i_1 < \cdots < i_k} \alpha_{i_1} \cdots \alpha_{i_k}$$

Remarque :

⇨ Comme dans le cas vu plus haut dans le cas où $n = 3$, on peut montrer que tout polynôme symétrique en les $\alpha_1, \dots, \alpha_n$ s'écrit comme un polynôme en les $\sigma_1, \dots, \sigma_n$. Cette propriété justifie leur appellation de polynômes symétriques *élémentaires*.

Proposition 44. *Soit $P \in \mathbb{K}[X]$ un polynôme scindé de degré n :*

$$\begin{aligned} P &= a_0 + a_1 X + \cdots + a_n X^n \quad (a_n \neq 0) \\ &= \lambda \prod_{k=1}^{n} (X - \alpha_k) \quad (\lambda = a_n) \end{aligned}$$

les α_k n'étant pas forcément deux à deux distincts. Alors :

$$\forall k \in [\![1, n]\!] \quad \sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$$

Exercices :

⇨ Soit $z_1, z_2, z_3 \in \mathbb{C}$ les racines de $2X^3 + 3X^2 + X + 1$. Calculer

$$a = \sum_{k=1}^{3} z_k^2 \qquad b = \sum_{k=1}^{3} z_k^3 \qquad c = \sum_{k=1}^{3} \frac{1}{z_k}$$

⇨ Montrer que si $n \geqslant 2$, la somme des racines n-ièmes de l'unité est nulle et le produit des racines n-ièmes de l'unité est égal à $(-1)^{n-1}$.