Chapitre 3

Racines d'un polynôme

3.1 Fonction polynôme

Définition 3.1 *Soit* $\mathrm{A} = a_0 + a_1\mathrm{X} + \cdots + a_n\mathrm{X}^n$ *un polynôme de* $\mathbb{K}[\mathrm{X}]$. *On appelle fonction polynôme associée à* A *l'application* $\tilde{\mathrm{A}} : \mathbb{K} \longrightarrow \mathbb{K}$ *qui à tout* x *de* $\mathbb{K}$ *fait correspondre l'élément* $\tilde{\mathrm{A}}(x) = a_0 + a_1x + \cdots + a_nx^n$ *de* $\mathbb{K}$.

Remarque. Comme on le verra plus loin, la confusion entre un polynôme et sa fonction polynôme associée n'a, dans le cas où le corps $\mathbb{K}$ est infini (et donc en particulier lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$) pas de conséquence fâcheuse. Dans la pratique, on confondra donc souvent A et $\tilde{\mathrm{A}}$.
C'est par contre tout autre chose lorsque $\mathbb{K}$ est un corps fini. Par exemple, si $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$, le polynôme $\mathrm{A} = \mathrm{X}+\mathrm{X}^2$ n'est pas nul (tous ses coefficients ne sont pas nuls) et pourtant la fonction polynôme associée $\overline{x} \longmapsto \overline{x} + \overline{x}^2$ est la fonction nulle…

Proposition 3.2 *Soient* $(\mathrm{A}, \mathrm{B}) \in (\mathbb{K}[\mathrm{X}])^2$ *et* $\lambda \in \mathbb{K}$. *On a* • $\widetilde{\mathrm{A} + \lambda\mathrm{B}} = \widetilde{\mathrm{A}} + \lambda\widetilde{\mathrm{B}}$ *et* • $\widetilde{\mathrm{AB}} = \widetilde{\mathrm{A}}\widetilde{\mathrm{B}}$.

Démonstration : Cela résulte de manière immédiate des définitions des opérations sur les polynômes et des définitions des opérations sur les fonctions. □

Schéma de Hörner

Gardons les notations précédentes et effectuons le calcul de $\mathrm{A}(a)$ pour un certain $a \in \mathbb{K}$.
Le coût en multiplications du calcul de $a_0 + a_1a + \cdots + a_na^n$ par la méthode « naturelle » est de $n - 1$ multiplications pour calculer les puissances $a^2, \cdots, a^n$, plus n multiplications pour calculer les termes $a_1a, \cdots, a_na^n$, soit au total $2n - 1$. Le schéma de Hörner consiste à calculer successivement

$$\begin{aligned}
p_n &= a_na^n \\
p_{n-1} &= (a_{n-1} + p_n)a = a_{n-1}a + a_na^2 \\
&\vdots \\
p_2 &= (a_2 + p_3)a = a_2a + a_3a^2 + \cdots + a_na^{n-1} \\
p_1 &= (a_1 + p_2)a = a_1a + \cdots + a_na^n
\end{aligned}$$

et enfin $\mathrm{A}(a) = a_0 + p_1$, ce qui fait seulement n multiplications.

Théorème 3.3 (Formule de Taylor) *On suppose le corps* $\mathbb{K}$ *de caractéristique nulle*[1]. *Pour tout polynôme* $\mathrm{A} = \sum_{k=0}^{n} a_k\mathrm{X}^k$ *et tout scalaire* a *de* $\mathbb{K}$, *on a :* $\mathrm{A}(\mathrm{X}) = \sum_{k=0}^{n} \frac{\mathrm{A}^{(k)}(a)}{k!}(\mathrm{X} - a)^k$.

1. Cette hypothèse n'est là que pour garantir que l'on puisse diviser par les $k!$. $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps de caractéristique nulle.

Démonstration : Écrivons $A(X) = \sum_{k=0}^{n} a_k(X-a+a)^k$. Si on développe chaque terme $(X-a+a)^k$ par la formule du binôme $(X-a+a)^k = \sum_{i=0}^{k} \binom{k}{i} a^{k-i}(X-a)^i$, on obtient, en réordonnant suivant les puissances de $(X-a)$,

$$A(X) = \sum_{k=0}^{n} b_k(X-a)^k$$

avec des coefficients b_k que l'on va expliciter autrement.
On a $A^{(0)}(a) = A(a) = b_0$ et, pour $\ell \in [\![1, n]\!]$, par linéarité de la dérivation à l'ordre ℓ

$$\begin{aligned}
A^{(\ell)}(X) &= \sum_{k=0}^{n} b_k \left((X-a)^k\right)^{(\ell)} \\
&= \underbrace{\sum_{k=0}^{\ell-1} b_k \left((X-a)^k\right)^{(\ell)}}_{=0} + \sum_{k=\ell}^{n} b_k \left((X-a)^k\right)^{(\ell)} \\
&= \sum_{k=\ell}^{n} b_k k(k-1)\cdots(k-\ell+1)(X-a)^{k-\ell} \\
&= b_\ell \ell! + \sum_{k=\ell+1}^{n} b_k k(k-1)\cdots(k-\ell+1)(X-a)^{k-\ell}.
\end{aligned}$$

En évaluant cette quantité en a, nous obtenons $A^{(\ell)}(a) = b_\ell \ell!$ c'est à dire $b_\ell = \dfrac{A^{(\ell)}(a)}{\ell!}\cdot$ On trouve donc bien finalement $A(X) = \sum_{k=0}^{n} \dfrac{A^{(k)}(a)}{k!}(X-a)^k$. □

Exemple. Pour $A = X^3 + X$ et $a = 1$ on obtient : $X^3 + X = 2 + 4(X-1) + 3(X-1)^2 + (X-1)^3$.

Remarque. La spécificité de cette formule de Taylor dans le cas polynomial est qu'il n'y a pas de reste.

Exercice 3.1 Trouver un polynôme $A \in \mathbb{R}[X]$ de degré inférieur ou égal à trois tel que $A(0) = 0$ et $A(1) = A'(1) = A''(1) = 2$.

3.2 Racines, ordre d'une racine

Définition 3.4 *Soient* A *un polynôme de* $\mathbb{K}[X]$ *et* a *un élément de* $\mathbb{K}$*. On dit que* a *est une racine de* A *si l'application polynomiale* $A : \mathbb{K} \longrightarrow \mathbb{K}$, $x \longmapsto A(x)$ *s'annule en* a *:* $A(a) = 0$.

Proposition 3.5 *Soient* A *un polynôme de* $\mathbb{K}[X]$ *et* a *un élément de* $\mathbb{K}$*.* a *est une racine de* A *si et seulement si* $X - a$ *divise* A.

Démonstration : Supposons que $X - a$ divise A, soit $A = (X-a)Q$. On obtient aussitôt $A(a) = (a-a)Q(a) = 0$.
Réciproquement, supposons que $A(a) = 0$. On peut faire la division euclidienne de A par $X - a$: $A = Q(X-a) + R$, où le degré de R est strictement inférieur à $1 = \deg(X-a)$ donc R est une constante c. En évaluant cette relation en a, on obtient $0 = A(a) = c$. Ainsi, $A = (X-a)Q$ et donc $X - a$ divise A. □

Remarque. La démonstration met en lumière le fait que le reste dans la division euclidienne de A par $\mathrm{X}-a$ n'est autre que $\mathrm{A}(a)$.

Exemple. Il existe Q tel que $\mathrm{X}^4-2\mathrm{X}^3+\mathrm{X}^2-\mathrm{X}-2=(\mathrm{X}-2)\mathrm{Q}$ car 2 est racine de $\mathrm{X}^4-2\mathrm{X}^3+\mathrm{X}^2-\mathrm{X}-2$. On trouve $\mathrm{X}^4-2\mathrm{X}^3+\mathrm{X}^2-\mathrm{X}-2=(\mathrm{X}-2)(\mathrm{X}^3+\mathrm{X}+1)$.

Proposition 3.6 *Un polynôme non nul de degré n de $\mathbb{K}[\mathrm{X}]$ a au plus n racines distinctes.*

Démonstration : Par récurrence sur n. Pour $n=0$, un polynôme constant non nul possède évidemment zéro racine.

Soit n fixé, supposons le résultat vrai pour les polynômes de degré n ; soit maintenant A un polynôme de degré $n+1$. Si A n'a aucune racine, le résultat est vrai pour A ; sinon soit a une racine de A ; par la proposition précédente on peut écrire $\mathrm{A}=(\mathrm{X}-a)\mathrm{Q}$ pour un polynôme Q, qui est clairement de degré n. Maintenant, si b est une racine de A, alors $0=\mathrm{A}(b)=(b-a)\mathrm{Q}(b)$ donc $b=a$ ou b est une racine de Q (on utilise l'hypothèse d'intégrité de $\mathbb{K}$) ; or Q a au plus n racines, donc A en a au plus $n+1$. $\square$

Conséquence. Le seul polynôme ayant une infinité de racines est le polynôme nul.

Exercice 3.2 On suppose le corps $\mathbb{K}$ infini. Montrer que si deux polynômes de $\mathbb{K}[\mathrm{X}]$ définissent la même fonction polynôme de $\mathbb{K}$ dans $\mathbb{K}$ alors ils sont égaux.

Définition 3.7 *Soient $\mathrm{A}\in\mathbb{K}[\mathrm{X}]$, $r\in\mathbb{N}^*$ et $a\in\mathbb{K}$. On dit que a est racine d'ordre r de A s'il existe un polynôme Q tel que $\mathrm{A}=(\mathrm{X}-a)^r\mathrm{Q}$ avec $\mathrm{Q}(a)\neq 0$. Autrement dit, a est racine d'ordre r de A si A est divisible par $(\mathrm{X}-a)^r$ mais pas par $(\mathrm{X}-a)^{r+1}$.*

Vocabulaire

Une racine est dite ***simple*** si elle est d'ordre 1, ***double*** si elle est d'ordre 2,...
D'une manière générale, l'entier r est appelé ***ordre de multiplicité*** de la racine.

Exemple. $\mathrm{A}=\mathrm{X}^5-9\mathrm{X}^4+25\mathrm{X}^3-9\mathrm{X}^2-54\mathrm{X}+54$, $a=3$.

$$\begin{aligned}\mathrm{A}&=(\mathrm{X}-3)(\mathrm{X}^4-6\mathrm{X}^3+7\mathrm{X}^2+12\mathrm{X}-18)\\&=(\mathrm{X}-3)^2(\mathrm{X}^3-3\mathrm{X}^2-2\mathrm{X}+6)\\&=(\mathrm{X}-3)^3(\mathrm{X}^2-2)\end{aligned}$$

3 est donc racine d'ordre 3 du polynôme A.

Exercice 3.3 Soit A un polynôme non constant de $\mathbb{K}[\mathrm{X}]$. Montrer que si $a_1,\cdots,a_p$ sont des racines de A d'ordres respectifs $k_1,\cdots,k_p$ alors A est divisible par $(\mathrm{X}-a_1)^{k_1}\cdots(\mathrm{X}-a_p)^{k_p}$.
En déduire qu'un polynôme non nul de degré n de $\mathbb{K}[\mathrm{X}]$ a au plus n racines (comptées avec multiplicité).

Théorème 3.8 *Soient $r\in\mathbb{N}^*$, $\mathrm{A}\in\mathbb{K}[\mathrm{X}]$ et $a\in\mathbb{K}$. a est racine d'ordre r du polynôme A si et seulement si*

$$\mathrm{A}(a)=\mathrm{A}'(a)=\ldots=\mathrm{A}^{(r-1)}(a)=0 \quad \textit{et} \quad \mathrm{A}^{(r)}(a)\neq 0.$$

Démonstration : Par la formule de Taylor, en notant $d=\deg \mathrm{A}$, on a $\mathrm{A}=\displaystyle\sum_{k=0}^{d}\frac{\mathrm{A}^{(k)}(a)}{k!}(\mathrm{X}-a)^k$.

- Si $\mathrm{A}(a)=\ldots=\mathrm{A}^{(r-1)}(a)=0$ et $\mathrm{A}^{(r)}(a)\neq 0$, on a nécessairement $d\geqslant r$ et

$$\mathrm{A}=\sum_{k=r}^{d}\frac{\mathrm{A}^{(k)}(a)}{k!}(\mathrm{X}-a)^k=(\mathrm{X}-a)^r\underbrace{\sum_{k=r}^{d}\frac{\mathrm{A}^{(k)}(a)}{k!}(\mathrm{X}-a)^{k-r}}_{\mathrm{Q}(\mathrm{X})}$$

et donc a est racine d'ordre r de A puisque $\mathrm{Q}(a) = \dfrac{\mathrm{A}^{(r)}(a)}{r!} \neq 0$.

• Réciproquement, si a est racine d'ordre r de A, on a $d \geqslant r$ et :

$$\mathrm{A} = \underbrace{\sum_{k=0}^{r-1} \frac{\mathrm{A}^{(k)}(a)}{k!}(\mathrm{X}-a)^k}_{\mathrm{R}} + (\mathrm{X}-a)^r \underbrace{\sum_{k=r}^{d} \frac{\mathrm{A}^{(k)}(a)}{k!}(\mathrm{X}-a)^{k-r}}_{\mathrm{Q}}.$$

L'écriture ci-dessus est celle (unique) de la division euclidienne de A par $(\mathrm{X}-a)^r$. Puisque $(\mathrm{X}-a)^r | \mathrm{A}$, on a $\mathrm{R} = 0$ d'où

$$\mathrm{A}(a) = \mathrm{A}'(a) = \ldots = \mathrm{A}^{(r-1)}(a) = 0.$$

Et comme $\mathrm{Q}(a) \neq 0$, $\mathrm{A}^{(r)}(a) \neq 0$. □

Exemple. On considère le polynôme précédent. On a $\mathrm{A}(3) = 0$.
Puis $\mathrm{A}' = 5\mathrm{X}^4 - 36\mathrm{X}^3 + 75\mathrm{X}^2 - 18\mathrm{X} - 54$ et $\mathrm{A}'(3) = 0$,
$\mathrm{A}'' = 20\mathrm{X}^3 - 108\mathrm{X}^2 + 150\mathrm{X} - 18$ et $\mathrm{A}''(3) = 0$
$\mathrm{A}''' = 60\mathrm{X}^2 - 216\mathrm{X} + 150$ et $\mathrm{A}'''(3) = 42 \neq 0$.

Polynôme d'interpolation de Lagrange

Théorème 3.9 *Soit $n \in \mathbb{N}^*$. Soient $a_1, \ldots, a_n$ des éléments deux à deux distincts de $\mathbb{K}$. Soient $b_1, \ldots, b_n$ des éléments de $\mathbb{K}$. Alors il existe un unique polynôme A de degré inférieur ou égal à $n-1$ vérifiant $\forall j \in [\![1, n]\!]$, $\mathrm{A}(a_j) = b_j$; ce polynôme est donné par la formule suivante :*

$$\mathrm{A} = \sum_{k=1}^{n} b_k \prod_{i \neq k} \frac{\mathrm{X} - a_i}{a_k - a_i}.$$

Démonstration : Il est immédiat que le polynôme A proposé convient bien. Supposons que B soit un autre polynôme solution. On a alors $\forall j \in [\![1, n]\!]$, $\mathrm{A}(a_j) - \mathrm{B}(a_j) = 0$. Le polynôme $\mathrm{A} - \mathrm{B}$, qui est de degré inférieur ou égal à $n-1$ (comme différence de tels polynômes), a alors au moins n racines (les a_j sont distincts). C'est donc le polynôme nul et $\mathrm{A} = \mathrm{B}$. □

Remarques.

- La formule ci-dessus est due au mathématicien Joseph Louis Lagrange (1736-1813) ; on parle du « polynôme d'interpolation de Lagrange associé aux couples $(a_1, b_1), \ldots, (a_n, b_n)$ ».
- l'hypothèse sur les a_i est nécessaire ; en effet, si ces valeurs ne sont pas deux à deux distinctes, alors il n'y a aucun polynôme solution.
- dès que d est supérieur ou égal à n, il existe une infinité de polynômes A de degré d tels que $\forall j \in [\![1, n]\!]$, $\mathrm{A}(a_j) = b_j$.

Exemple. Le polynôme d'interpolation de Lagrange A tel que $\mathrm{A}(-1) = 2$, $\mathrm{A}(0) = 1$ et $\mathrm{A}(1) = -1$ est

$$\mathrm{A} = 2\frac{\mathrm{X}(\mathrm{X}-1)}{(-1) \times (-2)} + \frac{(\mathrm{X}+1)(\mathrm{X}-1)}{1 \times (-1)} - \frac{(\mathrm{X}+1)\mathrm{X}}{2 \times 1} = -\frac{1}{2}\mathrm{X}^2 - \frac{3}{2}\mathrm{X} + 1$$

Dans le plan muni d'un repère orthonormé, on a ainsi trouvé une parabole passant par les trois points de coordonnées $(-1, 2)$, $(0, 1)$ et $(1, -1)$.

3.3 Racines et polynômes irréductibles

Définition 3.10 *Un polynôme est dit* ***scindé*** *s'il peut s'écrire comme produit de facteurs du premier degré.*

3.3.1 Cas des polynômes à coefficients complexes

Théorème 3.11 (d'Alembert-Gauss) *Tout polynôme non constant de* $\mathbb{C}[\mathrm{X}]$ *admet au moins une racine complexe.*

Corollaire 3.12 *Les polynômes irréductibles dans* $\mathbb{C}[\mathrm{X}]$ *sont exactement les polynômes du premier degré.*

Démonstration : On sait déjà que les polynômes du premier degré sont irréductibles. Montrons que ce sont les seuls. Les polynômes constants n'étant pas irréductibles, soit A un polynôme de $\mathbb{C}[\mathrm{X}]$ de degré au moins 2. A a alors au moins une racine α dans $\mathbb{C}$ (théorème précédent) et donc A a au moins trois diviseurs unitaires distincts (car de degrés différents) : 1, $\mathrm{X}-\alpha$ et $\frac{1}{\mathrm{coefdom(A)}}\mathrm{A}$. A n'est donc pas irréductible. $\square$

Corollaire 3.13 *Tout polynôme de* $\mathbb{C}[\mathrm{X}]$ *est scindé. Un polynôme de* $\mathbb{C}[\mathrm{X}]$ *de degré* d *a donc exactement* d *racines complexes (comptées avec multiplicité).*

3.3.2 Cas des polynômes à coefficients réels

Évidemment, tout polynôme à coefficients réels peut être vu comme polynôme à coefficients complexes (les réels étant des complexes particuliers).

Proposition 3.14 *Soient* $\mathrm{A} \in \mathbb{R}[\mathrm{X}]$ *et* $\alpha \in \mathbb{C}$. α *est racine de* A *(vu comme polynôme de* $\mathbb{C}[\mathrm{X}]$*) si et seulement si* $\overline{\alpha}$ *est racine de* A. *En particulier, les racines complexes non réelles de* A *sont deux à deux conjuguées.*

Exercice 3.4 Démontrer cette proposition.

Théorème 3.15 *Les polynômes irréductibles dans* $\mathbb{R}[\mathrm{X}]$ *sont*

- *les polynômes de degré 1.*
- *les polynômes de degré 2 sans racine dans* $\mathbb{R}$ *i.e. de la forme* $a\mathrm{X}^2+b\mathrm{X}+c$ *avec* $b^2-4ac<0$.

Tout polynôme non constant $\mathrm{A} \in \mathbb{R}[\mathrm{X}]$ *s'écrit donc comme produit de polynômes de ces types.*

Démonstration : Les polynômes mentionnés sont clairement irréductibles. Il reste à voir que tout $\mathrm{A} \in \mathbb{R}[\mathrm{X}]$ avec $\deg \mathrm{A} \geqslant 1$ est divisible par un polynôme du type mentionné. Si A a une racine réelle, c'est clair. Sinon, A peut être considéré comme appartenant à $\mathbb{C}[\mathrm{X}]$ et il a une racine $\alpha \in \mathbb{C} \setminus \mathbb{R}$ grâce au théorème de d'Alembert. La proposition précédente montre alors que $\bar{\alpha}$ est aussi racine de A. Ainsi A est divisible dans $\mathbb{C}[\mathrm{X}]$ par les deux polynômes irréductibles distincts $\mathrm{X}-\alpha$ et $\mathrm{X}-\bar{\alpha}$, donc par le produit

$$\mathrm{B} = (\mathrm{X}-\alpha)(\mathrm{X}-\bar{\alpha}) = \mathrm{X}^2 - 2\mathrm{Re}(\alpha)\mathrm{X} + |\alpha|^2$$

qui est un polynôme de degré 2 de $\mathbb{R}[\mathrm{X}]$ irréductible. La division euclidienne de A par B dans $\mathbb{R}[\mathrm{X}]$ s'écrit $\mathrm{A} = \mathrm{BQ} + \mathrm{R}$ avec $\deg \mathrm{R} < 2$. Cette relation peut être vue comme une égalité de polynômes de $\mathbb{C}[\mathrm{X}]$ et c'est donc aussi la division euclidienne de A par B dans $\mathbb{C}[\mathrm{X}]$. Par unicité du reste, on a $\mathrm{R} = 0$ et finalement A est divisible par B dans $\mathbb{R}[\mathrm{X}]$. $\square$

Remarque. On vient lors de cette démonstration d'établir le résultat suivant : si A et B sont deux polynômes à coefficients réels et si B divise A dans $\mathbb{C}[\mathrm{X}]$ alors B divise A dans $\mathbb{R}[\mathrm{X}]$.

Exercice 3.5 On considère le polynôme $A = X^6 - 6X^5 + 15X^4 - 20X^3 + 12X^2 - 4$. Sachant que A a au moins une racine multiple dans $\mathbb{C}$, donner la décomposition en facteurs irréductibles de A dans $\mathbb{R}[X]$ puis dans $\mathbb{C}[X]$.

Correction : Si α est une racine multiple de A alors α est racine de A (donc $X-\alpha$ divise A) et α est aussi racine de A' (donc $X-\alpha$ divise A'). Par suite $X-\alpha$ divise $\mathrm{pgcd}(A, A')$. On commence donc par déterminer ce pgcd. Or, $A' = 6X^5 - 30X^4 + 60X^3 - 60X^2 + 24X$. Les divisions euclidiennes successives donnent :

- $A = (\frac{1}{6}X - \frac{1}{6})A' - 2X^2 - 4X - 4$
- $A' = (X^2 - 2X + 2)(6X^3 - 18X^2 + 12X)$. Par suite, $\mathrm{pgcd}(A, A') = X^2 - 2X + 2$.

On peut alors factoriser A par ce pgcd :

$$A = (X^2 - 2X + 2)^2(X^2 - 2X - 1) = (X^2 - 2X + 2)^2\big(X - (1+\sqrt{2})\big)\big(X - (1-\sqrt{2})\big)$$

Cette dernière écriture est la décomposition en facteurs irréductibles de A dans $\mathbb{R}[X]$ (le polynôme de degré 2 intervenant ayant un discriminant strictement négatif).
Dans $\mathbb{C}[X]$ on obtient : $A = \big(X - (1+i)\big)^2\big(X - (1-i)\big)^2\big(X - (1+\sqrt{2})\big)\big(X - (1-\sqrt{2})\big)$

3.4 Relations entre coefficients et racines

Théorème 3.16 *Soit $A = a_0 + \cdots + a_{n-1}X^{n-1} + X^n$ un polynôme unitaire de degré $n > 0$, scindé sur $\mathbb{K}$. Soient $\alpha_1, ..., \alpha_n$ ses racines comptées avec multiplicité (une racine de multiplicité k figure k fois). Pour $k \in \{1, \cdots, n\}$, on note σ_k la somme des produits k à k des racines. de A. Alors :*

$$\begin{aligned}
-a_{n-1} &= \sum_{1\leqslant i\leqslant n} \alpha_i &&= \sigma_1 \\
a_{n-2} &= \sum_{1\leqslant i_1<i_2\leqslant n} \alpha_{i_1}\alpha_{i_2} &&= \sigma_2 \\
&\vdots \\
(-1)^k a_{n-k} &= \sum_{1\leqslant i_1<\cdots<i_k\leqslant n} \alpha_{i_1}\cdots\alpha_{i_k} &&= \sigma_k \\
&\vdots \\
(-1)^n a_0 &= \alpha_1\cdots\alpha_n &&= \sigma_n
\end{aligned}$$

En particulier, a_{n-1} est l'opposé de la somme des racines et $(-1)^n a_0$ est le produit des racines.

Démonstration : La décomposition en facteurs irréductibles de A s'écrit $A = (X-\alpha_1)\cdots(X-\alpha_n)$. En développant et en identifiant les coefficients, on obtient le résultat annoncé. □

Exemples. Pour un polynôme du second degré $X^2 + a_1X + a_0$ de racines α_1 et α_2, on a :

$$a_1 = -(\alpha_1 + \alpha_2) \qquad a_2 = \alpha_1\alpha_2$$

et pour un polynôme du troisième degré $X^3 + a_2X^2 + a_1X + a_0$ de racines $\alpha_1, \alpha_2, \alpha_3$, on a :

$$a_2 = -(\alpha_1 + \alpha_2 + \alpha_3) \qquad a_1 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 \qquad a_0 = -\alpha_1\alpha_2\alpha_3.$$

Lorsque $A = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$, cela donne :

$$-a_3 = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 \qquad a_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4$$

$$-a_1 = \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4 \qquad a_0 = \alpha_1\alpha_2\alpha_3\alpha_4$$

Remarque. Lorsque le polynôme n'est pas unitaire, on se ramène à ce cas en divisant par le coefficient dominant.

Remarque. L'expression $\sigma_k(\alpha_1, \cdots, \alpha_n) = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \alpha_{i_1} \cdots \alpha_{i_k}$ est dite k-ème *fonction symétrique élémentaire* des racines $\alpha_1, ..., \alpha_n$.

A retenir : Toute quantité qui dépend de manière symétrique des racines $\alpha_1, \cdots, \alpha_n$ peut s'exprimer en fonction des coefficients du polynôme A.

Exemple des formules de Newton

Pour tout entier k, les sommes N_k des puissances k-ièmes des racines d'un polynôme s'expriment en fonction des polynômes symétriques élémentaires en les racines au moyen de formules appelées formules de Newton. Par exemple, pour le polynôme $\mathrm{X}^2 + a_1\mathrm{X} + a_0$, on a :

$$\mathrm{N}_2 = \alpha^2 + \beta^2 = a_1^2 - 2a_0, \quad \mathrm{N}_3 = \alpha^3 + \beta^3 = -a_1^3 + 3a_0a_1.$$

Pour le polynôme $\mathrm{X}^3 + a_2\mathrm{X}^2 + a_1\mathrm{X} + a_0$, on a de même :

$$\mathrm{N}_2 = \alpha^2 + \beta^2 + \gamma^2 = a_2^2 - 2a_1, \quad \mathrm{N}_3 = \alpha^3 + \beta^3 + \gamma^3 = -a_2^3 + 3a_1a_2 - 3a_0.$$

Le dernier résultat s'obtient par exemple en écrivant :

$$\alpha^3 + \beta^3 + \gamma^3 = (\alpha + \beta + \gamma)^3 - 3(\alpha^2\beta + \beta^2\alpha + \alpha^2\gamma + \gamma^2\alpha + \beta^2\gamma + \gamma^2\beta) - 6\alpha\beta\gamma$$

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

Exercice 3.6 On note α_1, α_2, α_3 les trois racines complexes du polynôme $\mathrm{A} = \mathrm{X}^3 - \mathrm{X} + 1$. Calculer $\alpha_1^7 + \alpha_2^7 + \alpha_3^7$.

<u>Correction :</u> Les relations entre coefficients et racines s'écrivent (avec les notations précédentes) $\sigma_1 = -0 = 0$, $\sigma_2 = -1$ et $\sigma_3 = -1$. On effectue la division euclidienne de X^7 par A :

$$\mathrm{X}^7 = \mathrm{A}.(\mathrm{X}^4 + \mathrm{X}^2 - \mathrm{X} + 1) - 2\mathrm{X}^2 + 2\mathrm{X} - 1$$

Si α_i est une racine de A on a donc $\alpha_i^7 = -2\alpha_i^2 + 2\alpha_i - 1$ (puisque $\mathrm{A}(\alpha_i) = 0$).

$$\text{On en déduit } \alpha_1^7 + \alpha_2^7 + \alpha_3^7 \begin{aligned}[t] &= -2(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) + 2(\alpha_1 + \alpha_2 + \alpha_3) - 3 \\ &= -2(\sigma_1^2 - 2\sigma_2) + 2\sigma_1 - 3 \\ &= -2(0^2 - 2 \times 1) + 2 \times 0 - 3 = -7 \end{aligned}$$