

# Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.

Vincent LE GRUIEC  
Encadré par Matthieu ROMAGNY

23 mars 2023

## Table des matières

<b>1 Racines d'un polynôme</b>	<b>2</b>	<b>3 Polynômes symétriques</b>	<b>10</b>
1.1 Polynôme et fonction polynomiale . . .	2	3.1 Définitions . . . . .	10
1.2 Racine d'un polynôme . . . . .	2	3.2 Relations coefficients-racines . . . . .	10
1.3 Dérivation et lien avec les racines . . .	3	3.3 Structure des polynômes symétriques	11
1.4 Applications . . . . .	3	3.3.1 Un algorithme . . . . .	11
1.4.1 Interpolation polynomiale . . .	3	<b>4 Localisation des racines</b>	<b>12</b>
1.4.2 Interpolation de Lagrange . . .	4	4.1 Méthode de Newton . . . . .	13
1.4.3 Prolongement des identités . . .	5	4.1.1 La méthode . . . . .	13
<b>2 Racines de polynômes et extensions de corps</b>	<b>6</b>	4.1.2 Critère de convergence de la méthode . . . . .	14
2.1 Extensions de corps . . . . .	6	4.2 Les disques de Gerschgorin . . . . .	14
2.1.1 Définitions . . . . .	6	4.3 Théorème de Gauss-Lucas . . . . .	15
2.1.2 Sous-corps engendré par un ensemble fini . . . . .	7	4.4 Théorème de Kronecker . . . . .	15
2.1.3 Élément algébrique ou transcendant . . . . .	7	4.5 Théorème de Rouché . . . . .	16
2.2 Corps de rupture et corps de décomposition d'un polynôme . . . . .	8	<b>5 Racines et réduction des endomorphismes</b>	<b>18</b>
2.2.1 Corps de rupture . . . . .	8	5.1 Des polynômes pour l'étude des endomorphismes . . . . .	18
2.2.2 Corps de décomposition d'un polynôme quelconque . . . . .	8	5.1.1 Premiers critères de réduction	18
2.2.3 Lien avec les corps finis . . . . .	9	5.1.2 Critère de réduction par polynôme annulateur . . . . .	19
2.3 Clôture algébrique . . . . .	9	5.2 Des endomorphismes pour l'étude des polynômes . . . . .	19

## Introduction

Les polynômes sont des objets omniprésents dans le paysage mathématique. Le cœur de l'étude des polynômes réside dans la recherche de leurs racines. En effet une multitude de problèmes se ramènent à résoudre des équations polynomiales comme par exemple des problèmes d'optimisation en analyse ou la recherche de valeurs propres en algèbre. Cependant les apparences sont trompeuses, derrière leur apparence simple, les polynômes cachent bien leurs racines. On dispose de formules pour exprimer les racines d'un polynôme jusqu'au degré 4, hélas au-delà de ce degré il n'en n'existe pas (théorie de Galois). Ainsi, la plupart du temps on essaie de localiser les racines pour les approcher. Ce document développe une panoplie de thèmes pour la leçon 144 de l'agrégation de mathématiques. Mes choix ont conduit à diviser la leçon en cinq grandes parties comme on peut le voir dans la table des matières ci-dessus. La première partie présente les résultats de base sur les racines de polynômes et la factorisation. Cette partie, bien qu'elle puisse constituer le cœur de la leçon, est volontairement brève afin de laisser place à des résultats plus originaux dans la suite. La seconde partie développe des notions de la théorie des corps où les polynômes jouent un rôle central. La troisième partie rappelle les résultats classiques sur les polynômes symétriques ainsi que leur lien avec les racines de polynômes. La quatrième partie constitue une liste non exhaustive de résultats sur la localisation de racines. Enfin la dernière partie rappelle l'étroit lien entre réduction des endomorphismes et racines des polynômes. Il est classique de chercher les racines d'un polynôme pour réduire un endomorphisme, mais on propose une partie plus originale où l'on voit le sens réciproque, à savoir comment l'étude des endomorphismes peut permettre d'étudier les racines des polynômes.

Dans tout ce mémoire,  $\mathbb{K}$  désignera un corps commutatif et  $A$  un anneau commutatif.

## 1 Racines d'un polynôme

### 1.1 Polynôme et fonction polynomiale

On commence par rappeler la propriété universelle des anneaux de polynômes.

**Proposition 1 :** Soit  $u : A \rightarrow B$  un morphisme d'anneaux commutatifs, et soit  $b \in B$ . Alors il existe un unique morphisme d'anneaux  $\Psi_{u,b} : A[X] \rightarrow B$  vérifiant :

$$\Psi_{u,b}(a) = u(a) \quad \text{pour tout } a \in A \quad \text{et} \quad \Psi_{u,b}(X) = b .$$

Il est donc défini par

$$\Psi_{u,b} \left( \sum_{n \geq 0} a_n X^n \right) = \sum_{n \geq 0} u(a_n) b^n .$$

**Exemple 2 :** Un cas particulier est le suivant. On considère  $A$  un sous-anneau d'un anneau  $B$ , et soit  $b \in B$ . Si on applique la proposition 1 à l'inclusion naturelle  $u : A \hookrightarrow B$ , on obtient un morphisme d'anneaux, appelé *évaluation en  $b$* . Dans ce cas l'image de  $P \in A[X]$  est notée  $P(b)$ .

Plus explicitement, si  $P = \sum_{n \geq 0} a_n X^n$  et  $b \in B$ , on a

$$P(b) = \sum_{n \geq 0} a_n b^n$$

Ainsi, si  $P \in A[X]$ , on peut en particulier définir une *fonction polynomiale*

$$\tilde{P} : \begin{cases} A \longrightarrow A \\ a \longmapsto P(a) \end{cases}$$

Mais cette fonction ne caractérise pas nécessairement le polynôme  $P$ . Plus précisément, l'application

$$\begin{cases} A[X] \longrightarrow \mathcal{F}(A, A) \\ P \longmapsto \tilde{P} \end{cases}$$

n'est pas nécessairement injective. Par exemple si  $A = \mathbb{F}_2$ , la fonction polynomiale associée au polynôme  $P = X^2 - X$  est identiquement nulle. Ce n'est pas un cas isolé, on voit que si  $A = \mathbb{F}_{p^n}$  est le corps à  $p^n$  éléments, alors la fonction polynomiale associée au polynôme  $X^{p^n} - X$  est la fonction nulle. On verra que cette pathologie n'arrive pas dans le cadre d'un corps  $\mathbb{K}$  infini.

### 1.2 Racine d'un polynôme

Pour plus de commodité on va se placer dans le cadre des polynômes sur un corps  $\mathbb{K}$ , cependant il est à noter que la majeure partie des résultats qui suivent reste vrais sur un anneau commutatif intègre.

**Définition 3 :** Soit  $P \in \mathbb{K}[X]$ . On dit que  $a \in \mathbb{K}$  est une *racine* (ou un zéro) de  $P$  si  $P(a) = 0$ .

**Proposition 4 :** Soit  $P \in \mathbb{K}[X]$  un polynôme, ainsi que  $a \in \mathbb{K}$ . Alors  $a$  est racine de  $P$  si et seulement si  $X - a$  divise  $P$ .

*Démonstration.* On peut effectuer la division euclidienne de  $P$  par le polynôme  $X - a$ , ce qui nous donne  $Q \in \mathbb{K}[X]$  et  $R$  un polynôme constant tel que  $P = (X - a)Q + R$ . On obtient alors facilement que  $a$  est racine si et seulement si  $R = 0$ , c'est à dire  $X - a$  divise  $P$ .  $\square$

**Définition 5 :** Soit  $P \in \mathbb{K}[X]$ . On dit que  $a \in \mathbb{K}$  est une racine d'ordre (ou multiplicité)  $m$  de  $P$  si  $(X - a)^m$  divise  $P$  mais  $(X - a)^{m+1}$  ne divise pas  $P$ .

**Théorème 6 :** Soit  $P \in \mathbb{K}[X]$  et  $a_1, \dots, a_r \in \mathbb{K}$  des racines distinctes de  $P$  d'ordres respectif  $m_1, \dots, m_r$ . Alors il existe  $Q \in \mathbb{K}[X]$  tel que

$$P(X) = (X - a_1)^{m_1} \dots (X - a_r)^{m_r} Q(x) \quad \text{et} \quad \forall i \in \llbracket 1, r \rrbracket, Q(a_i) \neq 0$$

**Corollaire 7 :** Si  $P \in \mathbb{K}[X]$  est un polynôme non nul, alors  $P$  a au plus  $n$  racines (comptées avec leur multiplicité). En particulier un polynôme possédant un nombre de racines supérieur à son degré est nul.

**Remarque 8 :** Le résultat est faux sur un anneau quelconque. Par exemple sur l'anneau  $\mathbb{Z}/8\mathbb{Z}$  on peut considérer le polynôme  $P = \overline{4}X$  possède 3 racines, à savoir  $\overline{0}$ ,  $\overline{2}$  et  $\overline{4}$ . Pour autant  $P$  est de degré 1. On peut en fait montrer qu'un anneau commutatif  $A$  est intègre si et seulement si tout polynôme non nul  $P \in A[X]$  possède au plus  $\deg(P)$  racines dans  $A$ .

**Corollaire 9 :** Si le corps  $\mathbb{K}$  est infini, le morphisme de  $\mathbb{K}$ -algèbres

$$\begin{cases} \mathbb{K}[X] \longrightarrow \mathcal{F}(\mathbb{K}, \mathbb{K}) \\ P \longmapsto \tilde{P} \end{cases}$$

introduit au paragraphe 1.1 est injectif.

*Démonstration.* Il s'agit de montrer que le noyau est trivial. Soit  $P$  tel que  $\tilde{P}$  est identiquement nul sur  $\mathbb{K}$ . Alors, puisque  $\mathbb{K}$  est infini,  $P$  possède une infinité de racines et donc le corollaire 7 nous montre que  $P$  est nul.  $\square$

Ainsi, pour  $\mathbb{K}$  infini, on peut identifier polynôme et fonction polynomiale.

**Définition 10 :** Un polynôme  $P \in \mathbb{K}[X]$  est dit *scindé* sur  $\mathbb{K}$  si on peut l'écrire comme un produit de polynômes de degré 1 :

$$P = \lambda \prod_{i=1}^r (X - a_i)^{m_i} \quad \text{avec } \lambda \in \mathbb{K}, a_i \in \mathbb{K} \text{ et } m_i \in \mathbb{N}^* \quad \forall i \in \llbracket 1, r \rrbracket$$

**Définition 11 :** On dit que  $\mathbb{K}$  est *algébriquement clos* si tout polynôme est scindé dans  $\mathbb{K}[X]$ .

**Exemple 12 :** Le corps de réels n'est pas algébriquement clos tandis que celui des complexes l'est.

### 1.3 Dérivation et lien avec les racines

**Définition 13 :** Soit  $P = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \in \mathbb{K}[X]$ . On appelle polynôme dérivé de  $P$  le polynôme  $P' = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \dots + a_1$ .

**Remarque 14 :** Si  $P$  est constant on a évidemment  $P' = 0$ . La réciproque est fautive en caractéristique différente de 0, on peut par exemple considérer  $X^p$  en caractéristique  $p$ . On définit le polynôme dérivé  $n$ -ième, et on le note  $P^{(n)}$ , par  $P = P^{(0)}$  et  $P^{(n+1)} = (P^{(n)})'$ .

**Théorème 15 :** (*Formule de Taylor*) Soit  $P \in \mathbb{K}[X]$  de degré inférieur ou égal à  $n$ . Si le corps  $\mathbb{K}$  est de caractéristique nulle ou strictement supérieure à  $n$  alors  $P$  vérifie

$$\forall a \in \mathbb{K}, \quad P(X) = P(a) + \frac{P'(a)}{1!} (X - a) + \frac{P^{(2)}(a)}{2!} (X - a)^2 + \dots + \frac{P^{(n)}(a)}{n!} (X - a)^n$$

**Corollaire 16 :** Si le corps  $\mathbb{K}$  est de caractéristique nulle et si  $P \in \mathbb{K}[X]$  est non nul, alors  $a \in \mathbb{K}$  est racine d'ordre  $m$  de  $P$  si et seulement si

1.  $P^{(i)}(a) = 0$  pour tout  $i \in \llbracket 0, m-1 \rrbracket$
2.  $P^{(m)}(a) \neq 0$ .

**Remarque 17 :** Le résultat est faux en caractéristique non nulle, par exemple on peut considérer  $X^p$  encore une fois en caractéristique  $p$ . Cependant le résultat reste vrai pour caractériser les racines simples dans un corps quelconque.

## 1.4 Applications

### 1.4.1 Interpolation polynomiale

On suppose ici  $\mathbb{K}$  infini

Un problème classique est le suivant : On dispose d'une application  $f : \mathbb{K} \rightarrow \mathbb{K}$  et on souhaite l'approcher par un polynôme  $P \in \mathbb{K}[X]$  dans le sens où si l'on se donne  $x_0, \dots, x_n \in \mathbb{K}$ ,  $n+1$  points deux à deux distincts,  $P$  vérifie  $P(x_i) = f(x_i)$  pour tout  $i \in \llbracket 0, n \rrbracket$ .

On peut bien sûr reformuler le problème de la manière suivante : étant donnés  $x_0, \dots, x_n$  des points de  $\mathbb{K}$  distincts deux à deux et  $y_0, \dots, y_n$  des points de  $\mathbb{K}$ , on souhaite trouver un polynôme  $P \in \mathbb{K}[X]$  qui vérifie  $P(x_i) = y_i$  pour tout  $i \in \llbracket 0, n \rrbracket$ . Un tel polynôme est appelé polynôme interpolateur des données  $(x_i, y_i)_{i=0, \dots, n}$ . On va voir qu'un tel polynôme existe toujours et que de plus il en existe un unique de degré inférieur ou égal à  $n$ . Remarquons que les  $y_i$  n'ont pas besoin d'être distincts deux à deux. On peut par exemple les supposer tous égaux à 0, ce qui revient à chercher un polynôme dont les  $x_i$  sont les racines.

**Théorème 18 :** Soit  $n \geq 1$  et  $x_0, \dots, x_n \in \mathbb{K}$  deux à deux distincts. Alors le noyau de l'application linéaire

$$\begin{cases} \mathbb{K}_n[X] \longrightarrow \mathbb{K}^{n+1} \\ P \longmapsto (P(x_0), \dots, P(x_n)) \end{cases}$$

est trivial. En d'autres termes il s'agit d'une application linéaire injective entre deux espaces de même dimension, donc bijective. En particulier il existe un unique polynôme interpolant les  $(x_i, y_i)_{i=0, \dots, n}$  de degré inférieur ou égal à  $n$ .

*Démonstration.* C'est une conséquence immédiate du corollaire 7. Un polynôme non nul de degré au plus  $n$  ne peut avoir  $n + 1$  racines.  $\square$

On peut donc s'intéresser à trouver un tel polynôme. Une méthode naïve serait de poser

$$P = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$$

et de construire un système linéaire de  $n + 1$  équations à  $n + 1$  inconnues donné par les conditions  $P(x_i) = y_i$ . Matriciellement on obtient le système suivant :

$$\underbrace{\begin{pmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{pmatrix}}_{\mathbf{V}(x_0, \dots, x_n)} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{pmatrix}$$

On reconnaît une matrice de Vandermonde, dont on sait qu'elle est inversible du fait que les  $x_i$  soient distincts deux à deux, ainsi, algébriquement, on est sûr de trouver la solution de ce système, cependant inverser ce système à la main peut nous mettre bien à mal dès que  $n$  est sensiblement grand. Bien sur dans les faits on résout un tel système sûr machine à l'aide de notre logiciel de calcul numérique préféré, cependant ce problème est numériquement mal posé puisque si par exemple on veut interpoler une fonction sur l'intervalle  $[-\pi/8, \pi/8]$  selon une subdivision uniforme de 9 points, le déterminant de Vandermonde vaut  $2.6053 \times 10^{-21}$ . Plus on diminue le pas de la subdivision, plus la matrice associée au système se rapproche d'une matrice singulière ( $\det = 0$ ).

### 1.4.2 Interpolation de Lagrange

La méthode précédente consiste à résoudre un système pour trouver les coordonnées d'un polynôme interpolateur dans la base canonique. La méthode de Lagrange consiste à trouver une autre base de  $\mathbb{K}_n[X]$  dans laquelle les coordonnées seront simples] à exprimer.

Soit  $n$  un entier naturel puis  $x_0, x_1, \dots, x_n, (n + 1)$  points de  $\mathbb{K}$  deux à deux distincts. On cherche  $(n + 1)$  polynômes  $L_0, \dots, L_n$ , tous de degré au plus  $n$ , vérifiant les égalités :

$$\forall (i, j) \in \llbracket 0, n \rrbracket^2, L_i(x_j) = \delta_{i,j} = \begin{cases} 0 & \text{si } i \neq j \\ 1 & \text{si } i = j \end{cases}$$

Soit  $i$  un entier naturel élément de  $\llbracket 0, n \rrbracket$  donné. Le polynôme  $L_i$  est de degré au plus  $n$  et admet les  $n$  points deux à deux distincts  $x_j, j \neq i$ , pour racines. Par le théorème 6, il existe une constante  $C$  telle que

$$L_i = C \prod_{j \neq i} (X - x_j)$$

L'égalité  $L_i(x_i) = 1$  fournit alors  $C = \frac{1}{\prod_{j \neq i} (x_i - x_j)}$  et donc nécessairement

$$L_i = \prod_{j \neq i} \left( \frac{X - x_j}{x_i - x_j} \right)$$

Réciproquement, la famille trouvée convient.

**Proposition 19 :** Soient  $n$  un entier naturel puis  $x_0, x_1, \dots, x_n, (n+1)$  points de  $\mathbb{K}$  deux à deux distincts donnés. Il existe une et une seule famille, notée  $(L_i)_{0 \leq i \leq n}$ , de  $(n+1)$  polynômes de degré au plus  $n$  vérifiant :

$$\forall (i, j) \in \llbracket 0, n \rrbracket^2, L_i(x_j) = \delta_{i,j}$$

De plus :

$$\forall i \in \llbracket 0, n \rrbracket, L_i = \prod_{j \neq i} \left( \frac{X - x_j}{x_i - x_j} \right)$$

**Proposition 20 :** La famille  $(L_k)_{0 \leq k \leq n}$  est une base de  $\mathbb{K}_n[X]$ .

*Démonstration.* Les  $L_k$  sont tous dans  $\mathbb{K}_n[X]$ . Montrons que la famille  $(L_k)_{0 \leq k \leq n}$  est une famille libre de  $\mathbb{K}_n[X]$ . Soit  $(\lambda_0, \dots, \lambda_n) \in \mathbb{K}^{n+1}$

$$\sum_{i=0}^n \lambda_i L_i = 0 \Rightarrow \forall j \in \llbracket 0, n \rrbracket, \sum_{i=0}^n \lambda_i L_i(x_j) = 0 \Rightarrow \forall j \in \llbracket 0, n \rrbracket, \sum_{i=0}^n \lambda_i \delta_{i,j} = 0 \Rightarrow \forall j \in \llbracket 0, n \rrbracket, \lambda_j = 0.$$

Donc la famille  $(L_k)_{0 \leq k \leq n}$  est une famille libre dans l'espace de dimension  $n+1$ , c'est une base.  $\square$

**Théorème 21 :** Soient  $n$  un entier naturel,  $x_0, \dots, x_n$ , des points de  $\mathbb{K}$  deux à deux distincts et  $y_0, \dots, y_n$ , des points de  $\mathbb{K}$ . Il existe un et un seul polynôme  $P$  de degré au plus  $n$  vérifiant  $\forall j \in \llbracket 0, n \rrbracket, P(x_j) = y_j$  à savoir

$$P = \sum_{i=0}^n y_i L_i = \sum_{i=0}^n y_i \prod_{j \neq i} \left( \frac{X - x_j}{x_i - x_j} \right)$$

*Démonstration.* Soit  $P \in \mathbb{K}_n[X]$ . Notons  $(\lambda_0, \dots, \lambda_n)$  les coordonnées de  $P$  dans la base  $(L_i)_{0 \leq i \leq n}$  de  $\mathbb{K}_n[X]$ . On a donc  $P = \sum_{i=0}^n \lambda_i L_i$ . Maintenant, pour  $j$  élément de  $\llbracket 0, n \rrbracket$ ,

$$P(x_j) = \sum_{i=0}^n \lambda_i L_i(x_j) = \sum_{i=0}^n \lambda_i \delta_{i,j} = \lambda_j$$

Ainsi,

$$\forall j \in \llbracket 0, n \rrbracket, P(x_j) = y_j \Leftrightarrow \forall j \in \llbracket 0, n \rrbracket, \lambda_j = y_j.$$

$\square$

### 1.4.3 Prolongement des identités

L'idée est la suivante : prolonger certaines identités que l'on sait vraies sur un corps à un anneau quelconque. On va illustrer ce principe à travers un exemple type. Beaucoup de théorie se développe au-dessus de la notion de corps, par exemple le déterminant d'une matrice à coefficient dans un corps. On arrive facilement à étendre la notion de déterminant pour une matrice à coefficients dans un anneau quelconque, cependant il n'est pas clair que les propriétés usuelles soient conservées puisqu'elles reposent sur la notion de dimension d'un espace vectoriel sur un corps. On va pourtant voir qu'on peut les prolonger à l'aide de polynômes.

**Lemme 22 :** Soit  $\mathbb{K}$  un corps infini. Soit  $P \in \mathbb{K}[X_1, \dots, X_n]$ , alors

$$P = 0 \Leftrightarrow \tilde{P} = 0$$

*Démonstration.* la condition est clairement nécessaire et on procède par récurrence sur  $n$  pour la réciproque. Dans le cas  $n = 1$ , cela découle du corollaire 7. Pour  $n > 1$ , si on écrit  $P = \sum_{i=0}^d Q_i X_n^i$  avec  $Q_i$  élément de  $\mathbb{K}[X_1, \dots, X_{n-1}]$ , la condition devient

$$\forall a_1, \dots, a_{n-1} \in \mathbb{K}, \quad \forall a_n \in \mathbb{K}, \quad \sum_{i=0}^d F_i(a_1, \dots, a_{n-1}) a_n^i = 0.$$

Du cas  $n = 1$ , on en déduit que

$$\forall a_1, \dots, a_{n-1} \in \mathbb{K}, \quad Q_i(a_1, \dots, a_{n-1}) = 0$$

et on conclut par récurrence.  $\square$

Soit  $A$  un anneau commutatif unitaire. On va montrer que

$$\forall U, V \in M_n(A), \quad \det U \det V = \det UV.$$

Soient  $U = (u_{ij})_{i,j}, V = (v_{ij})_{i,j} \in M_n(A)$ . Considérons l'anneau  $B$  des polynômes à coefficients dans  $\mathbb{Z}$  et à  $2n^2$  indéterminées

$$B = \mathbb{Z}[X_{11}, \dots, X_{nn}, Y_{11}, \dots, Y_{nn}]$$

et considérons les matrices  $\tilde{U}, \tilde{V} \in M_n(B)$

$$\tilde{U} = \begin{pmatrix} X_{11} & \dots & X_{1n} \\ \vdots & \ddots & \vdots \\ X_{n1} & \dots & X_{nn} \end{pmatrix} \quad \text{et} \quad \tilde{V} = \begin{pmatrix} Y_{11} & \dots & Y_{1n} \\ \vdots & \ddots & \vdots \\ Y_{n1} & \dots & Y_{nn} \end{pmatrix}.$$

Il existe un unique morphisme d'anneaux  $\varphi : \mathbb{Z} \rightarrow A$  (donné par  $n \mapsto n1_A$ ). D'après la proposition 1, il existe un unique morphisme  $\Psi : B \rightarrow A$  vérifiant  $\Psi(n) = n1_A$  (c'est-à-dire  $\Psi \circ i = \varphi$ ),  $\Psi(X_{ij}) = u_{ij}$  et  $\Psi(Y_{ij}) = v_{ij}$ . On dispose donc du diagramme commutatif suivant :

$$\begin{array}{ccccc} \mathbb{Z} & \xrightarrow{i} & B & & \\ & \searrow \varphi & \downarrow \Psi & & \\ & & A & & \end{array} \quad \begin{array}{ccc} n & & X_{ij} \\ \downarrow & & \downarrow \\ n1_A & & u_{ij} \end{array} \quad \begin{array}{ccc} Y_{ij} \\ \downarrow \\ v_{ij} \end{array}$$

Comme  $\det$  est une application polynomiale de  $M_n(A)$  dans  $A$ , on a

$$\Psi(\det \tilde{U} \det \tilde{V} - \det(\tilde{U}\tilde{V})) = \det U \det V - \det(UV).$$

Il suffit donc de montrer que le polynôme  $\det \tilde{U} \det \tilde{V} - \det(\tilde{U}\tilde{V})$  à  $2n^2$  indéterminées et à coefficients dans  $\mathbb{Z}$  est nul. Comme  $\mathbb{Z} \subset \mathbb{C}$ , le polynôme

$$P = \det \tilde{U} \det \tilde{V} - \det(\tilde{U}\tilde{V}) \in B \subset \mathbb{C}[X_{11}, \dots, X_{nn}, Y_{11}, \dots, Y_{nn}]$$

définit une application polynomiale

$$\tilde{P} : \begin{cases} \mathbb{C}^{2n^2} \longrightarrow \mathbb{C} \\ (z_{11}, \dots, z_{nn}, z'_{11}, \dots, z'_{nn}) \longmapsto P(z_{11}, \dots, z_{nn}, z'_{11}, \dots, z'_{nn}). \end{cases}$$

Cette application polynomiale  $\tilde{P}$  est nulle puisque

$$\tilde{P}(z_{11}, \dots, z_{nn}, z'_{11}, \dots, z'_{nn}) = \det Z \det Z' - \det(ZZ')$$

où  $Z = (z_{ij})_{i,j}, Z' = (z'_{ij})_{i,j} \in M_n(\mathbb{C})$  et que  $\det Z \det Z' = \det(ZZ')$  (on s'est ramené à la situation connue du corps  $\mathbb{C}$ ). Comme  $\mathbb{C}$  est infini et intègre et comme l'application polynomiale  $\tilde{P}$  est nulle, on en déduit que  $P = 0$  par le lemme 22. Remarquons que l'on peut remplacer le corps  $\mathbb{C}$  par n'importe quel corps infini.

On a donné ici un exemple de prolongement à travers un exemple type, mais la méthode reste très générale et permet d'étendre de nombreuses autres relations matricielles.

## 2 Racines de polynômes et extensions de corps

### 2.1 Extensions de corps

#### 2.1.1 Définitions

**Définition 23 :** Soit  $K$  un corps. Une extension de  $K$  est un corps  $L$  contenant  $K$  comme sous-corps. On le note  $L/K$ . De manière équivalente c'est la donnée un couple  $(L, i : L \hookrightarrow L)$  où  $L$  est un corps et  $i$  un morphisme de corps nécessairement injectif.

On vérifie aisément que  $L$ , muni de son produit et de la loi externe

$$\left| \begin{array}{l} K \times L \longrightarrow L \\ (\lambda, x) \longmapsto \lambda x \end{array} \right.$$

est une  $K$ -algèbre associative unitaire

**Définition 24 :** On appelle degré de  $L/K$  la dimension de  $L$  comme  $K$ -espace vectoriel. On le note  $[L : K]$ .

**Exemple 25 :** Le corps  $\mathbb{C}$  est une extension de degré 2 par rapport à  $\mathbb{R}$ .

**Proposition 26 :** Soient  $K \subset L \subset M$  des corps,  $(e_i)_{i \in I}$  une base de  $L$  sur  $K$ ,  $(f_j)_{j \in J}$  une base de  $M$  sur  $L$ . Alors la famille  $(e_i f_j)_{(i,j) \in I \times J}$  est une base de  $M$  sur  $K$ .

**Corollaire 27 :** Dans la situation de 1.4, si les degrés sont finis, on a  $[M : K] = [M : L][L : K]$ .

### 2.1.2 Sous-corps engendré par un ensemble fini

**Définition 28 :** Si  $L$  est une extension de  $K$  ou une  $K$ -algèbre, et si  $x \in L$  on note  $K[x]$  le plus petit sous-anneau de  $L$  contenant  $K$  et  $x$ .

On peut décrire  $K[x]$  comme l'image du morphisme d'évaluation en  $x$

$$\Phi_x : \begin{cases} K[X] & \rightarrow L \\ P & \mapsto P(x) \end{cases}$$

Plus généralement, on note  $K[x_1, \dots, x_n]$  le plus petit sous-anneau de  $L$  contenant  $K$  et  $x_1, \dots, x_n$ .

**Définition 29 :** Si  $L$  est une extension de  $K$ , on note  $K(x)$  le plus petit sous-corps de  $L$  contenant  $K$  et  $x$ .

On peut le caractériser de la manière suivante :

$$K(x) = \left\{ \frac{P(x)}{Q(x)} \mid P, Q \in K[X], Q(x) \neq 0 \right\}$$

Plus généralement, on note  $K(x_1, \dots, x_n)$  le plus petit sous-corps de  $L$  contenant  $K$  et  $x_1, \dots, x_n$ .

**Remarque 30 :** Remarquons qu'en général  $K[x]$  n'est pas isomorphe à l'anneau de polynômes  $K[X]$ . La différence vient du fait que l'on peut avoir  $Q(x) = 0$  sans pour autant que  $Q$  soit le polynôme nul. Par exemple  $x = \sqrt{2}$  et  $P = X^2 - 2$  sur  $K = \mathbb{Q}$ . De même,  $K(x)$  n'est en général pas isomorphe à  $K(X)$ . Cette remarque fait l'objet d'étude de la section suivante.

**Lemme 31 :** Soit  $K$  un corps. Une  $K$ -algèbre intègre, de dimension finie sur  $K$ , est toujours un corps.

*Démonstration.* Soit  $A$  une  $K$ -algèbre. Soit  $x \in A \setminus \{0\}$  et  $\mu_x : A \rightarrow A$  la multiplication par  $x$ . C'est une application  $K$ -linéaire, injective (car  $A$  intègre). Comme  $A$  est un  $K$ -espace vectoriel de dimension finie, elle est automatiquement surjective, donc  $1 \in \text{Im}(\mu_x)$  donc  $x$  est inversible.  $\square$

**Corollaire 32 :** Soit  $K \subset L$  une extension finie de corps. Si  $L' \subset L$  est un sous-anneau contenant  $K$ , c'est un sous-corps. En particulier, pour tout  $x \in L$ ,  $K(x) = K[x]$ , et plus généralement, pour tout  $x_1, \dots, x_n \in L$ ,  $K(x_1, \dots, x_n) = K[x_1, \dots, x_n]$ .

*Démonstration.* Un sous-anneau d'un corps est toujours intègre. Comme  $L' \subset L$  et  $\dim_K(L) < \infty$ , on a aussi  $\dim_K(L') < \infty$ . Finalement  $L'$  est donc un corps par le lemme 31.  $\square$

### 2.1.3 Élément algébrique ou transcendant

Soit  $L$  une extension de  $K$ . Si  $P = \sum a_i X^i \in K[X]$  est un polynôme à coefficients dans  $K$ , on peut l'évaluer en un point  $x \in L$ . On a ainsi le morphisme d'évaluation en  $x$

$$\Phi_x : \begin{cases} K[X] & \rightarrow K[x] \\ P & \mapsto P(x) \end{cases}.$$

**Définition 33 :** Si le morphisme d'évaluation  $\Phi_x$  est injectif on dit que  $x$  est transcendant sur  $K$ . Sinon, on dit que  $x$  est algébrique sur  $K$ .

De manière équivalente  $x$  est algébrique sur  $K$  s'il possède un polynôme annulateur non nul à coefficients dans  $K$  et transcendant sinon.

**Remarque 34 :**

1. La notion dépend fortement de  $K$ . Par exemple,  $\pi$  est transcendant sur  $\mathbb{Q}$ , mais sur  $K = \mathbb{R}$ , il est algébrique : il est racine du polynôme  $X - \pi$ . Tout élément de  $K$  est algébrique sur  $K$ .
2. Si  $x$  est transcendant, alors  $K[x]$  est isomorphe à l'anneau des polynômes et  $K(x)$  est isomorphe au corps des fractions rationnelles

**Lemme 35 :** Si  $L$  est une extension finie de  $K$ , tout élément  $x \in L$  est algébrique sur  $K$ .

*Démonstration.* Puisque  $K[X]$  est de dimension infinie comme  $K$ -espace vectoriel,  $K[X]$  ne peut pas s'injecter dans  $L$  si  $\dim_K L < \infty$ . Par exemple si  $d = [L : K]$  alors la famille  $(1, x, \dots, x^d)$  est liée et induit un polynôme annulateur de degré au plus  $d$ .  $\square$

**Définition 36 :** Si  $x \in L$  est algébrique sur  $K$ , considérons l'idéal  $\ker \Phi_x = \{f \in K[X] \mid f(x) = 0\}$ . Comme  $K[X]$  est principal, il existe un unique polynôme irréductible unitaire  $M_x \in K[X]$  tel que  $\ker \Phi_x = \langle M_x \rangle$ . On l'appelle polynôme minimal de  $x$  sur  $K$ .

**Proposition 37 :** Soit  $L/K$  un extension. Alors  $x \in L$  est algébrique sur  $K$  si et seulement si  $K(x)/K$  est une extension finie. Dans ce cas  $(1, x, \dots, x^{d-1})$  est une  $K$ -base de  $K(x)$  où  $d = \deg M_x$ . En particulier  $K(x) = K[x]$  et  $[K(x) : K] = \deg M_x$ .

*Démonstration.* On a déjà remarqué dans le lemme 35 que si  $K(x)/K$  est de degré fini alors  $x \in K(x)$  est algébrique. Réciproquement, si  $x$  est algébrique, alors le premier théorème d'isomorphisme permet de factoriser le morphisme d'évaluation  $K[X]/\langle M_x \rangle \xrightarrow{\sim} K[x]$ . On sait par le lemme 31 que  $K[x]$  est un corps et on montre de manière classique, par une division euclidienne, que  $(1, x, \dots, x^{d-1})$  est une  $K$ -base de  $K[x]$ . On a donc que  $K[x]$  est un sous-corps de  $L$  contenant  $K$  et  $x$ , donc par définition de  $K(x)$ ,  $K(x) \subset K[x]$  et l'inclusion réciproque étant toujours respectée on a l'égalité voulue.  $\square$

**Définition 38 :** Soit  $L/K$  une extension et  $x \in L$  un élément algébrique sur  $K$ . Le degré de  $x$  sur  $K$  est le degré de l'extension  $K(x)/K$ , c'est donc aussi le degré de  $M_x$ .

**Proposition 39 :** Soit  $L$  une extension finie de  $K$  de degré  $d = [L : K]$ . Pour tout élément  $x \in L$ , le degré de  $x$  divise  $d$ .

*Démonstration.* Il suffit d'écrire  $[L : K] = [L : K[x]] \times [K[x] : K]$  par le corollaire 27.  $\square$

## 2.2 Corps de rupture et corps de décomposition d'un polynôme

### 2.2.1 Corps de rupture

**Lemme 40 :** Soit  $f \in K[X]$  un polynôme irréductible. Alors  $L = K[X]/\langle f \rangle$  est un corps. C'est une extension de  $K$  pour  $\pi|_K : K \hookrightarrow L$  la restriction à  $K$  de l'application quotient  $\pi$ .

*Démonstration.* C'est la même preuve que celle qui montre que  $\mathbb{Z}/p\mathbb{Z}$  est un corps, basée sur Bézout dans  $K[X]$ . Si  $\bar{g} \neq 0$ ,  $g \in K[X]$  n'est pas divisible par  $f$ . Comme  $f$  est irréductible,  $f \wedge g = 1$ , et il existe  $u, v \in K[X]$  tels que  $uf + gv = 1$ . Dans  $L$ , cette égalité donne  $\bar{g}\bar{v} = 1$ , donc  $\bar{g}$  est inversible.  $\square$

**Remarque 41 :** (*remarque fondamentale*) Notons  $x = \bar{X} \in L$  la classe de  $X$ . Par construction,  $x$  est une racine de  $f$  dans le corps  $L$ , et  $L = K[x]$ .

**Définition 42 :** Soit  $f \in K[X]$  un polynôme irréductible. Un corps de rupture pour  $f$  (sous-entendu relativement à  $K$ ) est une extension de  $K$  contenant une racine  $x$  de  $f$  et telle que  $L = K[x]$ .

La construction ci-dessus montre que  $K[X]/\langle f \rangle$  est un corps de rupture de  $f$  si  $f$  est irréductible. En fait, tout corps de rupture lui est isomorphe si on suppose  $f$  irréductible. L'unicité s'énonce de la façon suivante.

**Lemme 43 :** Soit  $L = K[x]$  un corps de rupture d'un polynôme  $f \in K[X]$  irréductible.

1. Etant donné  $(L', x')$  avec  $L'$  extension de  $K$ , et  $x' \in L'$  racine de  $f$ , il existe un unique morphisme  $\varphi : L \rightarrow L'$  envoyant  $x$  sur  $x'$  qui est l'identité sur  $K$ .
2. Si en plus  $L'$  est lui aussi un corps de rupture de  $f$ ,  $\varphi$  est un isomorphisme.

### 2.2.2 Corps de décomposition d'un polynôme quelconque

Ici, on prend un polynôme unitaire  $f \in K[X]$  qu'on ne suppose plus irréductible.

**Théorème 44 :** Soit  $K$  un corps et  $f \in K[X]$  un polynôme unitaire de degré  $d \geq 1$ . Il existe une extension finie  $L$  de  $K$  telle que  $f$  est scindé dans  $L[X]$  :

$$f = \prod_{i=1}^d (X - x_i)$$

avec  $x_i \in L$ . De plus  $[L : K] \leq d!$ .

*Démonstration.* On raisonne par récurrence sur  $d$ . Si  $d = 1$ , c'est trivial. Soit  $Q_1$  un facteur irréductible de  $f$ . Soit  $K \subset L_1 = K[\alpha]$  un corps de rupture associé à  $Q_1$ ,  $\alpha$  étant une racine de  $Q_1$ . On voit  $f(X)$  comme un polynôme dans  $L_1[X]$ ;  $f$  s'annule en  $\alpha \in L_1$  donc  $L_1[X]$ ,  $f$  s'écrit  $(X - \alpha)f_1$  avec  $f_1$  de degré  $\leq d - 1$ . Par hypothèse de récurrence, il existe une extension finie  $L$  de  $L_1$  telle que  $f_1$  est scindé dans  $L[X]$ , et  $[L : L_1] \leq (d - 1)!$ . En particulier,  $f = (X - \alpha)f_1$  est scindé dans  $L[X]$ . On a  $[L : K] = [L : L_1] \times [L_1 : K] \leq (d - 1)! \times d = d!$ .  $\square$

**Définition 45 :** Un corps de décomposition (ou extension de décomposition)  $L$  de  $f$  (relativement à  $K$ ), est une extension de  $K$  telle que  $f = \prod_{i=1}^d (X - x_i)$  est scindé dans  $L[X]$ , et  $L = K[x_1, \dots, x_d]$ .

Autrement dit, une extension de décomposition est une extension la plus petite possible dans laquelle  $f$  est scindé. Le théorème 44 montre l'existence d'un tel corps. Le lemme suivant assure également l'unicité de celui-ci dans le sens qu'il décrit.

**Lemme 46 :** Soit  $K \hookrightarrow L$  une extension de décomposition de  $f$ , et  $K \subset L'$  une autre extension.

1. Si  $f$  est scindé dans  $L'$ , il existe un morphisme  $L \hookrightarrow L'$  qui est l'identité sur  $K$
2. Si  $L'$  est aussi une extension de décomposition, un tel morphisme est un isomorphisme. En particulier, si  $K \subset L$  et  $K \subset L'$  sont 2 extensions de décomposition de  $f$ , elles sont isomorphes.

### 2.2.3 Lien avec les corps finis

**Théorème 47 :** Soit  $q \geq 2$  une puissance d'un nombre premier  $p$ . Alors il existe un corps fini à  $q$  éléments, unique à isomorphisme de  $\mathbb{F}_p$ -algèbres près. C'est le corps de décomposition du polynôme  $X^q - X \in \mathbb{F}_p[X]$ .

*Démonstration.* On montre tout d'abord que si  $K$  est un corps à  $q$  éléments alors c'est nécessairement le corps de décomposition de  $X^q - X$ . Si  $K$  est un corps à  $q$  éléments et si  $x \in K^*$ , on a  $x^{q-1} = 1$ , de sorte que tout élément de  $K$  est racine du polynôme  $X^q - X$  qui en possède au plus  $q$ . D'autre part le sous-corps premier de  $K$  est nécessairement  $\mathbb{F}_p$ , puisque le cardinal de  $K$  est une puissance de sa caractéristique. Comme  $X^q - X$  est à coefficients dans  $\mathbb{F}_p$ , on a bien  $K = \mathbb{F}_p[x_1, \dots, x_q]$  corps de décomposition de  $X^q - X$  où les  $x_i$  sont les racines. Réciproquement, soit  $K$  le corps de décomposition de  $X^q - X$  et soit  $k \subset K$  l'ensemble des racines de  $X^q - X$ . Alors,  $k$  est un corps, car si  $x, y$  sont dans  $k$ , on a  $x^q = x, y^q = y$ , donc aussi  $(xy)^q = xy$  et  $(x + y)^q = x + y$  car l'application  $x \mapsto x^q$  de  $K$  dans  $K$  n'est autre que l'automorphisme de Frobenius itéré  $n$  fois si on écrit  $q = p^n$ . De plus, si on pose  $P(X) = X^q - X$ , on a  $P'(X) = qX^{q-1} - 1 = -1$  car  $q$  est une puissance de la caractéristique. Il en résulte que les racines de  $P$  sont simples et donc on a  $|k| = q$  : on a obtenu un corps à  $q$  éléments. Enfin, il est clair que l'on a  $k = K$ .  $\square$

**Remarque 48 :** Ce résultat est purement théorique. Dans la pratique pour disposer d'un corps à  $p^n$  éléments on utilise le lemme 40. Par exemple pour construire  $\mathbb{F}_4$  le corps à  $2^2$  éléments on remarque facilement que  $P = X^2 + X + 1$  est irréductible sur  $\mathbb{F}_2$  et donc  $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/\langle P \rangle$ . Si on pose  $\alpha = \bar{X}$  alors  $\mathbb{F}_4 = \{0, 1, \alpha, 1 + \alpha\}$  et on peut explicitement calculer dans ce corps en ramenant les calculs dans la  $\mathbb{F}_2$ -base  $(1, \alpha)$  grâce à la relation  $\alpha^2 + \alpha + 1 = 0$ .

On peut d'ailleurs se poser la question de savoir si on peut toujours trouver un tel polynôme irréductible. Supposons que l'on veuille construire  $\mathbb{F}_{p^n}$ . On cherche un polynôme irréductible de degré  $n$  sur  $\mathbb{F}_p$ . On sait que  $\mathbb{F}_{p^n}^*$  est cyclique et on dispose donc d'un générateur  $\omega \in \mathbb{F}_{p^n}^*$  tel que  $\mathbb{F}_{p^n} = \{0, \omega, \dots, \omega^{p^n-1}\}$ . Le morphisme d'évaluation en  $\omega$ ,  $ev_\omega : \mathbb{F}_p[X] \rightarrow \mathbb{F}_{p^n}$  est alors bien défini car  $\mathbb{F}_{p^n}$  est de sous-corps premier  $\mathbb{F}_p$  est contient  $\omega$  et est surjectif par définition de  $\omega$ . Le polynôme minimal de  $\omega$  est alors un polynôme irréductible qui répond à la question  $\mathbb{F}_p[X]/\langle M_\omega \rangle \xrightarrow{\sim} \mathbb{F}_{p^n}$ . Remarquons que cela n'aide pas à trouver un tel polynôme car ni  $\omega$  ni  $M_\omega$  n'est facile à trouver en pratique, mais cela assure son existence.

## 2.3 Clôture algébrique

**Définition 49 :** Une extension  $K \subset L$  est algébrique si tout élément de  $L$  est algébrique sur  $K$ .

**Exemple 50 :** Une extension finie est algébrique. La réciproque n'est pas vraie. Par exemple, l'ensemble  $\overline{\mathbb{Q}}$  des nombres complexes qui sont algébriques sur  $\mathbb{Q}$  n'est pas de dimension finie sur  $\mathbb{Q}$ . L'extension  $\mathbb{Q} \subset \overline{\mathbb{Q}}$  est donc une extension algébrique qui n'est pas une extension finie.

**Définition 51 :** Un corps  $K$  est algébriquement clos si tout polynôme non constant admet une racine dans  $K$ . De manière équivalente, tout polynôme de  $K[X]$  est scindé dans  $K[X]$ .

**Théorème 52 :** (théorème fondamental de l'algèbre) Le corps  $\mathbb{C}$  est algébriquement clos.

C'est un résultat aux multiples démonstrations dans tous les domaines des mathématiques. La démonstration la plus élémentaire consiste à trouver  $z_0 \in \mathbb{C}$  tel que  $\inf_{z \in \mathbb{C}} |P(z)| = |P(z_0)|$ . La plus rapide est probablement de le voir comme un corollaire du théorème de Liouville. Une autre démonstration complète est présentée dans l'exemple 85.

**Définition 53 :** Une clôture algébrique de  $K$  est une extension  $L \supset K$  telle que  $L$  est algébrique sur  $K$ , et  $L$  est algébriquement clos.

**Exemple 54 :**  $\mathbb{C}$  est une clôture algébrique de  $\mathbb{R}$ .

**Contre-exemple 55 :**  $\mathbb{C}$  n'est pas une clôture algébrique de  $\mathbb{Q}$  car il contient au moins un élément transcendant sur  $\mathbb{Q}$ . En effet, Charles Hermite et Carl Louis Ferdinand von Lindemann ont respectivement démontré que  $e$  et  $\pi$  sont transcendants sur  $\mathbb{Q}$ .

**Théorème 56 :** (*Steinitz*) Tout corps  $K$  admet une clôture algébrique, unique à isomorphisme de  $K$ -algèbre près.

### 3 Polynômes symétriques

#### 3.1 Définitions

Soit  $A$  un anneau commutatif et  $A[X_1, \dots, X_n]$  l'anneau des polynômes à  $n$  indéterminées à coefficients dans  $A$ . On dispose d'une action naturelle du groupe symétrique  $\mathfrak{S}_n$  sur  $A[X_1, \dots, X_n]$

$$\begin{aligned} \mathfrak{S}_n \times A[X_1, \dots, X_n] &\longrightarrow A[X_1, \dots, X_n] \\ (\sigma, P) &\longmapsto P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) \end{aligned}$$

**Définition 57 :** On dit que  $P \in A[X_1, \dots, X_n]$  est symétrique s'il est fixe sous l'action décrite ci-dessus.

On vérifie facilement que l'ensemble des polynômes symétriques est un sous-anneau de  $A[X_1, \dots, X_n]$ .

**Exemple 58 :**

1. Si  $n = 3$ ,  $X_1 + X_2 + X_3$  est symétrique. Cependant ce n'est pas le cas si  $n = 4$ .
2. Si  $n = 3$ ,  $(X_1 - X_2)^2(X_1 - X_3)^2(X_2 - X_3)^2$  est symétrique.

En notant  $\mathcal{P}_k(\{1, \dots, n\})$  l'ensemble des combinaisons de  $k$  nombres pris dans l'ensemble  $\{1, 2, \dots, n\}$ , on note  $\sigma_{n,k}$  le polynôme de  $A[X_1, \dots, X_n]$  défini par

$$\sigma_{n,k}(X_1, \dots, X_n) = \sum_{I \in \mathcal{P}_k(\{1, \dots, n\})} \prod_{i \in I} X_i = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} X_{i_1} X_{i_2} \dots X_{i_k}$$

Ce polynôme est bien symétrique, puisqu'une permutation du groupe symétrique  $\mathfrak{S}_n$  envoie bijectivement une combinaison à  $k$  éléments sur une autre. Lorsque le contexte est clair on notera simplement  $\sigma_k$ .

**Définition 59 :** Le polynôme  $\sigma_k$  est appelé le  $k$ -ième polynôme symétrique élémentaire de  $A[X_1, \dots, X_n]$ .

**Exemple 60 :**  $\sigma_0(X_1, \dots, X_n) = 1$ ;  $\sigma_n(X_1, \dots, X_n) = X_1 \dots X_n$ ;  $\sigma_k(X_1, \dots, X_n) = 0$  si  $k > n$ ;  
 $\sigma_2(X_1, \dots, X_n) = \sum_{1 \leq i < j \leq n} X_i X_j$ ; Cas  $n = 3$ :  $\sigma_2(X_1, X_2, X_3) = X_1 X_2 + X_1 X_3 + X_2 X_3$ .

#### 3.2 Relations coefficients-racines

Soit  $K$  un corps et soit  $P = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \in K[X]$  de degré supérieur ou égal à 1. Soient  $\alpha_1, \dots, \alpha_n$  les racines de  $P$  dans une extension  $L/K$  dans laquelle  $P$  est scindé (voir section 2.2, si  $K = \mathbb{R}$  on peut considérer  $L = \mathbb{C}$  par exemple). Sur  $L$  notre polynôme s'écrit

$$P = a_n(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n)$$

On voit alors en développant selon les degrés que pour  $k \in \llbracket 1, n \rrbracket$ , on a

$$a_{n-k} = (-1)^k a_n \sigma_k(\alpha_1, \dots, \alpha_n)$$

que l'on peut encore énoncer comme dans la proposition suivante.

**Proposition 61 :** Soit  $P = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \in K[X]$  et  $\alpha_1, \dots, \alpha_n$  ses racines dans une extension dans laquelle il est scindé. Alors pour  $k \in \llbracket 0, n \rrbracket$ ,

$$a_k = (-1)^{n-k} a_n \sigma_{n-k}(\alpha_1, \dots, \alpha_n)$$

### 3.3 Structure des polynômes symétriques

**Théorème 62 :** Soit  $A$  un anneau commutatif. Pour tout polynôme symétrique  $P \in A[X_1, \dots, X_n]$ , il existe un unique polynôme  $Q \in A[\sigma_1, \dots, \sigma_n]$  tel que

$$P = Q(\sigma_1, \dots, \sigma_n)$$

Autrement dit, tout polynôme symétrique s'exprime de manière unique comme un polynôme en les polynômes symétriques élémentaires.

Plus formellement, le morphisme d'algèbres

$$\begin{aligned} A[X_1, \dots, X_n] &\rightarrow A[X_1, \dots, X_n] \\ P(X_1, \dots, X_n) &\mapsto P(\sigma_1(X_1, \dots, X_n), \dots, \sigma_n(X_1, \dots, X_n)) \end{aligned}$$

est injectif, et a pour image la sous-algèbre des polynômes symétriques, ou encore les polynômes symétriques élémentaires engendrent la sous-algèbre unitaire des polynômes symétriques, et sont algébriquement indépendants sur  $A$ .

**Exemple 63 :** Pour  $r \geq 1$ , posons  $S_r = X_1^r + \dots + X_n^r$ . On a  $S_1 = \sigma_1$ , et

$$\sigma_1^2 = \sum_{i=1}^n X_i^2 + 2 \sum_{i < j} X_i X_j,$$

d'où  $S_2 = \sigma_1^2 - 2\sigma_2$ .

**Corollaire 64 :** Soit  $P \in A[X]$  unitaire de degré  $n \geq 1$  et  $L$  un corps contenant  $A$  dans lequel  $P$  a toutes ses racines  $\alpha_1, \dots, \alpha_n$ . Alors pour tout polynôme symétrique  $S \in A[X_1, \dots, X_n]$ , on a

$$S(\alpha_1, \dots, \alpha_n) \in A$$

*Démonstration.* C'est une conséquence du théorème de structure et des relations coefficients-racines. En effet,  $S$  est un polynôme à coefficients dans  $A$  en les polynômes symétriques élémentaires des  $\alpha_1, \dots, \alpha_n$ , et ces derniers sont des coefficients de  $P \in A[X]$  (modulo un signe) puisque  $P$  est unitaire. Finalement le tout est dans  $A$ .  $\square$

**Remarque 65 :** Si on suppose que  $A$  est un corps, on dispose du même résultat sans supposer  $P$  unitaire, mais la démonstration est moins immédiate.

#### 3.3.1 Un algorithme

À défaut de proposer la preuve du théorème 62, on donne ici un algorithme pour trouver étant donné un polynôme symétrique  $P$  le polynôme  $Q$  vérifiant la relation du théorème 62.

**Définition 66 :** On définit un ordre total  $\prec$  sur les monômes de  $A[X_1, \dots, X_n]$  par

$$X_1^{s_1} X_2^{s_2} \dots X_n^{s_n} \prec X_1^{r_1} X_2^{r_2} \dots X_n^{r_n}$$

si la première fois qu'on a  $r_i \neq s_i$  on a  $r_i > s_i$ . C'est-à-dire, s'il existe un  $m$  avec  $r_i = s_i$  pour  $i < m$  et avec  $r_m > s_m$ . On appelle cet ordre l'ordre lexicographique.

**Exemple 67 :**  $X_1 \succ X_2$ ;  $X_1 \succ X_2^8 X_3^7 X_4^3$

**Définition 68 :** Le terme initial d'un polynôme non nul  $P \in A[X_1, \dots, X_n]$  est le terme de  $P$  qui est supérieur à tous les autres termes de  $P$  pour l'ordre lexicographique. On le note  $\text{in}(P)$ .

**Exemple 69 :** Par exemple dans  $P = -2X_1^2 X_3 + 3X_1 X_2 X_3 + X_2^3$  on a trié les trois termes pour qu'ils apparaissent dans l'ordre lexicographique. Le terme initial est  $\text{in}(P) = -2X_1^2 X_3$  parce qu'il est avant  $3X_1 X_2 X_3$  et  $X_2^3$  dans l'ordre lexicographique.

**Lemme 70 :** Soit  $P \in K[X_1, X_2, \dots, X_n]$  un polynôme symétrique non nul avec terme initial  $\text{in}(P) = aX_1^{r_1}X_2^{r_2} \cdots X_n^{r_n}$ . Alors on a  $r_1 \geq r_2 \geq \dots \geq r_n \geq 0$ .

L'idée est que si  $m = aX_1^{r_1}X_2^{r_2} \cdots X_n^{r_n}$  est le monôme initial, en appliquant une permutation de  $\mathfrak{S}_n$  on peut toujours transformer ce monôme  $m'$  en un nouveau vérifiant la relation du lemme sur les  $r_i$ , en particulier  $m' \succ m$ . Mais puisque  $P$  est symétrique, ce monôme est également un monôme de  $P$ , donc  $m \succ m'$ , et finalement  $m = m'$ .

**Lemme 71 :** Soit  $r_1 \geq r_2 \geq \dots \geq r_n \geq 0$  entiers, et posons  $Q = \sigma_1^{r_1-r_2}\sigma_2^{r_2-r_3} \cdots \sigma_{n-1}^{r_{n-1}-r_n}\sigma_n^{r_n}$ . Alors on a

$$\text{in}(Q) = X_1^{r_1}X_2^{r_2} \cdots X_n^{r_n}$$

En effet, les termes initiaux des polynômes symétriques élémentaires sont  $\text{in}(\sigma_i) = X_1X_2 \cdots X_i$ . On voit alors que

$$\text{in}(Q) = X_1^{r_1-r_2} (X_1X_2)^{r_2-r_3} \cdots (X_1 \cdots X_{n-1})^{r_{n-1}-r_n} (X_1 \cdots X_{n-1}X_n)^{r_n}.$$

La puissance totale de  $X_i$  dans  $\text{in}(Q)$  est

$$(r_i - r_{i+1}) + (r_{i+1} - r_{i+2}) + \cdots + (r_{n-1} - r_n) + r_n = r_i.$$

Donc on a bien  $\text{in}(Q) = X_1^{r_1}X_2^{r_2} \cdots X_n^{r_n}$ .

On a maintenant tous les outils pour développer l'algorithme. L'idée est la suivante : on se donne un polynôme symétrique  $P$ , et à l'aide du lemme 70 on va lui soustraire un polynôme en les polynômes symétriques élémentaires de sorte à éliminer le terme initial de  $P$ . On écrit donc  $P_1 = P - Q_1(\sigma_1, \dots, \sigma_n)$  où le degré de  $P_1$  est strictement inférieur à celui de  $P$  pour l'ordre lexicographique. On réitère alors l'opération sur  $P_1$  jusqu'à obtenir un polynôme nul au bout d'un certain nombre  $N$  d'étapes. On a alors  $P - \sum_{i=1}^N Q_i(\sigma_1, \dots, \sigma_n) = 0$  et donc  $P = Q(\sigma_1, \dots, \sigma_n)$  où  $Q = \sum_{i=1}^N Q_i$

---

#### Algorithme 1 Théorème de structure

---

```

1: procédure TROUVERQ( $P$ ) :
2:    $R \leftarrow P$ 
3:    $Q \leftarrow 0$ 
4:   Tant que  $R \neq 0$ , faire :
5:     Trouver  $aX_1^{r_1}X_2^{r_2} \cdots X_n^{r_n}$  le terme initial de  $R$ 
6:      $R \leftarrow R - a\sigma_1^{r_1-r_2}\sigma_2^{r_2-r_3} \cdots \sigma_{n-1}^{r_{n-1}-r_n}\sigma_n^{r_n}$ 
7:      $Q \leftarrow Q + aX_1^{r_1-r_2}X_2^{r_2-r_3} \cdots X_{n-1}^{r_{n-1}-r_n}X_n^{r_n}$ 
8:   Fin tant que
9:   return  $Q$ 
10: Fin procédure

```

---

La stricte décroissance des termes initiaux assure que l'algorithme se termine, et on obtient bien un polynôme  $Q$  vérifiant  $P = Q(\sigma_1, \dots, \sigma_n)$ .

**Exemple 72 :** Soit  $P = X_1^2X_3 + X_1^2X_2 + X_2^2X_1 + X_2^2X_3 + X_3^2X_1 + X_3^2X_2$ . On voit facilement qu'il est symétrique. On a  $\text{dlex}(P) = (2, 1, 0)$ . On considère donc

$$R_1 = P - \sigma_1^{2-1}\sigma_2^{1-0}\sigma_3^0 = P - \sigma_1\sigma_2 \quad \text{et} \quad Q_1 = X_1X_2$$

Un calcul explicite montre que  $R_1 = -3X_1X_2X_3$ . On reconnaît immédiatement  $-3\sigma_3$ . Donc finalement

$$P = Q(\sigma_1, \sigma_2, \sigma_3) \quad \text{avec} \quad Q(X_1, X_2, X_3) = X_1X_2 - 3X_3$$

## 4 Localisation des racines

Localiser les racines signifie trouver toutes les racines (réelles ou complexes) d'un polynôme et les isoler dans des boules ou intervalles aussi finement que possible. On souhaite faire cela pour plusieurs raisons. Cela peut servir d'étape initiale avant une méthode de Newton pour s'assurer de la convergence vers une racine donnée ou pour faire de l'arithmétique d'intervalles afin d'avoir des résultats exacts même en manipulant des racines approchées. On peut aussi faire cela pour obtenir des résultats d'existence (ou d'absence) de racines à des fins théoriques.

## 4.1 Méthode de Newton

### 4.1.1 La méthode

**La méthode :** Étant donné une fonction  $f : D \rightarrow \mathbb{R}$ , définie sur un domaine  $D \subset \mathbb{R}$ , on souhaite trouver  $\alpha \in D$  solution de l'équation  $f(x) = 0$ . Bien sûr dans le cadre de cette leçon  $f$  peut être remplacé par un polynôme. Pour approcher un zéro, on va introduire une suite  $(x_n)$  d'approximations successives convergent vers une solution de l'équation.

1. On part d'un point  $x_0$  proche de la solution (il faut donc avoir une vague idée de la localisation de notre racine comme évoqué dans l'introduction de la section).
2. À partir de  $x_0$ , on calcul un nouveau terme  $x_1$  de la manière suivante : On trace la tangente à la courbe de notre fonction en  $x_0$ . Sauf cas pathologique ( $f'(x_0) = 0$  par exemple, ce qui donnerait une tangente horizontale), la tangente tracée comme l'axe des abscisses en un point  $x_1$ .
3. On construit alors par itération les éléments de notre suite.

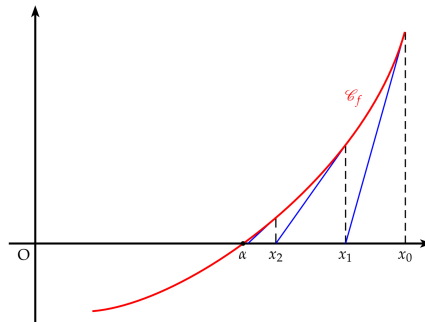


FIGURE 1 – Construction des premiers termes de la suite

On peut facilement établir la relation de récurrence reliant les éléments de notre suite. Par définition,  $x_{n+1}$  est l'abscisse du point d'intersection de la tangente à  $\mathcal{C}_f$  en  $x_n$  avec l'axe des abscisses. Puisque la tangente en question a pour équation  $y = f'(x_n)(x - x_n) + f(x_n)$ , on trouve la relation suivante :

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

Remarquons que la construction d'une telle suite nécessite uniquement que  $f$  soit dérivable sur les points de la suite et que cette dérivée s'annule pas, et que les termes de la suite restent dans le domaine de  $f$ . Cependant on n'a aucune assurance que notre suite converge. En cas de convergence, en voit en passant à la limite dans la relation de récurrence que la limite dans notre suite est bien un zéro de  $f$  lorsque  $f'(\alpha) \neq 0$ , c'est à dire que  $\alpha$  est racine simple.

Un exemple de non convergence :

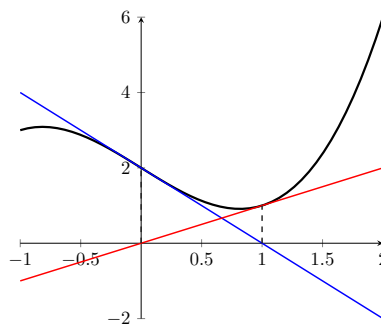


FIGURE 2 –  $x \mapsto x^3 - 2x + 2$  tracé en noir, ainsi que les deux tangentes en 0 et en 1.

Les tangentes à la courbe représentant la fonction  $x \mapsto x^3 - 2x + 2$  en 0 et en 1 coupent l'axe des abscisses en 1 et en 0 respectivement. Si l'on prend 0 ou 1 comme point de départ, la méthode oscille entre ces deux points et ne converge donc pas.

### 4.1.2 Critère de convergence de la méthode

On donne ici quelques critères de convergence de la méthode de Newton. On commence par un théorème d'existence de limite.

**Proposition 73 :** Soit  $f \in \mathcal{C}^2([a, b], \mathbb{R})$  et  $\alpha \in ]a, b[$  tel que  $f(\alpha) = 0$  et  $f'(\alpha) \neq 0$ . Il existe un réel  $\eta > 0$  tel que pour tout  $x_0 \in [\alpha - \eta, \alpha + \eta]$  la suite  $(x_n)_{n \in \mathbb{N}}$  définie par

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

converge vers  $\alpha$ .

La preuve consiste à appliquer le théorème de point fixe de Picard à la fonction  $x \mapsto x - f(x)/f'(x)$  en remarquant que l'hypothèse de régularité  $\mathcal{C}^2$  permet d'en satisfaire les hypothèses sur un certain voisinage de  $\alpha$ .

On donne ensuite un résultat sur la majoration de l'erreur d'approximation.

**Théorème 74 :** Soit  $\alpha$  une racine de  $f$ . On suppose  $f$  de classe  $\mathcal{C}^2$  sur un intervalle du type  $I = [\alpha - r, \alpha + r]$  pour un certain  $r > 0$  et que  $f'$  ne s'annule pas sur  $I$ . Soit  $M = \max_{x \in I} |f''(x)/f'(x)|$  et  $\eta := \min(r, \frac{1}{M})$ . Alors pour tout point initial  $x_0 \in [\alpha - \eta, \alpha + \eta]$  la suite définie dans la proposition 73 converge de manière quadratique vers  $\alpha$ . Plus précisément, on a

$$|x_p - \alpha| \leq \frac{1}{M} (M|x_0 - \alpha|)^{2^p}.$$

*Démonstration.* Il s'agit d'évaluer une majoration de  $\log|x_n - \alpha|$ . On pose  $N_f(x) = x - \frac{f(x)}{f'(x)}$ . La formule de Taylor-Lagrange s'écrit :

$$0 = f(\alpha) = f(x) + f'(x)(\alpha - x) + \frac{f''(\xi)}{2}(\alpha - x)^2, \text{ avec } \xi \text{ entre } x \text{ et } \alpha.$$

Partant de l'approximation  $x$ , la méthode de Newton fournit au bout d'une itération :

$$N_f(x) - \alpha = x - \frac{f(x)}{f'(x)} - \alpha = \frac{f''(\xi)}{2f'(x)}(x - \alpha)^2.$$

On a alors pour tout  $x \in I$  :

$$|N_f(x) - \alpha| \leq M|x - \alpha|^2.$$

Par récurrence immédiate, il vient :

$$M|x_n - \alpha| \leq (M|x_0 - \alpha|)^{2^n}.$$

En passant au logarithme :

$$\log|x_n - \alpha| \leq 2^n \log(M|x_0 - \alpha|) - \log(M).$$

La convergence de  $x_n$  vers  $a$  est donc quadratique, à condition que  $|x_0 - \alpha| < 1/M$ . □

Dans le cas où  $f$  est une fonction polynomiale à coefficients réels dont toutes les racines sont réelles et distinctes, on est presque toujours assuré de la convergence de la méthode de Newton. On a plus précisément le résultat suivant due à C. Masse en 1984 :

**Théorème 75 :** Soit  $f$  une fonction polynomiale de degré  $n \geq 1$  à coefficients réels dont toutes les racines sont réelles et distinctes et  $E$  l'ensemble des réels  $x_0$  pour lesquels la méthode de Newton associée à  $f$  de premier terme  $x_0$  diverge.

1. Pour  $n \leq 2$ ,  $E$  est vide ou réduit à un point.
2. Pour  $n = 2$ ,  $E$  est dénombrable.
3. Pour  $n \geq 4$ ,  $E$  est non dénombrable de mesure de Lebesgue nulle.

## 4.2 Les disques de Gerschgorin

Le théorème de Gerschgorin permet, étant donnée une matrice carrée  $A$ , de construire un domaine contenant toutes les valeurs propres de  $A$ .

**Théorème 76 :** Soit  $A = (a_{i,j})$  une matrice complexe de taille  $n$ . On appelle disques de Gershgorin associés à  $A$  les  $n$  disques de  $\mathbb{C}$  définis par

$$\left\{ z \in \mathbb{C} : |z - a_{i,i}| \leq \sum_{j \neq i} |a_{i,j}| \right\}$$

où  $i \in \{1, \dots, n\}$ . Si  $\lambda$  est une valeur propre de  $A$ , alors elle appartient à un des disques de Gershgorin de  $A$ .

*Démonstration.* La preuve de ce résultat est étonnamment simple. Prenons en effet  $x$  un vecteur propre (non nul) associé à la valeur propre, et soit  $i$  tel que  $|x_i|$  soit maximum. Puisque  $x$  est vecteur propre pour  $\lambda$ , on a

$$(\lambda - a_{i,i}) x_i = \sum_{j \neq i} a_{i,j} x_j.$$

On divise ensuite par  $x_i$  (qui n'est pas nul car  $x$  est non nul), on prend le module et on utilise l'inégalité triangulaire. On obtient donc :

$$|\lambda - a_{i,i}| \leq \sum_{j \neq i} |a_{i,j}| \cdot \frac{|x_j|}{|x_i|}.$$

qui à son tour donne le résultat, puisque  $|x_j|/|x_i| \leq 1$ . □

C'est un résultat très intéressant, car la recherche de valeurs propres est en général un problème compliqué (il faut trouver les racines d'un polynôme).

**Remarque 77 :** En appliquant le théorème à la matrice transposée de  $A$ , une nouvelle information est donnée sur la localisation des valeurs propres : elles se trouvent dans la réunion des disques de Gerschgorin associés aux colonnes.

### 4.3 Théorème de Gauss-Lucas

**Théorème 78 :** Soit  $P$  un polynôme non constant à coefficients complexes. Alors tout zéro de  $P'$  appartient à l'enveloppe convexe de l'ensemble des zéros de  $P$ .

*Démonstration.* Soit  $P(z) = c \prod_{i=1}^r (z - a_i)^{n_i}$  la décomposition de  $P$  en facteurs irréductibles : le complexe  $c$  est le coefficient dominant du polynôme, les complexes  $a_i$  en sont les zéros distincts, les entiers  $n_i$  leurs multiplicités respectives. On a alors :

$$\frac{P'(z)}{P(z)} = \sum_{i=1}^r \frac{n_i}{z - a_i}.$$

En particulier,

$$\sum_{i=1}^r \frac{n_i}{z - a_i} = 0 \quad \text{ou encore} \quad \sum_{i=1}^r n_i \frac{\bar{z} - \bar{a}_i}{|z - a_i|^2} = 0$$

ce qui s'écrit aussi

$$\left( \sum_{i=1}^r \frac{n_i}{|z - a_i|^2} \right) \bar{z} = \sum_{i=1}^r \frac{n_i}{|z - a_i|^2} \bar{a}_i$$

En prenant les conjugués, on voit que  $z$  est un barycentre à coefficients positifs des  $a_i$ . Le cas où  $z$  est aussi zéro de  $P$  est évident. □

### 4.4 Théorème de Kronecker

**Théorème 79 :** Soit  $P$  un polynôme unitaire de  $\mathbb{Z}[X]$  dont les racines complexes sont toutes de module inférieur ou égal à 1 et vérifiant  $P(0) \neq 0$ . Alors toutes les racines de  $P$  sont des racines de l'unité.

*Démonstration.* Notons  $z_1, z_2, \dots, z_n$  les racines complexes de  $P$  comptées avec leur multiplicité où  $n \geq 1$  désigne le degré de  $P$ , et soient  $\sigma_1, \dots, \sigma_n$  les fonctions symétriques élémentaires des  $z_i$ . On a donc

$$P(X) = X^n - \sigma_1 X^{n-1} + \dots + (-1)^n \sigma_n$$

et les  $\sigma_i$  sont dans  $\mathbb{Z}$ . Comme  $|z_i| \leq 1$  pour tout  $i \in \llbracket 1, n \rrbracket$ , on obtient, pour  $1 \leq p \leq n$ , la majoration

$$|\sigma_p| = \left| \sum_{I \in \mathcal{P}_r(\llbracket 1, n \rrbracket)} \prod_{i \in I} z_i \right| \leq \sum_{I \in \mathcal{P}_r(\llbracket 1, n \rrbracket)} 1 = \text{Card } \mathcal{P}_r(\llbracket 1, n \rrbracket) = \binom{n}{p}.$$

Ceci montre que l'ensemble  $\Omega_n$  des polynômes unitaires de  $\mathbb{Z}[X]$ , de degré  $n$ , dont les racines complexes sont de module inférieur ou égal à 1 est fini. En effet  $\sigma_p \in \mathbb{Z}$  car les coefficients de  $P$  le sont et donc la majoration ci-dessus décrit un nombre fini de choix pour chaque coefficient d'un polynôme appartenant à  $\Omega_n$ .

L'idée est alors de considérer pour tout  $k \in \mathbb{N}^*$  les polynômes

$$P_k(X) = (X - z_1^k) (X - z_2^k) \dots (X - z_n^k).$$

Ce sont des polynômes unitaires de degré  $n$  dont les racines  $z_i^k$  sont de module inférieur ou égal à 1. Pour tout  $r \in \llbracket 1, n \rrbracket$ , le coefficient de  $X^{n-r}$  dans  $P_k$  est  $(-1)^r \sigma_r(z_1^k, \dots, z_n^k)$ . Il s'agit d'un polynôme symétrique en  $z_1, z_2, \dots, z_n$  à coefficients dans  $\mathbb{Z}$ . Il est donc égal à un polynôme à coefficients entiers en les fonctions symétriques élémentaires des  $z_i$ , qui on le rappelle sont dans  $\mathbb{Z}$ . Il en résulte que, pour tout entier  $k$ , on a  $P_k \in \mathbb{Z}[X]$  et donc que  $P_k \in \Omega_n$ .

Comme  $\Omega_n$  est fini, et que chaque élément de  $\Omega_n$  admet au plus  $n$  racines complexes distinctes, l'ensemble des racines des éléments de  $\Omega_n$  est aussi fini. En particulier, pour tout  $i \in \llbracket 1, n \rrbracket$ , l'application

$$\begin{cases} \mathbb{N} \rightarrow \Omega_n \\ k \mapsto z_i^k \end{cases}$$

ne peut pas être injective. Par principe des tiroirs, il existe donc deux entiers  $k > \ell$  tels que  $z_i^k = z_i^\ell$ . Comme  $z_i$  est supposé non nul, on a  $z_i^{k-\ell} = 1$  et il s'agit d'une racine de l'unité. □

On propose maintenant une application de ce théorème.

**Lemme 80 :** Soit  $P$  un élément irréductible de  $\mathbb{Q}[X]$ . Alors les racines de  $P$  dans  $\mathbb{C}$  sont simples.

*Démonstration.* Comme  $P$  n'est pas constant et  $\mathbb{Q}$  est de caractéristique nulle,  $P'$  n'est pas nul. Puisque  $P$  est irréductible et  $P'$  est non nul et de degré strictement inférieur au degré de  $P$ ,  $P$  et  $P'$  sont premiers entre eux dans  $\mathbb{Q}[X]$ . Or le pgcd de deux polynômes ne dépend pas du corps de base (conséquence, par exemple, de l'algorithme d'Euclide), on en déduit que  $P$  et  $P'$  sont premiers entre eux sur également sur  $\mathbb{C}$  et que les racines complexes de  $P$  sont simples. □

**Corollaire 81 :** Soit  $P \in \mathbb{Z}[X]$  unitaire tels que toutes ses racines complexes soient de module inférieur ou égal à 1. Si  $Q$  est un facteur irréductible de  $P$  alors  $Q$  est un polynôme cyclotomique ou  $Q = X$ . En outre, si  $P$  est irréductible alors  $P = X$  ou  $P$  est un polynôme cyclotomique.

*Démonstration.* Soit  $Q \in \mathbb{Z}[X]$  un facteur irréductible unitaire de  $P$  et supposons  $Q \neq X$ .  $Q$  étant irréductible, on a  $Q(0) \neq 0$ . Par le théorème de Kronecker, ses racines sont des racines de l'unité : il existe  $n \in \mathbb{N}$  tel que les racines de  $Q$  soient dans  $\mathbb{U}_n$ . En effet, pour toute racine  $z_i$  il existe un entier  $n_i$  tel que  $z_i \in \mathbb{U}_{n_i}$ . On peut donc poser  $n := \text{ppcm}(n_i)$ . Le polynôme  $Q$  étant irréductible sur  $\mathbb{Z}$  (et donc sur  $\mathbb{Q}$ ), il est scindé à racines simples sur  $\mathbb{C}$  par le lemme 80. Donc  $Q$  divise  $X^n - 1 = \prod_{d|n} \phi_d$ , avec  $\phi_d$  les polynômes cyclotomiques. Or ces derniers sont irréductibles, donc  $Q = \phi_d$  pour  $d$  un diviseur de  $n$ . □

## 4.5 Théorème de Rouché

**Théorème 82 :** *Principe de l'argument.* Soit  $f$  une fonction méromorphe sur un ouvert  $U \subset \mathbb{C}$  simplement connexe dont l'ensemble  $F$  des zéros et des pôles est fini. Alors pour tout lacet  $\gamma$  à image dans  $U \setminus F$ ,

$$\frac{1}{2i\pi} \int_{\gamma} \frac{f'(z)}{f(z)} dz = \sum_{z_j \in F} v_{z_j}(f) \text{Ind}_{\gamma}(z_j)$$

où  $v_{z_j}(f)$  est la valuation de  $f$  en  $z_j$  c'est-à-dire l'ordre de  $z_j$  si  $z_j$  est un zéro et l'opposé de l'ordre de  $z_j$  si c'est un pôle et  $\text{Ind}_{\gamma}(z_j)$  est l'indice du point par rapport au lacet.

**Remarque 83 :** Si  $\gamma$  est un lacet simple positivement orienté formant le bord  $\partial K$  d'un compact  $K$ , la relation ci-dessus se réécrit :

$$\frac{1}{2i\pi} \int_{\gamma} \frac{f'(z)}{f(z)} dz = Z_{f,K} - P_{f,K}$$

où  $Z_{f,K}$  et  $P_{f,K}$  représentent respectivement le nombre de zéros et de pôles de  $f$  dans  $K$  comptés avec leur multiplicité.

Le principe de l'argument permet de compter le nombre de tours que fait l'image de  $\gamma$  par  $f$  autour de l'origine.

**Théorème 84 :** (de Rouché) Soit  $U \subset \mathbb{C}$  un ouvert simplement connexe, soient  $f$  et  $g$  deux fonctions méromorphes sur  $U$  avec un ensemble fini  $F$  de zéros et de pôles. Soit  $\gamma$  un lacet simple à image dans  $U \setminus F$  formant le bord  $\partial K$  d'un compact  $K$ . Si  $|f(z) - g(z)| < |g(z)|$  pour tout point  $z$  de  $\gamma$  alors

$$Z_f - P_f = Z_g - P_g$$

où  $Z_f$  et  $P_f$  sont respectivement le nombre de zéros et de pôles de  $f$  (en tenant compte de leur multiplicité) contenus dans  $K$ .

*Démonstration.* Si  $|f(z) - g(z)| < |g(z)|$  pour tout  $z \in \gamma$ , alors  $f$  et  $g$  ne s'annulent pas sur  $\gamma$  (sinon l'inégalité stricte ne pourrait pas être vérifiée). Soit  $h$  la fonction méromorphe sur  $U$ , holomorphe et ne s'annulant pas sur  $\gamma$  définie par :

$$h = \frac{f}{g}.$$

Pour tout point  $z$  de  $\gamma$ ,

$$|h(z) - 1| = \frac{|f(z) - g(z)|}{|g(z)|} < 1.$$

L'image de  $\gamma$  par  $h$  est donc contenue dans le disque ouvert de rayon 1 et de centre 1 et par conséquent elle ne tourne pas autour de l'origine. En appliquant le principe de l'argument on a donc :

$$\frac{1}{2\pi i} \int_{\gamma} \frac{h'(z)}{h(z)} dz = 0.$$

D'autre part,

$$\frac{h'(z)}{h(z)} = \frac{f'(z)}{f(z)} - \frac{g'(z)}{g(z)}.$$

Par conséquent,

$$\frac{1}{2\pi i} \int_{\gamma} \frac{f'(z)}{f(z)} dz - \frac{1}{2\pi i} \int_{\gamma} \frac{g'(z)}{g(z)} dz = 0.$$

Finalement, en utilisant à nouveau le principe de l'argument, on obtient

$$Z_f - P_f = Z_g - P_g.$$

□

**Exemple 85 :** Démonstration du théorème fondamental de l'algèbre. Soit un polynôme  $P$  à coefficients dans  $\mathbb{C}$  et défini par :

$$P(z) = a_0 + a_1 z + \dots + a_n z^n$$

en supposant  $a_n \neq 0$ . Soit  $R > 0$  suffisamment grand pour que pour tout  $z \in C(0, R)$  (cercle de rayon  $R$ ) on ait :

$$|P(z) - a_n z^n| = |a_0 + \dots + a_{n-1} z^{n-1}| < |a_n z^n|$$

Étant donné que  $a_n z^n$  admet un zéro d'ordre  $n$  à l'origine,  $P$  doit admettre  $n$  zéros dans le disque ouvert  $D(0, R)$  par application du théorème de Rouché. De ce point de vue on a montré un peu plus que le théorème de d'Alembert-Gauss car on donne en plus un disque dans lequel les racines se trouvent : si  $P$  un polynôme de degré  $n$  normalisé (le coefficient de  $z^n$  est 1) et  $A$  le plus grand module des autres coefficients de  $P$ . Alors  $P$  a exactement  $n$  racines (comptées avec leurs multiplicités) à l'intérieur du cercle de centre 0 et de rayon  $1 + A$ .

**Exemple 86 :** Trouvons le nombre de zéros de  $P(z) = 9z^5 + 5z - 3$  dans la couronne  $\{z \in \mathbb{C}, 1/2 < |z| < 5\}$ . D'abord on considère  $\gamma_1 = \partial B_{1/2}(0)$ . On pose  $g(z) = 5z - 3$ . On a  $P$  et  $g$  holomorphes sur  $\mathbb{C}$ . Pour  $|z| = 1/2$ ,  $|P(z) - g(z)| = 9 \frac{1}{2^5}$  et  $|g(z)| = |5z - 3| \geq \frac{1}{2}$ . Donc on peut appliquer le théorème de Rouché et conclure que  $P$  n'a pas de zéros dans  $\text{Int}(\gamma) = B_{1/2}(0)$  car c'est le cas pour  $g$ .

En suite on considère  $\gamma_2 = \partial B_5(0)$ . Soit  $g(z) = 9z^5$ . Pour  $|z| = 5$ ,  $|P(z) - g(z)| = |5z - 3| < 28$  et  $|g(z)| = |9z^5| = 9 \cdot 5^5 > |P(z) - g(z)|$ . Comme  $g$  a un zéro d'ordre 5 dans  $B_5(0)$ , on conclut que  $P$  a aussi 5 zéros dans  $B_5(0)$ , et donc 5 zéros dans la couronne  $\{z \in \mathbb{C}, 1/2 < |z| < 5\}$ .

De manière générale, on peut toujours localiser les racines d'un polynôme dans une certaine couronne :

**Corollaire 87 :** Soit  $P$  un polynôme de degré  $n$  s'écrivant

$$P(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0$$

et soient les deux nombres  $A = \max(|a_0|, |a_1|, \dots, |a_{n-1}|)$ ,  $B = \max(|a_1|, |a_2|, \dots, |a_n|)$ . Les racines de  $P$  sont dans la couronne

$$\frac{1}{1 + B/|a_0|} \leq |z| < 1 + \frac{A}{|a_n|}.$$

où on convient que la borne inférieure vaut 0 si  $a_0 = 0$ .

## 5 Racines et réduction des endomorphismes

On développe ici l'étroit lien qui existe entre la recherche de racines et de leur multiplicité et la réduction des endomorphismes. Dans une première partie on redonne sans démontrer, et en admettant que les définitions de base sont connues, les résultats classiques d'algèbre linéaire qui nous donne des critères de diagonalisation et de trigonalisation selon les racines d'un polynôme annulateur de notre endomorphisme. Dans cette première partie c'est l'étude des polynômes qui sert d'outils à la réduction. Dans une seconde partie on s'intéressera à l'aspect réciproque souvent moins connu : comment la réduction peut servir d'outil pour l'étude des polynômes.

### 5.1 Des polynômes pour l'étude des endomorphismes

On considère un  $\mathbb{K}$ -espace vectoriel  $E$  de dimension finie  $n$ . Quitte à se fixer une base, on va considérer l'ensemble  $\mathcal{M}_n(\mathbb{K})$  des matrices carrées de taille  $n \times n$  à coefficient dans  $\mathbb{K}$  pour étudier  $\mathcal{L}(E)$ . Étant donnée une matrice  $A \in \mathcal{M}_n(\mathbb{K})$  on peut lui associer un polynôme de la manière suivante

$$\chi: \begin{cases} \mathcal{M}_n(\mathbb{K}) \longrightarrow \mathbb{K}[X] \\ A \longmapsto \chi_A(X) := \det(X \text{Id}_n - A) \end{cases}$$

#### 5.1.1 Premiers critères de réduction

**Définition 88 :** Soit  $A \in \mathcal{M}_n(\mathbb{K})$ . Le polynôme  $\chi_A(X) := \det(X \text{Id}_n - A)$  s'appelle le polynôme caractéristique de  $A$ . Si  $f \in \mathcal{L}(E)$ , le polynôme caractéristique de la matrice de  $f$  dans une base de  $E$  ne dépend pas de la base et on l'appelle le polynôme caractéristique de  $f$ .

**Proposition 89 :** Soit  $A \in \mathcal{M}_n(\mathbb{K})$ . Les valeurs propres de  $A$  sont exactement les racines de  $\chi_A$ .

**Théorème 90 :** Soit  $A \in \mathcal{M}_n(\mathbb{K})$ . Alors les deux assertions suivantes sont équivalentes :

1.  $A$  est diagonalisable.
2.  $\chi_A$  est scindé sur  $\mathbb{K}$  et la multiplicité algébrique des racines (*i.e* leur multiplicité en tant que racine du polynôme) coïncide avec leur multiplicité géométrique (*i.e* la dimension du sous-espace propre qui leur est associé).

**Théorème 91 :** Une matrice  $A \in \mathcal{M}_n(\mathbb{K})$  est trigonalisable si et seulement si son polynôme caractéristique  $\chi_A$  est scindé sur  $\mathbb{K}$ .

**Remarque 92 :** En particulier toute matrice  $A \in \mathcal{M}_n(\mathbb{K})$  est trigonalisable sur  $\mathbb{C}$  par le théorème 52.

On fait maintenant le lien entre les coefficients du polynôme caractéristique et les valeurs propres de la matrice. Dans le théorème qui suit  $A$  est une matrice à coefficients dans  $\mathbb{C}$  (étant entendu qu'une matrice à coefficients réels est un élément de  $\mathcal{M}_n(\mathbb{C})$ ) de sorte que son polynôme caractéristique est scindé sur  $\mathbb{C}$  d'après le théorème de d'Alembert-Gauss :

$$\chi_A = \prod_{k=1}^n (X - \lambda_k)$$

On pose  $\sigma_1 = \sum_{k=1}^n \lambda_k$ ,  $\sigma_n = \prod_{k=1}^n \lambda_k$  et plus généralement, pour  $k \in \llbracket 1, n \rrbracket$ ,

$$\sigma_k = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} \lambda_{i_1} \dots \lambda_{i_k}$$

Les relations entre coefficients et racines d'un polynôme scindé fournissent immédiatement :

**Proposition 93 :** Soit  $A \in \mathcal{M}_n(\mathbb{C})$ .

$$\chi_A = X^n - \sigma_1 X^{n-1} + \dots + (-1)^k \sigma_k X^{n-k} + \dots + (-1)^n \sigma_n.$$

En particulier,

$$\text{Tr}(A) = \lambda_1 + \dots + \lambda_n \text{ et } \det(A) = \lambda_1 \times \dots \times \lambda_n$$

### 5.1.2 Critère de réduction par polynôme annulateur

Soit  $P = a_n X^n + \dots a_1 X + a_0 \in \mathbb{K}[X]$ . On définit les fonctions polynômes sur  $\mathcal{M}_n(\mathbb{K})$  comme suit : Pour tout  $A \in \mathcal{M}_n(\mathbb{K})$ ,  $P(A) = a_n A^n + \dots a_1 A + a_0 \text{Id}_n \in \mathcal{M}_n(\mathbb{K})$ .

**Théorème 94 :** Soit  $A \in \mathcal{M}_n(\mathbb{K})$ . Alors  $A$  est diagonalisable si et seulement s'il existe un polynôme annulateur  $P \in \mathbb{K}[X]$  de  $A$  scindé à racine simple sur  $\mathbb{K}$ .

Soit  $A \in \mathcal{M}_n(\mathbb{K})$  et  $I = \{P \in \mathbb{K}[X] \mid P(A) = 0\}$ . Le  $\mathbb{K}$ -espace vectoriel  $\mathcal{M}_n(\mathbb{K})$  est de dimension finie égale à  $n^2$ . Ainsi la famille  $(\text{Id}_n, f, \dots, f^{n^2})$  de  $n^2 + 1$  vecteur est liée. Autrement dit, il existe des scalaires  $a_0, \dots, a_{n^2}$  non tous nuls tel que  $P = a_0 + a_1 X + \dots a_{n^2} X^{n^2}$  soit un élément de  $I$  non trivial. Puisque  $\mathbb{K}[X]$  est principal car euclidien, on dispose de la définition suivante :

**Définition 95 :** Soit  $A \in \mathcal{M}_n(\mathbb{K})$  et  $I = \{P \in \mathbb{K}[X] \mid P(A) = 0\}$ . Par ce qui précède il existe un unique polynôme  $\mu_A \in \mathbb{K}[X]$  tel que  $I = \langle \mu_A \rangle$ . Le polynôme  $\mu_A$  est appelé polynôme minimal de  $A$ .

Le théorème 94 peut se reformuler de la manière suivante :

**Proposition 96 :**  $A \in \mathcal{M}_n(\mathbb{K})$  est diagonalisable si et seulement si son polynôme minimal est scindé à racine simple.

## 5.2 Des endomorphismes pour l'étude des polynômes

On pourrait croire que la réduction doit beaucoup à la connaissance des polynômes, ce n'est pas entièrement faux, mais dans la pratique c'est souvent l'inverse qui se passe. Dans l'étude des racines d'un polynôme, la réduction a su devenir un outil. Pour cela, étant donné un polynôme  $P$ , on va lui associer une certaine matrice  $C_P$  qu'on appelle matrice compagnon du polynôme  $P$ .

Soit  $P = X^n + a_{n-1}x^{n-1} + \dots a_1 X + a_0$  un polynôme unitaire de degré  $n$ . Remarquons que le supposer unitaire n'a pas d'impact sur les racines. On lui associe sa matrice  $C_P$  donnée par

$$C_P = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}$$

Par un développement de déterminant par rapport à la première ligne et une récurrence on montre facilement la proposition suivante

**Proposition 97 :** Le polynôme caractéristique de  $C_P$  est  $P$ . En vertu de la proposition 89, les valeurs propres de  $C_P$  sont exactement les racines du polynôme  $P$ .

Ainsi l'application  $P \mapsto C_P$  fournit un inverse à droite à l'application  $A \mapsto \chi_A$ . Entendons par là, puisque l'application  $\chi$  n'est pas injective, que l'on voit la matrice compagnon comme un choix à l'image réciproque de  $P$ .

**Proposition 98 :** Le polynôme minimal de  $C_P$  est égal à son polynôme caractéristique. En particulier par la proposition 96  $C_P$  est diagonalisable si et seulement si  $P$  est à racines simples.

**Proposition 99 :** (*Borne de Cauchy*) Soit  $P = X^n + \sum_{i=0}^{n-1} a_i X^i$  un polynôme unitaire de degré  $n$  dans  $\mathbb{C}[X]$ . On pose

$$R = \max \{|a_0|, 1 + |a_1|, 1 + |a_2|, \dots, 1 + |a_{n-1}|\}.$$

Si  $\lambda$  est une racine de  $P$  (donc une valeur propre de  $C_P$ ) alors on a  $|\lambda| \leq R$ .

*Démonstration.* Soit  $v = (v_1, \dots, v_n)$  un vecteur propre associé à  $\lambda$  et  $v_k$  tel que le maximum des  $|v_i|$  est atteint pour  $i$  de 1 à  $n$ . Comme  $v$  est non nul (c'est un vecteur propre!), on a  $v_k \neq 0$ . En regardant l'égalité  $C_P v = \lambda v$  sur la  $k$ -ième coordonnée, on trouve

$$v_{k-1} - a_{k-1}v_n = \lambda v_k, \text{ si } k > 1, \text{ et } -a_0 v_n = \lambda v_k, \text{ si } k = 1.$$

Supposons  $k > 1$ . Il vient, en divisant par  $v_k$  et en utilisant l'inégalité triangulaire

$$|\lambda| \leq \left| \frac{v_{k-1}}{v_k} \right| + |a_{k-1}| \cdot \left| \frac{v_n}{v_k} \right| \leq 1 + |a_{k-1}| \leq R.$$

Le cas  $k = 1$  est analogue.  $\square$

On va maintenant développer une méthode, la méthode  $QR$ , qui permet d'approcher les valeurs propres d'une matrice.

**Théorème 100 :** Soit  $A \in \text{GL}_n(\mathbf{C})$  une matrice dont les valeurs propres sont de modules deux à deux distincts. On peut trouver une matrice inversible  $P \in \text{GL}_n(\mathbf{C})$  et des complexes  $\lambda_1, \dots, \lambda_n \in \mathbf{C}$  triés par modules décroissants tels que

$$A = P\Lambda P^{-1} \quad \text{avec} \quad \Lambda := \text{diag}(\lambda_1, \dots, \lambda_n).$$

De plus, on suppose que la matrice  $P$  admet une décomposition LU. Définissons la suite  $(A_k)_{k \in \mathbf{N}^*}$  de matrices de la manière suivante :

1. on pose  $A_1 = A$ ;
2. pour tout entier  $k \in \mathbf{N}^*$ , on pose  $A_{k+1} := R_k Q_k$  où le couple  $(Q_k, R_k)$  est la décomposition QR de la matrice  $A_k$ .

Alors

$$(A_k)_{i,i} \longrightarrow \lambda_i, \quad i \in \llbracket 1, n \rrbracket.$$

*Démonstration. Première étape : Égalités utiles.* Montrons d'abord, en effectuant une récurrence sur l'entier  $k \geq 1$ , que

$$A_{k+1} = \mathcal{Q}_k^* A \mathcal{Q}_k \quad \text{avec} \quad \mathcal{Q}_k := Q_1 \cdots Q_k. \quad (1)$$

Pour  $k = 1$ , comme  $A = Q_1 R_1$ , on a

$$A_2 = R_1 Q_1 = Q_1^* A Q_1 = \mathcal{Q}_1^* A \mathcal{Q}_1.$$

Maintenant, si la relation (1) est vraie pour un rang  $k \geq 1$ , alors

$$\begin{aligned} A_{k+2} &= R_{k+1} Q_{k+1} = Q_{k+1}^* A_{k+1} Q_{k+1} \\ &= Q_{k+1}^* \mathcal{Q}_k^* A \mathcal{Q}_k Q_{k+1} \\ &= \mathcal{Q}_{k+1}^* A \mathcal{Q}_{k+1}. \end{aligned}$$

Par ailleurs, on peut écrire

$$\begin{aligned} A^k &= Q_1 R_1 \times \cdots \times Q_1 R_1 \\ &= Q_1 \times R_1 Q_1 \times \cdots \times R_1 Q_1 \times R_1 \\ &= Q_1 \times A_2 \times \cdots \times A_2 \times R_1 \\ &= Q_1 \times Q_2 R_2 \times \cdots \times Q_2 R_2 \times R_1 = \cdots = \mathcal{Q}_k \mathcal{R}_k. \quad (2) \end{aligned}$$

*Deuxième étape : Une autre décomposition QR de la matrice  $A^k$ .* Notons  $P = QR$  et  $P^{-1} = LU$  les décompositions QR et LU des matrices  $P$  et  $P^{-1}$ . Pour tout entier  $k \in \mathbf{N}^*$ , on écrit alors

$$A^k = P\Lambda^k P^{-1} = QR \times \Lambda^k L\Lambda^{-k} \times \Lambda^k U.$$

Comme la matrice  $L$  est triangulaire inférieure de diagonale 1, on sait que

$$(\Lambda^k L\Lambda^{-k})_{i,j} = \begin{cases} 0 & \text{si } i < j, \\ 1 & \text{si } i = j, \\ (\lambda_i/\lambda_j)^k L_{i,j} & \text{si } i > j \end{cases}$$

et, avec les inégalités  $|\lambda_i/\lambda_j| < 1$ , on peut écrire

$$\Lambda^k L\Lambda^{-k} \longrightarrow I_n$$

Notons  $\Lambda^k L\Lambda^{-k} = I_n + F_k$  avec  $F_k \longrightarrow 0$ . Alors

$$R \times \Lambda^k L\Lambda^{-k} = R(I_n + F_k) = (I_n + RF_k R^{-1}) R.$$

Comme  $F_k \rightarrow 0$ , les matrices  $I_n + RF_k R^{-1}$  sont inversibles à partir d'un certain rang, donc elles admettent une unique décomposition QR

$$I_n + RF_k R^{-1} = \tilde{Q}_k \tilde{R}_k$$

Comme  $I_n + RF_k R^{-1} \rightarrow 0$ , en utilisant la compacité du groupe orthogonal et l'unicité de la décomposition QR, on montre que

$$\tilde{Q}_k \rightarrow I_n \quad \text{et} \quad \tilde{R}_k \rightarrow I_n.$$

Avec les différentes égalités et la relation (2), on peut écrire

$$\begin{aligned} A^k &= Q \times (I_n + RF_k R^{-1}) R \times \Lambda^k U \\ &= Q \tilde{Q}_k \tilde{R}_k R \Lambda^k U = \mathcal{Q}_k \mathcal{R}_k. \end{aligned}$$

Par ailleurs, on peut trouver une matrice diagonale  $D_k$  de coefficients diagonaux unitaires telle que la matrice  $D_k^{-1} \tilde{R}_k R \Lambda^k U$  soit de diagonale strictement positive. Par unicité de la décomposition QR, on obtient alors

$$Q \tilde{Q}_k D_k = \mathcal{Q}_k \quad \text{et} \quad D_k^{-1} \tilde{R}_k R \Lambda^k U = \mathcal{R}_k$$

*Conclusion* : Comme  $A = QR\Lambda R^{-1}Q^{-1}$ , l'égalité (1) donne alors

$$\begin{aligned} A_{k+1} &= (Q \tilde{Q}_k D_k)^* \times QR\Lambda R^{-1}Q^{-1} \times Q \tilde{Q}_k D_k \\ &= D_k^* \tilde{Q}_k^* R \Lambda R^{-1} \tilde{Q}_k D_k. \end{aligned}$$

Comme  $\tilde{Q}_k \rightarrow I_n$ , on obtient

$$\tilde{Q}_k^* R \Lambda R^{-1} \tilde{Q}_k \rightarrow R \Lambda R^{-1} = \begin{pmatrix} \lambda_1 & & (*) \\ & \ddots & \\ & & \lambda_n \end{pmatrix}.$$

Finalement, comme les matrices  $D_k$  sont diagonales, les diagonales des matrices  $A_{k+1}$  convergent vers la matrice  $\Lambda$ . □

Ainsi, si l'on part de notre polynôme  $P$  et qu'on applique la méthode  $QR$  à  $C_P$ , on voit apparaître les racines de  $P$  sur la diagonale de la limite de la suite  $(A_k)$  construite dans le théorème 100.

## Références

- [Ber20] Grégory BERHUY : *Algèbre : le grand combat, cours et exercices*. Mathématiques en devenir. Calvage & Mounet, Paris, 2e édition, 2020.
- [BMP05] Vincent BECK, Jérôme MALICK et Gabriel PEYRÉ : *Objectif agrégation : mathématiques*. H & K, Paris, 2e édition, 2005.
- [CG17] Philippe CALDERO et Jérôme GERMONI : *Nouvelles histoires hédonistes de groupes et de géométries*. Mathématiques en devenir. Calvage & Mounet, Paris, 2e édition, 2017.
- [Cia06] Philippe Gaston CIARLET : *Introduction à l'analyse numérique matricielle et à l'optimisation : cours et exercices corrigés*. Dunod, Paris, 2006.
- [FGN14] Serge FRANCINO, Hervé GIANELLA et Serge NICOLAS : *Exercices de mathématiques des oraux de l'École polytechnique et des écoles normales supérieures. Tome I, Algèbre*. Cassini, Paris, 3e édition, 2014.
- [Gou08] Xavier GOURDON : *Algèbre*. Les maths en tête. Ellipses, Paris, 2e éd édition, 2008.
- [Per96] Daniel PERRIN : *Cours d'algèbre*. CAPES-agrég mathématiques. Ellipses, Paris, 1996.
- [QQ17] Hervé QUEFFÉLEC et Martine QUEFFÉLEC : *Analyse complexe et applications : cours et exercices*. Mathématiques en devenir. Calvage & Mounet, Paris, 2017.
- [Rom19] Jean-Etienne ROMBALDI : *Éléments d'analyse réelle*. EDP sciences, Les Ulis, 2e édition édition, 2019.
- [Rom21] Jean-Étienne ROMBALDI : *Mathématiques pour l'agrégation : algèbre et géométrie*. De Boeck supérieur, Louvain-la-Neuve (Belgique) Paris, 2e éd édition, 2021.