144

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

Soit $\mathbb{K}$ un corps commutatif. A un anneau factoriel.

I. Définitions et premières propriétés.

1. Polynôme et racines de polynomes. [GOU] p.54

Def 1 : On appelle polynôme à coefficient dans $\mathbb{K}$ toute suite $P=(a_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ tous nuls à partir d'un certain rang.
Un tel polynôme P s'écrit $P=\sum_{n\in\mathbb{N}} a_n X^n$ où $X=(0,1,0,\dots 0,\dots)$
On note alors l'ensemble des polynômes à coefficients dans $\mathbb{K}$: $\mathbb{K}[X]$.

Def 2 : On appelle degré d'un polynôme $P=(a_n)_{n\in\mathbb{N}}$ le plus grand indice n tel que $a_n\neq 0$. On le note $\deg P$ (avec convention $\deg P=-\infty$ si $P=0$).

Ex 3 : $(1,0,2,1,0,\dots)=1+2X^2+X^3$ et est de degré 3.

Def 4 : On définit la division euclidienne de A par $B\neq 0$ sur $\mathbb{K}[X]$ par :
$$\exists!\, Q,R\in\mathbb{K}[X]^2 \ /\ A=QB+R \text{ avec } \deg R<\deg B.$$

Def 5 : Soit $P\in\mathbb{K}[X]$. On dit que $a\in\mathbb{K}$ est une racine de P si $P(a)=0$

Def 6 : Soit $P\in\mathbb{K}[X]$, $a\in\mathbb{K}$. On dit que a est une racine d'ordre h de P si $(X-a)^h\,|\,P$ et $(X-a)^{h+1}\nmid P$.

Ex 7 : $P(X)=(X-a)^2(X-b)$ ⇝ a et b racines de P de mult. 2 et 1.

Def 8 : Soit $P=a_0+a_1X+\dots+a_nX^n\in\mathbb{K}[X]$.
On appelle polynôme dérivé de P le polynôme $P'=a_1+2a_2X+\dots+na_nX^{n-1}$.

Théorème 9 : (Formule de Taylor)
Si car $\mathbb{K}=0$, tout polynôme P de $\mathbb{K}[X]$ de degré inférieur ou égal à n vérifie :
$$\forall a\in\mathbb{K}:\ P(X)=P(a)+\frac{(X-a)}{1!}P'(a)+\dots+\frac{(X-a)^n}{n!}P^{(n)}(a).$$

Conséquence 10 : Si car $\mathbb{K}=0$ et si $P\in\mathbb{K}[X]$, $P\neq 0$, alors $a\in\mathbb{K}$ est racine d'ordre h de P ssi :
(I) $\forall i,\ 0\leq i\leq h-1$: $P^{(i)}(a)=0$ (II) $P^{(h)}(a)\neq 0$.

Prop. 11 : Si $P\in\mathbb{K}[X]$ est de degré $n\geq 1$, alors P a au plus n racines (comptées avec leur ordre de multiplicité).

Rq 12 : Ce n'est pas vrai sur les anneaux en général, par ex : $\mathbb{Z}/4\mathbb{Z}[X]$.
$P(X)=2X$ a 2 racines : 0 et 2 alors que $\deg P=1$.

Def 13 : Un polynôme $P\in\mathbb{K}[X]$ est dit scindé sur $\mathbb{K}$ si on peut écrire
$$P=\lambda(X-a_1)^{h_1}\dots(X-a_r)^{h_r} \quad \text{avec } \lambda\in\mathbb{K},\ \forall i\in[\![1,r]\!]: a_i\in\mathbb{K},\ h_i\in\mathbb{N}^*.$$

Ex 14 : $P=(X^2-2)=(X-\sqrt{2})(X+\sqrt{2})$ scindé sur $\mathbb{R}$ mais pas sur $\mathbb{Q}$.

2. Fonctions symétriques élémentaires et polynômes. [GOU] p.60 [CVA] p.31.

Def 15 : Soit un polynôme $P=a_0X^n+a_1X^{n-1}+\dots+a_{n-1}X+a_n\in\mathbb{K}[X]$, $a_0\neq 0$, scindé sur $\mathbb{K}$ et dont les racines (comptées avec leur ordre de multiplicité) sont $x_1,\dots x_n$ (de sorte que $P=a_0(X-x_1)\dots(X-x_n)$).
On pose $\forall p\in[\![1,n]\!]$:
$$\sigma_p=\sum_{1\leq i_1<\dots<i_p\leq n} x_{i_1}\dots x_{i_p}$$
σ_p est appelé $p$ième fonction symétrique élémentaire en les racines de P.

Rq 16 : Pour le $P\in\mathbb{K}[X]$ de la def. 15, si on développe sa forme factorisé on obtient :
$$P=a_0(X-x_1)\dots(X-x_n)=a_0(X^n-(x_1+\dots+x_n)X^{n-1}+\dots+(-1)^n x_1\dots x_n)$$
$$=a_0(X^n-\sigma_1X^{n-1}+\dots+(-1)^n\sigma_n).$$

On en déduit donc :

Théorème 17 : Relation coefficients - racines.
Pour le $P\in\mathbb{K}[X]$ de la def. 15, on a :
$$\forall p\in[\![1,n]\!]:\ \sigma_p=(-1)^p\frac{a_p}{a_0}.$$

En particulier : $\sigma_1=\sum_{i=1}^n x_i=-\frac{a_1}{a_0}$ et $\sigma_n=\prod_{i=1}^n x_i=(-1)^n\frac{a_n}{a_0}$.

Ex 18 : Résolution dans $\mathbb{R}$ du système $\begin{cases} x+y+z=1 \\ x^2+y^2+z^2=11 \\ 1/x+1/y+1/z=-1 \end{cases}$ (E).

On a alors (E) $\Longleftrightarrow \begin{cases} \sigma_1 = 1 \\ \sigma_1^2 - 2\sigma_2 = 11 \\ \sigma_2 = -\sigma_3 \end{cases}$ Donc x, y, z sont les racines de : $X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3$.

Def 19 : Soit $P \in \mathbb{K}[X]_m$ scindé et unitaire de racines : $x_1, \dots x_m \in \mathbb{K}$.
On appelle <u>somme de Newton</u> :

$$k \in \mathbb{N} : \quad s_k(x_1, \dots x_m) := \sum_{i=1}^{m} x_i^k .$$

Prop. 20 : Soit $P \in \mathbb{K}[X]_m$ scindé unitaire de racines : $x_1, \dots x_m \in \mathbb{K}$.
Alors $\forall k \geq m$: $s_k + a_{m-1} s_{k-1} + \dots + a_1 s_{k-m+1} + a_0 s_{k-m} = 0$.

On appelle cette égalité : <u>Identité de Newton</u>.

II. Extension de corps. [Per] p. 60.

1. Irréductibilité.

Def. 21 : 2 polynômes $P, Q \in \mathbb{K}[X]$ sont associés s'$\exists \lambda \in \mathbb{K} \setminus \{0\}$ tel que $P = \lambda Q$.

Def. 22 : Un polynôme $P \in \mathbb{K}[X]$ est dit irréductible dans $\mathbb{K}[X]$ si P n'est pas constant et si ses seuls diviseurs dans $\mathbb{K}[X]$ sont les constantes non nulles et les polynômes associés à P.

Prop 23 : Soit $\begin{cases} P = a_m X^m + \dots + a_0 \in \mathbb{Z}[X] \\ p \in \mathbb{Z} \text{ un nombre premier.} \end{cases}$ avec $a_m \not\equiv 0 \mod p$.

On note $\bar{P}$ la réduction de $P \mod p\mathbb{Z}$.
Alors $\bar{P}$ irréductible dans $\mathbb{Z}/p\mathbb{Z} \Rightarrow P$ irréductible sur $\mathbb{Q}$.

De plus, on a l'équivalence :
P irréductible sur $\mathbb{Z} \Longleftrightarrow P$ irréductible sur $\mathbb{Q}$ avec $\mathrm{pgcd}_{i \in [\![1,m]\!]}(a_i) = 1$.

Ex 24 : $X^5 - 6X^3 + 2X^2 - 4X + 5$ est irréductible dans $\mathbb{Z}[X]$.

2. Définitions et propriétés sur les extensions de corps.

Def 25 : Si $\mathbb{L}$ et $\mathbb{K}$ sont des corps avec $\mathbb{K} \subset \mathbb{L}$ alors $\mathbb{L}$ est une extension de corps de $\mathbb{K}$.

Def 26 : Soit $\mathbb{K} \subset \mathbb{L}$ une extension et soit $\alpha \in \mathbb{L}$.
Soit $\varphi : \mathbb{K}[X] \to \mathbb{L}$, $P \mapsto P(\alpha)$.

(I) Si φ est injectif on dit que α est transcendant sur $\mathbb{K}$.
(II) Sinon, on dit que <u>α est algébrique sur $\mathbb{K}$</u>.
Dans ce cas $\exists P \in \mathbb{K}[X]$ unitaire / $\mathrm{Ker}\,\varphi = (P)$. $(P \neq 0)$.
On appelle alors P le polynôme minimal de α sur $\mathbb{K}$.

Def 27 : Une extension $\mathbb{K} \subset \mathbb{L}$ est dite algébrique si $\forall \alpha \in \mathbb{L}$, α algébrique sur $\mathbb{K}$.

Def 28 : Soit $\mathbb{K}$ un corps, $P \in \mathbb{K}[X]$ un polynôme irréductible.
Une extension $\mathbb{K} \subset \mathbb{L}$ est appelé corps de rupture de P sur $\mathbb{K}$ si $\mathbb{L} = \mathbb{K}(\alpha)$ avec $P(\alpha) = 0$.

Def 29 : Soit $P \in \mathbb{K}[X]$ de degré m. On appelle corps de décomposition de P sur $\mathbb{K}$ une extension $\mathbb{L}$ de $\mathbb{K}$ tel que :
(I) P est scindé sur $\mathbb{L}$.
(II) Les racines de P engendrent $\mathbb{L}$ sur $\mathbb{K}$ (càd $\mathbb{L}$ minimal qui vérifie (I)).

Ex 30 : $P(X) = X^4 - X^2 - 2 \in \mathbb{Q}[X]$.
On a $\begin{cases} \mathbb{Q}[X]/(X^2-2) = \mathbb{Q}(\sqrt{2}) \text{ corps de rupture de } P \text{ sur } \mathbb{Q}. \\ \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(i+\sqrt{2}) \text{ corps de décomposition de } P \text{ sur } \mathbb{Q}. \end{cases}$

Def 31 : Soit $\mathbb{L} = \mathbb{K}(\alpha)$ une extension de $\mathbb{K}$, et P le polynôme minimal de α. On appelle <u>degré de l'extension</u>, ou encore degré de α l'entier : $\dim_{\mathbb{K}} \mathbb{L} = [\mathbb{L} : \mathbb{K}] = \deg P$.

Prop. 32 : Soit $P \in \mathbb{K}[X]$ avec $\deg P = m > 0$. Alors P irréductible sur $\mathbb{K}$ <u>ssi</u> P n'a pas de racines dans les extensions $\mathbb{L}$ de $\mathbb{K}$ qui vérifient : $[\mathbb{K} : \mathbb{L}] \leq m/2$.

Def 33 : $\mathbb{K}$ est algébriquement clos si $\forall P \in \mathbb{K}[X]$, P est scindé dans $\mathbb{K}$.

Théorème 34 : (d'Alembert-Gauss) $\mathbb{C}$ est algébriquement clos.

III. Applications.

1. Réduction des matrices. [GOU] p. 162. [CVA] p. 33.

<u>Déf 35</u> : Soit $A \in M_n(\mathbb{K})$.
On appelle <u>polynôme caractéristique</u> de A le poly. de $\mathbb{K}[X]$:
$\chi_A(X) = \det(XI_n - A)$.

<u>Prop. 36</u> : λ est vp. de A <u>ssi</u> $\chi_A(\lambda) = 0$.

<u>Théorème 37</u> : Cayley-Hamilton : Soit $A \in M_n(\mathbb{K})$: $\chi_A(A) = 0_n$

<u>Prop 38</u> : On appelle <u>polynôme minimal</u> de $A \in M_n(\mathbb{K})$ le plus petit polynôme annulateur de A au sens de la divisibilité. On le note μ_A.

<u>Déf 39</u> : Soit $P = X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathbb{K}[X]$.
On note C_P sa matrice compagnon définie par $C_P = \begin{pmatrix} 0 & & 0 & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -a_{n-2} \\ 0 & & 1 & -a_{n-1} \end{pmatrix}$

<u>Prop. 40</u> : $\chi_{C_P}(X) = P(X) \in \mathbb{K}[X]$.

<u>Prop. 41</u> : Une matrice $A \in M_n(\mathbb{K})$ est trigonalisable <u>ssi</u> χ_A est scindé sur $\mathbb{K}$.

<u>Ex 42</u> : $A = \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}$ est trigonalisable sur $\mathbb{R}$.

<u>Prop. 42</u> : Soit $A \in M_n(\mathbb{K})$. On a alors :
χ_A scindé à racines simples dans $\mathbb{K} \Rightarrow A$ est diagonalisable.
μ_A scindé racine simple $\Leftrightarrow A$ diagonalisable.

<u>Prop. 43</u> : Pour $A \in M_n(\mathbb{K})$ on a : μ_A scindé racine simple $\Leftrightarrow A$ diagonalisable.

<u>Prop. 44</u> : Soit $A \in M_n(\mathbb{C})$ tel que $\mathrm{Tr}(A^k) = 0 \quad \forall 1 \leq k \leq n$.
Alors A est une matrice nilpotente. **DEV 1.**

<u>Rq 45</u> : La réciproque est vraie.

2. Localisation des racines / valeurs propres. [CVA] p. 52.

<u>Prop. 46</u> : Soit $P \in \mathbb{R}[X]$, unitaire de degré n.
On a : P scindé sur $\mathbb{R} \Leftrightarrow |\mathrm{Im}(z)|^n \leq |P(z)|$ pour tout $z \in \mathbb{C}$.

<u>Prop 47</u> : Soient $(P_k)_{k \geq 0}$ suite de polynômes unitaires de $\mathbb{C}[X]_n$.
P un polynôme unitaire de $\mathbb{C}[X]_n$.
Soient $\forall k \in \mathbb{N}$: $(\lambda_{k,i})_{1 \leq i \leq n}$ les racines de P_k.
$(\lambda_i)_{1 \leq i \leq n}$ les racines de P.
Alors $P_k \xrightarrow[k \to +\infty]{} P$ pour la topologie normique d'espace
$\Leftrightarrow \forall i \in [\![1,n]\!] : \lambda_{k,i} \xrightarrow[k \to +\infty]{} \lambda_i$. **DEV.2**

<u>Rq 48</u> : Si $(A_k)_{k \geq 0} \in M_n(\mathbb{K})$ converge $A \in M_n(\mathbb{K})$ alors les vp de A_k convergent vers les vp de A.

<u>Th. 49</u> : Soit $P = X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathbb{C}[X]$.
Soit $R = \max\{|a_0|, 1+|a_1|, 1+|a_2|, \dots 1+|a_{n-1}|\}$ appelée borne de Cauchy.
Alors si λ est racine de P : $|\lambda| \leq R$.

<u>Prop. 50</u> : Disques de Gershgorin.
Soit $A = (a_{ij})_{1 \leq i,j \leq n} \in M_n(\mathbb{C})$. On considère $\forall i \in [\![1,n]\!]$ le disque $D_i \subset \mathbb{C}$ de centre a_{ii} et de rayon $\sum_{i \neq j} |a_{ij}|$, appelé disque de Gershgorin.
Alors si λ est vp. de A, on a $\lambda \in \bigcup_{i \in [\![1,n]\!]} D_i$.

<u>Ex 51</u> : $A = \begin{pmatrix} 2i & 1 \\ 2 & -3i \end{pmatrix}$ a pour disques de Gershgorin : $D_1 = (2i, 1)$ et $D_2 = (-3i, 2)$
Donc A est inversible car $0 \notin D_1 \cup D_2$ donc 0 pas vp. de A.

3. Applications aux corps finis. [Per] p. 80

<u>Déf 52</u> : Le n-ième polynôme cyclotomique est donné par la formule :
$$\phi_n(X) = \prod_{\substack{\omega \text{ racine} \\ \text{primitive } n\text{-ième de } 1}} (X - \omega).$$

<u>Prop. 53</u> : On a la formule : $X^n - 1 = \prod_{d | n} \phi_d(X)$. **DEV.3**

<u>Théorème 54</u> : Kronecker.
Soit $\mathcal{P}$ l'ensemble des polynômes unitaires P de $\mathbb{Z}[X]$ tel que toute racine complexe z de P est de module $|z| \leq 1$.
Alors si $P(z) = 0$ avec $P \in \mathcal{P}$ alors soit $z = 0$, soit z est une racine de l'unité.

<u>Corollaire 55</u> : Soit $P \in \mathbb{Z}[X]$ unitaire, irréductible de $\mathbb{Z}$ tel que ttes les racines de P soit de module ≤ 1. Alors $P = X$ ou P est un polynôme cyclotomique.

<u>Déf 56</u> : Soit $\mathbb{F}$ un corps. Si $\mathbb{F}$ est fini on a car$(\mathbb{F}) = p$ un nombre premier.
De plus $q = |\mathbb{F}| = p^n$, $n \geq 1$. On note alors $\mathbb{F} = \mathbb{F}_q$ corps fini d'ordre q.

<u>Ex 57</u> : $\mathbb{F}_4 = \mathbb{F}_2[X] / (X^2 + X + 1) = \{0, 1, j, j^2\}$.

<u>Rq 58</u> : Soit $q = p^n$, p premier. Alors $\mathbb{F}_q$ est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

Developpement : Soit $A \in M_n(\mathbb{C})$, $tr(A^k) = 0 \ \forall k \in [\![1,n]\!] \Rightarrow A$ nilpotente

Soit $A \in M_n(\mathbb{C})$, $tr(A^k) = 0 \ \forall k \in [\![1,n]\!] \Rightarrow A$ nilpotente

. Montrons d'abord que A possede une valeur propre nulle.
On rappelle que $\forall A, B \in M_n(\mathbb{C})$, $Tr(BA) = Tr(AB)$ donc $\forall P \in GL_n(\mathbb{C})$ $Tr(PAP^{-1}) = Tr(A)$. $\mathbb{C}$ est algebriquement clos donc χ_A est scindé et A est donc semblable à une matrice triangulaire T. On a donc l'existence de $P \in GL_n(\mathbb{C})$ tel que $A = PTP^{-1}$ et $Tr(A) = Tr(T)$.
En trigonalisant A on obtient que $tr(A)$ est la somme des valeurs propres de A. De meme $A^k = PT^kP^{-1}$ donc $Tr(A^k) = Tr(T^k)$ donc $tr(A^k)$ est la somme des puissances kieme des valeurs propres de A donc des racines de χ_A. Soit λ_i, $i \in [\![1,n]\!]$ les racines de χ_A avec repetition
$tr(A^k) = \sum_{i=1}^{n} \lambda_i^k =: s_k(\lambda_1, \dots, \lambda_n)$
$\chi_A(X) = \prod_{i=1}^{n} (X - \lambda_i) = X^n + \sum_{k=1}^{n} (-1)^k e_k(\lambda_1, \dots, \lambda_n) X^{n-k}$ avec e_k les fonctions symetriques élementaires données par $e_k(\lambda_1, \dots, \lambda_n) = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} \lambda_{i_1} \times \dots \times \lambda_{i_k}$.
On evalue l'égalité en $X = \lambda_j$
$0 = \lambda_j^n + \sum_{k=1}^{n} (-1)^k e_k(\lambda_1, \dots, \lambda_n) \lambda_j^{n-k}$
On somme toutes les égalités obtenuent pour j de 1 à n
On obtient $0 = s_n(\lambda_1, \dots, \lambda_n) + \sum_{k=1}^{n} (-1)^k e_k(\lambda_1, \dots, \lambda_n) s_{n-k}(\lambda_1, \dots, \lambda_n)$ avec $s_0(\lambda_1, \dots, \lambda_n) = n$
D'apres l'hypothese $s_k(\lambda_1, \dots, \lambda_n) = 0 \ \forall k \in [\![1,n]\!]$
On obtient donc $0 = (-1)^n e_n(\lambda_1, \dots, \lambda_n) s_0(\lambda_1, \dots, \lambda_n) = n \, e_n(\lambda_1, \dots, \lambda_n)$ si n est non nul dans le corps Or $\mathbb{C}$ est de caracteristique 0 donc n est non nul.
On a donc $0 = e_n(\lambda_1, \dots, \lambda_n) = \lambda_1 \times \lambda_2 \times \dots \times \lambda_n$ donc il existe $i \in [\![1,n]\!]$ tel que λ_i est nulle. donc A admet une valeur propre nulle.

. Montrons par recurrence que A est nilpotente.
Pour $n = 1$ c'est vrai car A a une seule valeur propre qui est nulle donc elle est nilpotente.
Supposons que pour $n-1$ l'hypothese est vrai.
A possede une valeur propre nulle donc elle est semblabe à une matrice B triangulaire par blocs de blocs diagonaux (0) de taille 1 et A_{n-1} de taille $n-1$.
$B = \begin{pmatrix} \boxed{0} & * \cdots * \\ 0 & \\ \vdots & \boxed{A_{n-1}} \\ 0 & \end{pmatrix}$
D'apres les regles de calcul par blocs A^k est encore triangulaire par blocs pour tout k et ses blocs diagonaux sont (0) et A_{n-1}^k. On a donc $tr(A_{n-1}^k) = 0 \ \forall k \in [\![1,n-1]\!]$ donc d'apres l'hypothese A_{n-1} est nilpotente. Donc le determinant par blocs $\det(XId - B) = \begin{vmatrix} X & * \cdots * \\ 0 & \\ \vdots & |XId - A_{n-1}| \\ 0 & \end{vmatrix}$ implique que χ_A de A vaut $\chi_A = X \chi_{A_{n-1}} = X^n$ donc A est nilpotente d'apres Cayley-Hamilton.

Si il reste du temps on peut faire la reciproque:

On suppose A nilpotente d'indice m

On a X^m qui annule, le polynome minimal de A divise X^m

donc $\chi_A(X) = X^n$ donc A n'a que des valeurs propres nulles

donc $\forall k \in [\![1, n]\!] : Tr(A^k) = 0$.

Compl. ...

Énoncé : Soient $\left|\begin{array}{l}(P_k)_{k\geq 0} \text{ une suite de polynômes unitaires de } \mathbb{C}[X]_n. \\ P \text{ un polynôme unitaire de } \mathbb{C}[X]_n\end{array}\right.$

Soient $\left|\begin{array}{l}\forall k \in \mathbb{N} : (\lambda_{k,i})_{1\leq i\leq n} \text{ les racines de } P_k. \\ (\lambda_i)_{1\leq i\leq n} \text{ les racines de } P.\end{array}\right.$

On va Mq : $P_k \xrightarrow[k\to+\infty]{} P$ pour la topo. normique d'espace $\Leftrightarrow$ $\forall i \in [\![1,n]\!] : \lambda_{k,i} \xrightarrow[k\to+\infty]{} \lambda_i$
(càd coef. vers coef.)

($\Leftarrow$) Supp. que $\forall i \in [\![1,n]\!] : \lambda_{k,i} \xrightarrow[k\to+\infty]{} \lambda_i$

On sait, comme P_k est unitaire dans $\mathbb{C}[X]_n$, que son coeff. en X^{n-m} pour $m \in [\![1,n]\!]$ est :

$$\underbrace{e_{k,m} = \sum_{1\leq i_1<\ldots<i_m\leq n} \prod_{s=1}^{m} \lambda_{k,i_s}}. \quad \text{par la relat}^\circ \text{ coeff.-racines.}$$

Or :

$$\xrightarrow[k\to+\infty]{} \sum_{1\leq i_1<\ldots<i_m\leq n} \prod_{s=1}^{m} \lambda_{i_s} = e_m \quad \text{d'après notre hypothèse.}$$

De plus, e_m est le coeff en X^{n-m} $(m\in[\![1,n]\!])$ de P.

Donc $P_k \xrightarrow[k\to+\infty]{} P$.

($\Rightarrow$) Supposons que $P_k \xrightarrow[k\to+\infty]{} P$. (tjrs pour la topo. normique d'espace).

Étape 1 : $\forall k\in\mathbb{N}$, $\exists i_k \in [\![1,n]\!]$ qui minimise $|\lambda_1 - \lambda_{k,i_k}|$.

$$\Rightarrow \quad 0 \leq |\lambda_1 - \lambda_{k,i_k}|^n \leq \prod_{i=1}^{n} |\lambda_1 - \lambda_{k,i}| = |P_k(\lambda_1)| \underset{\text{par hypoth.}}{\xrightarrow[k\to+\infty]{}} |P(\lambda_1)| = 0 \text{ car } \lambda_1 \text{ racine de } P.$$

On a donc qu'ainsi définit : $\lambda_{k,i_k} \xrightarrow[k\to+\infty]{} \lambda_1$.

On ré-ordonne désormais les racines de chaque P_k de sorte que $\forall k\in\mathbb{N}$: λ_{k,i_k} soit remplacé par $\lambda_{k,1}$.

Étape 2 : On peut par l'étape 1 écrire, $\forall k\in\mathbb{N}$: $\left|\begin{array}{ll}P_k = (X-\lambda_{k,1})\,Q_k(X) & \text{avec } Q_k(X)\in\mathbb{C}[X]_{n-1} \text{ unitaire.} \\ P = (X-\lambda_1)\,Q(X) & \text{avec } Q(X)\in\mathbb{C}[X]_{n-1} \text{ unitaire.}\end{array}\right.$

On note, $\forall k\in\mathbb{N}$, les coeff. de P_k en X^m : $a_{k,m}$, $m\in[\![1,n]\!]$.

$$\rightsquigarrow \quad P_k(X) = X^n + a_{k,n-1}X^{n-1} + a_{k,n-2}X^{n-2} + \ldots + a_{k,1}X + a_{k,0}.$$

De m̂, on note les coeffs de P en X^m : a_m.
Q_k — : $b_{k,m}$
Q — : b_m.

On va Mq $Q_k \xrightarrow[k\to+\infty]{} Q$. (tjrs pour la topo. normique d'espace)

Grâce à l'égalité : $P_k(X) = (X-\lambda_{k,1})\,Q_k(X)$ on a :

$$a_{k,m} = b_{k,m-1} - \lambda_{k,1}\, b_{k,m}$$

$$\Rightarrow b_{k,m-1} = a_{k,m} + \lambda_{k,1}\, b_{k,m}. \quad (*)$$

On a donc, en remarquant que $a_{k,n}=1$ et $b_{k,n}=0$:

$$b_{k,m} = a_{k,m+1} + \lambda_{k,1} b_{k,m+1}.$$

$$\overset{(*)}{=} a_{k,m+1} + \lambda_{k,1}\left(a_{k,m+2} + \lambda_{k,1} b_{k,m+2}\right).$$

$$= \dots$$

$$= a_{k,m+1} + \lambda_{k,1} a_{k,m+2} + \lambda_{k,1}^{2} a_{k,m+3} + \dots + \lambda_{k,1}^{n-m-2} a_{k,n-1} + \lambda_{k,1}^{n-m-1} \underbrace{b_{k,n-1}}_{= \underset{1}{a_{k,n}} + \lambda_{k,1} \underset{0}{b_{k,n}}}.$$

De même, par l'égalité : $P(X) = (X-\lambda_1)Q(X)$

$$b_m = a_{m+1} + \lambda_1 a_{m+2} + \dots + \lambda_1^{n-m-2} a_{n-1} + \lambda_1^{n-m-1}$$

Or comme par hypoth. : $P_k \underset{k\to+\infty}{\to} P$ alors $\forall m \in [\![1,n]\!] : a_{k,m} \to a_m$.

et par l'étape 1 : $\lambda_{k,1} \underset{k\to+\infty}{\to} \lambda_1$.

On a donc $\forall m \in [\![1,n]\!] : b_{k,m} \underset{k\to+\infty}{\to} b_m$

Donc $Q_k \underset{k\to+\infty}{\to} Q$.

* Étape 3 : On va montrer le résultat par récurrence sur le degré :

H.R : " Si $P_k \underset{k\to+\infty}{\to} P$ alors quitte à réordonner les racines $\lambda_{k,i}$ de P_k : $\lambda_{k,i} \underset{k\to+\infty}{\to} \lambda_i \ \forall i \in [\![1,n]\!]$ ".

• $n=1$: On a $P(X) = X - a$ $a \in \mathbb{C}$.
et $P_k(X) = X - a_k$ avec $a_k \in \mathbb{C}\ \forall k \geq 0$ et $a_k \underset{k\to+\infty}{\to} a$ par hypoth. ($P_k \to P$ pour la topo. norm. d'espace).

Donc comme a_k seule racine de P_k et a seule racine de P on a le résultat voulu.

• Supposons l'H-R. vraie au rg n.

Soit $P_k \in \mathbb{C}_{n+1}[X]$ / $P_k \underset{k\to+\infty}{\to} P \in \mathbb{C}_{n+1}[X]$.

On peut par l'étape 1 réordonner les racines de P_k de sorte que $\lambda_{k,1} \underset{k\to+\infty}{\to} \lambda_1$.

Ainsi : $\begin{cases} P_k(X) = (X-\lambda_{k,1})Q_k(X) & \text{avec } Q_k \in \mathbb{C}_n[X] \text{ unitaire et } Q_k \underset{k\to+\infty}{\to} Q. \\ P(X) = (X-\lambda_1)Q(X). & Q \in \mathbb{C}_n[X] \text{ unitaire} \end{cases}$

Donc par H-R, quitte à réordonner les racines que Q_k, on a que : $\mathrm{rac}(Q_k) \underset{k\to+\infty}{\to} \mathrm{rac}(Q)$.

Or comme les racines de P_k, resp. P sont : $(\lambda_{k,1}, \mathrm{rac}(Q_k))$, resp. $(\lambda_1, \mathrm{rac}(Q))$, on a bien que $\forall i \in [\![1,n+1]\!] : \lambda_{k,i} \underset{k\to+\infty}{\to} \lambda_i$.

Rq : * Pour les matrices : Si $A_k \underset{k}{\to} A$, $A_k, A \in M_n(\mathbb{C})$ alors $\overset{\text{vp de } A_k}{\lambda_{k,i}} \to \lambda_i \leftarrow$ vp de A.

En effet, $M \mapsto \chi_M$ est C^0 (CVA p.47).

$\Rightarrow \chi_{A_k} \underset{k\to+\infty}{\to} \chi_A$ $\Rightarrow$ en réordonnant : $\lambda_{k,i} \to \lambda_i \ \forall i \in [\![1,n]\!]$

poly. unitaire de $\mathbb{C}_n[X]$.

* Pour le cas $\mathbb{K} = \mathbb{R}$ il y a une méthode plus simple / plus courte p. 57 CVA.

Développement 3: Théorème de Kronecker Réf: CVA p. 35

Théorème: Soit $\mathcal{P}$ l'ensemble des polynômes unitaires P de $\mathbb{Z}[X]$ dont les racines (complexes) z sont de module $|z| \leq 1$. Alors si $P(z)=0$ avec $P \in \mathcal{P}$

On a:
* soit z est nul
* soit z est une racine de l'unité.

Démonstration: Afin de montrer ce résultat, nous allons procéder en plusieurs étapes:

① On considère l'ensemble $\mathcal{P}_n = \{P \in \mathcal{P} / \deg(P) = n\}$ où $n > 0$; On montre que le coefficient a_k en X^k d'un tel polynôme vérifie $|a_k| \leq \binom{n}{k}$. Ceci prouvera que $\mathcal{P}_n$ est fini.

② On considère ensuite l'ensemble R_n, constitué des racines des éléments de $\mathcal{P}_n$. On montre que $\chi_{C_p^m} \in \mathcal{P}_n$ $\forall m \in \mathbb{N}$, ce qui implique que si $z \in R_n$ alors $z^m \in R_n$ pour tout m de $\mathbb{N}$.

. Etape 1 Soit $P \in \mathcal{P}_n$. $P = a_0 + a_1 X + a_2 X^2 + \dots a_{n-1} X^{n-1} + X^n$

Le polynôme P a n racines complexes, notons les $z_1, z_2, \dots z_n$.

P se factorise de la façon suivante: $P(X) = (X - z_1) \times (X - z_2) \times \dots \times (X - z_n)$

C'est ici que la relation coefficient-racine intervient:

P est unitaire alors $\forall k \in [\![1, n]\!]$ $\sigma_k = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} z_{i_1} \times \dots z_{i_k}$

De plus $a_{n-k} = (-1)^k \sigma_k$, l'inégalité triangulaire nous donne: $|a_{n-k}| \leq \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} |z_{i_1} \times \dots z_{i_k}| \leq \sum_{1 \leq i_1 < i_2 < \dots \leq i_k \leq n} 1$

Cette somme représente le nombre de parties à k éléments dans un ensemble à n éléments.

D'où $|a_k| \leq \binom{n}{n-k} = \binom{n}{k}$. Les coefficients de P sont donc bornés et puisqu'ils sont entiers, il y en a un nombre fini donc $\mathcal{P}_n$ est fini.

Etape 2 : Puisque $\mathcal{P}_n$ est fini alors l'ensemble $\mathcal{R}_n$ l'est aussi. Montrons que pour $P \in \mathcal{P}_n$, $\chi_{C_P^m} \in \mathcal{P}_n$.

* $\chi_{C_P^m}$ est unitaire et de degré n car C_P^m est dans $\mathcal{M}_n(\mathbb{Z})$.
* Le spectre d'un polynôme en une matrice est donné par les valeurs propres de cette matrice sous certaines conditions :

H2G2 p172 $\left\{\right.$ Si $Q \in \mathbb{C}[X]$, $A \in \mathcal{M}_n(\mathbb{Z})$, Alors le spectre de $Q(A)$ est l'ensemble des $Q(\lambda)$ où λ parcourt les valeurs propres de A.

Ainsi en choisissant $Q = X^m$ et $A = C_P$, on voit que le spectre de $Q(A) = C_P^m$ est décrit par les z^m, où z est racine de P.
Donc toutes ses racines sont de module inférieur à 1, d'où $\chi_{C_P^m} \in \mathcal{P}_n$, et $z^m \in \mathcal{R}_n$ pour tout m dans $\mathbb{N}$.

Conclusion Puisque $\mathcal{R}_n$ est fini, l'application : $\varphi_z : \begin{array}{l} \mathbb{N}^* \longrightarrow \mathcal{R}_n \\ m \longmapsto z^m \end{array}$ (où $z \in \mathcal{R}_n$) n'est pas injective. On a alors l'existence de deux entiers distincts m et m' tels que $z^m = z^{m'}$.

Ceci prouve le résultat :
* soit $z = 0$
* soit $z^{m-m'} = 1$ $(m > m')$.

<u>Corollaire:</u> Soit $P \in \mathbb{Z}[X]$, unitaire et irréductible sur $\mathbb{Z}$ et à racines de module ≤ 1. Alors $P = X$ ou P est un polynôme cyclotomique.

<u>Démonstration:</u> Supposons $P \neq X$. Puisque P est irréductible, on en déduit que $P(0) \neq 0$. D'après le théorème de Kronecker, les racines de P sont racines de l'unité. Ainsi il existe $N \in \mathbb{N}^*$ tel que $\forall z$ racine de P : $z^N - 1 = 0$. De plus P est à racines simples, sinon il ne serait pas irréductible. Ainsi $P / X^N - 1$

Or $X^N - 1 = \prod_{d/N} \phi_d$ est la décomposition en facteurs irréductibles de $X^N - 1$ dans $\mathbb{Z}[X]$. Puisque P est irréductible, on a alors $P = \phi_d$ où d/N.