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

Mohamed NASSIRI

Les polynômes sont un excellent outil formel avec lequel on peut faire des calculs. Comme pour les nombres premiers, l'idée va être de donner une décomposition "atomique" des polynômes. Pour cela, on aura besoin de trouver les racines de P. Cependant, la tâche va être compliquée par la dépendance du corps où l'on étudie les polynômes ... Par exemple, X^2+X+1 est irréductible sur $\mathbb{F}_2$ (il n'a pas de racine dans ce corps donc on ne peut pas le factoriser en produit de deux polyômes de degré 1 ...) et pourtant sur $\mathbb{C}$, $X^2+X+1=(X-j)(X-\overline{j})$ ...

Pour savoir si un polynôme est irréductible (et donc s'il est (in)utile de chercher des racines), deux critères intéressants méritent d'être mis en avant : le critère d'Eisenstein et le critère de "réduction modulo". Par de la simple arithmétique, ils permettent de dire si un polynôme est irréductible.

Une autre approche va être de regarder, pour un polynôme $P \in K[X]$, les extensions du corps K où P admet une racine. De là va émerger la notion de *corps de rupture*. Par exemple, pour $P(X)=X^3-2 \in \mathbb{Q}[X]$, on va se placer dans l'extension $\mathbb{Q}(\sqrt[3]{2})$ et constater que P a bien une racine dans cette extenstion (c'est $\sqrt[3]{2}$ ...) Mais manque de bol, il manque des racines ... : $j\sqrt[3]{2}$ et $\overline{j}\sqrt[3]{2}$

Précedemment, on a "cassé" notre polynôme mais pas "totalement décomposé". L'autre idée est de regarder, pour un polynôme $P \in K[X]$, une ou des extensions du corps K où P sera totalement scindé. On parle de *corps de décomposition*. Pour notre précédent exemple, le corps de décomposition de X^3-2 est $\mathbb{Q}(j, \sqrt[3]{2})$.

Dernière petite remarque, un corps de décomposition est a priori différent d'un corps de rupture comme on a pu le voir par l'exemple précédent. Cependant, pour les corps finis, cette notion coïncide ...

L'introduction des polynômes symétriques va nous permettre de mettre en avant des relations entre les racines d'un polynôme et ses coefficients.

Une des étapes dans la recherche de racines est leur localisation et les méthodes approchées pour déterminer leur valeur. On peut évoquer notamment les disques de Gershgorin appliquée à la matrice compagnon, le théorème de Gauss-Lucas, et la méthode de Newton.

Références

[GOZ] Théorie de Galois, Ivan Gozard ♠
[GOUal] Les maths en tête : Algèbre, Xavier Gourdon
[ROU] Petit guide de calcul différentiel, François Rouvière
[FGNal1] Algèbre 1 Oraux X-ENS, Serge Francinou, Hervé Gianella et Serge Nicolas ♠

Développements

Existence et unicité des corps finis
Théorème de Gauss-Lucas

1 Racines de polynômes

1.1 Racines et irréductibilité [GOZ] p.8 → 12

Définition 1 *Soit A un anneau. Un polynôme $P \in A[X]$ est dit irréductible dans $A[X]$ si et seulement si son dégré est supérieur ou égal à 1 et ses seuls diviseurs dans $A[X]$ sont les polynômes uP où $u \in A^*$ et les élements de A^**

Définition 2 *Soit k un sous-corps d'un corps K et $P \in k[X]$. Une racine (ou un zéro) de P dans K est un élément $\alpha \in K$ tel que $P(\alpha)=0$.*
La multiplicité de α comme racine de P est le plus grand $n \in \mathbb{N}$ tel que $(X-a)^n$ divise $P(X)$ dans $K[X]$.

Proposition 3 *(i) Tout polynôme de degré 1 est irréductible.*
(ii) Tout polynôme irréductible de degré >1 n'a pas de racine dans K.
(iii) La réciproque de (ii) est fausse.
(iv) Toutefois la réciproque de (ii) est vraie pour les polynômes de degré 2 ou 3.

Proposition 4 *Soit $P(X)=a_nX^n+...+a_1X+$*

$a_0 \in \mathbb{Z}[X]$ *avec* $a_n \neq 0$ *et* $a_0 \neq 0$. *Si le rationnel* α *est zéro de* $P(X)$, *en notant* $\alpha = p/q$ *(avec* $(p,q) \in \mathbb{Z}^* \times \mathbb{N}^*$ *et* $pgcd(p,q) = 1$*), alors* $p|a_0$ *et* $q|a_n$.

Définition 5 *Soit* A *un anneau factoriel. Pour tout polynôme non nul* $P \in A[X]$, *on appelle contenu de* P *et on note* $c(P)$, *le pgcd des coefficients de* P.
P *est dit primitif si et seulement si* $c(P) = 1$.

Proposition 6 *(i) Le produit de deux polynômes primitifs est primitif.*
(ii) $\forall (P,Q) \in (A[X]\backslash\{0\})^2,\ c(PQ) = c(P)c(Q)$.

Théorème 7 *Soient* A *un anneau factoriel,* K=*Frac(A) le corps des fractions de* A *et* $P \in A[X]$ *de degré supérieur ou égal à 1.*
P *est irréductible dans* $A[X]$ *si et seulement si* P *est irréductible dans K[X] et* $c(P) = 1$.

Théorème 8 *Critère d'Eisenstein : Soient* A *un anneau factoriel,* K=*Frac(A) le corps des fractions de* A *et* $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ *de degré* $n \geq 1$.
On suppose qu'il existe un élément p *irréductible de* A *tel que :*

$$(i)\ p \nmid a_n \quad , \quad (ii)\ p \mid a_0, ..., a_{n-1} \quad , \text{et} \quad (iii)\ p^2 \nmid a_0$$

Alors P *est irréductible dans K[X].*

Application 9 *Pour tout* p *premier, le polynôme* $\Phi_{p,\mathbb{Q}}(X) = \sum_{i=0}^{p-1} X^i$ *est irréductible dans* $\mathbb{Z}[X]$.

Théorème 10 *Soient* A *un anneau factoriel,* K=*Frac(A) le corps des fractions de* A *et* $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ *de degré* $n \geq 1$.
Soient I *un idéal premier de* A, $B = A/I$ *l'anneau quotient (qui est donc intègre) et* L=*Frac(B) le corps des fractions de* B. *On suppose que* $a_n \notin I$.
Si le réduit $\overline{P}$ *de* P *modulo* I *est irréductible dans L[X], alors* P *est irréductible dans K[X].*

Exemple 11 *Avec* $A = \mathbb{Z}$, $I = (p)$ *où* p *est un nombre premier, alors* $K = \mathbb{Q}$ *et* $B = \mathbb{F}_p = L$, *on a, par exemple, que* $P(X) = X^3 - 127X^2 + 3608X + 19$ *est irréductible dans* $\mathbb{Z}[X]$ *(*$p = 2$*).*

1.2 Racines et polynômes symétriques [GOU] p.78

Définition 12 *Soit* A *un anneau commutatif unitaire. Un polynôme* $P \in A[X_1, ..., X_n]$ *est dit symétrique si pour tout* $\sigma \in \mathcal{S}_n$, $P(X_{\sigma(1)}, ..., X_{\sigma(n)}) = P(X_1, ..., X_n)$.

Exemple 13 *Dans* $\mathbb{R}[X,Y,Z]$, P=XY+YZ+ZX *est symétrique.*

Définition 14 *On appelle polynômes symétriques élémentaires de* $A[X_1, ..., X_n]$ *les polynômes notés* Σ_p $(1 \leq p \leq n)$ *et définis par*

$$\Sigma_p = \Sigma X_1 ... X_p = \Sigma_{i_1 < ... < i_p} X_{i_1} ... X_{i_p}$$

Exemple 15 $\Sigma_1 = \Sigma X_1 = X_1 + ... + X_n$
$\Sigma_2 = \Sigma X_1 X_2 = \Sigma_{i<j} X_i X_j$
$\Sigma_n = X_1 ... X_n$

Théorème 16 (admis) *Soit* $P \in A[X_1, ..., X_n]$ *un polynôme symétrique. Alors il existe un unique polynôme* $\Phi \in A[X_1, ..., X_n]$ *tel que* $P = \Phi(\Sigma_1, ..., \Sigma_n)$.

Exemple 17 *Dans* $A[X_1, ..., X_n]$, $\Sigma X_1^2 = \Sigma_1^2 - 2\Sigma_2^2$.

Proposition 18 *Relation coefficients/racines :*
Si $P(X) = (X - a_1)...(X - a_n)$, *alors*

$$P(X) = X^n + \sum_{i=1}^{n} (-1)^i \Sigma_i(a_1, ...a_n) X^{n-i}$$

Proposition 19 *Formules de Newton*

Application 20 *Trace de nilpotent*

2 Extensions algébriques et polynôme minimal [GOZ] p.30 → 33

Définition 21 *Soit* K *un corps, et* L *une extension de* K. *Pour* $a \in L$, *on considère le morphisme de* K*-algèbres suivant :*

$$\begin{aligned} ev_a : K[X] &\to L \\ P(X) &\mapsto P(a) \end{aligned}$$

- Si ev_a *est injective,* a *est dit algébrique sur* K,
- Sinon, a *est dit transcendant sur* K

Théorème 22 *Si* a *est transcendant :*
(i) L'application

$$\begin{aligned} \widetilde{ev_a} : K(X) &\to K(a) \\ f(X) = \frac{P(X)}{Q(X)} &\mapsto f(a) = P(a)Q(a)^{-1} \end{aligned}$$

est un ismorphisme de K*-algèbres.*
(ii) $[K(a) : K] = +\infty$

Remarque 23 *Pour le reste de cette partie, on suppose que* a *est algébrique.*

Définition 24 $K[X]$ *étant principal,* $\mathrm{Ker}(ev_a)$ *est un idéal principal de* $K[X]$ *engendré par un unique polynôme* $\pi_{a,K}(X) \in K[X]$ *appelé polynôme minimal de* a *sur* K.

Proposition 25 *(i) Soit* $P(X) \in K[X]$. *(*P *est le polynôme minimal de* a*)* $\Leftrightarrow$ *(*$P(X)$ *est unitaire,* $P(a)$=0 *et pour tout polynôme* $R(X) \in K[X]\backslash\{0\}$ *vérifiant* $R(a)$=0, *on a* $\deg(P) \leq \deg(R)$*).*
(ii) Soit $P(X) \in K[X]$. *(*P *est le polynôme minimal de* a*)* $\Leftrightarrow$ *(*$P(X)$ *est unitaire,* $P(a)$=0 *et le polynôme* $P(X)$ *est irréductible dans* $K[X]$*).*

Exemple 26 *Soient $n \in \mathbb{N}^*$ et $\alpha = 2^{1/n}$. On a $\pi_{\alpha,\mathbb{Q}}(X) = X^n - 2$.*

Proposition 27 *En notant $m = \deg(\pi_{a,K}(X))$, alors la famille $(a^i)_{i\in[\![0,m-1]\!]}$ est une base de K[a] en tant que K-e.v.*

Proposition 28 *(i) K(a)=K[a]*
(ii) Soit L une extension de K. Si $a \in L^*$ est algébrique sur K, alors $a^{-1} \in K[a]$
(iii) L'application

$$K(X)/(\pi_{a,K}(X)) \to K(a)$$
$$\overline{P(X)} \mapsto P(a)$$

est un ismorphisme de K-algèbres.

3 Adjonction de racines

3.1 Corps de rupture [GOZ] p.57→59

Définition 29 *Soient K un corps et $P \in K[X]$ un polynôme irréductible dans K[X]. On dit que le corps L est un corps de rupture de P si et seulement si L est une extension simple de K engendré par K et une racine, notée α, de P.*

Exemple 30 *$\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de $P(X) = X^3 - 2$.*

Théorème 31 *Soient K un corps et $P \in K[X]$ un polynôme irréductible dans K[X].*
(i) Il existe un corps de rupture de P.
(ii) Si $L = K(\alpha)$ et $L' = K(\beta)$ sont deux corps de rupture de P, alors L et L' sont K-isomorphes

Corollaire 32 *Soient K un corps et $P \in K[X]$ un polynôme de degré $n \geq 1$. Il existe une extension algébrique simple L de K dans laquelle P possède (au moins) une racine.*

Proposition 33 *Soit $P \in K[X]$ un polynôme de degré $n \geq 1$. P(X) est irréductible dans K[X] si et seulement si P(X) n'a pas de racine dans les extensions L de K telles que $[L : K] \leq n/2$.*

Exemple 34 *X^4+X+1 est irréductible sur $\mathbb{F}_2$ car il n'a pas de racines dans $\mathbb{F}_2$, ni $\mathbb{F}_4$.*

Proposition 35 *Soient $P \in K[X]$ un polynôme irréductible de degré $n \geq 1$ et L une extension de degré m de K avec pgcd(m,n)=1. Alors P(X) est irréductible dans L[X].*

Exemple 36 *$X^3 + X + 1$ est irréductible sur $\mathbb{Q}(i)$ comme sur $\mathbb{Q}$.*

3.2 Corps de décomposition [GOZ] p.59-60

Théorème 37 *Soient K un corps, E une extension de K et $P \in K[X]$ un polynôme de degré $n \geq 1$. On dit que E est un corps de décomposition de P sur K si et seulement si :*
(i) $\exists a \in E$ et $(\alpha_1, ..., \alpha_n) \in E^n$ tel que, dans E[X], $P(X) = a(X - \alpha_1)...(X - \alpha_n)$
(ii) $E = K(\alpha_1, ..., \alpha_n)$

Exemple 38 • *$\mathbb{C} = \mathbb{R}(i)$ est le corps de décomposition sur $\mathbb{R}$ de $X^2 + 1$*
• *$\mathbb{Q}(\sqrt{2})$ est le corps de décomposition sur $\mathbb{R}$ de $X^2 - 2$*

Théorème 39 (admis) *Soient K un corps et $P \in K[X]$ un polynôme de degré $n \geq 1$.*
(i) Il existe un corps de décomposition Σ de P sur K, avec $[\Sigma : K] \leq n!$
(ii) Si Σ et Σ' sont deux corps de décomposition de P sur K, alors ils sont K-isomorphes

3.3 Corps algébriquement clos [GOZ] p.62-63

Proposition-Définition 40 *Soit K un corps. Les conditions suivantes sont équivalentes :*
(i) Tout polynôme de degré ≥ 1 de K[X] est scindé sur K ;
(ii) Tout polynôme de degré ≥ 1 de K[X] admet au moins une racine dans K ;
(iii) Les seuls polynômes irréductibles de K[X] sont ceux de degré 1 ;
(iv) Toute extension algébrique de K est identique à K lui-même.
On dit alors que K est algébriquement clos.

Exemple 41 *$\mathbb{Q}$ et $\mathbb{R}$ ne sont pas algébriquement clos*

Proposition 42 *Tout corps algébriquement clos est infini.*

Théorème 43 *Théorème de D'Alembert-Gauss :*
$\mathbb{C}$ est algébriquement clos.

Corollaire 44 • *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*
• *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 qui n'ont pas de racine réelle.*

3.4 Corps finis [GOZ] p.85→87

Théorème 45 ♠ *Existence et unicité des corps finis* ♠
Soit p un nombre premier et $n \in \mathbb{N}^*$. On note $q = p^n$.
(1) *Il existe un unique corps fini à q éléments. Il est*

le corps de décomposition sur $\mathbb{F}_p$ de $X^q - X$. On le note $\mathbb{F}_q$
(2) $\mathbb{F}_q = \mathbb{F}_p[X]/(\pi)$, où π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$.
(3) Si π est un polynôme irréductible de degré n sur $\mathbb{F}_p$, alors $\pi(x) \mid X^q - X$ dans $\mathbb{F}_p[X]$, donc est scindé sur $\mathbb{F}_q$.

Remarque 46 *L'assertion (3) se traduit par le fait que, dans les corps finis, le corps de rupture est égal au corps de décomposition.*

Exemple 47 $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$.
Comme j est racine de $X^2 + X + 1$, on a

$$\mathbb{F}_4 = \mathbb{F}_2(j) = \{0, 1, j, j^2 = 1 + j\}$$

4 Localisation de racines

4.1 Règle de Cauchy [GOUal] p.83-84

Proposition 48 *Soit $P = X^n + a_1 X^{n-1} + ... + a_{n-1}X + a_n \in \mathbb{C}[X]$. On note $\rho \geq 0$ le plus grand des modules des racines de P, et on suppose que les a_i ne sont pas tous nuls, de sorte que $\rho \neq 0$. Alors*

$$\rho \leq \sup\left\{1, \sum_{i=1}^{n} |a_i|\right\}$$

Corollaire 49 *Sous les mêmes hypothèses que précedemment, on a*

$$\rho \leq 1 + \sup_{1 \leq i \leq n} |a_i|$$

4.2 Théorème de Gauss-Lucas [FGNal1] p.229 →231

Théorème 50 *Théorème de Gauss-Lucas*
♠ *Soit $P \in \mathbb{C}[X]$ un polynôme non constant. Les racines de P' sont dans l'enveloppe convexe des racines de P.*

Application 51 *Le plus grand entier n tel que les racines non nulles de $(X+1)^n - X^n - 1$ soient de module 1 est 7.*

Application 52 *Soit $P \in \mathbb{C}[X]$ un polynôme non constant, Δ une droite du plan complexe, H_1 et H_2 les deux demi-plans ouverts limités par Δ. On suppose que P' a une racine dans H_1. Alors $P(H_1) = \mathbb{C}$.*

4.3 Méthode de Newton [ROU] p.140 → 143

Théorème 53 • *Soit $f : [c, d] \to \mathbb{R}$, une fonction de classe C^2, telle que $f(c) < 0 < f(d)$, et $f'(x) > 0$, $\forall x \in [c, d]$.*
Soit a l'unique solution de $f(x) = 0$ et $F(x) = x - f(x)/f'(x)$.
Alors pour $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$, $\exists \alpha > 0$ tel que $I =]a - \alpha, a + \alpha[$ soit stable par F et $\forall x_0 \in I$, (x_n) converge à l'ordre 2 vers a.
• *De plus, si f est convexe, $\forall x_0 \in [a, d]$, la méthode converge et on a :*

$$0 \leq x_{n+1} - a \leq C(x_n - a)^2 \text{ et}$$

$$x_{n+1} - a \sim \frac{1}{2}\frac{f''(a)}{f'(a)}(x_n - a)^2 \text{ si } n \to +\infty$$

Questions

Exercice : Soit $P(X) = a_n X^n + ... + a_1 X + a_0 \in \mathbb{Z}[X]$ avec $a_n \neq 0$ et $a_0 \neq 0$. Si le rationnel α est zéro de $P(X)$, en notant $\alpha = p/q$ (avec $(p,q) \in \mathbb{Z}^* \times \mathbb{N}^*$ et $\text{pgcd}(p,q) = 1$). Montrer que $p|a_0$ et $q|a_n$.

Solution : Soit $\alpha = p/q$ une racine rationnelle de P (avec $(p,q) \in \mathbb{Z}^* \times \mathbb{N}^*$ et $\text{pgcd}(p,q) = 1$). Alors,

$$\begin{aligned} 0 = P\left(\frac{p}{q}\right) = a_n \left(\frac{p}{q}\right)^n + ... + a_1 \left(\frac{p}{q}\right) + a_0 &\Rightarrow a_n p^n + ... + a_1 p q^{n-1} + a_0 q^n = 0 \\ &\Rightarrow p(a_n p^{n-1} + ... + a_1 q^{n-1}) = -a_0 q^n \\ &\Rightarrow p|a_0 \text{ car } \text{pgcd}(p,q) = 1 \end{aligned}$$

En faisant la même chose avec q, on a $q|a_n$.

Exercice : Soit $P \in \mathbb{C}[X]$ tel que $P(X) = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$ avec $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$. On suppose que P' a une racine double ω.
Montrer que les points M_1, M_2 et M_3 d'affixes respectives α_1, α_2 et α_3 forment un triangle équilatéral de centre ω.

Solution : $P(X) = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$ et que P' a une racine double ω, on en déduit que $P'(X) = 3(X-\omega)^2$. Par suite, en intégrant, on a $P(X) = (X-\omega)^3 + c$ où $c \in \mathbb{C}$

Soit α une des racines de P, on a donc

$$\begin{aligned} P(\alpha) = 0 &\Rightarrow (\alpha-\omega)^3 = -c := re^{i\theta} \\ &\Rightarrow \begin{cases} |\alpha-\omega|^3 = r \\ \arg((\alpha-\omega)^3) = \theta \ [2\pi] \end{cases} \\ &\Rightarrow \begin{cases} |\alpha-\omega| = r^{1/3} \\ 3\arg(\alpha-\omega) = \theta + 2k\pi, \ k \in \mathbb{Z} \end{cases} \\ &\Rightarrow \begin{cases} |\alpha-\omega| = r^{1/3} \\ \arg(\alpha-\omega) = \frac{1}{3}(\theta + 2k\pi), \ k \in \{0,1,2\} \end{cases} \\ &\Rightarrow \alpha - \omega = r^{1/3} e^{\frac{i}{3}(\theta+2k\pi)} \ k \in \{0,1,2\} \end{aligned}$$

Il s'agit de l'écriture complexe d'un triangle équilatéral de sommets M_1, M_2 et M_3 d'affixes respectives α_1, α_2 et α_3 de centre ω (et de rayon $r^{1/3}$ pour le cercle circonscrit).

Exercice : Soit $M \in \mathcal{M}_n(\mathbb{C})$. Montrer que l'équivalence suivante :
(i) M est nilpotente.
(ii) $\forall k \geq 1$, $\text{Tr}(M^k) = 0$.

Solution : Avant de montrer cette équivalence, on a besoin d'un petit lemme fort utile :

Lemme : (M est nilpotente) $\Leftrightarrow$ (Toutes les valeurs propres de M sont nulles)
Démonstraton
$\Rightarrow$: Si M est nilpotente, alors il existe un entier k tel que $M^k = 0$. Par suite, le polynôme X^k est annulateur de M et ainsi son polynôme minimal est de la forme $\Pi_M(X) = X^d$ avec $d \leq k$ et donc les valeurs

propres de M sont nulles.

$\underline{\Leftarrow :}$ Si toutes les valeurs propres de M sont nulles, alors le polynôme caractéristique de M est X^n, et par le théorème de Cayley-Hamilton, on a $M^n = 0$ donc M est nilpotente.

□

Revenons à notre exercice !
$\underline{(i) \Rightarrow (ii)}$: On suppose que M est nilpotente, donc par le lemme, toutes ses valeurs propres $\lambda_1, ..., \lambda_n$ sont nulles. De plus, comme on est dans $\mathcal{M}_n(\mathbb{C})$, on peut trigonaliser M, et donc

$$M = \begin{pmatrix} \lambda_1 & * & \cdots & * \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix} \quad \Rightarrow \quad M^k = \begin{pmatrix} \lambda_1^k & * & \cdots & * \\ 0 & \lambda_2^k & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & \lambda_n^k \end{pmatrix}$$

Par suite, $\mathrm{Tr}(M^k) = \sum_{i=1}^n \lambda_i^k = 0$ car chaque $\lambda_i = 0$

$\underline{(ii) \Rightarrow (i)}$: Soit $M \in \mathcal{M}_n(\mathbb{C})$ et on suppose que $\forall k \geq 1$, $\mathrm{Tr}(M^k) = \sum_{i=1}^n \lambda_i^k = 0$. On va utiliser les formules de Newton. En notant

$$P(X) = (X - \lambda_1)...(X - \lambda_n) \text{ on sait que } P(X) = X^n + \sum_{k=1}^{n} (-1)^k \Sigma_k(\lambda_1, ...\lambda_n) X^{n-k}$$

et en notant,

$$P_k = \sum_{i=1}^{n} X_i^k, \quad \text{on a} \quad P_k = \sum_{i=1}^{k-1} ((-1)^{i-1} \Sigma_i P_{k-i}) + (-1)^{k-1} k \Sigma_k$$

Si on montre que $\Sigma_k = 0$ $\forall k \in [\![1, n]\!]$, on a fini ! En effet, on aura

$$P(X) = X^n + \sum_{k=1}^{n} (-1)^k \underbrace{\Sigma_k(\lambda_1, ...\lambda_n)}_{=0} X^{n-k} = X^n$$

Or, par hypothèse, $P_k = \sum_{i=1}^n \lambda_i^k = 0$, mais également $P_{k-i} = \sum_{i=1}^n \lambda_i^{k-i} = 0$ car on suppose $\forall k \geq 1$, $\mathrm{Tr}(M^k) = 0$. Ainsi, $\forall k \in [\![1, n]\!]$,

$$0 = P_k = \sum_{i=1}^{k-1} ((-1)^{i-1} \Sigma_i \underbrace{P_{k-i}}_{=0}) + (-1)^{k-1} k \Sigma_k \quad \Rightarrow \quad \Sigma_k = 0$$

Ainsi $P(X) = X^n$ et par le théorème de Cayley-Hamilton, on a $0 = P(M) = M^n$ donc M est nilpotente.

Exercice : Pour $n \in \mathbb{N}^*$, on pose $P_n(x) = -1 + x + x^2 + ... + x^n$ pour $x \in \mathbb{R}$.
1) Montrer que l'équation $P_n(x) = 0$ admet une unique solution positive x_n et que $x_n \in]0, 1]$.
2) Calculer $P_{n+1}(x_n)$ et montrer que la suite (x_n) converge.
3) Calculer $\lim\limits_{n \to +\infty} x_n^n$ et en déduire $\lim\limits_{n \to +\infty} x_n$.

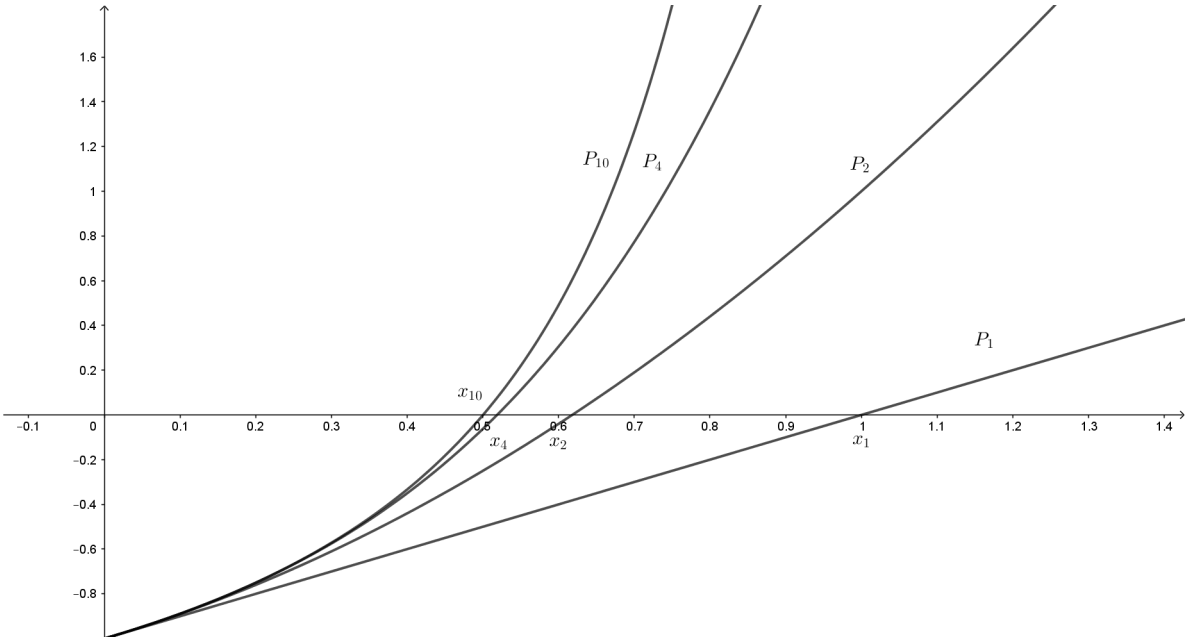
Solution : 1) Soit $n \in \mathbb{N}^*$, la fonction $x \mapsto P_n(x)$ est continue et vérifie $P_n(0) = -1$ et $P_n(1) = -1 + n \geq 0$ donc par le théorème des valeurs intermédiaires, l'équation $P_n(x) = 0$ admet une solution $x_n \in]0, 1]$. De plus, la fonction $x \mapsto P_n(x)$ est strictement croissante car $P_n'(x) = 1 + 2x + ... + nx^{n-1} > 0$ $\forall x \geq 0$. Donc la solution x_n est unique.

2) On a

$$P_{n+1}(x_n) = -1 + x_n + x_n^2 + ... + x_n^n + x_n^{n+1} = \underbrace{P_n(x_n)}_{=0} + x_n^{n+1} = x_n^{n+1}$$

Ainsi, $P_{n+1}(x_n) > 0$, et par croissance de la fonction $x \mapsto P_{n+1}(x)$, on en déduit que $x_{n+1} < x_n$ et donc que la suite (x_n) est strictement décroissante. De plus, étant bornée, la suite (x_n) converge vers une limite l.

3) La suite (x_n) est strictement décroissante, on a donc $0 < x_n \leq x_2 < x_1 = 1$, donc $\lim\limits_{n\to+\infty} x_n^n = 0$.
Pour ne pas parachuter la solution, il est important de voir le comportement de la suite des polynômes P_n et ainsi de la suite (x_n).



Tracé de quelques polynômes P_n et de x_n

On constate que la suite (x_n) semble converger vers $\frac{1}{2}$. Finissons-en !

On a, pour tout $n \geq 1$,

$$P_n\left(\frac{1}{2}\right) = -1 + \left(\frac{1}{2}\right) + \left(\frac{1}{2}\right)^2 + ... + \left(\frac{1}{2}\right)^n = -1 + \frac{1}{2}\frac{1-\left(\frac{1}{2}\right)^n}{1-\frac{1}{2}} = -\left(\frac{1}{2}\right)^n < 0$$

Par conséquent, $x_n > 1/2$. De plus,

$$0 = P_n(x_n) = -1 + x_n + x_n^2 + ... + x_n^n = -1 + \frac{x_n + x_n^{n+1}}{1 - x_n}$$

Par passage à la limite (en se rappelant que $\lim\limits_{n\to+\infty} x_n^n = 0$), on a :

$$0 = -1 + \frac{l+0}{1-l} \quad \Rightarrow \quad 0 = l - 1 + l \quad \Rightarrow \quad l = \frac{1}{2}$$