COMPOSITION DE MATHEMATIQUES

Epreuve commune aux ENS de Cachan et de Lyon

Durée : 4 heures

Introduction

Le but du problème est l'étude d'une technique intervenant dans un domaine lié à l'arithmétique, domaine appelé "théorie des nombres p-adiques". Une vague idée que l'on peut donner de l'adjectif p-adique est celle d'une suite d'entiers $(x_i)_{i\geq 1}$ vérifiant la condition de *cohérence* :

$$x_{i+1} \equiv x_i \pmod{p^i} \quad \text{pour tout } i.$$

$$\begin{array}{ll} & \vdots \\ x_3 : & \mathbf{Z}/p^3\mathbf{Z} \\ & \downarrow \\ x_2 : & \mathbf{Z}/p^2\mathbf{Z} \\ & \downarrow \\ x_1 : & \mathbf{Z}/p\mathbf{Z} \end{array}$$

Un cas fréquent est celui où p est un nombre premier, mais ce n'est pas là le seul exemple. On peut évoquer une telle suite à l'aide d'un schéma (c.f. la figure encadrée à droite) dans lequel les flèches verticales désignent successivement les réductions modulo p, modulo p^2 ...

L'épreuve est essentiellement consacrée au développement d'une méthode permettant (sous certaines conditions) de "remonter" une solution x d'une congruence polynomiale $P(x) \equiv 0 \pmod{p}$ en une solution de la même congruence mais modulo p^2 puis p^3, etc. Le problème fournit ensuite quelques applications de cette méthode à des polynômes ou à des matrices (et non pas à des nombres !) avec comme conséquences :

- surjectivité de l'exponentielle : $\mathrm{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$
- existence de racines carrées, cubiques, ..., dans $\mathrm{GL}_n(\mathbb{C})$
- existence de la décomposition $A = D+N$, D diagonalisable, N nilpotente, $DN = ND$

Partie I : Préliminaires relatifs aux congruences et aux polynômes

Soit $\mathbf{A}$ un anneau *commutatif* unitaire dont l'élément unité est noté 1. On rappelle que la relation $x \equiv y \pmod{a}$, pour $x, y, a, \in \mathbf{A}$ signifie que $x - y \in \mathbf{A}a = \{\lambda a \mid \lambda \in \mathbf{A}\}$; on rappelle également qu'un élément $z \in \mathbf{A}$ est *inversible modulo* a s'il existe un $z' \in \mathbf{A}$ tel que $zz' \equiv 1 \pmod{a}$; on dit alors que l'élément $z' \in \mathbf{A}$ est *un* inverse de z modulo a.

1. Vérifier *rapidement* que :

$$x \equiv y \pmod{a},\ x' \equiv y' \pmod{a} \Rightarrow x + x' \equiv y + y' \pmod{a} \text{ et } xx' \equiv yy' \pmod{a}.$$

et que $x \equiv y \pmod{a} \Rightarrow P(x) \equiv P(y) \pmod{a}$ pour tout polynôme P à coefficients dans $\mathbf{A}$.

2. Vérifier qu'un élément $z \in \mathbf{A}$ inversible modulo a et inversible modulo b est inversible modulo ab ; en particulier si z est inversible modulo a, il est inversible modulo a^i pour tout $i \in \mathbb{N}^*$.

On note $\mathbf{A}[X]$ l'anneau des polynômes à coefficients dans $\mathbf{A}$: $\mathbf{A}[X]$ est donc constitué des sommes $a_0 + a_1X + \cdots + a_nX^n$, où les a_i appartiennent à $\mathbf{A}$; les opérations (addition, multiplication) sont définies de manière habituelle et confèrent à $\mathbf{A}[X]$ une structure d'anneau commutatif unitaire. La dérivée de $P(X) = a_0 + a_1X + a_2X^2 \cdots + a_nX^n$, notée $P'(X)$, est le polynôme $a_1 + 2a_2X + \cdots + na_nX^{n-1}$. On désigne par $\mathbf{A}[X,Y]$ l'anneau $\mathbf{A}[X][Y]$.

3. Soit $P \in \mathbf{A}[X]$. En utilisant l'identité $X^n - Y^n = (X-Y)(X^{n-1} + X^{n-2}Y + \cdots + XY^{n-2} + Y^{n-1})$, montrer l'existence d'un polynôme $Q(X,Y) \in \mathbf{A}[X,Y]$ tel que $P(Y) - P(X) = (Y-X)Q(X,Y)$.
Que vaut $Q(X,X)$? Montrer également l'existence d'un polynôme $R(X,Y) \in \mathbf{A}[X,Y]$ tel que :

$$P(X+Y) = P(X) + YP'(X) + Y^2R(X,Y).$$

Quelle relation existe-t-il entre Q et R ?

Partie II : Une méthode de "remontée modulaire"

Dans toute cette partie, on désigne par $\mathbf{A}$ un anneau *commutatif* unitaire, par P un polynôme à coefficients dans $\mathbf{A}$, et par a un élément de l'anneau $\mathbf{A}$.

1. Soit $x \in \mathbf{A}$ tel que $P(x) \equiv 0 \pmod{a^i}$ où i est un entier ≥ 1. Si $P'(x)$ est inversible modulo a, montrer l'existence d'un $\lambda \in \mathbf{A}$ pour lequel $y = x + \lambda a^i$ vérifie la congruence :

$$P(y) \equiv 0 \pmod{a^{i+1}}.$$

Montrer que la classe de y modulo a^{i+1} ne dépend pas du choix d'un inverse de $P'(x)$ modulo a ; expliciter y en fonction de x et d'*un* inverse de $P'(x)$ modulo a ;

2. Un exemple : soit z' un inverse modulo a d'un élément z. Comment appliquer la question précédente pour exhiber l'élément $z'(2-zz')$ comme un inverse de z modulo a^2 ?

3. Soit une solution $x = x_1$ de $P(x) \equiv 0 \pmod{a}$ telle que $P'(x_1)$ soit inversible modulo a ; en utilisant la question **I.1**, expliquer comment construire par récurrence une suite $(x_i)_{i\geq 1}$ telle que :

$$P(x_i) \equiv 0 \pmod{a^i}, \qquad x_{i+1} \equiv x_i \pmod{a^i}.$$

Cette construction utilise *un* inverse de $P'(x_1)$ modulo a ; montrer que le choix d'un autre inverse conduit à une suite $(y_i)_{i\geq 1}$ telle que :

$$x_i \equiv y_i \pmod{a^i} \quad \text{pour tout } i.$$

4. Soit $i \geq 1$ fixé et $x, y \in \mathbf{A}$ vérifiant :

$$y \equiv x \pmod{a}, \quad P(y) \equiv P(x) \pmod{a^i}, \quad P'(x) \text{ inversible modulo } a.$$

En utilisant la question **I.3**, montrer que $y \equiv x \pmod{a^i}$.

5. On reprend les hypothèses et les notations de la question **II.3**. Montrer que pour $i \geq 1$ fixé, le système de congruences :

$$P(z) \equiv 0 \pmod{a^i}, \qquad z \equiv x_1 \pmod{a},$$

admet une unique solution z modulo a^i, égale à x_i.

Partie III : Troncature de l'exponentielle et du logarithme

Etant donné deux polynômes P, Q à coefficients dans $\mathbb{C}$, $Q \neq 0$, on note $P \bmod Q$ le reste de la division de P par Q : c'est l'unique polynôme R vérifiant :

$$\deg R < \deg Q, \qquad R \equiv P \pmod{Q} \qquad (\text{on convient que } \deg 0 = -\infty).$$

On définit une famille de polynômes "exponentielles tronquées" $(e_n)_{n\geq 1}$ à coefficients dans $\mathbb{Q}$ par :

$$e_1(T) = 1, \qquad e_2(T) = 1+T, \qquad e_3(T) = 1 + T + \frac{T^2}{2}, \quad \ldots,$$

$$e_n(T) = 1 + \frac{T}{1!} + \frac{T^2}{2!} + \cdots + \frac{T^{n-1}}{(n-1)!}$$

1. En appliquant la partie **II** à l'anneau $\mathbf{A} = \mathbb{Q}[T]$, montrer l'existence et l'unicité d'un polynôme $l_n(T)$, de degré $< n$, à coefficients dans $\mathbb{Q}$, tel que :

$$l_n(1) = 0, \qquad e_n(l_n(1+T)) \equiv 1 + T \pmod{T^n} \tag{1}$$

2. Pour $m \leq n$ calculer $e_m(l_n(1+T)) \bmod T^m$ puis $l_n(1+T) \bmod T^m$. En déduire, en dérivant la congruence (1) de la question précédente, le polynôme $l_n'(1+T)$ puis expliciter le polynôme $l_n(1+T)$.

3. On souhaite montrer que $l_n(e_n(T)) \equiv T \pmod{T^n}$; pour cela on pose $Q_n(T) = l_n(e_n(T))$. Calculer $e_n(Q_n(T)) \bmod T^n$ puis en déduire $Q_n(T) \bmod T^n$.

4. On rappelle qu'une matrice $A \in \mathrm{M}_n(\mathbb{C})$ est nilpotente si l'une de ses puissances est nulle et qu'une matrice unipotente est une matrice de la forme $\mathrm{I}_n + A$ où A est une matrice nilpotente (I_n désigne la matrice identité $n \times n$). Montrer que l'exponentielle réalise une bijection de l'ensemble des matrices nilpotentes de $\mathrm{M}_n(\mathbb{C})$ sur l'ensemble des matrices unipotentes de $\mathrm{M}_n(\mathbb{C})$; montrer que cette bijection et son inverse sont des applications polynomiales "à coefficients rationnels" que l'on explicitera.

5. Soit $\lambda \in \mathbb{C} - \{0\}$; si A est une matrice telle que $A - \lambda I_n$ soit nilpotente, montrer l'existence de $B \in \mathrm{M}_n(\mathbb{C})$ telle que $\exp(B) = A$. En déduire que l'exponentielle réalise une surjection de $\mathrm{M}_n(\mathbb{C})$ sur $\mathrm{GL}_n(\mathbb{C})$. Est-ce une injection ?

Partie IV : Racines m-ièmes dans $\mathrm{GL}_n(\mathbb{R})$ ou $\mathrm{GL}_n(\mathbb{C})$

On applique la partie II à l'anneau $\mathbf{A} = K[X]$ où K désigne un sous-corps de $\mathbb{C}$ et on fournit quelques applications à l'anneau de matrices $\mathrm{M}_n(\mathbb{R})$ ou $\mathrm{M}_n(\mathbb{C})$.

1. Soit λ un élément *non nul* de K possédant une racine cubique dans K ; montrer que, quelque soit $k \in \mathbb{N}^*$, la congruence suivante :

$$Q(X)^3 \equiv X \pmod{(X-\lambda)^k},$$

admet une solution $Q(X) \in K[X]$.

2. Plus généralement, soient $\lambda \in K$ et $P \in K[X]$ tel que $P(x) = \lambda$ ait une solution $\mu \in K$ vérifiant $P'(\mu) \neq 0$; montrer que, quelque soit $k \in \mathbb{N}^*$, la congruence suivante :

$$P(Q(X)) \equiv X \pmod{(X-\lambda)^k},$$

admet une solution $Q(X) \in K[X]$.

3. Soient $T_1, T_2 \in K[X]$ deux polynômes *premiers entre eux* ; on suppose qu'il existe des polynômes $Q_1, Q_2 \in K[X]$ tels que :

$$P(Q_1(X)) \equiv X \pmod{T_1}, \qquad P(Q_2(X)) \equiv X \pmod{T_2}.$$

Montrer qu'il existe un polynôme $Q \in K[X]$ tel que $P(Q(X)) \equiv X \pmod{T_1 T_2}$.

4. On suppose que l'application $K \ni x \to P(x) \in K$ est surjective et que $T \in K[X]$ est un polynôme *scindé sur* K vérifiant :

$$\text{si } P(\mu) \text{ est racine de } T \text{ alors } P'(\mu) \neq 0.$$

Déduire des questions précédentes que l'équation suivante admet une solution en $Q(X) \in K[X]$:

$$P(Q(X)) \equiv X \pmod{T(X)}.$$

Examiner le cas particulier $P(X) = X^m$ pour $m \in \mathbb{N}^*$.

5. Soit $m \in \mathbb{N}^*$; en appliquant la question précédente, montrer que pour toute matrice inversible $A \in \mathrm{GL}_n(\mathbb{C})$ il existe $B \in \mathrm{GL}_n(\mathbb{C})$, *polynôme en* A, tel que $B^m = A$. Question analogue pour $\mathrm{GL}_n(\mathbb{R})$ en supposant que m impair et que $A \in \mathrm{GL}_n(\mathbb{R})$ a toutes ses valeurs propres réelles.

6. Soit $aX^2 + bX + c$ ($a \neq 0$) un trinôme à coefficients *réels* sans racine réelle. Caractériser, à l'aide d'une racine $\alpha \in \mathbb{C}\backslash\mathbb{R}$ de aX^2+bX+c, les polynômes *réels* multiples de aX^2+bX+c. Montrer que pour $m \in \mathbb{N}^*$, la congruence $Q(X)^m \equiv X \pmod{(aX^2+bX+c)}$ admet une solution $Q(X) \in \mathbb{R}[X]$ de degré 1.

En déduire que pour tout $m \in \mathbb{N}^*$ et $k \in \mathbb{N}^*$, la congruence :

$$Q(X)^m \equiv X \pmod{(aX^2+bX+c)^k},$$

admet une solution $Q(X) \in \mathbb{R}[X]$.

7. Plus généralement, soit $T(X) \in \mathbb{R}[X]$ sans racine réelle. Montrer que pour $m \in \mathbb{N}^*$, la congruence :

$$Q(X)^m \equiv X \pmod{T(X)},$$

admet une solution $Q(X) \in \mathbb{R}[X]$. En déduire que si $A \in \mathrm{M}_n(\mathbb{R})$ est sans valeur propre réelle, elle possède, pour tout $m \in \mathbb{N}^*$, une racine m-ième dans $\mathrm{M}_n(\mathbb{R})$ qui est un polynôme en A.

Partie V : A propos de la décomposition "diagonalisable + nilpotente"

On désigne dans cette partie par A une matrice $n \times n$ à coefficients dans un sous-corps K de $\mathbb{C}$ (par exemple l'un des trois corps $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) ; on désire montrer l'existence d'une décomposition :

(2) $A = D + N$, avec D, N polynômes en A à coefficients dans K, D diagonalisable dans $\mathbb{C}$, N nilpotente.

A noter que cela entraîne $DN = ND$ et le fait que D et N sont à coefficients dans le même corps K que la matrice A.
On rappelle qu'un polynôme $R \in K[X]$ est irréductible s'il n'est pas constant et si ses seuls diviseurs sont les constantes et les polynômes λR avec $\lambda \in K^*$; tout polynôme de $K[X]$ s'écrit de manière essentiellement unique comme un produit de polynômes irréductibles de $K[X]$.
On dit qu'un polynôme à coefficients dans K, de degré ≥ 1, est sans facteur carré s'il est produit de polynômes irrréductibles distincts c'est-à-dire si les exposants intervenant dans sa décomposition primaire sont tous égaux à 1.

1. Soit $\chi \in K[X]$ de degré ≥ 1 ; montrer l'existence et l'unicité d'un polynôme $P \in K[X]$, unitaire, sans facteur carré, tel que :

$$P \text{ divise } \chi, \quad \chi \text{ divise une puissance de } P.$$

Montrer qu'un polynôme à coefficients dans K sous-corps de $\mathbb{C}$ est sans facteur carré si et seulement si il est premier avec sa dérivée. En déduire une expression de P en fonction de χ et $\mathrm{pgcd}(\chi, \chi')$.

2. On désigne maintenant par χ le polynôme caractéristique de la matrice A et par P le polynôme intervenant dans la question précédente. Montrer qu'une matrice annulée par le polynôme P est diagonalisable dans $\mathbb{C}$.

3. On raisonne dans le sous-anneau (commutatif) $\mathbf{A} \subset \mathrm{M}_n(K)$ constitué des matrices de la forme $Q(A)$ avec $Q \in K[X]$ et on pose $B = P(A)$. Montrer, dans cet anneau, que $P'(A)$ est inversible modulo B ; comment calculer un inverse de $P'(A)$ modulo B ?

4. Construire une suite de matrices $(A_i)_{i\geq 1}$ telle que :

$$A_i \in \mathbf{A}, \quad P(A_i) \equiv 0 \pmod{B^i}, \quad A_i \equiv A \pmod{B}$$

En remarquant que B est nilpotente, montrer l'existence d'une décomposition **(2)**.

5. Montrer qu'en fait pour tout polynôme sans facteur carré P à coefficients dans K (K désigne toujours un sous-corps de $\mathbb{C}$), on peut définir une suite de polynômes $(Q_i)_{i\geq 1}$ telle que :

$$P(Q_i(X)) \equiv 0 \pmod{P^i}, \quad Q_i(X) \equiv X \pmod{P}.$$

En déduire de nouveau l'existence d'une décomposition **(2)**.

Partie I : Préliminaires relatifs aux congruences et aux polynômes

1. Soient a, x, x', y, y' des éléments de $\mathbf{A}$ vérifiant $x \equiv y \pmod a$ et $x' \equiv y' \pmod a$, c'est à dire $x-y \in \mathbf{A}a$ et $x'-y' \in \mathbf{A}a$.
Comme $\mathbf{A}a$ est un sous-groupe additif de $\mathbf{A}$, il s'ensuit que $(x-y)+(x'-y') \in \mathbf{A}a$, soit que $(x+x')-(y+y') \in \mathbf{A}a$, d'où $x+x' \equiv y+y' \pmod a$.
Comme $\mathbf{A}a$ est un idéal de $\mathbf{A}$, $x(x'-y')+y'(x-y) \in \mathbf{A}a$, soit $xx'-yy' \in \mathbf{A}a$, d'où $xx' \equiv yy' \pmod a$.
Une récurrence simple permet d'inférer de ce résultat que, pour tout entier naturel i, $x^i \equiv y^i \pmod a$.
Soit $(\alpha_i)_{i\geq 0}$ une suite d'éléments de $\mathbf{A}$. Après avoir constaté que, pour tout i, $\alpha_i x^i \equiv \alpha_i y^i \pmod a$, une récurrence simple permet encore de montrer que, pour tout entier naturel n, $\sum_{i=0}^{n} \alpha_i x^i \equiv \sum_{i=0}^{n} \alpha_i y^i \pmod a$.
On conclut donc que, pour tout polynôme P à coefficient dans $\mathbf{A}$, $P(x) \equiv P(y) \pmod a$.

2. Si z est inversible modulo a et inversible modulo b, il existe des éléments z', λ, z'' et μ de $\mathbf{A}$ tels que $zz'-1=\lambda a$ et $zz''-1=\mu b$. Il vient alors $(zz'-1)(zz''-1)=(\lambda a)(\mu b)$, soit $z(z'+z''-zz'z'')-1=(-\lambda\mu)(ab)$, ce qui prouve que z est inversible modulo ab.

3. Posons $P=a_0+a_1X+a_2X^2+\cdots+a_nX^n=\sum_{k=0}^{n} a_kX^k$. Dans l'anneau $\mathbf{A}[X,Y]$,
$P(Y)-P(X)=\sum_{k=0}^{n} a_k(Y^k-X^k)=(Y-X)\sum_{k=1}^{n} a_k\Big(\sum_{i=0}^{k-1} Y^{k-1-i}X^i\Big)$, ce qui établit l'existence du polynôme $Q(X,Y)$ de l'énoncé.

Il vient* ainsi $Q(X,X)=\sum_{k=1}^{n} a_k\Big(\sum_{i=0}^{k-1} X^{k-1}\Big)=\sum_{k=1}^{n} ka_kX^{k-1}=P'(X)$.
D'autre part, $P(X+Y)-P(X)=YQ(X,X+Y)$. Or le polynôme $Q(X,Y)$ est un élément, que nous noterons S, de $\mathbf{A}[X][Y]$, c'est à dire un polynôme "en Y" à coefficients dans $\mathbf{A}[X]$. Il existe donc un polynôme $T \in \mathbf{A}[X][Y,Z]$ tel que $S(Y+Z)-S(Z)=YT(Z,Y+Z)$, ce qui donne, en substituant X à Z et en revenant ainsi dans $\mathbf{A}[X][Y]$, $S(Y+X)-S(X)=YR(X,Y)$, où l'on a noté $R(X,Y)=T(X,Y+X)$.
On obtient $Q(X,X+Y)-Q(X,X)=YR(X,Y)$, soit $Q(X,X+Y)=P'(X)+YR(X,Y)$, ce qui, conjoint à $P(X+Y)-P(X)=YQ(X,X+Y)$, donne finalement $P(X+Y)-P(X)=YP'(X)+Y^2R(X,Y)$.
On aurait peut-être aussi bien fait d'écrire
$P(X+Y)-P(X)=\sum_{k=0}^{n} a_k\Big(\sum_{j=0}^{k}\binom{k}{j}Y^jX^{k-j}\Big)-\sum_{k=0}^{n} a_kX^k=\sum_{k=1}^{n} a_k\Big(\sum_{j=1}^{k}\binom{k}{j}Y^jX^{k-j}\Big)$, soit
$P(X+Y)-P(X)=\sum_{j=1}^{n} Y^j\Big(\sum_{k=j}^{n} a_k\binom{k}{j}X^{k-j}\Big)=YP'(X)+Y^2\sum_{j=2}^{n} Y^{j-2}\Big(\sum_{k=j}^{n} a_k\binom{k}{j}X^{k-j}\Big)$.
Enfin, nous avons vu que $Q(X,X+Y)=P'(X)+YR(X,Y)$, soit $Q(X,Y)=P'(X)+(Y-X)R(X,Y-X)$.

Partie II : Une méthode de "remontée modulaire"

Comme l'énoncé nous y invite implicitement, nous userons de la même lettre pour dénoter un polynôme $\sum_{k=0}^{n} a_kX^k \in \mathbf{A}[X]$ et la fonction polynomiale $x \to \sum_{k=0}^{n} a_kx^k$ de $\mathbf{A}$ dans $\mathbf{A}$ qui lui est associée.

---

* Signalons une petite ambiguïté de l'énoncé : l'anneau $\mathbf{A}$ n'étant pas nécessairement intègre, il pouvait se faire que Q ne soit pas unique et que le polynôme $Q(X,X)$ dépende effectivement du choix de Q.
Le candidat pouvait cependant entendre : "Que vaut $Q(X,X)$ pour le polynôme Q que vous avez trouvé ?"
De toutes façons, la chose n'est pas bien grave puisque Q est unique. En effet, si $D \in \mathbf{A}[X,Y]$ est tel que $(Y-X)D(X,Y)=0$, en écrivant $D(X,Y)=\sum_{k=0}^{n} D_k(X)Y^k$, on obtient $\sum_{k=0}^{n} D_k(X)Y^{k+1}=\sum_{k=0}^{n} XD_k(X)Y^k$ d'où il vient, pour tout $k \geq 1$, $XD_k(X)=D_{k-1}(X)$, et $XD_0(X)=0$, d'où $D(X,Y)=0$.
De même, le polynôme R de la question suivante est unique.

1. Pour tout $\ell \in \mathbf{A}$, $P(x+\ell a^i) = P(x) + \ell a^i P'(x) + \ell^2 a^{2i} R(x, \ell a^i)$.
Comme $i \geq 1$, $2i \geq i+1$, et $\ell^2 a^{2i} R(x, \ell a^i) \equiv 0 \pmod{a^{i+1}}$.
D'autre part, il existe $k \in \mathbf{A}$ tel que $P(x) = ka^i$.
On peut ainsi écrire, pour tout $\ell \in \mathbf{A}$, $P(x+\ell a^i) \equiv (\ell P'(x) + k)\, a^i \pmod{a^{i+1}}$.
Il suffit donc, pour que $P(x+\ell a^i) \equiv 0 \pmod{a^{i+1}}$ soit vérifié, qu'il existe $h \in \mathbf{A}$ tel que $\ell P'(x) + k = ha$, ou encore que $\ell P'(x) \equiv -k \pmod{a}$.
Il suffit enfin, pour que cette dernière relation soit vérifiée, que $\ell \equiv -k\mu \pmod{a}$, où μ est *un* inverse de $P'(x)$ modulo a.
Il existe donc un élément $\lambda \in \mathbf{A}$, par exemple $\lambda = -k\mu$, tel que $P(x+\lambda a^i) \equiv 0 \pmod{a^{i+1}}$.
La question de l'indépendance de la classe de y modulo a^{i+1} relativement au choix d'un inverse de $P'(x)$ modulo a étant assez obscure, puisque nous avons établi l'existence de λ en exhibant certes une solution dépendant de μ mais sans raisonner par condition nécessaire, nous allons simplement montrer que, si $y = x + \lambda a^i$ et $y' = x + \lambda' a^i$ vérifient $P(y') \equiv P(y) \pmod{a^{i+1}}$, alors $y' \equiv y \pmod{a^{i+1}}$, ce qui épuisera la question.**
Comme $P(x+\lambda a^i) \equiv P(x) + \lambda a^i P'(x) \pmod{a^{i+1}}$ et $P(x+\lambda' a^i) \equiv P(x) + \lambda' a^i P'(x) \pmod{a^{i+1}}$, la relation de congruence étant transitive, $\lambda' a^i P'(x) \equiv \lambda a^i P'(x) \pmod{a^{i+1}}$. Comme $P'(x)$ est inversible modulo a, $P'(x)$ est inversible modulo a^{i+1} (voir I.2), et l'on tire de la relation ci-dessus que $\lambda' a^i \equiv \lambda a^i \pmod{a^{i+1}}$, d'où, en ajoutant x, il vient $y' \equiv y \pmod{a^{i+1}}$.
Enfin, on conclut que $y = x + \lambda a^i$ vérifie $P(y) \equiv 0 \pmod{a^{i+1}}$ si et seulement si $y \equiv x - k\mu a^i \pmod{a^{i+1}}$, soit si et seulement si $y \equiv x - \mu P(x) \pmod{a^{i+1}}$.

2. Signalons que $z'(2-zz')$ est un inverse de z modulo a^2 puisque $zz'(2-zz') - 1 = -(zz'-1)^2$ et qu'il existe $k \in \mathbf{A}$ tel que $zz' - 1 = ka$.
Pour répondre proprement à la question, considérons le polynôme $P = zX - 1$ et l'élément $x = z'$.
Nous savons que $P(x) \equiv 0 \pmod{a^1}$ et que $P'(x) = z$ est inversible modulo a, d'inverse $\mu = z'$. Nous pouvons donc affirmer que $P\big(x - \mu P(x)\big) \equiv 0 \pmod{a^2}$, autrement dit que $P\big(z' - z'(zz'-1)\big) \equiv 0 \pmod{a^2}$, c'est à dire $zz'(2-zz') - 1 \equiv 0 \pmod{a^2}$, ce qu'il fallait obtenir.

3. Choisissons un inverse μ de $P'(x_1)$ modulo a, et définissons la suite $(x_i)_{i\geq 1}$ par son premier terme x_1 et la relation de récurrence $x_{i+1} = x_i - \mu P(x_i)$.
Considérons, pour tout entier naturel non nul i, la proposition $\mathcal{H}_i$ suivante :

"$P(x_i) \equiv 0 \pmod{a^i}$ et $P'(x_i)$ est inversible modulo a d'inverse μ".

$\mathcal{H}_1$ est vraie par hypothèse.
Pour tout entier naturel non nul i, $\mathcal{H}_i \Rightarrow \mathcal{H}_{i+1}$:
Le résultat (II.1) appliqué à $\mathcal{H}_i$ permet d'affirmer que $P(x_{i+1}) \equiv 0 \pmod{a^{i+1}}$.
D'autre part, comme $P(x_i) \equiv 0 \pmod{a^i}$, $x_{i+1} = x_i - \mu P(x_i) \equiv x_i \pmod{a^i}$, et donc $x_{i+1} \equiv x_i \pmod{a}$.
D'après le dernier résultat de la question (I.1), $P'(x_{i+1}) \equiv P'(x_i) \pmod{a}$, ce qui prouve que $P'(x_{i+1})$ est inversible modulo a d'inverse μ.
En conclusion, la proposition $\mathcal{H}_i$ est vraie pour tout i, et nous avons vu en cours de démonstration que $x_{i+1} \equiv x_i \pmod{a^i}$.
Soit maintenant ν un autre inverse de $P'(x_1)$, et soit $(y_i)_{i\geq 1}$ la suite définie par son premier terme $y_1 = x_1$ et la relation de récurrence $y_{i+1} = y_i - \nu P(y_i)$.
Considérons, pour tout entier naturel non nul i, la proposition $\mathcal{H}_i$ suivante :

"$y_i \equiv x_i \pmod{a^i}$".

** L'auteur du problème a pu vouloir dire : "montrer que la classe de $x - k\mu a^i$ modulo a^{i+1} ne dépend pas du choix de l'inverse μ de $P'(x)$ modulo a", ce qui n'est pas tout à fait la même chose.
Pour répondre à cette question imaginaire, il convient d'abord de montrer que deux inverses μ et μ' de $P'(x)$ modulo a sont eux-mêmes nécessairement congrus modulo a. Et en effet, $\mu P'(x) \equiv 1 \pmod{a}$ et $\mu' P'(x) \equiv 1 \pmod{a}$ impliquent que $(\mu' - \mu)P'(x) \equiv 0 \pmod{a}$, d'où, en multipliant par μ, $\mu' - \mu \equiv 0 \pmod{a}$, soit $\mu' \equiv \mu \pmod{a}$.
Bref, h étant un élément de $\mathbf{A}$ tel que $\mu' - \mu = ha$, $(x - k\mu a^i) - (x - k\mu' a^i) = (\mu' - \mu)a^i = ha^{i+1}$.
Observons réciproquement que, si μ est un inverse de $P'(x)$ modulo a et si $\mu' \equiv \mu \pmod{a}$, alors μ' est aussi un inverse de $P'(x)$ modulo a.

$\mathcal{H}_1$ est vraie par hypothèse.
Pour tout entier naturel non nul i, $\mathcal{H}_i \Rightarrow \mathcal{H}_{i+1}$:
Posons $x'_{i+1} = x_i - \nu P(x_i)$. D'après le résultat de la question (II.1), $x'_{i+1} \equiv x_{i+1} \pmod{a^{i+1}}$, puisque ν est aussi un inverse de $P'(x_i)$ modulo a.
Posons $S = X - \nu P$: $y_{i+1} - x'_{i+1} = S(y_i) - S(x_i) = (y_i - x_i)S'(x_i) + (y_i - x_i)^2 R(x_i, y_i - x_i)$. Or $S' = 1 - \nu P'$ et donc $S'(x_i) \equiv 0 \pmod{a}$. On en déduit que $(y_i - x_i)S'(x_i) \equiv 0 \pmod{a^{i+1}}$, puis, comme $2i \geq i+1$, que $y_{i+1} \equiv x'_{i+1} \pmod{a^{i+1}}$. Finalement, $y_{i+1} \equiv x_{i+1} \pmod{a^{i+1}}$.

Note : on pourrait en fait définir $x_{i+1} = x_i - \mu_i P(x_i)$ et on ne voit pas pourquoi l'auteur du problème affirme que cette "construction utilise *un* inverse de $P'(x_1)$ modulo a". Elle utilise en fait une suite $(\mu_i)_{i\geq 1}$ d'inverses de $P'(x_1)$ modulo a, qui sont d'ailleurs tous inverses modulo a de n'importe lequel des $P'(x_j)$.
On peut reprendre ce qui vient d'être fait pour obtenir le même résultat, en changeant "*un* inverse de $P'(x_1)$ modulo a" par "*une suite* d'inverses de $P'(x_1)$ modulo a".

4. Comme $P'(x)$ est inversible modulo a, $P'(x)$ est inversible modulo a^i : notons λ l'un de ses inverses modulo a^i.
Nous savons que $P(y) - P(x) = (y-x)P'(x) + (y-x)^2 R(x, y-x)$, et donc $(y-x)P'(x) \equiv -(y-x)^2 R(x, y-x) \pmod{a^i}$, soit $y - x \equiv k(y-x)^2 \pmod{a^i}$, où $k = -\lambda R(x, y-x)$. Or il existe $\ell \in \mathbf{A}$ tel que $y - x = \ell a$. Donc $y - x \equiv k\ell^2 a^2 \pmod{a^i}$, et il vient que $y - x \equiv k_2 a^4 \pmod{a^i}$, où $k_2 = k^3\ell^4$. Et ainsi de suite : on montre de proche en proche que, pour tout entier $p \geq 1$, il existe $k_p \in \mathbf{A}$ tel que $y - x \equiv k_p a^{2^p} \pmod{a^i}$. En considérant un entier q tel que $2^q \geq i$, on obtient $y - x \equiv 0 \pmod{a^i}$.

5. Considérons à nouveau la suite $(x_i)_{i\geq 1}$ définie en (II.3). Il est clair que, pour l'entier $i \geq 1$ fixé, $z = x_i$ est solution du système de congruences $\begin{cases} P(z) \equiv 0 \pmod{a^i} \\ z \equiv x_1 \pmod{a} \end{cases}$ puisque $P(x_i) \equiv 0 \pmod{a^i}$ et que $x_i \equiv x_{i-1} \equiv \cdots \equiv x_1 \pmod{a}$.
Si z en est une autre solution, alors $z \equiv x_i \pmod{a}$ puisque $z \equiv x_1 \pmod{a}$ et $x_i \equiv x_1 \pmod{a}$, et $P(z) \equiv P(x_i) \pmod{a^i}$ puisque ces éléments sont tous deux congrus à 0 modulo a^i, et enfin $P'(x_i)$ est inversible modulo a. En s'appuyant sur le résultat de la question (II.4), on conclut que $z \equiv x_i \pmod{a^i}$.

Note : on peut ajouter que, si z est solution et si $z' \equiv z \pmod{a^i}$, alors z' est aussi solution puisqu'alors $P(z') \equiv P(z) \pmod{a^i}$ et $z' \equiv z \equiv x_1 \pmod{a^i}$.

Partie III : Troncature de l'exponentielle et du logarithme

1. Cas $\underline{n = 1}$. Les conditions $\deg \ell_1 < 1$ et $\ell_1(1) = 0$ impliquent que ℓ_1 est le polynôme nul. La réciproque est immédiate.
Cas $\underline{n > 1}$. Nous pouvons appliquer les résultats de la partie II avec $i = n$, $P(X) = e_n(X) - (1+T)$, $x_1 = 0$ et $a = T$ parce que :

- $P'(X) = e_{n-1}(X)$, d'où $P'(0) = 1$ est inversible modulo T.
- $P(0) = -T \equiv 0 \pmod{T}$.

Il existe donc un élément $\Lambda(T) \in \mathbf{Q}[T]$ tel que $P\big(\Lambda(T)\big) \equiv 0 \pmod{T^n}$ et que $\Lambda(T) \equiv 0 \pmod{T}$, et nous savons qu'un élément quelconque de $\mathbf{Q}[T]$ est solution si et seulement s'il est congru à $\Lambda(T)$ modulo T^n (voir II.5).
Il en existe donc une et une seule qui soit de degré strictement inférieur à n, et cette solution n'est autre que $L_n = \Lambda \bmod T^n$.
Enfin, comme l'application $U(T) \to U(1+T)$ de $\mathbf{Q}[T]$ dans lui-même est bijective et conserve le degré, il existe un et un seul polynôme $\ell_n(T) \in \mathbf{Q}[T]$ tel que $\deg \ell_n(T) < n$ et $L_n(T) = \ell_n(1+T)$. On conclut que $\ell_n(T)$ est solution de (1) et est la seule.

2. Posons $r_{m,n}(T) = e_n(T) - e_m(T)$. Le polynôme $r_{m,n}(T)$ est de valuation m et, comme $\ell_n(1+T)$ est de valuation supérieure ou égale à 1, puisque $\ell_n(1) = 0$, le polynôme $r_{m,n}\big(\ell_n(1+T)\big)$ est de valuation supérieure ou égale à m. On conclut que $r_{m,n}\big(\ell_n(1+T)\big) \equiv 0 \pmod{T^m}$.
Il vient donc que $e_m\big(\ell_n(1+T)\big) \equiv e_n\big(\ell_n(1+T)\big) \pmod{T^m}$. Comme $1 \leq m \leq n$, $e_n\big(\ell_n(1+T)\big) \equiv 1+T \pmod{T^m}$. Ainsi, $e_m\big(\ell_n(1+T)\big) \equiv 1+T \pmod{T^m}$, ce qui permet de conclure que

- Si $m > 1$, $e_m\big(\ell_n(1+T)\big) \bmod T^m = 1+T$.

- $e_1\big(\ell_n(1+T)\big) \bmod T = 1$.

Le système (1) écrit en remplaçant n par m admet une unique solution modulo T^m, $\ell_m(T)$ étant son unique représentant de degré strictement inférieur à m. On conclut donc que $\ell_n(1+T) \bmod T^m = \ell_m(1+T)$.
Il existe un polynôme $R_n(T) \in \mathbf{Q}[T]$ tel que $e_n\big(\ell_n(1+T)\big) = 1 + T + R_n(T)T^n$. Il vient donc par dérivation $e'_n\big(\ell_n(1+T)\big)\ell'_n(1+T) = 1 + T^{n-1}\big(nR_n(T) + TR'_n(T)\big)$, d'où $e_{n-1}\big(\ell_n(1+T)\big)\ell'_n(1+T) \equiv 1 \pmod{T^{n-1}}$, ce qui implique encore que $(1+T)\ell'_n(1+T) \equiv 1 \pmod{T^{n-1}}$, soit finalement qu'il existe un polynôme $S(T) \in \mathbf{Q}[T]$ tel que $(1+T)\ell'_n(1+T) = 1 + T^{n-1}S(T)$.
Si $n > 1$, on constate donc que $\ell'_n(1+T)$ est le quotient d'ordre $n-2$ de la division suivant les puissances croissantes de 1 par $1+T$, d'où $\ell'_n(1+T) = 1 - T + T^2 - T^3 + \cdots + (-1)^{n-2}T^{n-2} = \sum_{k=0}^{n-2}(-1)^k T^k$.

Comme $\ell_n(1) = 0$, il vient immédiatement $\ell_n(1+T) = \sum_{k=1}^{n-1} \frac{(-1)^{k-1}}{k} T^k$.

Nous avons vu plus haut que ℓ_1 est le polynôme nul.

3. Il est clair que $e_1\big(Q_1(T)\big) \bmod T = 1$ et que $Q_1(T) \bmod T = 0$. On supposera donc $n > 1$.
On a $e_n\big(Q_n(T)\big) = e_n\big(\ell_n\big(e_n(T)\big)\big) \equiv e_n(T) \pmod{T^n}$, et donc $e_n\big(Q_n(T)\big) \bmod T^n = e_n(T)$.
Nous pouvons appliquer les résultats de la partie II avec $i = n$, $P(X) = e_n(X) - e_n(T)$, $x_1 = 0$ et $a = T$ parce que :

- $P'(X) = e_{n-1}(X)$, d'où $P'(0) = 1$ est inversible modulo T.
- $P(0) \equiv 0 \pmod{T}$.

Le système $P\big(\Lambda(T)\big) \equiv 0 \pmod{T^n}$ et $\Lambda(T) \equiv 0 \pmod{T}$ admet donc une unique solution $\Lambda(T) \in \mathbf{Q}[T]$ modulo T^n.
Or $Q_n(T)$ et T en sont manifestement deux solutions, et l'on peut conclure que $Q_n(T) \equiv T \pmod{T^n}$, soit que $Q_n(T) \bmod T^n = T$.

4. Notons respectivement $\mathcal{N}_n(\mathbf{C})$ et $\mathcal{U}_n(\mathbf{C})$ l'ensemble des matrices nilpotentes et l'ensemble des matrices unipotentes de $\mathcal{M}_n(\mathbf{C})$.
Si $N \in \mathcal{N}_n(\mathbf{C})$ et si ν est le degré de nilpotence de N, alors $1 \leq \nu \leq n$. Donc $\exp(N) = e_\nu(N) = e_n(N) = I_n + NN'$ où N' est une matrice polynomiale en N qui *commute* avec N. La matrice NN' est donc nilpotente et $\exp(N) \in \mathcal{U}_n(\mathbf{C})$. L'exponentielle peut donc être considérée comme une application de $\mathcal{N}_n(\mathbf{C})$ dans $\mathcal{U}_n(\mathbf{C})$.
De même, $\ell_\nu(I_n + N) = \ell_n(I_n + N) = NN''$ où N'' est une matrice polynomiale en N qui *commute* avec N. La matrice NN'' est donc nilpotente et $\ell_n(I_n + N) \in \mathcal{N}_n(\mathbf{C})$. Ainsi, ℓ_n (que l'on peut appeler "logarithme") peut être considérée comme une application de $\mathcal{U}_n(\mathbf{C})$ dans $\mathcal{N}_n(\mathbf{C})$.
Nous avons vu que $\ell_n\big(e_n(T)\big) \equiv T \pmod{T^n}$; il vient donc, pour toute matrice $N \in \mathcal{N}_n(\mathbf{C})$, $\ell_n\big(e_n(N)\big) = N$ puisque le degré de nilpotence de N est inférieur ou égal à n.
Soit une matrice quelconque $U \in \mathcal{U}_n(\mathbf{C})$, s'écrivant $U = I_n + N$ où $N \in \mathcal{N}_n(\mathbf{C})$. Nous avons vu que $e_n\big(\ell_n(1+T)\big) \equiv 1 + T \pmod{T^n}$, et donc $e_n\big(\ell_n(U)\big) = U$, pour la même raison.
L' application $\exp : \mathcal{N}_n(\mathbf{C}) \to \mathcal{U}_n(\mathbf{C})$ et l'application $\ln : \mathcal{U}_n(\mathbf{C}) \to \mathcal{N}_n(\mathbf{C})$ sont donc bijectives et réciproques l'une de l'autre.
De plus, nous avons vu que ce sont des applications "polynomiales" à coefficients rationnels, puisque, sur $\mathcal{N}_n(\mathbf{C})$, $\exp(N) = e_n(N)$ et que, sur $\mathcal{U}_n(\mathbf{C})$, $\ln(U) = \ell_n(U)$.

5. Soit A une matrice telle que $N = A - \lambda I_n$ soit nilpotente.
On sait que l'exponentielle "complexe" est surjective de $\mathbf{C}$ sur $\mathbf{C}^*$: il existe donc un complexe μ tel que $\lambda = e^\mu$.
Pour toute matrice $M \in \mathcal{M}_n(\mathbf{C})$, comme M commute avec μI_n, $\exp(M - \mu I_n) = \exp(M)\exp(-\mu I_n) = \big(\exp(M)\big)\big(e^{-\mu} I_n\big) = (1/\lambda)\exp(M)$.
La matrice M vérifie donc $\exp(M) = A$ si et seulement si elle vérifie $\exp(M - \mu I_n) = (1/\lambda)A$. Or $(1/\lambda)A = I_n + (1/\lambda)N$, et donc $(1/\lambda)A \in \mathcal{U}_n(\mathbf{C})$. Il existe ainsi une (unique) matrice $B' \in \mathcal{N}_n(\mathbf{C})$ telle que $\exp(B') = (1/\lambda)A$, et il existe donc une matrice $B \in \mathcal{M}_n(\mathbf{C})$ telle que $\exp(B) = A$, par exemple la matrice $B = B' + \mu I_n$.
Rappelons avant de poursuivre que, pour toute matrice $M \in \mathcal{M}_n(\mathbf{C})$, $\exp(M) \in \mathrm{GL}_n(\mathbf{C})$: en effet, comme M et $-M$ commutent, $\exp(M)\exp(-M) = \exp(M - M) = \exp(O_n) = I_n$. L'exponentielle peut donc être considérée comme une application de $\mathcal{M}_n(\mathbf{C})$ dans $\mathrm{GL}_n(\mathbf{C})$.

On aperçoit d'emblée que l'injectivité de l'exponentielle n'est plus qu'un lointain souvenir, puisque les matrices $B' + \mu I_n$ et $B' + (\mu + 2i\pi)I_n$ ont toutes deux une exponentielle égale à A et que, comme $\lambda \neq 0$, $A \in \mathrm{GL}_n(\mathbf{C})$.

Considérons maintenant une matrice $A \in \mathrm{GL}_n(\mathbf{C})$ ainsi que l'endomorphisme u de $\mathbf{C}^n$ qui lui est associé dans la base canonique de ce $\mathbf{C}$-espace vectoriel.

Comme le corps $\mathbf{C}$ est algébriquement clos, le polynôme caractéristique χ_u de u est scindé sur $\mathbf{C}$ et s'écrit $\prod_{i=1}^{p}(\lambda_i - X)^{\nu_i}$; $\mathbf{C}^n$ est somme directe des sous-espaces caractéristiques $F_i = \ker(\lambda_i I_n - u)^{\nu_i}$, chaque sous-espace F_i est stable par u et, en notant u_i la restriction de u à F_i, $(\lambda_i I_n - u_i)^{\nu_i}$ est nul.

Cela étant, A est donc semblable à une matrice diagonale *par blocs*, c'est à dire qu'il existe une matrice $H \in \mathrm{GL}_n(\mathbf{C})$ et une matrice A' diagonale *par blocs* telles que $A = HA'H^{-1}$.

La matrice A' s'écrit $\begin{pmatrix} A_1 & O & \dots & O \\ O & A_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & O \\ O & \dots & O & A_p \end{pmatrix}$ et chaque bloc A_i, d'ordre ν_i, est tel que la matrice $(\lambda_i I_{\nu_i} - A_i)^{\nu_i}$ est nulle. La matrice $A_i - \lambda_i I_{\nu_i}$ est donc nilpotente. Si l'on ajoute que $\lambda_i \neq 0$ puisque λ_i est valeur propre de A et que A est régulière, on peut affirmer qu'il existe une matrice $B_i \in \mathcal{M}_{\nu_i}(\mathbf{C})$ telle que $\exp(B_i) = A_i$.

Soit la matrice $B' = \begin{pmatrix} B_1 & O & \dots & O \\ O & B_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & O \\ O & \dots & O & B_p \end{pmatrix}$.

Les calculs par blocs étant ce qu'ils sont, il vient $\exp(B') = \begin{pmatrix} \exp(B_1) & O & \dots & O \\ O & \exp(B_2) & \ddots & \vdots \\ \vdots & \ddots & \ddots & O \\ O & \dots & O & \exp(B_p) \end{pmatrix} = A'$.

Enfin, $\exp(HB'H^{-1}) = H\exp(B')H^{-1} = HA'H^{-1} = A$.

Il existe donc une matrice $B \in \mathcal{M}_n(\mathbf{C})$ telle que $\exp(B) = A$, par exemple la matrice $B = HB'H^{-1}$.

L'application exp : $\mathcal{M}_n(\mathbf{C}) \to \mathrm{GL}_n(\mathbf{C})$ est donc sujective. Nous avons vu qu'elle n'est pas injective.

Partie IV : Racines m-ièmes dans $\mathrm{GL_n(R)}$ ou $\mathrm{GL_n(C)}$

1. Soit $\mu \in \mathbf{K}$ une racine cubique de λ. Il est clair que $\mu \neq 0$.

En considérant l'anneau $\mathbf{A}[Y] = \mathbf{K}[X][Y]$, nous pouvons appliquer les résultats de la partie II avec $i = k$, $P(Y) = Y^3 - X$, $x_1 = \mu$ et $a = X - \lambda$ parce que :

- $P'(Y) = 3Y^2$, d'où $P'(\mu) = 3\mu^2 \neq 0$ est inversible modulo $X - \lambda$.
- $P(\mu) = \mu^3 - X = \lambda - X \equiv 0 \pmod{(X - \lambda)}$.

Le système $P\big(Q(X)\big) \equiv 0 \pmod{(X - \lambda)^k}$ et $Q(X) \equiv \mu \pmod{(X - \lambda)}$ admet donc une solution $Q(X) \in \mathbf{K}[X]$, qui est d'ailleurs unique modulo $(X - \lambda)^k$.

Or la congruence $Q(X)^3 \equiv X \pmod{(X - \lambda)^k}$ s'écrit $P\big(Q(X)\big) \equiv 0 \pmod{(X - \lambda)^k}$ et ce qui vient d'être dit prouve qu'elle admet au moins une solution $Q(X) \in \mathbf{K}[X]$; on peut ajouter qu'elle en admet une et une seule, modulo $(X - \lambda)^k$, vérifiant $Q(\lambda) = \mu$.

2. Considérons le polynôme $\Pi \in \mathbf{K}[X][Y]$ défini par $\Pi(Y) = P(Y) - X$.

Nous pouvons appliquer les résultats de la partie II en y remplaçant P par Π, et avec $i = k$, $x_1 = \mu$ et $a = X - \lambda$ parce que :

- $\Pi'(Y) = P'(Y)$, d'où $P'(\mu) \neq 0$ est inversible modulo $X - \lambda$.
- $\Pi(\mu) = P(\mu) - X = \lambda - X \equiv 0 \pmod{(X - \lambda)}$.

Le système $\Pi\big(Q(X)\big) \equiv 0 \pmod{(X - \lambda)^k}$ et $Q(X) \equiv \mu \pmod{(X - \lambda)}$ admet donc une solution $Q(X) \in \mathbf{K}[X]$, qui est d'ailleurs unique modulo $(X - \lambda)^k$.

Or la congruence $P\big(Q(X)\big) \equiv X \pmod{(X - \lambda)^k}$ s'écrit $\Pi\big(Q(X)\big) \equiv 0 \pmod{(X - \lambda)^k}$ et ce qui vient d'être dit prouve qu'elle admet au moins une solution $Q(X) \in \mathbf{K}[X]$; on peut ajouter qu'elle en admet une et une seule, modulo $(X - \lambda)^k$, vérifiant $Q(\lambda) = \mu$.

3. Comme T_1 et T_2 sont *premiers entre eux*, il existe deux polynômes U_1 et U_2 tels que $U_1T_1 - U_2T_2 = 1$. Posons $V_1 = (Q_2 - Q_1)U_1$ et $V_2 = (Q_2 - Q_1)U_2$: on a $V_1T_1 - V_2T_2 = Q_2 - Q_1$, soit $Q_1 + V_1T_1 = Q_2 + V_2T_2$. Notons Q ce dernier polynôme : il est clair que $Q \equiv Q_1 \pmod{T_1}$ et $Q \equiv Q_2 \pmod{T_2}$.
Note : comme T_1 et T_2 sont *premiers entre eux*, le théorème chinois permet directement d'affirmer qu'il existe un polynôme $Q \in \mathbf{K}[X]$ tel que $Q \equiv Q_1 \pmod{T_1}$ et $Q \equiv Q_2 \pmod{T_2}$. Il permet d'ailleurs aussi d'affirmer que ce polynôme est unique modulo T_1T_2, mais peu importe ici.
Le polynôme P, à coefficients dans $\mathbf{K}$, est à coefficients dans $\mathbf{K}[X]$ et, en appliquant le dernier résultat de la question (I.1), on constate que $P\big(Q(X)\big) \equiv P\big(Q_1(X)\big) \pmod{T_1(X)}$ et $P\big(Q(X)\big) \equiv P\big(Q_2(X)\big) \pmod{T_2(X)}$.
Ainsi, $P\big(Q(X)\big) \equiv X \pmod{T_1}$ et $P\big(Q(X)\big) \equiv X \pmod{T_2}$. Le polynôme $P\big(Q(X)\big) - X$, divisible par chacun des polynômes *premiers entre eux* T_1 et T_2, est divisible par leur produit et donc $P\big(Q(X)\big) \equiv X \pmod{T_1T_2}$.
Signalons pour la suite que ce résultat se généralise d'emblée : si $T_1, T_2, \ldots, T_m$ sont des polynômes appartenant à $\mathbf{K}[X]$ et premiers entre eux *deux à deux*, et s'il existe des polynômes $Q_1, Q_2, \ldots, Q_m$ appartenant à $\mathbf{K}[X]$ tels que, pour tout i, $P\big(Q_i(X)\big) \equiv X \pmod{T_i}$, alors il existe un polynôme $Q \in \mathbf{K}[X]$ tel que $P\big(Q(X)\big) \equiv X \pmod{T_1T_2 \ldots T_m}$. On raisonne par récurrence sur m en observant que, si T_{m+1} est premier avec chacun des polynômes $T_1, T_2, \ldots, T_m$, alors il est premier avec leur produit $T_1T_2 \ldots T_m$.

4. Le polynôme T, que l'on peut supposer unitaire puisque $\mathbf{K}$ est un corps, étant scindé sur $\mathbf{K}$, il existe $m \in \mathbf{N}^*$ et il existe m éléments de $\mathbf{K}$, $\lambda_1, \lambda_2, \ldots, \lambda_m$, distincts deux à deux, et m entiers naturels non nuls, $k_1, k_2, \ldots, k_m$, tels que $T(X) = \prod_{i=1}^{m} (X - \lambda_i)^{k_i}$.
Posons $T_i(X) = (X - \lambda_i)^{k_i}$. La fonction $x \mapsto P(x)$ étant surjective, l'équation $P(x) = \lambda_i$ admet une solution μ_i et l'on sait alors, puisque $T\big(P(\mu_i)\big) = 0$, que $P'(\mu_i) \neq 0$.
On peut donc affirmer, d'après le résultat de la question 2, qu'il existe un polynôme $Q_i(X) \in \mathbf{K}[X]$ tel que $P\big(Q_i(X)\big) \equiv X \pmod{T_i}$. Comme $T = \prod_{i=1}^{m} T_i$ et que les polynômes T_i sont premiers entre eux deux à deux, il existe $Q(X) \in \mathbf{K}[X]$ tel que $P\big(Q(X)\big) \equiv X \pmod{T(X)}$.
Considérons maintenant le cas particulier $P(X) = X^m$.
Si $m \geq 2$, l'étude précédente s'applique (et donc on a l'existence de $Q(X)$) si l'application $x \mapsto x^m$ est surjective de $\mathbf{K}$ dans $\mathbf{K}$ et si le polynôme T est scindé et n'admet pas zéro comme racine (pour que l'on puisse affirmer que, pour tout $\mu \in \mathbf{C}$, si μ^m est racine de T, alors $m\mu^{m-1} \neq 0$).
Si $m = 1$, l'existence de Q est triviale : il suffit de prendre $Q(X) = X$.

5. Le polynôme caractéristique de la matrice A, que nous noterons T, est scindé sur $\mathbf{C}$ et n'admet pas 0 comme racine puisque A est inversible. D'autre part, l'application $x \mapsto x^m$ est surjective de $\mathbf{C}$ dans $\mathbf{C}$; on peut donc appliquer la question précédente avec $P(X) = X^m$, et il existe donc $Q \in \mathbf{C}[X]$ tel que $\big(Q(X)\big)^m \equiv X \pmod{T(X)}$. Or d'après le théorème de Cayley-Hamilton, $T(A) = 0$ donc $\big(Q(A)\big)^m = A$.
En posant $B = Q(A)$, on obtient donc $B^m = A$ et A étant inversible, B l'est également.
Dans le cas où le corps $\mathbf{K}$ est celui des réels, si l'on suppose m impair, l'application $x \mapsto x^m$ est à nouveau surjective de $\mathbf{R}$ dans $\mathbf{R}$. Si on suppose en outre que A a toutes ses racines réelles, son polynôme caractéristique est scindé sur $\mathbf{R}$ et on peut donc appliquer la question 4 et établir comme ci-dessus l'existence de $B \in \mathrm{GL}_n(\mathbf{R})$ telle que $B^m = A$.

Note : il ne faut cependant pas croire que, si $B^m = A$, B soit nécessairement "polynomiale en A". Par exemple, si $A = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 & -1 & 1/2 \\ 0 & 2 & -1 & 0 \\ 0 & 3 & -2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, $B^2 = A$, mais B n'est pas polynomiale en A.

6. Si α est l'une des racines de $aX^2 + bX + c$, l'autre est $\bar{\alpha}$ et tout polynôme réel qui admet α comme racine admet aussi $\bar{\alpha}$ comme racine et est donc multiple de $aX^2 + bX + c$. La réciproque étant évidente, on a montré qu'un polynôme réel est multiple de $aX^2 + bX + c$ si et seulement s'il admet α pour racine.
Si Q est un polynôme réel, $Q(X)^m \equiv X \pmod{(aX^2 + bX + c)}$ si et seulement si $Q(X)^m - X$ est un multiple de $aX^2 + bX + c$, soit, d'après ce qui précède, si et seulement si $Q(\alpha)^m = \alpha$. Cherchons Q sous la

forme $uX+v$ où u et v sont des réels. Soit $z \in \mathbf{C}$ tel que $z^m = \alpha$. Comme $\alpha \notin \mathbf{R}$, il existe $(u,v) \in \mathbf{R}^2$ tel que $z = u\alpha + v$ et donc $(u\alpha+v)^m = \alpha$ et $(uX+v)^m \equiv X \pmod{(aX^2+bX+c)}$.
On applique maintenant le (II.5) avec $\mathrm{A} = \mathbf{R}[X]$, $\mathrm{a} = aX^2+bX+c$, $x_1 = uX+v$, $P(Y) = Y^m - X$ et enfin $i = k$; on en déduit qu'il existe $Q \in \mathbf{R}[X]$ tel que $Q(X)^m \equiv X \pmod{(aX^2+bX+c)^k}$, puisque :

- $P(uX+v) \equiv 0 \pmod{\mathrm{a}}$, ce qui découle de $(uX+v)^m \equiv X \pmod{(aX^2+bX+c)}$.
- $P'(uX+v) = m(uX+v)^{m-1}$ est inversible modulo a, parce que, aX^2+bX+c n'admettant pas de racine réelle, c est non nul, que m est non nul, et que $-\dfrac{1}{mc}(aX+b)(uX+v)P'(uX+v) \equiv -\dfrac{1}{c}(aX^2+bX) \equiv 1 \pmod{(aX^2+bX+c)}$.

7. T étant un polynôme réel sans racines réelles, T s'écrit sous la forme $T = \prod_{i=1}^{p} T_i$ où T_i est une puissance d'un polynôme réel du second degré sans racines réelles. Pour $i \neq j$, les polynômes T_i et T_j sont premiers entre eux, et il résulte de la question précédente et de la question (IV.3) qu'il existe $Q(X) \in \mathbf{R}[X]$ tel que $Q(X)^m \equiv X \pmod{T(X)}$.
Si A est une matrice réelle sans valeurs propres réelles, son polynôme caractéristique T est sans racines réelles et on peut lui appliquer la question précédente. Or $T(A) = 0$ donc $Q(A)^m = A$ et par suite il existe une matrice $B = Q(A) \in \mathcal{M}_n(\mathbf{R})$ telle que $B^m = A$.

PARTIE V : À propos de la décomposition "diagonale + nilpotente"

1. On peut écrire $\chi = \lambda \prod_{i=1}^{p} P_i^{\alpha_i}$ où $\lambda \in \mathbf{K}$ et les P_i sont des polynômes irréductibles et unitaires. Pour que P divise χ, il est nécessaire que ses seuls diviseurs irréductibles soient des polynômes P_i ; pour que χ divise une puissance de P, il est nécessaire que tous les P_i divisent P. Comme P doit être sans facteur carré et unitaire, nécessairement $P = \prod_{i=1}^{p} P_i$, ce qui prouve l'unicité de P. Comme ce polynôme $\prod_{i=1}^{p} P_i$ est manifestement solution du problème posé, on a prouvé son existence et son unicité.
Si P est sans facteur carré, $P = \prod_{i=1}^{p} P_i$ où les P_i sont irréductibles. On a alors $P' = \sum_{j=1}^{p} P_j' \prod_{\substack{1 \leq i \leq p \\ i \neq j}} P_i$. On constate que pour $1 \leq k \leq p$, P_k ne divise pas P_k', donc ne divise pas P', et est donc premier avec P' : P est donc premier avec P'. Réciproquement, si P est premier avec sa dérivée, il n'a aucune racine double dans $\mathbf{C}$, donc n'est divisible par aucun polynôme qui soit le carré d'un polynôme à coefficients dans $\mathbf{C}$ et, a fortiori, est un polynôme sans facteur carré de $K[X]$.
Soient le polynôme $T = \mathrm{pgcd}(\chi, \chi')$ et le polynôme P vérifiant $\chi = TP$, T étant choisi de sorte que le polynôme P soit *unitaire*.
Il est clair que P divise χ. Montrons que χ divise une puissance de P.
Soit Q un facteur irréductible de χ : montrons que Q divise P. S'il n'en était pas ainsi, Q diviserait T et donc χ'. Posons $\chi = Q^\alpha R$, avec R et Q premiers entre eux et $\alpha \in \mathbf{N}^*$. On a $\chi' = \alpha Q^{\alpha-1}Q'R + Q^\alpha R'$. Le polynôme Q, étant irréductible, est premier avec Q' : donc Q^α divise χ mais ne divise pas χ', et donc ne divise pas T. Or $\chi = PT$, donc Q divise P, ce qui est absurde.
On a donc montré que tous les facteurs irréductibles de χ divisent P, donc χ divise une puissance de P.
Il reste à montrer que P est sans facteur carré, et il suffit pour cela de montrer que P est premier avec sa dérivée. Supposons qu'il n'en soit pas ainsi et soit Q un polynôme irréductible diviseur commun à P et P'. On a $P = Q^\alpha P_1$, avec Q et P_1 premiers entre eux. Et de même $T = Q^\beta T_1$, avec Q et T_1 premiers entre eux. On a aussi $P' = \alpha Q' Q^{\alpha-1}P_1 + Q^\alpha P_1'$ et donc, puisque Q et Q' sont premiers entre eux, $\alpha \geq 2$. Par ailleurs, $\chi = PT = Q^{\alpha+\beta}P_1T_1$. On a alors $\chi' = (\alpha+\beta)Q^{\alpha+\beta-1}Q'T_1P_1 + Q^{\alpha+\beta}(T_1P_1)'$. Donc $Q^{\alpha+\beta-1}$ divise χ et χ' et donc divise T : ainsi, $\alpha+\beta-1 \leq \beta$ et donc $\alpha \leq 1$, ce qui est contradictoire avec $\alpha \geq 2$ trouvé ci-dessus.
On a donc établi que $P = \dfrac{\chi}{\mathrm{pgcd}(\chi,\chi')}$ (par abus de notation).

2. Le polynôme P, étant premier avec sa dérivée, n'a pas de racine double dans $\mathbf{C}$. Il en résulte que toute matrice complexe annulée par P est diagonalisable dans $\mathbf{C}$.

3. Le polynôme P étant premier avec sa dérivée, il existe (d'après le théorème de Bezout) deux polynômes U et V à coefficients dans $\mathbf{K}$ tels que $PU + P'V = 1$. On en déduit que $P'(A)V(A) = I - BU(A)$, ce qui prouve que $P'(A)$ est inversible modulo B.
Pour calculer un inverse de $P'(A)$, il suffit de calculer un couple de polynômes (U, V) tels que $PU+P'V = 1$. (On sait qu'un tel couple s'obtient par divisions successives de P par P', puis de P' par le reste obtenu précédemment, et ainsi de suite jusqu'à obtenir un reste constant ; on procède alors à une combinaison des différentes relations obtenues.)

4. On construit une suite de matrices $(A_i)_{i\geq 1}$ comme on a construit une suite $(x_i)_{i\geq 1}$ dans le (II.3) avec $x_1 = A$ et $a = B$.
Il existe une puissance de P qui est égale au polynôme caractéristique de A, donc B est nilpotente et donc $B^n = 0$. Par ailleurs, d'après le (II.5), il existe une matrice unique D telle que $P(D) \equiv 0 \pmod{B^n}$ et $D \equiv A \pmod{B}$. Donc $P(D) = 0$ et, comme on l'a vu au (V.2), D est diagonalisable sur $\mathbf{C}$. Par ailleurs, il existe $Q \in \mathbf{K}[X]$ tel que $C = A+BQ(A)$. Posons $N = BQ(A)$. N est un polynôme en A (puisque $B = P(A)$) et, comme B est nilpotente et commute avec A, la matrice N est également nilpotente. On a ainsi établi l'existence d'une décomposition (2).

5. Soit P un polynôme sans facteur carré à coefficients dans $\mathbf{K}$. On considère l'anneau $\mathbf{A} = \mathbf{K}[X]$. Les hypothèses du (II.3) sont vérifiées avec le polynôme P déjà défini, considéré comme polynôme à coefficients dans $\mathbf{K}[X]$, et $x_1 = X$ et $a = P(X)$. D'après l'égalité de Bezout, $P'(x_1)$ est inversible modulo a et donc, pour i entier fixé, il existe $Q_i \in \mathbf{K}[X]$ tel que $P\big(Q_i(X)\big) \equiv 0 \pmod{P^i}$ et $Q_i(X) \equiv X \pmod{P}$.
En substituant A à X, on obtient : $P\big(Q(A)\big) = P^i(A)R(A)$ et $Q_i(A) = A + P(A)S(A)$ où R et S sont des polynômes à coefficients dans $\mathbf{K}$. On prend alors pour P le même polynôme que dans (V.2) et on conclut comme dans (V.4).