Devoir de Mathématiques n°5

Kévin Polisano
MP*

Jeudi 15 octobre 2009

Partie I : préliminaires relatifs aux congruences et polynômes

1. $x-y=\lambda a,\ x'-y'=\lambda' a \Rightarrow (x+x')-(y+y')=(\lambda+\lambda')a=\lambda'' a$ soit $x+x'\equiv y+y'[a]$.

$xx'-yy'=x(x'-y')+y'(x-y)=x\lambda' a+y'\lambda a=(x\lambda'+y'\lambda)a=\lambda'' a$ soit $xx'\equiv yy'[a]$.

On a donc en particulier $x^k\equiv y^k[a]$ et par compatibilité de la somme $P(x)\equiv P(y)[a]$.

2. $zz'\equiv 1[a]$ et $zz''\equiv 1[b]$ donc $(zz'-1)(zz''-1)=(\lambda a)(\lambda' b)=(\lambda\lambda')(ab)\equiv 0[ab]$, or :

$$(zz'-1)(zz''-1)=z(zz'z''-z'-z'')+1\Rightarrow z(z'+z''-zz'z'')\equiv 1[ab]$$

On a ainsi exhibé l'inverse de z modulo ab.

3. Soit $P(X)=\sum_{k=0}^{n}a_kX^k$, on a compte tenu de l'identité $Y^k-X^k=(Y-X)\sum_{i=0}^{n-1}Y^{n-1-i}X^i$:

$$P(Y)-P(X)=(Y-X)\sum_{k=1}^{n}a_k\left(\sum_{i=0}^{k-1}Y^{k-1-i}X^i\right)=(Y-X)Q(X,Y)\ (1)$$

Calculons $Q(X,X)$:

$$Q(X,X)=\sum_{k=1}^{n}a_k\left(\sum_{i=0}^{k-1}X^{k-1}\right)=\sum_{k=1}^{n}ka_kX^{k-1}$$

qui n'est autre que le polynôme dérivé $\Rightarrow Q(X,X)=P'(X)$.

On applique la formule de Taylor pour les polynômes :

$$P(X+Y)=P(X)+P'(X)Y+Y^2\sum_{k=2}^{n}\frac{P^{(k)}(X)}{k!}Y^{k-2}=P(X)+P'(X)Y+Y^2R(X,Y)\ (2)$$

Effectuons le changement $Y\leftarrow Y-X$, l'égalité devient :

$$P(Y)-P(X)=(Y-X)[P'(X)+(Y-X)R(X,Y-X)]=(Y-X)Q(X,Y)$$

Partie II : méthode de remontée modulaire

1. $P(x) \equiv 0[a^i] \Leftrightarrow P(x) = ka^i$ avec $k \in A$. Notons z' un inverse de $P'(x)$ mod a.

Montrons que $\lambda = -kz'$ convient en appliquant (2) :

$$P(x-kz'a^i) = P(x)-kP'(x)z'a^i+(-kz'a^i)^2R(x,-kz'a^i) = ka^i-k(1+\beta a)a^i+a^{i+1}(k^2z'^2a^{i-1}R(x,-kz'a^i))$$

$$P(y) = a^{i+1}[-k\beta + k^2z'^2a^{i-1}R(x,-kz'a^i)] \equiv 0[a^{i+1}]$$

On choisit donc $y = x + \lambda a^i = x - z'ka^i = x - z'P(x)$.

Prenons un autre inverse de $P'(x)$ disons z'', $y' = x - z''P(x)$ et : $y - y' = (z'' - z')P(x)$.

Or il est clair que $z'' \equiv z'[a] \Leftrightarrow z'' - z' = \alpha a$ et $P(x) = ka^i$ d'où :

$$y - y' = \alpha k a^{i+1} \equiv 0[a^{i+1}]$$

Donc la classe de y modulo a^{i+1} ne dépend pas du choix de l'inverse.

2. Considérons $P(X) = zX - 1$. On a $P(z') = zz' - 1 \equiv 0[a]$ et $P'(z') = z$ bien inversible.

On applique ce qui précède $y = z' - z'ka$ où $ka = zz' - 1$ d'où $y = z'(1 - (zz' - 1)) = z'(2 - zz')$

$$P(y) = z[z'(2 - zz')] - 1 \equiv 0[a^2]$$

3. On construit la suite (x_i) par récurrence :

<u>Initialisation</u> : $P(x_1) \equiv 0[a]$, $P'(x_1)z'_1 \equiv 1[a]$.

On forme $x_2 = x_1 - z'_1P(x_1) \Rightarrow x_2 \equiv x_1[a]$. D'après 1. on a $P(x_2) \equiv 0[a^2]$.

Or d'après I.1 $x_2 \equiv x_1[a] \Rightarrow P'(x_2) \equiv P'(x_1)[a]$ ce qui permet d'enclencher la récurrence.

<u>Hérédité</u> : Supposons $P(x_i) \equiv 0[a^i]$ et $P'(x_i)z'_i \equiv 1[a^i]$.

On forme $x_{i+1} = x_i - z'_iP(x_i) \Rightarrow x_{i+1} \equiv x_i[a^i]$. $P(x_{i+1}) \equiv 0[a^{i+1}]$.

Et on a aussi $x_{i+1} \equiv x_i[a]$ d'où $P'(x_{i+1}) \equiv P'(x_i)[a]$ inversible. □

Si on part d'un autre inverse de $P'(x_1)$ on a $y_2 \equiv x_2[a^2]$ d'après II.1.

Par récurrence ensuite puisque $x_{i+1} \equiv x_i[a^i]$ et $y_{i+1} \equiv x_i[a^i]$ il vient :

$$y_i \equiv x_i[a^i]$$

5. x_i construit comme *supra* est une solution du système, avec en outre $P'(x_i)$ inversible.

Soit y_i une autre solution, on a alors $P(y_i) \equiv P(x_i)[a^i]$ et $y_i \equiv x_i[a]$.

Par conséquent d'après 4. on a $y_i \equiv x_i[a^i]$ d'où l'unicité modulo a^i.

Partie III : troncature de l'exponentielle et du logarithme

1. Considérons le polynôme suivant :

$$P(X) = 1 + \frac{X}{1!} + \frac{X^2}{2!} + \cdots + \frac{X^{n-1}}{(n-1)!} - (1+T) \in \mathbb{Q}[T][X]$$

D'après II.5 il existe une unique solution au système :

$$P(l_n(1+T)) \equiv 0[T^n] \text{ et } l_n(1+T) \equiv 0[T] \Leftrightarrow e_n(l_n(1+T)) \equiv 1+T[T^n] \text{ et } l_n(1) = 0 \ (*)$$

(on a bien les hypothèses $P(0_A) = T \equiv 0[T]$ et $P'(0_A) = 1$ inversible modulo T).

2. Ecrivons :

$$e_m(l_n(1+T)) = e_n(l_n(1+T)) - \left(\frac{l_n(1+T)^m}{m!} + \cdots + \frac{l_n(1+T)^{n-1}}{(n-1)!}\right)$$

Or $e_n(l_n(1+T)) = 1 + T + T^n R(T)$ et $l_n(1+T) = TS(T)$ soit en remplaçant il vient :

$$\forall 1 \leqslant m \leqslant n,\ e_m(l_n(1+T)) \equiv 1 + T[T^m]$$

Dérivons $(*)$ c'est-à-dire : $e_n(l_n(1+T)) = \displaystyle\sum_{k=0}^{n-1} \frac{l_n(1+T)^k}{k!} = 1 + T + T^n R(T)$:

$$l_n'(1+T) \sum_{k=0}^{n-2} \frac{l_n(1+T)^{k-1}}{(k-1)!} = 1 + nT^{n-1}R(T) + T^n R'(T) = 1 + T^{n-1}U(T)$$

soit :

$$e_{n-1}(l_n(1+T))l_n'(1+T) \equiv 1[T^{n-1}]$$

Or pour $m = n-1$ on a $e_m(l_n(1+T)) \equiv 1 + T[T^{n-1}]$ donc $(1+T)l_n'(1+T) \equiv 1[T^{n-1}]$.

Mais on connait un inverse de $1+T$ modulo T^{n-1} puisque l'on a l'identité :

$$T^{n-1} - 1 = (T-1)\sum_{k=0}^{n-2} T^k \Rightarrow 1 = (1+T)\sum_{k=0}^{n-2}(-1)^k T^k [T^{n-1}]$$

Ainsi :

$$l_n'(1+T) \equiv \sum_{k=0}^{n-2}(-1)^k T^k [T^{n-1}]$$

On intègre et sachant que $l_n(1) = 0$ on obtient finalement :

$$l_n(1+T) = T - \frac{T^2}{2} + \frac{T^3}{3} - \cdots + (-1)^{n-1}\frac{T^{n-1}}{n-1}$$

qui est le logarithme tronqué comme on pouvait s'y attendre.

3. En utilisant $(*)$ on a :

$$e_n(Q_n(T)) = e_n \circ l_n\left[1 + \left(\frac{T}{1!} + \frac{T^2}{2!} + \cdots + \frac{T^{n-1}}{(n-1)!}\right)\right] \equiv 1 + \left(\frac{T}{1!} + \frac{T^2}{2!} + \cdots + \frac{T^{n-1}}{(n-1)!}\right)[(e_n(T)-1)^n]$$

En factorisant $e_n(T)-1$ par T on a alors $e_n(Q_n(T)) \equiv e_n(T)[T^n]$.

Posons $P = e_n$, $x = Q_n(T)$ et $y = T$, on va vérifier les hypothèses de la question II.4 :

On vient de voir que $P(x) \equiv P(y)[T^n]$. On a aussi :

$$Q_n(T) = l_n(e_n(T)) = l_n\left[1+(e_n(T)-1)\right] \equiv (e_n(T)-1)-\frac{(e_n(T)-1)^2}{2}+\cdots+(-1)^{n-1}\frac{(e_n(T)-1)^{n-1}}{(n-1)} \equiv 0[T]$$

Donc $x \equiv y[T]$. Enfin d'après III.2 :

$$P'(x) = e_{n-1}(Q_n(T)) = e_{n-1}[l_n(1+(e_n(T)-1))] \equiv 1+\left(T+\frac{T^2}{2!}+\cdots+\frac{T^{n-1}}{(n-1)!}\right)[(e_n(T)-1)^{n-1}] \equiv 1[T]$$

Par conséquent $x \equiv y[T^n]$ soit $Q_n(T) \equiv T[T^n]$ i.e $l_n(e_n(T)) \equiv T[T^n]$.

4. Montrons tout d'abord que l'exponentielle d'une matrice nilpotente est bien unipotente :

Notons p l'indice de nilpotence de M, on a bien :

$$\exp(M) = \sum_{k=0}^{+\infty}\frac{1}{k!}M^k = e_p(M) = I_n + \underbrace{M\sum_{k=1}^{p-1}\frac{1}{k!}M^{k-1}}_{\text{nilpotente}}$$

Soit $U = I_n + M'$ avec M' nilpotente d'indice p',

$$l_{p'}(I_n+(U-I_n)) = M' - \frac{M'^2}{2!}+\cdots+(-1)^{p'}\frac{M'^{p'-1}}{(p'-1)!}$$

est nilpotente (mettre M' en facteur).

La bijection résulte du fait que e_p et l_p sont réciproques l'une de l'autre (cf $(*)$ et 3.).

5. Notons $M = A-\lambda I_n$ nilpotente. On a $\frac{1}{\lambda}A = I_n + \frac{1}{\lambda}M$ unipotente.

On peut donc appliquer 4. : il existe une matrice M' nilpotente telle que $\exp(M') = \frac{1}{\lambda}A$.

Ici j'utilise la surjectivité de l'exponentielle complexe (HP mais je ne vois pas comment faire autrement), il existe $\lambda' \in \mathbb{C}$ tel que $e^{\lambda'} = \lambda$ et puisque M' et $\lambda' I_n$ commutent :

$$\exp(M'+\lambda' I_n) = A$$

Je n'ai pas réussi à conclure quant à la surjectivité de l'exponentielle de $M_n(\mathbb{C})$ sur $GL_n(\mathbb{C})$.

On a vu l'an passé qu'elle n'était pas injective, en considérant la matrice

$$C_\theta = \begin{pmatrix} 0 & \theta \\ -\theta & 0 \end{pmatrix}$$

On remarque que $C_\theta^2 = -\theta^2 I_2$, on sépare alors les puissances selon la parité :

$$\sum_{k=0}^{\infty}\frac{1}{k!}C_\theta^k = \left(\sum_{k=0}^{\infty}(-1)^k\frac{\theta^{2k}}{(2k+1)!}\right)C_\theta + \left(\sum_{k=0}^{\infty}(-1)^k\frac{\theta^{2k}}{(2k)!}\right)I_2 = \frac{\sin(\theta)}{\theta}C_\theta + \cos(\theta)I_2$$

D'où :

$$\exp(C_\theta) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}$$

On a par exemple $\exp(C_{2\pi}) = \exp(C_0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $C_{2\pi} \neq C_0$.

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

1. Considérons $P(Y) = Y^3 - X \in K[X][Y]$ et μ la racine cubique de λ dans K. On a :

$$P(\mu) = \mu^3 - X = \lambda - X \equiv 0[X-\lambda] \text{ et } P'(\mu) = 2\mu^2 \neq 0 \text{ d'inverse } \frac{1}{2}(\mu - \frac{1}{\mu^2}X)[X-\lambda]$$

Donc d'après la partie II :

$$\forall k \in \mathbb{N}^*,\ \exists Q \in K[X],\ P(Q(X)) \equiv 0[(X-\lambda)^k] \Leftrightarrow Q(X)^3 \equiv X[(X-\lambda)^k]$$

remarque : on n'a plus forcément unicité puisque l'on n'impose pas $Q(X) \equiv \mu[X-\lambda]$.

2. Même principe on considère $R(Y) = P(Y) - X$, $R(\mu) = P(\mu) - X = \lambda - X \equiv 0[X-\lambda]$ et $R'(\mu) = P'(\mu) \neq 0$ inversible dans K, ainsi $[P'(\mu)]^{-1}(X-\lambda)$ est un inverse de $R'(\mu)$ modulo $X-\lambda$. Les hypothèses sont de nouveau vérifiées donc l'équation suivante admet une solution pour tout $k \in \mathbb{N}^*$:

$$P(Q(X)) \equiv X[(X-\lambda)^k]$$

3. L'existence a démontré fait directement pensé au théorème des restes chinois, mais je n'arrive pas l'utiliser proprement...

4. Le polynôme T est scindé sur K donc de la forme :

$$T(X) = \prod (X-\lambda_i)^{\alpha_i}$$

Comme l'application $x \mapsto P(x)$ est une surjection, $\forall i, \exists \mu_i \backslash P(\mu_i) = \lambda_i$.

Les $P(\mu_i)$ sont racines de T donc $P'(\mu_i) \neq 0$. Ainsi d'après 2. les équations :

$$P(Q_i(X)) \equiv X[(X-\lambda_i)^{\alpha_i}]$$

admettent des solutions. Et les facteurs $(X-\lambda_i)^{\alpha_i}$ sont premiers entre eux donc d'après 3. :

$$P(Q(X)) \equiv X[\prod (X-\lambda_i)^{\alpha_i}] \Leftrightarrow P(Q(X)) \equiv X[T]$$

admet une solution.

5. On se place dans $K = \mathbb{C}$, et choisissons pour T le polynôme caractéristique de A.

T est scindé sur $\mathbb{C}$, en outre $x \mapsto P(x) = x^m$ y est surjective donc une racine de T $\lambda = P(\mu)$. Montrons que $P'(\mu) \neq 0$. Supposons le contraire : $P'(\mu) = m\mu^{m-1} = 0 \Leftrightarrow \mu = 0$ par suite on aurait $P(\mu) = 0 = \lambda$ donc 0 serait valeur propre de A, absurde puisque A inversible.

Donc d'après 4. il existe $Q \in \mathbb{C}[X]$ tel que :

$$Q(X)^m = X + T(X)U(X)$$

D'après le théorème de Cayley-Hamilton $T(A) = 0$ d'où :

$$Q(A)^m = A$$

Ainsi $B = Q(A)$ convient et est inversible par passage au déterminant.

Le cas réel est similaire car on suppose que toutes les valeurs propres de A sont réelles (donc son polynôme caractéristique T est scindé sur $\mathbb{R}$) et m est pris impair donc $x \mapsto x^m$ définit bien une surjection. Le reste de la démonstration est identique.

6. Je ne vois pas ce qu'on entend par caractériser, est-ce simplement $(X-\alpha)(X-\overline{\alpha})Q(X)$?

7. T est sans racine réelle, donc se décompose comme suit :

$$T(X) = \prod_i (a_i X^2 + b_i X + c_i)^{\alpha_i}$$

où les facteurs sont premiers entre eux. Donc d'après 6. et 3. l'équation :

$$Q(X)^m \equiv X[T]$$

admet une solution. De même on prend $T = \chi_A$ qui est bien sans racine réelle puisque A n'a pas de valeur propre réelle, puis on évalue en A :

$$Q(A)^m = A$$

Partie V : à propos de la décomposition de Dunford

1. Soit $\chi \in K[X]$ de degré n, l'écriture nous fait bien sûr pensé au polynôme caractéristique d'une matrice. On peut en effet faire de χ le polynôme caractéristique de sa matrice compagnon $A \in \mathcal{M}_n(K)$. Notons u l'endomorphisme associé de K^n, et P son polynôme minimal (qui est unitaire et sans facteur carré). On sait d'après le cours que $P \,|\, \chi$ (conséquence du théorème de Cayley-Hamilton) et $\chi \,|\, P^n$ (on se place dans $\mathcal{M}_n(K[X])$, on effectue une CL pour obtenir $P(X) = (A - XI_n)Q(X)$ et on passe au déterminant).

J'ai trouvé une preuve plus élémentaire (en cherchant la question suivante) mais dans le doute je laisse la précédente : le polynôme χ peut se décomposer dans $K[X]$ comme produit de polynômes irréductibles unitaires $\chi = \lambda \chi_1^{m_1} \chi_2^{m_2} \cdots \chi_s^{m_s}$. On peut alors prendre $P = \chi_1 \chi_2 \cdots \chi_s$ qui divise bien χ et il existe un entier r tel que P^r divise χ (prendre le ppcm des ordres de multiplicité).

remarque : n'y a-t-il pas une erreur d'énoncé quant à l'unicité ?

Montrons qu'un polynôme $P \in K[X]$ est sans facteur carré ssi $\mathrm{pgcd}(P, P') = 1$.

$\boxed{\Leftarrow}$ Par contraposée, supposons $P = Q^2 R$ alors en dérivant :

$$P' = Q(2Q'R + QR') \Rightarrow Q\ P \text{ et } Q \,|\, P' \Rightarrow \mathrm{pgcd}(P, P') \neq 1$$

$\boxed{\Rightarrow}$ Ecrivons $P = P_1^{m_1} P_2^{m_2} \cdots P_s^{m_s}$ et dérivons, on obtient :

$$P' = \sum_{i=1}^{s} m_i P_i' \frac{P}{P_i}$$

Par contraposée de nouveau supposons $\text{pgcd}(P, P') \neq 1$, alors il existe P_i divisant P'. Pour $j \neq i$, P_i divise les $\frac{P}{P_j}$ dans la somme donc P_i divise $m_i P_i' \frac{P}{P_i}$. Comme P_i ne peut pas diviser P_i' c'est qu'il divise $\frac{P}{P_i}$ donc P_i^2 divise P, P possède un facteur carré.

Ecrivons $\chi = \chi_i^{m_i} Q$ et dérivons :

$$\chi' = (m_i \chi_i' Q + \chi_i Q') \chi_i^{m_i - 1}$$

χ_i étant irréductible, il n'a pas de facteur carré donc est premier avec χ_i', par conséquent l'ordre de multiplicité de χ_i dans χ' est exactement $m_i - 1$, on en déduit alors (avec $P = \chi_1 \chi_2 \cdots \chi_s$) :

$$\chi = \lambda \text{pgcd}(\chi, \chi') P \Leftrightarrow P = \frac{\chi}{\lambda \text{pgcd}(\chi, \chi')}$$

2. P est scindé dans $\mathbb{C}$ et sans facteur carré donc séparablement scindé dans $\mathbb{C}$. Ainsi si une matrice l'annule alors elle est diagonalisable dans $\mathbb{C}$.

3. P est sans facteur carré donc premier avec P', d'après le théorème de Bézout :

$$\exists (U, V) \in K[X]^2, \quad UP + VP' = 1$$

On évalue en A : $V(A)P'(A) \equiv I_n[B]$. Ainsi $P'(A)$ est inversible modulo B d'inverse $V(A)$.

Pour calculer V (donc l'inverse $V(A)$) on applique l'algorithme d'Euclide étendu à P et P'.

4. On a $P'(A)$ inversible modulo B et bien sûr $P(A) \equiv 0[B]$ donc d'après II.3 et II.5 on peut construire une telle suite :

$$P(A_i) \equiv 0[B^i], \quad A_i \equiv A[B]$$

Puisque $\chi \,|\, P^r \Leftrightarrow P^r = \chi Q$ d'après le théorème de Cayley-Hamilton :

$$P(A)^r = \chi(A) Q(A) = 0 \Rightarrow B \text{ nilpotente}$$

Donc pour $i = r$ par exemple on a $P(A_i) = 0$ donc A_i diagonalisable dans $\mathbb{C}$ d'après V.2.

Alors $A = A_i + RB$ qui est bien la somme d'une matrice diagonalisable et nilpotente.

5. Vérifions les hypothèses de II.3 avec $a = P$, $x_1 = X$ et $z = Q_i(X)$:

$P(x_1) = P(X) \equiv 0[P]$ et $P'(x_1) = P'(X)$ inversible modulo P car sans facteur carré donc premier avec P :

$$UP + VP' = 1 \Rightarrow VP' \equiv 1[P]$$

$$P(Q_i(X)) \equiv 0[P^i], \quad Q_i(X) \equiv X[P]$$

On prend alors $i = r$ et on évalue en A, on retrouve la décomposition de Dunford.