

AGRÉGATION INTERNE

DE MATHÉMATIQUES

Session 2010, épreuve 1

– NOTATIONS ET PRÉLIMINAIRES –

- Étant donnés deux entiers  $p$  et  $q$  tels que  $p \leq q$ , on note  $[p, q]$  l'ensemble des **entiers**  $k$  vérifiant  $p \leq k \leq q$ .
- Dans ce problème  $K$  désigne un corps commutatif de caractéristique différente de deux.
- Pour tout polynôme  $P$  de  $K[X]$ , on note  $d^\circ P$  le degré de  $P$  (on rappelle que, par convention, le polynôme 0 a pour degré  $-\infty$ ).
- Un polynôme non nul  $P$  de  $K[X]$  est dit normalisé si le coefficient du terme de plus haut degré est égal à 1.
- Pour tout entier naturel  $m$ ,  $K_m[X]$  désigne le sous-espace vectoriel de  $K[X]$  constitué des polynômes de degré inférieur ou égal à  $m$ .
- Si  $E$  est un  $K$ -espace vectoriel, on notera  $E^*$  son espace dual.
- Soient  $E$  et  $F$  deux  $K$ -espaces vectoriels. On note  $\mathcal{L}(E, F)$  l'ensemble des applications linéaires de  $E$  à valeurs dans  $F$ . Pour toute application  $f \in \mathcal{L}(E, F)$ , on appelle transposée de  $f$  l'application (linéaire) notée  ${}^t f$  définie sur  $F^*$  et à valeurs dans  $E^*$  par :

$$\forall \varphi \in F^*, {}^t f(\varphi) = \varphi \circ f$$

- On note  $\mathcal{M}_p(K)$  l'algèbre des matrices carrées de taille  $p$  à coefficients dans  $K$ .
- On identifiera les vecteurs de  $K^p$  aux matrices correspondantes de  $\mathcal{M}_{p,1}(K)$ .
- Si  $A$  et  $B$  sont deux polynômes de  $K[X]$ , avec  $B$  non nul, on note  $A \bmod B$  le reste de la division euclidienne de  $A$  par  $B$ .
- Soient  $A, B, C$  des polynômes de  $K[X]$ . On écrira  $A \equiv B \bmod C$  si  $C$  divise  $A - B$ .
- Pour tout couple  $(A, B) \in K[X]^2$  avec  $(A, B) \neq (0, 0)$ , on note  $A \wedge B$  le pgcd du couple  $(A, B)$  (c'est donc un polynôme normalisé).
- Soit  $E$  un  $K$ -espace vectoriel non nul. On note  $\mathcal{S}(E)$  l'espace vectoriel des suites de  $E$  indexées par  $\mathbf{N}$ . On aura l'occasion d'utiliser l'application  $\sigma : \mathcal{S}(E) \rightarrow \mathcal{S}(E)$  qui à une suite  $u = (u_n)_{n \in \mathbf{N}}$  de  $E$  associe la suite  $\sigma(u)$  définie par :

$$\forall n \in \mathbf{N}, [\sigma(u)]_n = u_{n+1}$$

Cette application  $\sigma$ , nommée **décalage d'indices**, est clairement un endomorphisme de l'espace  $\mathcal{S}(E)$ .

- Soit  $P = \sum_{k=0}^r p_k X^k \in K[X]$ . On désigne par  $P(\sigma)$  l'endomorphisme de  $\mathcal{S}(E)$  défini par substitution de  $\sigma$  à  $X$  :

$$P(\sigma) = p_0 \text{Id} + p_1 \sigma + \dots + p_r \sigma^r$$

On rappelle que, pour tout couple  $(P, Q) \in K[X]^2$  on a :

$$(P + Q)(\sigma) = P(\sigma) + Q(\sigma) \quad \text{et} \quad (PQ)(\sigma) = P(\sigma) \circ Q(\sigma).$$

- Pour toute suite  $u = (u_n)_{n \in \mathbf{N}} \in \mathcal{S}(E)$ , on appelle **annulateur** de  $u$  le sous-ensemble de  $K[X]$ , noté  $\text{Ann}(u)$ , défini par :

$$\text{Ann}(u) = \{P \in K[X] / P(\sigma)(u) = 0\}$$

- Une suite  $u = (u_n)_{n \in \mathbf{N}} \in \mathcal{S}(E)$  est dite **linéaire récurrente** s'il existe un entier  $r \geq 0$  ainsi que des scalaires  $q_0, q_1, \dots, q_r$  tels que  $q_0 \neq 0$  et :

$$\forall n \in \mathbf{N}, q_0 u_{n+r} + q_1 u_{n+r-1} + \dots + q_{r-1} u_{n+1} + q_r u_n = 0$$

– **Partie I : polynôme minimal d'une suite linéaire récurrente** –

Dans cette partie  $E$  et  $F$  sont des  $K$ -espaces vectoriels non nuls.

1. Soient  $u = (u_n)_{n \in \mathbf{N}} \in \mathcal{S}(E)$ ,  $P = \sum_{k=0}^r p_k X^k \in K[X]$ . Calculer, pour  $n \in \mathbf{N}$ ,  $[P(\sigma)(u)]_n$ .
2. Soit  $u = (u_n)_{n \in \mathbf{N}} \in \mathcal{S}(E)$ .
  - (a) Démontrer que la suite  $u$  est linéaire récurrente si et seulement si  $\text{Ann}(u) \neq \{0\}$ .
  - (b) Démontrer que si  $u$  est linéaire récurrente, alors il existe un unique polynôme normalisé noté  $\pi_u$  tel que  $\text{Ann}(u) = \pi_u \cdot K[X]$ .

Le polynôme  $\pi_u$  s'appelle le **polynôme minimal** de la suite  $u$ .

3. Dans cette question on prend  $E = K = \mathbf{R}$ .
  - (a) Démontrer que la suite  $(2^n + 3^n)$  est linéaire récurrente et donner son polynôme minimal.
  - (b) Démontrer que la suite  $(n^2 2^n)_{n \in \mathbf{N}}$  est linéaire récurrente et donner son polynôme minimal.
  - (c) Est-ce que la suite  $(n!)_{n \in \mathbf{N}}$  est linéaire récurrente ?

4. Soit  $T \in \mathcal{L}(E, F)$ . Pour toute suite  $u = (u_n)_{n \in \mathbf{N}} \in \mathcal{S}(E)$ , on note  $T(u)$  la suite de  $F$  définie par :

$$\forall n \in \mathbf{N}, [T(u)]_n = T(u_n)$$

Démontrer que si  $u$  est linéaire récurrente, alors il en est de même de  $T(u)$  et le polynôme  $\pi_{T(u)}$  divise  $\pi_u$ .

5. On note  $\mathcal{R}(E)$  le sous-ensemble de  $\mathcal{S}(E)$  formé des suites linéaires récurrentes.  $\mathcal{R}(E)$  est-il un sous-espace vectoriel de  $\mathcal{S}(E)$  ?
6. **Un exemple important** : dans cette question on considère une matrice  $A \in \mathcal{M}_p(K)$  ainsi que deux éléments non nuls  $V$  et  $W$  de  $K^p$ . On leur associe la suite scalaire  $u = (u_n)_{n \in \mathbf{N}}$  définie par  $u_n = {}^t W A^n V$ .

- (a) Démontrer que la suite  $(A^n)_{n \in \mathbf{N}}$  est linéaire récurrente et que le polynôme minimal de cette suite est égal au polynôme minimal de la matrice  $A$ .

Dans la suite ce polynôme minimal sera noté  $\pi_A$ .

- (b) Vérifier que les suites  $\beta = (A^n V)_{n \in \mathbf{N}}$  et  $u$  sont linéaires récurrentes et que :

$$\pi_u \mid \pi_\beta \quad \text{et} \quad \pi_\beta \mid \pi_A$$

Dans la suite  $\pi_\beta$  sera noté  $\pi_{A,V}$  et  $\pi_u$  sera noté  $\pi_{W,A,V}$ .

- (c) Donner un majorant du degré de  $\pi_{W,A,V}$ .
- (d) Que peut-on dire de  $\pi_{W,A,V}$ ,  $\pi_{A,V}$ ,  $\pi_A$  lorsque  $\pi_{W,A,V}(A)$  est nul ?

– **Partie II : une caractérisation des suites linéaires récurrentes scalaires** –

Dans cette partie on cherche à caractériser les suites récurrentes à valeurs dans le corps  $K$ . On introduit à cette fin les notations suivantes : pour toute suite  $u = (u_n)_{n \in \mathbf{N}} \in \mathcal{S}(K)$  et pour tout entier  $m \geq 0$ , on note  $H_m(u)$  la matrice de  $\mathcal{M}_{m+1}(K)$  définie par  $H_m(u) = [u_{i+j-2}]_{(i,j) \in [1, m+1]^2}$  et on désigne par  $D_m(u)$  son déterminant (rappel : ce déterminant est de taille  $m+1$ ).

1. On suppose ici que  $K = \mathbf{R}$  et on choisit pour  $u$  la suite de Fibonacci définie par :

$$u_0 = 0, u_1 = 1; \forall n \in \mathbf{N}, u_{n+2} = u_{n+1} + u_n$$

- (a) Calculer  $D_m(u)$  pour tout entier  $m \geq 0$ .
- (b) Quel est le polynôme minimal de la suite  $u$  ?

2. On suppose ici que  $u = (u_n)_{n \in \mathbf{N}} \in \mathcal{S}(K)$  est une suite linéaire récurrente de polynôme minimal

$$\pi_u = X^s + q_1 X^{s-1} + \cdots + q_{s-1} X + q_s$$

Démontrer que pour tout entier  $m \geq s$ ,  $D_m(u) = 0$ .

3. Réciproquement soit  $u = (u_n)_{n \in \mathbf{N}} \in \mathcal{S}(K)$  pour laquelle il existe un entier  $s \geq 1$  vérifiant :

$$D_{s-1}(u) \neq 0 \quad \text{et} \quad \forall m \geq s, D_m(u) = 0$$

On se propose de démontrer que  $u$  est linéaire récurrente et de donner une méthode de calcul de son polynôme minimal.

- (a) Quel est le rang de la matrice  $H_s(u)$  ?

- (b) Démontrer qu'il existe un unique  $s$ -uplet  $(q_1, q_2, \dots, q_s) \in K^s$  tel que :

$$H_s(u) \cdot \begin{bmatrix} q_s \\ q_{s-1} \\ \vdots \\ q_1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix}$$

- (c) On pose, pour tout entier  $m \geq s$  :

$$\lambda_m = u_m + q_1 u_{m-1} + \cdots + q_{s-1} u_{m-s+1} + q_s u_{m-s}$$

Que vaut  $\lambda_m$  lorsque  $m$  appartient à l'intervalle  $[s, 2s]$  ?

- (d) Démontrer que :

$$D_{s+1}(u) = \begin{vmatrix} u_0 & u_1 & \cdots & u_{s-1} & 0 & 0 \\ u_1 & u_2 & \cdots & u_s & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ u_{s-1} & u_s & \cdots & u_{2s-2} & 0 & 0 \\ u_s & u_{s+1} & \cdots & u_{2s-1} & 0 & \lambda_{2s+1} \\ u_{s+1} & u_{s+2} & \cdots & u_{2s} & \lambda_{2s+1} & \lambda_{2s+2} \end{vmatrix}$$

En déduire que  $\lambda_{2s+1} = 0$ .

- (e) Plus généralement, soit  $m \geq s+1$  pour lequel

$$\lambda_s = \lambda_{s+1} = \cdots = \lambda_{2s} = \cdots = \lambda_{m+s-1} = 0$$

Démontrer que :

$$D_m(u) = \begin{vmatrix} u_0 & u_1 & \cdots & u_{s-1} & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ u_{s-1} & \cdots & \cdots & u_{2s-2} & 0 & 0 & \cdots & 0 \\ u_s & \cdots & \cdots & u_{2s-1} & 0 & \cdots & 0 & \lambda_{m+s} \\ \vdots & & & \vdots & 0 & & \ddots & * \\ \vdots & & & \vdots & 0 & \lambda_{m+s} & & \vdots \\ u_m & \cdots & \cdots & u_{m+s-1} & \lambda_{m+s} & * & \cdots & * \end{vmatrix}$$

(On détaillera les opérations effectuées ainsi que l'ordre dans lequel elles sont faites).

- (f) Conclure que la suite  $u$  est linéaire récurrente de polynôme minimal

$$\pi_u = X^s + q_1 X^{s-1} + \cdots + q_{s-1} X + q_s$$

- **Partie III : polynômes minimaux en algèbre linéaire** -

Pour tout polynôme  $P \in K[X]$ , on note  $\text{coeff}(P, k)$  le coefficient d'indice  $k$  de  $P$ .

1. Soit  $F \in K[X]$  un polynôme normalisé, de degré  $m \geq 1$ . On lui associe l'application

$$\Phi : K[X] \times K[X] \rightarrow K, (P, Q) \mapsto \text{coeff}(PQ \bmod F, m-1)$$

- (a) Vérifier que  $\Phi$  est bilinéaire et symétrique.  
 (b) Soit  $P \in K[X]$  tel que pour tout  $Q \in K[X]$ ,  $\Phi(P, Q) = 0$ . Démontrer que  $F$  divise  $P$ . Étudier la réciproque.

**Indication :** on pourra introduire  $r = d^\circ(P \bmod F)$ .

- (c) Soit  $\Phi_{m-1}$  la restriction de  $\Phi$  à  $K_{m-1}[X] \times K_{m-1}[X]$ .  $\Phi_{m-1}$  est-elle dégénérée ?  
 (d) Soit  $G \in K_{m-1}[X]$ . On considère la suite  $u = (u_k)_{k \in \mathbf{N}}$  définie par  $u_k = \Phi(X^k, G)$ .  
 i) Démontrer qu'un polynôme  $P$  appartient à  $\text{Ann}(u)$  si et seulement si pour tout entier  $i$  on a  $\Phi(PG, X^i) = 0$ .  
 ii) En déduire que  $u$  est linéaire récurrente et que son polynôme minimal est donné par :

$$\pi_u = \frac{F}{F \wedge G}$$

Dans la suite du problème on considère une matrice  $A \in \mathcal{M}_n(K)$  ainsi qu'un vecteur  $V \in K^n$  non nul. On utilise les notations des questions précédentes en prenant  $F = \pi_{A,V}$ , de degré  $m$ .

2. Soit  $E$  le sous-espace de  $K^n$  engendré par  $\{A^k V, k \in \mathbf{N}\}$ . Démontrer que l'application

$$\Theta : K_{m-1}[X] \rightarrow E, P \mapsto P(A).V$$

est un isomorphisme de  $K$ -espaces vectoriels.

3. Soit  $\rho : K^n \rightarrow E^*$  l'application qui, à  $W \in K^n$  associe la forme linéaire

$$\rho(W) : E \rightarrow K, z \mapsto {}^t W.z.$$

Montrer que  $\rho$  est linéaire et surjective.

4. Soit  $\varphi : K_{m-1}[X] \rightarrow K_{m-1}[X]^*$  l'application définie par :

$$\forall (P, Q) \in K_{m-1}[X] \times K_{m-1}[X], \varphi(P)(Q) = \Phi(P, Q)$$

Expliquer pourquoi  $\varphi$  est un isomorphisme de  $K$ -espaces vectoriels.

5. On note  $\Gamma = \varphi^{-1} \circ {}^t \Theta \circ \rho$ .

- (a) Que peut-on dire de  $\Gamma$  ?  
 (b) Démontrer que pour tout  $P \in K_{m-1}[X]$  et pour tout  $W \in K^n$  :

$$\Phi(\Gamma(W), P) = {}^t W.P(A).V$$

- (c) Vérifier que cette relation est vraie pour tout polynôme  $P$  de  $K[X]$ .  
 (d) Conclure que pour tout  $W \in K^n$  :

$$\pi_{W,A,V} = \frac{\pi_{A,V}}{\pi_{A,V} \wedge \Gamma(W)}$$

- (e) En déduire qu'il existe au moins un vecteur  $W$  de  $K^n$  pour lequel  $\pi_{W,A,V} = \pi_{A,V}$ .

Dans la fin de cette partie on cherche dans quelle mesure on peut « espérer » que  $\pi_{W,A,V}$  soit égal à  $\pi_{A,V}$ .

**Notations :** on rappelle qu'un polynôme  $P = P(X_1, X_2, \dots, X_n)$  à  $n$  indéterminées est un élément de l'algèbre  $K[X_1, X_2, \dots, X_n]$  qui peut se définir comme  $(K[X_1, X_2, \dots, X_{n-1}])[X_n]$  pour  $n > 1$ . On peut noter  $P$  ainsi :

$$P = \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n}.$$

Pour un tel polynôme, chacun de ses **monômes**  $a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n}$  a pour degré total  $i_1 + \dots + i_n$ , et le **degré total** de  $P$  est le plus grand des degrés totaux de ses monômes non nuls.

6. Soient  $R \in K[X_1, X_2, \dots, X_n]$  un polynôme **non nul** de degré total  $d$ , à  $n$  indéterminées et  $S$  un sous-ensemble fini non vide de  $K$ . Montrer que l'ensemble

$$\Omega_S = \{(s_1, s_2, \dots, s_n) \in S^n / R(s_1, s_2, \dots, s_n) = 0\}$$

possède au plus  $d \cdot [\text{Card } S]^{n-1}$  éléments.

**Indication :** on pourra procéder par récurrence sur  $n$ .

7. On admet le résultat suivant : étant donnés deux polynômes non nuls

$$A = \sum_{k=0}^n a_k X^k, \quad B = \sum_{k=0}^m b_k X^k \in K[X]$$

avec  $b_m \neq 0$ , ces polynômes sont premiers entre eux si et seulement si le déterminant ci-dessous n'est pas nul :

$$\begin{array}{cccccccc} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \ddots & \vdots & \vdots & b_0 & \ddots & \vdots \\ \vdots & a_1 & \ddots & 0 & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & a_0 & b_m & \vdots & \ddots & 0 \\ a_n & \vdots & & a_1 & 0 & b_m & & b_0 \\ 0 & a_n & & \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_n & 0 & \cdots & 0 & b_m \end{array}$$

←----- m -----←----- n -----→

Ce déterminant s'appelle le **résultant** de  $(A, B)$ . On le notera  $\text{Res}(A, B)$ .

On considère comme dans la question 6 un sous-ensemble  $S$  de  $K$  qui est fini et admet au moins  $m$  éléments.

- (a) Démontrer que l'ensemble :

$$\left\{ W = (w_1, w_2, \dots, w_n) \in S^n / \pi_{A,V} \wedge \Gamma(W) = 1 \right\}$$

possède au moins  $[\text{Card } S]^n - m \cdot [\text{Card } S]^{n-1}$  éléments.

- (b) On choisit au hasard (de manière équiprobable) un  $n$ -uplet  $W$  dans  $S^n$ . Déduire de ce qui précède un minorant de la probabilité pour que  $\pi_{W,A,V} = \pi_{A,V}$ .

## - Partie IV : l'algorithme de Berlekamp-Massey -

*Le but de cette partie est de fournir un algorithme efficace dans la recherche du polynôme minimal d'une suite linéaire récurrente scalaire lorsqu'on connaît à l'avance une majoration du degré de ce polynôme. La méthode proposée est indépendante des parties II et III.*

Dans cette partie  $A$  et  $B$  sont deux polynômes de  $K[X]$  pour lesquels  $d^\circ A = m$ ,  $d^\circ B = n$ , avec  $m \geq n \geq 1$ . On rappelle que l'algorithme d'Euclide fournit par divisions euclidiennes successives deux familles finies  $(Q_i)_{i \in [1, l]}$  et  $(R_i)_{i \in [0, l+1]}$  de  $K[X]$  vérifiant :

$$\begin{cases} R_0 = A, R_1 = B \\ R_{i-1} = Q_i R_i + R_{i+1} \quad \text{pour } i \in [1, l] \quad \text{avec } \forall i \in [1, l], 0 \leq d^\circ R_{i+1} < d^\circ R_i \\ R_l = A \wedge B, R_{l+1} = 0 \end{cases}$$

On considère les deux familles finies de polynômes  $(S_i)_{i \in [0, l+1]}$  et  $(T_i)_{i \in [0, l+1]}$  définies par :

$$S_0 = 1, S_1 = 0, T_0 = 0, T_1 = 1 \quad \text{et pour } i \in [1, l], \begin{cases} S_{i+1} = S_{i-1} - Q_i S_i \\ T_{i+1} = T_{i-1} - Q_i T_i \end{cases}$$

1. Démontrer les propriétés suivantes :

- (a) Pour tout  $i \in [0, l + 1]$ ,  $S_i A + T_i B = R_i$ .
- (b) Pour tout  $i \in [0, l]$ ,  $S_{i+1} T_i - S_i T_{i+1} = (-1)^{i+1}$ . En déduire la valeur de  $S_i \wedge T_i$ , pour  $i \in [0, l + 1]$ .
- (c) Pour tout  $i \in [0, l + 1]$ ,  $R_i \wedge T_i = A \wedge T_i$ .
- (d)  $d^\circ T_1 \leq d^\circ T_2$ , et pour tout  $i \in [2, l]$ ,  $d^\circ T_i < d^\circ T_{i+1}$ .
- (e) Pour tout  $i \in [1, l + 1]$ ,  $d^\circ T_i = m - d^\circ R_{i-1}$ .  
On peut alors démontrer de même (mais cela n'est pas demandé) que pour tout  $i \in [2, l + 1]$ ,  $d^\circ S_i = n - d^\circ R_{i-1}$ .

2. On fixe ici un entier  $k \in [0, m[$  et on s'intéresse aux deux problèmes suivants :

( $\mathcal{P}_1$ ) : trouver un couple  $(R, T) \in K[X]^2$  vérifiant :

$$TB \equiv R \pmod{A}, \quad T \wedge A = 1, \quad d^\circ R < k, \quad d^\circ T \leq m - k$$

( $\mathcal{P}_2$ ) : trouver un couple  $(R, T) \in K[X]^2$  vérifiant :

$$TB \equiv R \pmod{A}, \quad d^\circ R < k, \quad d^\circ T \leq m - k$$

Soit  $j \in [1, l + 1]$  pour lequel  $d^\circ R_j < k \leq d^\circ R_{j-1}$ .

- (a) Démontrer que le couple  $(R_j, T_j)$  est une solution de ( $\mathcal{P}_2$ ). À quelle condition est-il une solution de ( $\mathcal{P}_1$ ) ?
- (b) Inversement, on suppose qu'il existe un couple  $(R, T)$  solution de ( $\mathcal{P}_1$ ). Démontrer que :

$$\begin{cases} R_j \wedge T_j = 1 \\ \text{il existe } P \in K[X] \setminus \{0\} \text{ tel que } R = PR_j, T = PT_j \\ P \wedge A = 1 \end{cases}$$

**Indication** : on pourra s'intéresser au polynôme  $R_j T - R T_j$  puis à  $S_j T - T S_j$ .

3. Soit  $u = (u_n)_{n \in \mathbb{N}} \in \mathcal{S}(K)$ . On lui associe la suite de polynômes  $(B_r)_{r \in \mathbb{N}^*}$  définie par :

$$B_r = \sum_{k=0}^{2r-1} u_k X^k. \text{ On suppose qu'il existe deux polynômes } H = \sum_{k=0}^s q_k X^k \text{ et } R \text{ vérifiant :}$$

$$q_0 = 1, \quad d^\circ R < s, \quad \text{et } \forall r \geq s, \quad H B_r \equiv R \pmod{X^{2r}}$$

Démontrer alors que  $u$  est linéaire récurrente et que  $\sum_{k=0}^s q_{s-k} X^k \in \text{Ann}(u)$ .

4. Réciproquement, soit  $u = (u_n)_{n \in \mathbb{N}} \in \mathcal{S}(K)$  une suite linéaire récurrente non nulle dont

$$Q = \sum_{k=0}^s q_k X^{s-k} \text{ (avec } q_0 = 1) \text{ est un polynôme annulateur.}$$

(a) Dans ces conditions, démontrer que :

i) il existe un polynôme  $R$  de degré strictement inférieur à  $s$  tel que pour tout entier  $r \geq s$  :

$$Q^* B_r \equiv R \pmod{X^{2r}}, \quad \text{où } Q^*(X) = X^s Q\left(\frac{1}{X}\right) = \sum_{k=0}^s q_k X^k$$

ii) Si  $Q = \pi_u$ , alors  $s = \max(1 + d^\circ R, d^\circ Q^*)$  et  $Q^* \wedge R = 1$ .

(b) On reprend les notations de la question 1 avec  $A = X^{2r}$ ,  $B = B_r$ , pour  $r \geq s$ ; on choisit  $k = r$  et on considère un entier  $j \in [1, l + 1]$  tel que  $d^\circ R_j < r \leq d^\circ R_{j-1}$ .

i) Vérifier que

$$T_j B_r \equiv R_j \pmod{X^{2r}}, \quad R_j \wedge T_j = T_j \wedge X^{2r} = 1, \quad d^\circ T_j \leq r, \quad d^\circ R_j < r$$

ii) En déduire qu'il existe  $P \in K[X] - \{0\}$  tel que :

$$\pi_u^* = P T_j, \quad R = P R_j \quad \text{et} \quad P \wedge X^{2r} = 1$$

iii) Conclure que, quitte à multiplier  $T_j, R_j$  par un élément non nul de  $K$ , on peut supposer que  $T_j(0) = 1$  et que le polynôme minimal  $\pi_u$  est alors donné par :

$$\pi_u(X) = X^s T_j\left(\frac{1}{X}\right) \quad \text{où } s = \max(1 + d^\circ R_j, d^\circ T_j)$$