ANALYSE NUMÉRIQUE

OBJECTIFS ET NOTATIONS

1. Pour toute application u de classe C^2 définie sur un ouvert de $\mathbb{R}^2$ et à valeurs dans $\mathbb{R}$, on désigne par Δu son laplacien, c'est à dire l'application définie sur cet ouvert par:

$$\Delta u = \frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2}.$$

2. On considère un nombre réel strictement positif a et, dans le plan rapporté à un repère orthonormé, on désigne par D le carré $]0, a[\times]0, a[$ dont la frontière est notée ∂D. Etant données deux applications continues f, définie sur ∂D et à valeurs dans $\mathbb{R}$, et F, définie sur D et à valeurs dans $\mathbb{R}$, on considère le problème P[f, F] suivant:

Déterminer les applications continues $u: \overline{D} \to \mathbb{R}$, telles que:
a) u est de classe C^2 sur D, et $\Delta u = F$ sur D.
b) $u = f$ sur ∂D.

3. Lorsque l'espace vectoriel K^n, où $K = \mathbb{R}$ ou $\mathbb{C}$, est rapporté à sa base canonique, on identifie les endomorphismes de K^n à leur matrice dans celle-ci.
On normera l'espace vectoriel K^n à l'aide de l'une des normes usuelles définies par:

$$\|x\|_2 = \sqrt{\sum_{k=1}^{n} |x_k|^2} \quad ; \quad \|x\|_\infty = \sup_{1 \le k \le n} |x_k|.$$

Dans ce cas, l'espace vectoriel des matrices carrées à coefficients dans K sera normé par la norme subordonnée à $\| \cdot \|_2$ ou $\| \cdot \|_\infty$.
On rappelle que, pour une telle matrice A, la norme subordonnée à $\| \cdot \|$ est définie par:

$$\|A\| = \sup\{ \frac{\|Ax\|}{\|x\|} \ / \ x \in K^n, \ x \neq 0 \}.$$

Dans le préambule du problème, *qui est indépendant de la suite* , on établit un résultat d'unicité concernant les solutions du problème P[f, F], et un résultat d'existence à propos du cas particulier F = 0.
On étudie ensuite quelques algorithmes numériques rapides d'approximation des solutions de ce problème P[f, F].

I. PREAMBULE.

1°) Principe du maximum et unicité des solutions de P[f, F].

a) Soit $u: D \to \mathbb{R}$ une application de classe C^2 admettant un maximum relatif en un point (x_o, y_o) appartenant à D. Prouver: $\Delta u(x_o, y_o) \le 0$.

b) Soit $u: \overline{D} \to \mathbb{R}$ une application continue sur $\overline{D}$, de classe C^2 sur D, nulle sur ∂D et telle que $\Delta u = 0$ sur D.

- On suppose qu'il existe au moins un point (x_1, y_1) de D tel que $u(x_1, y_1) > 0$.

Etablir l'existence d'un réel $\varepsilon > 0$ tel que l'application $u_\varepsilon: \overline{D} \to \mathbb{R}$ définie par:

$$u_\varepsilon(x,y) = u(x,y) + \varepsilon (x^2 + y^2)$$

ait un maximum relatif sur D.

- En déduire que u est nulle sur D.

c) Montrer que le problème P[f, F] admet au plus une solution.

2°) Existence de solutions au problème P[f, 0].

a) On considère dans cette question une fonction g définie sur [0, a], à valeurs dans $\mathbb{R}$, continue sur [0, a], de classe C^1 par morceaux sur [0, a], et s'annulant en 0 et en a.
On suppose que la fonction f du problème P[f, 0] vérifie pour x, y appartenant à [0, a]:

$$f(0,y) = f(a,y) = f(x,a) = 0 \quad ; \quad f(x,0) = g(x).$$

- Etablir l'existence d'une suite de nombres réels (b_n) telle que l'on ait sur [0, a] l'égalité suivante, avec convergence normale de la série:

$$g(x) = \sum_{n=1}^{+\infty} b_n \sin\left(\frac{n\pi x}{a}\right)$$

(On pourra prolonger la fonction g en une fonction impaire 2a-périodique).

- Déterminer pour tout entier $n \geq 1$ une fonction h_n définie sur [0, a], à valeurs dans $\mathbb{R}$, de classe C^2 sur [0, a], telle que la fonction u_n définie sur $\overline{D}$ par:

$$u_n(x,y) = \sin(\frac{n\pi x}{a}) h_n(y)$$

vérifie $\Delta u_n = 0$ sur D, et enfin telle que $h_n(0) = 1$, $h_n(a) = 0$.
Les fonctions h_n étant ainsi fixées, prouver que la somme u de la série $\Sigma b_n u_n$ est solution du problème P[f, 0].

b) On suppose enfin que les restrictions aux quatre côtés de D de la fonction continue f du problème P[f, 0] sont de classe C^1 par morceaux.
Achever la résolution de ce problème P[f, 0] à l'aide des résultats obtenus précédemment.

(On pourra retrancher à f un polynôme $\alpha + \beta X + \gamma Y + \delta XY$ convenablement choisi).

II. RESOLUTION NUMERIQUE DU PROBLEME P[f, F].

On désigne désormais par n et N des entiers supérieurs à 1 tels que $n = 2^N - 1$.

A] Etude de la transformation de Fourier discrète.

L'espace $\mathbb{C}^{n+1}$ est rapporté à sa base canonique et muni de la norme $\| \cdot \|_2$ définie dans le préambule.
On convient de poser $\omega_{n+1} = \exp[2i\pi / (n+1)]$, et d'appeler:

- polynôme associé à un élément $a = (a_0, a_1, ..., a_n)$ de $\mathbb{C}^{n+1}$ le polynôme:

$$A(X) = a_0 + a_1 X \ \ldots \ + a_n X^n = \sum_{k=0}^{n} a_k X^k.$$

- transformation de Fourier discrète de $\mathbb{C}^{n+1}$ l'application Φ_{n+1} associant à tout élément $a = (a_0, a_1, ..., a_n)$ de $\mathbb{C}^{n+1}$ l'élément suivant de $\mathbb{C}^{n+1}$:

$$\Phi_{n+1}(a) = \left(A(1), A(\omega_{n+1}) \ \ldots \ , A(\omega_{n+1}^p), \ \ldots \ , A(\omega_{n+1}^n)\right).$$

1°) Propriétés générales de l'application Φ_{n+1}.

a) Etablir que Φ_{n+1} est un automorphisme de l'espace vectoriel $\mathbb{C}^{n+1}$.

b) Exprimer pour tout a de $\mathbb{C}^{n+1}$ la norme de $\Phi_{n+1}(a)$ en fonction de la norme de a.

c) Expliciter la matrice M_{n+1} de l'automorphisme Φ_{n+1} dans la base canonique.

En déduire que l'inverse de Φ_{n+1} est défini par:

$$\Phi_{n+1}^{-1}(a) = \frac{1}{n+1}\left(A(1), A(\omega_{n+1}^{-1}), \ \ldots \ , A(\omega_{n+1}^{-p}), \ \ldots \ , A(\omega_{n+1}^{-n})\right).$$

2°) Etude d'un algorithme récursif de calcul de $\Phi_{n+1}(a)$.

Etant donné un élément $a = (a_0, a_1, ..., a_n)$ de C^{n+1}, on lui associe les deux éléments notés $b = (a_0, a_2, a_4, ..., a_{n-1})$ et $c = (a_1, a_3, a_5, ..., a_n)$ de $C^{(n+1)/2}$, et l'on considère alors leurs transformées de Fourier discrètes, notées respectivement:

$$\Phi_{n+1}(a) = (\alpha_0, \alpha_1, \ldots, \alpha_n) \quad et \quad \begin{cases} \Phi_{\frac{n+1}{2}}(b) = \left(\beta_0, \beta_1, \ldots, \beta_{\frac{n-1}{2}}\right). \\ \Phi_{\frac{n+1}{2}}(c) = \left(\gamma_0, \gamma_1, \ldots, \gamma_{\frac{n-1}{2}}\right). \end{cases}$$

a) On suppose connus $\Phi_{(n+1)/2}(b)$ et $\Phi_{(n+1)/2}(c)$ et l'on considère l'algorithme suivant (dans lequel la notation A ← B indique que l'on affecte à la variable complexe A la valeur de la variable complexe B):

E ← 1 ;
pour p **de** 0 **à** (n-1)/2 **faire:**
début
$F \leftarrow E.\gamma_p$; $\alpha_p \leftarrow \beta_p + F$; $\alpha_{p+\frac{n+1}{2}} \leftarrow \beta_p - F$; $E \leftarrow \omega_{n+1}.E$;
fin ;

Prouver que l'élément $(\alpha_0, \alpha_1, ..., \alpha_{n-1}, \alpha_n)$ de C^{n+1} ainsi obtenu est égal à $\Phi_{n+1}(a)$.

b) Soient u_N et v_N les nombres des additions et multiplications complexes nécessaires au calcul de $\Phi_{n+1}(a)$ par l'algorithme récursif décrit ci-dessous (et ne tenant pas compte du calcul des nombres ω_{n+1}, supposés connus):

- Si N = 1, on calcule $\Phi_2(a_0, a_1) = (a_0 + a_1, a_0 - a_1)$ et donc $u_1 = 2$ et $v_1 = 0$.
- Sinon, on calcule récursivement $\Phi_{(n+1)/2}(b)$ et $\Phi_{(n+1)/2}(c)$ en effectuant pour chacun d'eux u_{N-1} additions complexes et v_{N-1} multiplications complexes, et l'on obtient $\Phi_{n+1}(a)$ par l'algorithme développé ci-dessus à la question (a).

Exprimer u_N et v_N en fonction de u_{N-1}, v_{N-1} et N.

En déduire en fonction de N, puis de n, le nombre d'additions et multiplications complexes (resp. réelles) nécessaires au calcul de $\Phi_{n+1}(a)$.

c) Comparer enfin ces nombres d'opérations à ceux qui résulteraient du calcul de $\Phi_{n+1}(a)$ par utilisation répétée de l'algorithme de Hörner.

On rappelle que le calcul de $P(x) = a_p x^p + ... + a_1 x + a_0$ par cet algorithme s'effectue de la façon suivante:

$$P(x) = (... ((a_p x + a_{p-1})x + a_{p-2}) ... + a_1)x + a_0.$$

B] Etude de matrices tridiagonales.

Dans cette partie, on désigne par m un nombre réel donné et par:

- T_m la matrice tridiagonale d'ordre n dont les éléments t_{ij} sont définis pour $1 \le i, j \le n$ par $t_{ii} = m$, $t_{ij} = -1$ si $|i-j| = 1$, et $t_{ij} = 0$ sinon.

- A_m la matrice carrée d'ordre n^2 tridiagonale par blocs d'ordre n égale à:

$$A_m = \begin{bmatrix} T_m & -I & 0 & \cdots & 0 \\ -I & T_m & -I & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & -I & T_m & -I \\ 0 & \cdots & 0 & -I & T_m \end{bmatrix}.$$

(la matrice - I désignant ci-dessus l'opposée de la matrice identité d'ordre n).

On identifiera selon l'habitude un vecteur de l'espace euclidien $\mathbb{R}^n$ à la matrice-colonne de ses composantes dans la base canonique de $\mathbb{R}^n$.

1°) Résolution du système $T_mX = B$.

a) On considère la suite (p_k) définie pour tout entier $k \geq 1$ par:

$$p_1 = m \quad , \quad p_{k+1} = m - \frac{1}{p_k}.$$

Etablir que cette suite est définie pour tout entier $k \geq 1$ lorsque $m > 2$.

b) On considère une matrice-colonne B d'ordre n et le système $T_mX = B$ avec $m > 2$.

Donner un équivalent du nombre d'opérations réelles nécessitées par la résolution du système $T_mX = B$ par la méthode du pivot de Gauss sans échanges de lignes.

2°) Localisation des valeurs propres d'une matrice carrée.

a) Soit $M = (m_{ij})$ une matrice carrée complexe d'ordre n telle que l'on ait:

$$\forall i \in \{1,2, \ \ldots \ ,n\}, \qquad r_i = \sum_{\substack{j=1 \\ j \neq i}}^{n} |m_{i,j}| < |m_{i,i}|.$$

Montrer que M est inversible.

b) En déduire que toute valeur propre de M appartient à la réunion des boules fermées de centre d'affixe m_{ii} et de rayon r_i.

3°) Etude des éléments propres des matrices T_m et A_m.

a) Montrer que si λ est valeur propre de T_m, il existe un réel θ appartenant à $[0, \pi]$ tel que $\lambda = m - 2\cos\theta$. Déterminer alors les valeurs θ_k appartenant à $[0, \pi]$ pour lesquelles $\lambda_k = m - 2\cos\theta_k$ est effectivement valeur propre de T_m.

b) Déterminer le vecteur propre V_k associé à λ_k dont la première composante est égale à $\sin\theta_k$, et montrer que $||V_k||^2 = (n+1)/2$.

En déduire une matrice orthogonale symétrique P, indépendante de m, telle que PT_mP soit une matrice diagonale D_m.

c) Soit O la matrice carrée d'ordre n^2 diagonale par blocs d'ordre n tous égaux à P (et donc orthogonale et symétrique). Calculer le produit OA_mO.

4°) Etude des éléments propres des matrices A_m.

a) On considère n nombres réels $x_1, x_2, \ldots, x_n$, un vecteur propre V de T_m, puis le vecteur W à n^2 composantes défini par blocs de la façon suivante:

$$W = \begin{pmatrix} x_1 V \\ x_2 V \\ \vdots \\ x_n V \end{pmatrix}.$$

A quelle condition sur $x_1, x_2, \dots, x_n$ le vecteur W est-il vecteur propre de A_m?
En déduire les valeurs propres et vecteurs propres de A_m, et vérifier que, lorsque m = 4, ces valeurs propres sont les réels $\lambda_{pq} = 4\sin^2[p\pi/2(n+1)] + 4\sin^2[q\pi/2(n+1)]$, $1 \le p, q \le n$.
b) En déduire une matrice orthogonale symétrique Q, indépendante de m, telle que QA_mQ soit une matrice diagonale.

C] Discrétisation du problème P[f, F] par différences finies.

1°) Approximation discrète à 5 points du Laplacien.

Soit u une fonction continue de $\overline{D}$ dans $\mathbb{R}$, dont les dérivées quatrièmes $\partial^4u/\partial x^4$ et $\partial^4u/\partial y^4$ existent sur $\overline{D}$ en étant bornées par un nombre réel M_4.
Etablir, pour $0 \le x-h < x+h \le a$, $0 \le y-h < y+h \le a$, la majoration suivante:

$$\left|\frac{u(x-h,y)+u(x+h,y)+u(x,y-h)+u(x,y+h)-4u(x,y)}{h^2} - \Delta u(x,y)\right| \le \frac{M_4 h^2}{6}.$$

On introduit maintenant quelques notations valables pour toute la suite du problème.

- On pose $h = a/(n+1)$ et P_{ij} désigne le point de coordonnées (ih, jh) pour $0 \le i, j \le n+1$.

L'ensemble de ces points P_{ij} appartenant à D (resp. ∂D) est noté D_n (resp. ∂D_n).

- Pour toute application u_n de l'ensemble noté $\overline{D_n} = D_n \cup \partial D_n = \{P_{ij} / 0 \le i, j \le n+1\}$ dans $\mathbb{R}$, on convient de poser $u_{ij} = u_n(P_{ij})$ et, pour tout point P_{ij} appartenant à D_n:

$$\Delta_{5,n}u_n(P_{i,j}) = \Delta_{5,n}u_{i,j} = \frac{1}{h^2}\left(u_{i+1,j}+u_{i-1,j}+u_{i,j+1}+u_{i,j-1}-4u_{i,j}\right).$$

On conviendra d'appeler laplacien discret à 5 points de u_n cette application $\Delta_{5,n}u_n$ définie de D_n dans $\mathbb{R}$.

- On définit les normes suivantes pour toute application de D_n (resp. $\overline{D_n}$) dans $\mathbb{R}$:

$$\begin{cases} \|u_n\|_\infty = \sup\{|u_n(P)| \ / \ P \in D_n \ (resp.\ \overline{D_n})\}. \\ \|u_n\|_2 = \sqrt{\sum_{P\in D_n} u_n^2(P)} \quad (resp.\ \sqrt{\sum_{P\in \overline{D}_n} u_n^2(P)}). \end{cases}$$

Pour tout couple d'applications $f_n: \partial D_n \to \mathbb{R}$ et $F_n: D_n \to \mathbb{R}$, on se propose alors d'étudier le problème $P_{5,n}[f_n, F_n]$ suivant:

Trouver les applications $u_n: \overline{D_n} \to \mathbb{R}$ telles que:
a) $\Delta_{5,n}u_n = F_n$ sur D_n.
b) $u_n = f_n$ sur ∂D_n.

2°) Existence et unicité des solutions de $P_{5,n}[f_n, F_n]$.

A toute application u_n définie sur $\overline{D_n}$ à valeurs dans $\mathbb{R}$, on associe la matrice-colonne X:

$${}^tX = (u_{1,1}, u_{1,2}, \dots, u_{1,n} ; u_{2,1}, u_{2,2}, \dots, u_{2,n} ; \dots\dots\dots ; u_{n,1}, u_{n,2}, \dots, u_{n,n})$$

(La notation ${}^tX$ désignant ici la matrice transposée de la matrice-colonne X).

Etablir que u_n est solution du problème $P_{5,n}[f_n, F_n]$ si et seulement si:

- $u_n(P_{ij}) = f_n(P_{ij})$ pour tout point P_{ij} appartenant à ∂D_n.
- X est solution d'un système d'équations $A_4X = B$ que l'on explicitera.

En déduire l'existence et l'unicité d'une solution u_n au problème $P_{5,n}[f_n, F_n]$.

3°) Première méthode de résolution du système $A_4X = B$.

En considérant la matrice orthogonale symétrique Q de B.4°, telle que $A' = QA_4Q$ est diagonale, le système $A_4X = B$ équivaut à un système $A'X' = B'$, où $X' = QX$, $B' = QB$.

On se propose alors de résoudre le système $A_4X = B$ de la façon suivante:
- on effectue le produit par blocs $B' = QB$, les calculs étant réalisés à l'aide de la transformation de Fourier discrète.
- on résout le système diagonal $A'X' = B'$.
- on effectue le produit par blocs $X = QX'$, les calculs étant réalisés à l'aide de la transformation de Fourier discrète.

Déterminer un équivalent du nombre des opérations réelles ainsi effectuées.

4°) Deuxième méthode de résolution du système $A_4X = B$.

En considérant la matrice orthogonale symétrique O de B.3°, telle que $A' = OA_4O$ est tridiagonale par blocs diagonaux, le système $A_4X = B$ équivaut à un système $A'X' = B'$ où $X' = OX$, $B' = OB$.

a) En modifiant l'ordre des équations et des inconnues dans ce système $A'X' = B'$, montrer que celui-ci est équivalent à un système $A"X" = B"$ dont la matrice A" est diagonale par blocs, les blocs diagonaux étant du type T_m défini précédemment à la partie B, avec des scalaires m que l'on précisera.

b) On se propose alors de résoudre le système $A_4X = B$ de la façon suivante:
- on calcule $B' = OB$ à l'aide de la transformation de Fourier discrète. On en déduit B".
- on résout le système diagonal $A"X" = B"$ en résolvant n systèmes tridiagonaux. On en déduit X'.
- on calcule $X = OX'$ à l'aide de la transformation de Fourier discrète.

Déterminer un équivalent du nombre des opérations réelles ainsi effectuées.

5°) Principe du maximum discret et applications.

a) Prouver que si une application $u_n: \overline{D_n} \to \mathbb{R}$ est telle que $\Delta_{5,n}u_n \geq 0$, alors u_n atteint son maximum sur ∂D_n.

Retrouver ainsi l'existence et l'unicité des solutions du système $A_4X = B$.

b) On considère l'application $v_n: \overline{D_n} \to \mathbb{R}$ définie par $v_{ij} = (i^2 + j^2)h^2/4$ et une application quelconque $u_n: \overline{D_n} \to \mathbb{R}$ supposée nulle sur ∂D_n.

A l'aide des applications $w_+ = M_nv_n + u_n$ et $w_- = M_nv_n - u_n$ où $M_n = ||\Delta_{5,n}u_n||_\infty$, établir que:

$$\|u_n\|_\infty \leq \frac{a^2}{2}\|\Delta_{5,n}u_n\|_\infty .$$

c) En déduire une majoration de la norme matricielle $||(A_4)^{-1}||_\infty$.

6°) Convergence et ordre de la méthode.

a) On considère un problème P[f, F] admettant une solution notée u et l'on suppose que les dérivées quatrièmes $\partial^4u/\partial x^4$ et $\partial^4u/\partial y^4$ de cette solution u existent sur $\overline{D}$ en étant bornées par un nombre réel M_4.

Soit u_n la solution unique du problème $P_{5,n}[f_n, F_n]$ où f_n et F_n sont les restrictions de f et F à ∂D_n et D_n respectivement.

Donner en fonction de M_4 et de n un majorant des erreurs $||u - u_n||_\infty$ et $||u - u_n||_2$.

(la lettre u désignant ici, par abus de langage, la restriction de u à $\overline{D_n}$).

b) On étudie le problème P[f, F] dont $u(x, y) = \sin(\pi x/a)\sin(\pi y/a)$ est solution.

Décrire et résoudre le problème $P_{5,n}[f_n, F_n]$ associé.

Déterminer un équivalent de $||u - u_n||_\infty$ dans ce cas particulier, et comparer à la majoration de $||u - u_n||_\infty$ obtenue ci-dessus.

7°) Approximation discrète à 9 points du Laplacien.

On considère à nouveau un problème P[f, F] admettant une solution notée u, dont on suppose que les dérivées sixièmes existent et sont bornées sur $\overline{D}$.

a) Soit (x, y) un point de D. Déterminer le développement limité à l'ordre 5 suivant les puissances de h de l'expression suivante:

$$[u(x+h,y+h)+u(x+h,y-h)+u(x-h,y+h)+u(x-h,y-h)]$$
$$+4[u(x+h,y)+u(x-h,y)+u(x,y+h)+u(x,y-h)]-20u(x,y).$$

Pour toute application u_n de $\overline{D_n}$ vers $\mathbb{R}$, on pose:

$$\Delta_{9,n}u_n(P_{i,j}) = \Delta_{9,n}u_{i,j} = \frac{1}{6h^2}[(u_{i+1,j+1}+u_{i+1,j-1}+u_{i-1,j+1}+u_{i-1,j-1})$$
$$+4(u_{i+1,j}+u_{i-1,j}+u_{i,j+1}+u_{i,j-1})-20u_{i,j}].$$

On conviendra d'appeler laplacien discret à 9 points de u_n cette application $\Delta_{9,n}u_n$ définie de D_n dans $\mathbb{R}$.

Pour tout couple d'applications $f_n: \partial D_n \to \mathbb{R}$ et $F_n: \overline{D_n} \to \mathbb{R}$, on se propose alors d'étudier le problème $P_{9,n}[f_n, F_n]$ suivant:

Trouver les applications $u_n: \overline{D_n} \to \mathbb{R}$ telles que:
a) $\Delta_{9,n}u_n = F_n + h^2\Delta_{5,n}F_n/12$ sur D_n.
b) $u_n = f_n$ sur ∂D_n.

b) On reprend les notations du 2°. Etablir qu'une application $u_n: \overline{D_n} \to \mathbb{R}$ est solution du problème $P_{9,n}[f_n, F_n]$ si et seulement si:

- $u_n(P_{ij}) = f_n(P_{ij})$ pour tout point P_{ij} appartenant à ∂D_n.
- X est solution d'un système d'équations MX = B dont on explicitera la matrice M par blocs, à l'aide des matrices T_m définies précédemment à la partie B.

En déduire l'existence et l'unicité d'une solution u_n au problème $P_{9,n}[f_n, F_n]$ et, en résolvant ce système MX = B de l'une des façons décrites précédemment, donner un équivalent du nombre d'opérations nécessaires à sa résolution.

c) Soit u_n la solution unique du problème $P_{9,n}[f_n, F_n]$ où f_n et F_n désignent les restrictions de f et F (dont on justifiera le prolongement à $\overline{D}$) à ∂D_n et $\overline{D_n}$ respectivement.

Donner en fonction de n un majorant de l'erreur $||u - u_n||_\infty$.

(la lettre u désignant ici, par abus de langage, la restriction de u à $\overline{D_n}$).

D] Résolution du système $A_4X = B$ par l'algorithme de Bünemann.

On notera désormais A et T les matrices carrées A_4 et T_4 introduites en B.

1°) On considère la suite de polynômes définie par $F_0(X) = X$ et $F_{k+1}(X) = (F_k(X))^2 - 2$.

a) Pour tout réel θ, exprimer $F_k(2\cos\theta)$ et $F_k(2\mathrm{ch}\theta)$ en fonction de θ et de k.

En déduire la décomposition de F_k en produit de polynômes irréductibles réels.

b) Calculer les normes matricielles $||F_k(T)||_2$, $||(F_k(T))^{-1}||_2$ et en déduire que:

$$\begin{cases} \left\| \left(\prod_{j=0}^{k-1} F_j(T) \right)^{-1} \right\|_2 \leq \exp(-(2^k-1)Argch\left[2-\cos\frac{\pi}{n+1}\right]). \\ \left\| \left(\prod_{j=0}^{k-1} F_j(T) \right)^{-1} F_k(T) \right\|_2 \leq \exp(Argch\left[2+\cos\frac{\pi}{n+1}\right]). \end{cases}$$

2°) On décompose le système par blocs AX = B en $n = 2^N - 1$ systèmes, notés (E_k):

$$(E_k) \quad -X_{k-1} + TX_k - X_{k+1} = B_k \quad (1 \le k \le n, \quad X_0 = X_{n+1} = 0).$$

On traite ce système récursivement de la façon décrite ci-dessous:
A la première étape:
- on conserve définitivement les (n+1)/2 systèmes (E_1), (E_3), ... , (E_{n-2}), (E_n).

Ces systèmes permettront plus tard de déterminer X_1 , X_3 , ... , X_{n-2} , X_n comme solutions de systèmes tridiagonaux en fonction de X_2 , X_4 , ... , X_{n-1}.
- on multiplie pour $1 \le j \le (n-1)/2$ le système (E_{2j}) par $F_0(T) = T$ et on lui ajoute les systèmes (E_{2j-1}) et (E_{2j+1}), et l'on passe à l'étape suivante.

A la deuxième étape, on conserve définitivement les systèmes (E_2), (E_6), ... , (E_{n-5}), (E_{n-1}) tandis que l'on multiplie pour $1 \le j \le (n-3)/4$ le système (E_{4j}) par $F_1(T)$ avant de lui ajouter les systèmes (E_{4j-2}) et (E_{4j+2}).
Poursuivant récursivement, on parvient à l'issue de la $k^{ième}$ étape ($1 \le k \le N-1$) de l'algorithme à un système (Σ_k), s'exprimant par blocs d'ordre n de la façon suivante:

$$\begin{bmatrix} F_k(T) & -I & 0 & \cdots & 0 \\ -I & F_k(T) & -I & \ddots & \vdots \\ 0 & -I & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & F_k(T) & -I \\ 0 & \cdots & 0 & -I & F_k(T) \end{bmatrix} \begin{bmatrix} X_{2^k} \\ \vdots \\ X_{i.2^k} \\ \vdots \\ X_{2^N-2^k} \end{bmatrix} = \begin{bmatrix} B^{(k)}_{2^k} \\ \vdots \\ B^{(k)}_{i.2^k} \\ \vdots \\ B^{(k)}_{2^N-2^k} \end{bmatrix}.$$

On précisera le système obtenu à l'issue de la $(N-1)^{ième}$ étape de l'algorithme.

a) On pose (avec la convention que les vecteurs dont l'indice inférieur i est tel que $i \le 0$ ou $i \ge n+1$ sont nuls):

$$\begin{cases} P^{(1)}_{2i} = T^{-1}B_{2i} \\ Q^{(1)}_{2i} = B_{2i-1} + 2P^{(1)}_{2i} + B_{2i+1} \end{cases}$$

puis, pour $2 \le k \le N-1$ et $1 \le i \le 2^{N-k} - 1$:

$$\begin{cases} P^{(k)}_{i.2^k} = P^{(k-1)}_{i.2^k} + (F_{k-1}(T))^{-1}\left(P^{(k-1)}_{i.2^k-2^{k-1}} + Q^{(k-1)}_{i.2^k} + P^{(k-1)}_{i.2^k+2^{k-1}}\right). \\ Q^{(k)}_{i.2^k} = Q^{(k-1)}_{i.2^k-2^{k-1}} + 2P^{(k)}_{i.2^k} + Q^{(k-1)}_{i.2^k+2^{k-1}}. \end{cases}$$

Prouver la formule suivante:

$$B^{(k)}_{i.2^k} = F_k(T)P^{(k)}_{i.2^k} + Q^{(k)}_{i.2^k}.$$

Que devient le système (Σ_k) avec les nouvelles variables ainsi introduites?
b) Expliquer comment résoudre le système AX = B par la méthode récursive décrite ci-dessus en n'effectuant que des additions de vecteurs et des résolutions de systèmes tridiagonaux.
Déterminer un équivalent du nombre des opérations réelles ainsi effectuées.
c) Exprimer en fonction de X_1 , X_2 , ... , X_n et de T les vecteurs suivants:

$$P^{(k)}_{i.2^k} \quad ; \quad Q^{(k)}_{i.2^k}.$$

Etudier à l'aide de la norme $\| \cdot \|_2$ la stabilité numérique de l'algorithme obtenu.
La méthode proposée s'appliquerait-t-elle aussi au système de la question C.7°?

***

MÉCANIQUE GÉNÉRALE

L'objet de ce problème est une étude du cas particulier du Problème plan des trois corps que constitue le « Problème restreint circulaire ». Après la mise en équations du problème, on étudie l'existence de configurations d'équilibre et leur stabilité ; puis on détermine, grâce à l'intégrale première de Jacobi, les « régions de Hill », qui contiennent les projections des solutions dans le plan de configuration.

PREMIÈRE PARTIE

Dans cette première partie, on se propose d'écrire les équations différentielles qui décrivent les solutions du Problème plan des trois corps, et de déterminer les intégrales premières classiques de ce système.

Considérons trois corps ponctuels P_0, P_1, P_2, de masses respectives, non nulles, m_0, m_1, m_2, constituant un système (S) isolé dans un plan fixe, et s'attirant mutuellement suivant la loi de Newton.

Soient $X_0, Y_0, X_1, Y_1, X_2, Y_2$, les coordonnées cartésiennes des trois corps P_0, P_1, P_2, relativement à un système orthonormé d'axes absolus OXY, et r_0, r_1, r_2, leurs distances mutuelles :

$$r_0 = |P_1 P_2|, r_1 = |P_2 P_0|, r_2 = |P_0 P_1|.$$

On supposera, dans tout le problème, que les unités sont choisies de telle sorte que la constante de gravitation soit égale à l'unité.

1.1. Montrer que ce problème, à six degrés de liberté, admet un lagrangien de la forme suivante (où le point désigne la dérivation par rapport au temps t) :

$$L(\underline{X}, \underline{Y}, \dot{\underline{X}}, \dot{\underline{Y}}) = \frac{1}{2}(m_0(\dot{X}_0^2 + \dot{Y}_0^2) + m_1(\dot{X}_1^2 + \dot{Y}_1^2) + m_2(\dot{X}_2^2 + \dot{Y}_2^2)) + \frac{m_0 m_1}{r_2} + \frac{m_1 m_2}{r_0} + \frac{m_2 m_0}{r_1}.$$

1.2. Écrire les équations de Lagrange (1.2.) engendrées par le lagrangien (1.1.) [on écrira seulement les trois premières équations, en $\ddot{X}_0, \ddot{X}_1, \ddot{X}_2$, en remarquant que les trois dernières en $\ddot{Y}_0, \ddot{Y}_1, \ddot{Y}_2$ sont analogues].

1.3. Déduire de la forme du lagrangien, que le système différentiel (1.2.) admet l'intégrale première de l'énergie.

1.4. En appliquant au système (S) le théorème du moment cinétique relativement au point fixe 0, montrer que le système (1.2.) admet l'intégrale première du moment cinétique, que l'on écrira.

1.5. Montrer que le théorème de la quantité de mouvement, appliqué au système (S), permet de caractériser le mouvement du centre de masse G du système (on notera X_G, Y_G, les coordonnées de G dans le repère choisi). Préciser le nature de ce mouvement.

1.6. En combinant convenablement, d'une part les trois premières équations du système (1.2.), d'autre part les trois dernières, montrer que ce système admet quatre intégrales premières (deux d'entre elles sont dépendantes du temps) qui caractérisent le type de mouvement du centre de gravité G, mis en évidence dans la question précédente ; écrire ces quatre intégrales premières.

1.7. L'existence de ces quatre intégrales permet de réduire l'ordre du système différentiel (1.2.) : c'est l' « élimination du centre de gravité », qui conduit à regarder le système (S) comme un système à quatre degrés de liberté.

Pour effectuer cette réduction, on place le centre de gravité G à l'origine du système de coordonnées G X Y, qui, d'après la question 1.5., constitue un repère absolu. Puis on définit les « variables symétriques de Jacobi », q_1, q_2, q_3, q_4, comme les composantes (q_1, q_2), dans le repère G X Y, du vecteur $\overrightarrow{P_0 P_1}$, et les composantes (q_3, q_4) de $\overrightarrow{G_{01} P_2}$ (où G_{01} désigne le centre de gravité des corps P_0 et P_1 affectés des masses m_0 et m_1).

1.7.1. Exprimer les variables de Jacobi q_1, q_2, q_3, q_4, en fonction des coordonnées X_i, Y_i utilisées dans la question 1.1.

1.7.2. Montrer que, relativement aux vitesses $\dot{q}_1, \dot{q}_2, \dot{q}_3, \dot{q}_4$, l'énergie cinétique T du système (S) s'écrit :

$$T = \frac{1}{2}\mu_1(\dot{q}_1^2 + \dot{q}_2^2) + \frac{1}{2}\mu_2(\dot{q}_3^2 + \dot{q}_4^2)$$

où les coefficients μ_1 et μ_2 sont appelés « masses réduites de Jacobi ». Déterminer μ_1 et μ_2.

1.7.3. Écrire le lagrangien L du système en utilisant les variables de Jacobi et leurs dérivées par rapport à t.

1.8. Pour écrire le système différentiel engendré par le lagrangien L, on définit les variables de Poisson canoniquement conjuguées des variables q_i, par les relations suivantes :

$$p_i = \frac{\partial L}{\partial \dot{q}_i} \qquad (i = 1, 2, 3, 4).$$

Montrer que les équations de Lagrange engendrées par L sont équivalentes aux équations de Hamilton :

$$(1.3.) \qquad \begin{cases} \dot{q}_i = \dfrac{\partial H}{\partial p_i} \\ \\ \dot{p}_i = -\dfrac{\partial H}{\partial q_i} \end{cases} \qquad (i = 1, 2, 3, 4)$$

engendrées par le hamiltonien H défini par :

$$H(\underline{q}, \underline{p}) = T(\underline{p}) - U(\underline{q}),$$

où l'on a posé :

$$\underline{q} = {}^t(q_1, q_2, q_3, q_4) \text{ et } \underline{p} = {}^t(p_1, p_2, p_3, p_4).$$

1.9. Montrer que le hamiltonien H est une intégrale première du système différentiel (1.3.).

DEUXIÈME PARTIE

On veut maintenant étudier le « Problème restreint circulaire des trois corps », défini à partir du système (S) décrit dans la première partie, lorsque la masse m_2 du corps P_2 est petite devant m_0 et m_1. On pose désormais : $m_2 = \varepsilon$. On va montrer que le problème se découple alors en un Problème des deux corps P_0 et P_1 d'une part, et, d'autre part, un problème dans lequel on étudie le mouvement de P_2 dans le champ créé par les deux « primaires » P_0 et P_1 en rotation uniforme l'une par rapport à l'autre. L'étude de ce mouvement se fait dans un système d'axes tournants liés aux corps P_0 et P_1.

2.1. Montrer que si, dans le développement de Taylor du lagrangien L déterminé à la question 1.7.3., relativement au petit paramètre ε, on ne conserve que les termes d'ordres 0 et 1, ce lagrangien s'écrit :

$$(2.1.)\ L = \frac{m_0 m_1}{2(m_0 + m_1)}(\dot{q}_1^2 + \dot{q}_2^2) + \frac{m_0 m_1}{r_2} + \varepsilon\left(\frac{1}{2}(\dot{q}_3^2 + \dot{q}_4^2) + \frac{m_1}{r_0} + \frac{m_0}{r_1}\right).$$

2.2. Montrer qui si ε tend vers zéro, le système différentiel engendré par le lagrangien (2.1.) se découple en deux systèmes, le premier (2.2.) régissant un mouvement képlérien des deux corps P_0 et P_1 (indépendamment du corps P_2), et le deuxième (2.3.) déterminant le mouvement de P_2 dans le champ créé par P_0 et P_1.

2.3. Montrer que le système (2.2.) admet des solutions de la forme :

$$\text{(2.4.)} \qquad \begin{cases} q_1 = a\cos nt, \\ q_2 = a\sin nt, \end{cases}$$

caractérisant un mouvement de rotation uniforme de P_0 et P_1 autour de leur centre de gravité G_{01}.

Quelle relation doivent alors vérifier la distance a et la vitesse de rotation n ?

2.4. Calculer, en fonction de m_0, m_1 et a, l'énergie totale h_0 associée aux solutions circulaires précédentes du système (P_0, P_1).

2.5. On suppose, dans toute la suite, que les corps P_0 et P_1 ont un mouvement de rotation uniforme autour de G_{01}, tel qu'il a été déterminé aux questions 2.3. et 2.4. Pour étudier les mouvements du corps P_2 dans le champ créé par P_0 et P_1, on considère le système tournant d'axes orthonormés direct $G_{01}xy$, où $\overrightarrow{G_{01}x}$ est porté par le vecteur $\overrightarrow{G_{01}P_1}$ et orienté dans le même sens. Soient x et y les coordonnées cartésiennes de P_2 dans ce repère tournant.

2.5.1. Montrer que les composantes, dans le repère tournant, de la vitesse absolue de P_2, sont respectivement :

$$\dot{x} - ny \quad \text{et} \quad \dot{y} + nx.$$

En déduire le lagrangien $\mathscr{L}(x, y, \dot{x}, \dot{y})$ relatif à l'unité de masse de P_2.

2.5.2. On définit les variables de Poisson X et Y, canoniquement conjuguées de x et y, par les relations :

$$X = \frac{\partial \mathscr{L}}{\partial \dot{x}}, \qquad Y = \frac{\partial \mathscr{L}}{\partial \dot{y}}.$$

Écrire le hamiltonien $\mathscr{H}(x, y, X, Y)$ de ce système, c'est-à-dire la fonction : $X\dot{x} + Y\dot{y} - \mathscr{L}$, exprimée en variables canoniques x, y, X, Y.

Montrer que le système différentiel engendré par le hamiltonien $\mathscr{H}$ admet l'intégrale première de l'énergie :

$$\text{(2.5.)} \qquad \mathscr{H} = k.$$

Cette intégrale première est habituellement appelée « intégrale de Jacobi ».

2.5.3. On pose :

$$\Omega(x, y) = \frac{m_0}{r_1} + \frac{m_1}{r_0} + \frac{n^2}{2}(x^2 + y^2).$$

Montrer que le système hamiltonien engendré par $\mathscr{H}(x, y, X, Y)$ est équivalent au système des deux équations du second ordre :

$$\begin{cases} \ddot{x} - 2n\dot{y} = \dfrac{\partial \Omega}{\partial x}, \\ \ddot{y} + 2n\dot{x} = \dfrac{\partial \Omega}{\partial y}. \end{cases}$$

2.5.4. Montrer qu'une combinaison simple de ces deux équations différentielles permet de retrouver l'intégrale première de Jacobi, sous la forme suivante :

$$\frac{1}{2}(\dot{x}^2 + \dot{y}^2) - \Omega(x, y) = k.$$

TROISIÈME PARTIE

N.B. — *Cette troisième partie peut être traitée indépendamment des deux premières.*

On poursuit ici l'étude du « Problème restreint circulaire des trois corps » : les « primaires » P_0 et P_1 (de masses m_0 et m_1) ont, l'une par rapport à l'autre, un mouvement circulaire uniforme de vitesse angulaire n, la distance $P_0 P_1$ étant égale à a; le corps P_2, dont la masse est petite devant m_0 et m_1, et qui ne pertube pas le mouvement de P_0 et P_1, est repéré, dans les axes tournants $G_{01}\,x\,y$ liés à la droite $P_0 P_1$ ($\overrightarrow{G_{01}\,x}$ étant porté par $\overrightarrow{P_0 P_1}$), par ses coordonnées cartésiennes x et y, et sa vitesse relative, dans ce repère tournant, a pour composantes $\dot{x}$ et $\dot{y}$. Comme cela a été démontré précédemment, le mouvement de P_2 dans ce repère tournant est décrit par le système différentiel :

$$(3.1.)\qquad \begin{cases} \ddot{x} - 2n\dot{y} = \dfrac{\partial \Omega}{\partial x}, \\ \ddot{y} + 2n\dot{x} = \dfrac{\partial \Omega}{\partial y}, \end{cases}$$

avec :
$$\Omega(x, y) = \frac{m_0}{r_1} + \frac{m_1}{r_0} + \frac{n^2}{2}(x^2 + y^2)$$

où
$$\begin{cases} r_0^2 = \left(x - \dfrac{m_0}{m_0 + m_1}\, a\right)^2 + y^2, \\ r_1^2 = \left(x + \dfrac{m_1}{m_0 + m_1}\, a\right)^2 + y^2, \end{cases}$$

et :
$$n^2 a^3 = m_0 + m_1.$$

On a également démontré que ce système admet l'intégrale première de Jacobi :

$$(3.2.)\qquad \frac{1}{2}(\dot{x}^2 + \dot{y}^2) - \Omega(x, y) = k,$$

où k est la « constante de Jacobi ».

Dans cette troisième partie, on démontre l'existence de configurations d'équilibre pour le Problème restreint circulaire (qui, d'ailleurs, existent également dans le Problème général des trois corps) : dans ces solutions particulières, les distances mutuelles des trois corps restent invariables au cours du temps. On étudie ensuite la stabilité de certaines de ces solutions particulières. Enfin, à partir de l'étude de ces configurations d'équilibre, on décrit, dans le plan de configuration, des régions où sont confinées les trajectoires de P_2 (« régions de Hill »).

3.1. Montrer que les solutions d'équilibre du système (3.1.) sont caractérisées par les points critiques de la fonction Ω. À quels mouvements correspondent ces solutions d'équilibre, pour un observateur lié au repère d'inertie dont l'origine est le centre de gravité du système ?

3.2. Montrer qu'il existe deux points d'équilibre $L_4(x_4, y_4)$ et $L_5(x_5, y_5)$ [on prendra : $y_4 > 0$ et $y_5 < 0$] qui déterminent des solutions pour lesquelles les trois corps P_0, P_1, P_2 sont placés aux sommets d'un triangle équilatéral ; on appelle ces points : « configurations d'équilibre de Lagrange ».

3.3. Montrer que, si $L_3(x_3, 0)$ définit une configuration alignée d'équilibre des trois corps disposés dans l'ordre $P_0 P_1 P_2$, alors x_3 est solution d'une équation algébrique du cinquième degré qu'on écrira explicitement.

(On démontre, et nous admettrons, que cette équation algébrique a une racine réelle unique x_3, caractérisant la « configuration alignée d'Euler » $P_0 P_1 P_2$, et que, de même, il existe deux autres configurations alignées d'équilibre, correspondant respectivement à l'ordre $P_0 P_2 P_1$ (point d'Euler $L_2(x_2, 0)$) et à l'ordre $P_2 P_0 P_1$ (point d'Euler $L_1(x_1, 0)$). On démontre aussi que les cinq points L_1, L_2, L_3, L_4, L_5 sont les seules configurations d'équilibre du Problème restreint, et que celles-ci existent également pour le Problème général des trois corps.)

3.4. Pour étudier la stabilité des points de Lagrange, on définit les solutions voisines de ces équilibres, en posant (on se place, par exemple, au voisinage du point L_4) :

$$\begin{cases} x = x_4 + \xi, \\ y = y_4 + \eta, \end{cases}$$

où x_4 et y_4 sont les coordonnées de L_4 déterminées à la question 3.2.

Écrire le système linéarisé (3.3.) déduit du système (3.1.), et que vérifient les variables ξ et η.

3.5. Pour déterminer les variétés stables et instables associées au point d'équilibre L_4, on cherche des solutions du système (3.3.) ayant la forme :

$$\begin{cases} \xi = e^{\lambda t} \\ \eta = s \cdot e^{\lambda t}. \end{cases}$$

Montrer que λ doit alors être racine d'une équation bicarrée que l'on écrira. En déduire que le point de Lagrange L_4 est un équilibre stable du système linéalisé (3.3.) si, et seulement si :

$$\nu^2 > \frac{23}{27},$$

avec :

$$\nu = \frac{m_0 - m_1}{m_0 + m_1}.$$

3.6. Montrer, en utilisant l'intégrale de Jacobi (3.2.), que la projection des solutions dans le plan de configuration (x, y) est contenue dans des régions (appelées « régions de Hill ») dont la forme dépend de la valeur de la constante de Jacobi k, et dont la frontière est la courbe de vitesse nulle dans le repère tournant.

3.7. Supposons que l'on donne aux masses m_0 et m_1 des valeurs telles que :

$$\Omega(L_4) = \Omega(L_5) < \Omega(L_1) < \Omega(L_3) < \Omega(L_2).$$

Sachant que les points L_4 et L_5 sont des minima de la fonction Ω, et que les points L_1, L_2, L_3 sont des cols de Ω, indiquer succinctement, dans le plan (x, y), quelle est la forme des régions de Hill, lorsque l'on donne à l'opposé $-k$ de la constante de Jacobi, des valeurs appartenant successivement aux intervalles suivants :

a. $\Omega(L_2) < -k < +\infty$,

b. $\Omega(L_3) < -k < \Omega(L_2)$,

c. $\Omega(L_1) < -k < \Omega(L_3)$,

d. $\Omega(L_4) < -k < \Omega(L_1)$,

e. $-\infty < -k < \Omega(L_4)$.

PROBABILITÉS ET STATISTIQUES

Notations et préliminaires.

1. *Variable aléatoire réelle.*

Dans tout le problème X (avec ou sans indice) note une *variable aléatoire réelle* (une v.a.r. en abrégé), de loi notée $\mathbb{P}_X$, de *fonction de répartition* (en abrégé f.r.) $F_X(t) = \mathbb{P}(X \leq t)$, continue à droite. On notera $F_X(t^-)$ sa limite à gauche. $\mathbb{E}$ est l'espérance mathématique associée à $\mathbb{P}$. La *fonction caractéristique* de X est la fonction $\varphi_X(t) = \mathbb{E}(e^{itX})$.

La *transformée de Fourier* d'une fonction réelle de variable réelle f, Lebesgue-intégrable, est $\widehat{f}(t) = \int f(x)e^{itx}dx$. Si la loi de X a une densité f, φ_X n'est autre que $\widehat{f}$. Une *médiane* μ est un réel vérifiant $\mathbb{P}(X \leq \mu) \geq 1/2$, $\mathbb{P}(X \geq \mu) \geq 1/2$. On admet le

Théorème de Radon-Nikodym (sur $\mathbb{R}$): Si la loi de X est *absolument continue*, c'est à dire que pour toute partie N de mesure de Lebesgue nulle, $\mathbb{P}(X \in N) = 0$ alors elle a une densité, c'est-à-dire qu'il existe une fonction p positive et intégrable telle que $\mathbb{P}(X \in A) = \int_A p(x)dx$.

Le *support topologique* de la loi de X est le plus petit fermé F tel que $\mathbb{P}_X(F) = 1$, soit encore $\mathbb{P}(X \in F) = 1$, et le réel x appartient à ce support si et seulement si

$$\text{Pour tout } \varepsilon > 0, \mathbb{P}(X \in]x - \varepsilon, x + \varepsilon[) > 0.$$

On dit la v.a.r. X *dégénérée* (ou la loi de X dégénérée) s'il existe un réel a tel que $\mathbb{P}(X = a) = 1$.

La loi de X est dite *diffuse* si la f.r. associée est continue, *discrète* si la f.r. ne croît que par sauts (elle est alors concentrée sur un ensemble dénombrable). Elle est dite *singulière* si elle est diffuse et s'il existe un ensemble N de mesure de Lebesgue nulle avec $\mathbb{P}(X \in N) = 1$. Sa *fonction de concentration* (ou sa concentration) est la fonction définie sur $\mathbb{R}^+$ par

$$Q_X(t) = \sup_{y \in \mathbb{R}} \mathbb{P}(X \in [y, y + t]). \tag{1}$$

En particulier, $Q_X(0)$ n'est nul que si la loi de X est diffuse, et sinon a pour valeur le saut maximum de cette loi. On fait la convention que $Q_X(t)$ vaut 0 pour $t < 0$.

Enfin, si $I = [a, b]$ est un segment fermé et y un réel, $I + y$ note le segment translaté $[a + y, b + y]$.

2. *Convergence en loi, relative compacité.*

Une suite de v.a.r. $\{Y_n\}$ est dite *relativement compacte en loi* si:

$$\forall \varepsilon > 0, \ \exists M \text{ tel que } \forall n, \mathbb{P}(|Y_n| \geq M) \leq \varepsilon.$$

Cette condition équivaut à la propriété : De toute suite extraite on peut extraire une sous-suite convergente en loi.

3. *Nombres de Pisot-Salem.*

Ce paragraphe a pour but d'introduire les nombres de Pisot-Salem et d'en donner deux propriétés essentielles. Les Polynômes étudiés ici sont ceux de $\mathbb{Q}[X]$ (Polynômes à coefficients rationnels) ou de $\mathbb{Z}[X]$ (Polynômes à coefficients entiers).

Un Polynôme *unitaire* P est un Polynôme de $\mathbb{Z}[X]$, dont le coefficient du terme de plus haut degré vaut 1. Un Polynôme est *irréductible* s'il n'a pas *dans* $\mathbb{Q}[X]$ d'autres diviseurs que les nombres rationnels. Rappelons deux propriétés de ces Polynômes (qu'*on ne demande pas de démontrer*):

p1: Dans $\mathbb{Q}[X]$, si A est irréductible et s'il a une racine (dans $\mathbb{C}$) commune avec B, alors A divise B.

p2: Si A est unitaire et s'il est factorisable *dans* $\mathbb{Q}[X]$ en $A = B \cdot C$, alors on peut choisir B et C unitaires.

Un *entier algébrique* est (au sens strict) une racine d'un Polynôme unitaire irréductible mais aussi, grâce à p2, toute racine d'un Polynôme unitaire.

On peut donc associer à un entier algébrique θ un Polynôme P_θ, à la fois irréductible et unitaire, *unique*, dont il est racine. Les autres racines de P_θ sont des entiers algébriques, dits *conjugués* de θ.

Le *degré* de θ est le degré de P_θ. Ainsi les entiers sont des entiers algébriques (de degré 1) et sont les seuls entiers algébriques sans conjugués.

Nombres de Pisot: θ est un nombre de Pisot si θ est un entier algébrique dont tous les conjugués sont de module strictement inférieur à 1. Leur ensemble est noté S.

On remarquera que, le produit des racines d'un Polynôme unitaire étant un entier non nul si 0 n'est pas racine de ce Polynôme, $|\theta| > 1$ pour $\theta \in S$ (sauf si $|\theta| = 0$ ou si $|\theta| = 1$).

Dans tout le problème $\{X_i | i \in \mathbb{N}^*\}$ désigne une suite de v.a.r. indépendantes dont on note $\{S_n | n \in \mathbb{N}^*\}$ la suite des sommes partielles

$$S_n = X_1 + X_2 + \cdots + X_n.$$

La partie **A** est consacrée à la démonstration de quelques propriétés élémentaires de la concentration.

L'une d'entre elles est utilisée dans la partie **B** pour prouver le Théorème de Jessen.

La partie **C**, indépendante, est consacrée à la preuve du Théorème de pureté.

Les parties **D** et **E** sont consacrées à la construction de Probabilités sur $\mathbb{R}$ vérifiant diverses conditions de support. Elles utilisent les résultats des parties précédentes.

A. *Propriétés de la fonction de concentration.*

La fonction de concentration Q_X est définie par la formule (1).

1°) Montrer que si $t > 0$, $Q_X(t) > 0$.

2°) Soit t un réel positif ou nul fixé.

a) Soit $\{a_n\}$ une suite telle que $\mathbb{P}(X \in [a_n, a_n + t])$ converge vers une limite $q(t) > 0$. Montrer que la suite $\{a_n\}$ est bornée.

b) Soit $\{a_n\}$ une suite qui converge vers a. Montrer que

$$\text{limsup}_n \mathbb{P}(X \in [a_n, a_n + t]) \leq \mathbb{P}(X \in [a, a + t])$$

(se donnant $\varepsilon > 0$, on pourra minorer $\mathbb{P}(X \in]a - \varepsilon, a + \varepsilon + t[)$). En déduire que si $\mathbb{P}(X \in [a_n, a_n + t])$ tend vers $Q_X(t)$, alors $\mathbb{P}(X \in [a, a + t]) = Q_X(t)$.

c) En déduire qu'il existe un segment I_t de longueur t tel que $Q_X(t) = \mathbb{P}(X \in I_t)$ (On dit que I_t "réalise la concentration").

3 °) Par un raisonnement analogue, prouver que Q_X est continue à droite, puis que Q_X est une fonction de répartition.

4 °) Montrer qu'une CNS pour que X soit dégénérée est que $Q_X(t) = 1$ pour tout $t > 0$.

5 °) a) Soit μ une médiane de X et t tel que $Q_X(t) > 1/2$; soit I_t réalisant cette concentration. Montrer que $\mu \in I_t$, et en déduire que

$$\mathbb{P}(|X| \leq t + |\mu|) \geq Q_X(t) \geq \mathbb{P}(|X| \leq t/2).$$

b) Soit $\{Y_n\}$ une suite de v.a.r. Démontrer qu'une CNS pour que cette suite soit relativement compacte en loi est que:

c1) l'ensemble de leurs médianes μ_n soit borné.

c2) il existe Q, f.r. sur $\mathbb{R}^+$ qui minore toutes les Q_{Y_n} .

6 °) Soient s et t deux réels positifs. Soit I_t un segment de longueur t. Montrer que

$$\mathbb{P}(X \in I_t) + \mathbb{P}(X \in I_t - s) \leq Q_X(t + s) + Q_X(t - s).$$

Dans les deux questions suivantes, X et Y sont deux v.a.r *indépendantes.*

7 °) Prouver que $\mathbb{P}(X + Y \in [a, a + t]) \leq Q_X(t)$ et en déduire

$$Q_{X+Y}(t) \leq \min[Q_X(t), Q_Y(t)]. \tag{2}$$

8 °) Le but de cette question est de prouver l'assertion

(3) Sauf si Y est dégénérée, il existe au moins un $t > 0$ où l'inégalité stricte $Q_{X+Y}(t) < Q_X(t)$ est vérifiée.

a) Montrer que si Y n'est pas dégénérée, il existe $s > 0$ tel que le support de la loi de Y contienne deux points distincts u et $u + s$.

b) Soient $t > 0$ tel que $Q_{X+Y}(t) = Q_X(t)$, et I_t réalisant $Q_{X+Y}(t)$; montrer que $\mathbb{P}(X \in I_t - y) = Q_X(t)$ pour $\mathbb{P}_Y$-presque tout y, puis, en utilisant 2 °) b), que $\mathbb{P}(X \in I_t - y) = Q_X(t)$ pour tout y du support de $\mathbb{P}_Y$.

c) Soit $t > 0$ tel que $Q_{X+Y}(t) = Q_X(t)$. Etablir l'inégalité

$$2Q_X(t) \leq Q_X(t + s) + Q_X(t - s) .$$

d) Conclure en étudiant les accroissements de la suite $\{Q_X(ns) | n \in \mathbb{N}\}$.

B. *Théorème de Jessen.*

On suppose que $\{S_n\}$ est presque surement convergente et on note S sa limite p.s., R_n le reste $S - S_n$. On utilisera les notations p, p_n, q_n, r_n pour les sauts maximaux (les valeurs en 0 des différentes fonctions de concentrations) respectivement pour les lois de S, X_n, S_n et R_n, de sorte que le cas où la loi de S n'est pas diffuse se caractérise par

$$0 < p = Q_S(0). \tag{4}$$

Dans cette partie, par abus de langage, on parlera de "concentration" pour "valeur en 0 de la fonction de concentration".

1°) On note α le produit infini $\Pi_n p_n$.

a) Montrer que $p \leq q_n \leq p_n$ puis que si l'une des X_n est diffuse, S l'est.

b) Soit x_n tel que $p_n = \mathbb{P}(X_n = x_n)$. Montrer que

$$\alpha \leq \mathbb{P}(\forall n, S_n = x_1 + x_2 + \cdots + x_n);$$

en déduire que si $\alpha > 0$, alors la série $\Sigma_n x_n$ converge.

c) Que peut on dire de $\mathbb{P}(S = \Sigma_n x_n)$? Prouver que:

$$\text{Si } \Pi_n p_n > 0, \text{ alors } p > 0.$$

d) Montrer que $q_n \downarrow p$.

On suppose $p > 0$ dans les questions 2°)3°)4°) qui suivent. On remarque que si U et V sont deux v.a.r. indépendantes, et si a est un réel, alors

$$\mathbb{P}(U + V = a) = \Sigma_{x \in \mathcal{D}} \mathbb{P}(U = x)\mathbb{P}(V = a - x)$$

où $\mathcal{D}$ est l'ensemble des points de discontinuité de la f.r. de U. Dans la suite on allègera encore cette formule en l'écrivant

$$\mathbb{P}(U + V = a) = \Sigma_x \mathbb{P}(U = x)\mathbb{P}(V = a - x)\ .$$

2°) On se ramène par une translation au cas où S réalise au point 0 sa concentration. Soit $\mathcal{V}$ un voisinage symétrique de 0. Etablir l'inégalité:

$$p = \mathbb{P}(S = 0) = \Sigma_x \mathbb{P}(S_n = x)\mathbb{P}(R_n = -x) \leq r_n \mathbb{P}(S_n \in \mathcal{V}) + q_n \mathbb{P}(R_n \notin \mathcal{V}). \tag{5}$$

Montrer que l'hypothèse de convergence entraîne $\lim_n \mathbb{P}(R_n \notin \mathcal{V}) = 0$, puis que $\lim_{\mathcal{V}} \limsup_n \mathbb{P}(S_n \in \mathcal{V}) = p$. Prouver que $r_n \to 1$, puis que $r_n \uparrow 1$ et que $p_n \to 1$.

3°) En déduire que pour n grand, chacune des concentrations r_n et p_n est atteinte en un point unique. Posant $r_n = \mathbb{P}(R_n = y_n)$, $p_n = \mathbb{P}(X_n = x_n)$, en majorant convenablement $\mathbb{P}(X_n = x_n; R_n \neq y_n)$, $\mathbb{P}(X_n \neq x_n; R_n = y_n)$ et enfin $\mathbb{P}(X_n + R_n = y; X_n \neq x_n; R_n \neq y_n)$, prouver que pour n grand:

a) $y_{n-1} = x_n + y_n$

b) $r_{n-1} = \mathbb{P}(R_{n-1} = y_{n-1}) = r_n p_n + \Sigma_{x \neq 0} \mathbb{P}(R_n = y_n - x)\mathbb{P}(X_n = x_n + x)$.

4°) En déduire que $r_{n-1} \leq r_n p_n + (1 - r_n)(1 - p_n)$ (n grand)

5°) Prouver le

Théorème de Jessen: Si les X_i sont indépendantes et si leur série converge, une CNS pour que la loi de leur somme ne soit pas diffuse est que le produit infini des sauts maximum $\Pi_n p_n$ soit strictement positif.

C. *Théorème de Wintner.*

Dans cette partie comme dans la précédente S_n converge presque surement et on note S sa limite p.s. On suppose de plus que les lois des X_i sont discrètes et concentrées sur les A_i dénombrables. On note B pour la réunion des A_i, qu'on suppose énuméré: $B = (b_m | m \in \mathbb{N})$. Enfin C est l'ensemble des sommes *finies* de termes $\varepsilon_k b_k$, où les b_k sont pris dans B (avec redoublements possibles) et les ε_k valent 1 ou -1. Soit $\mathcal{B}_n$ la σ-algèbre du futur, c'est-à-dire celle engendrée par les $X_k, k > n$.

1 °) Soit E un Borélien.

a) Montrer que l'évenement $F = (S \in E + C)$ est un évenement de $\mathcal{B}_n$ (on calculera l'intersection de F par $\cap_{i=1}^{n}(X_i = x_i)$ pour les x_i dans A_i).

b) Que vaut $\mathbb{P}(F)$ pour un tel F ?

2 °) Montrer que C est dénombrable et que $C + C = C - C = C$ (suivant la convention usuelle, $A + B$ désigne $\{a + b | a \in A, b \in B\}$).

3 °) Montrer que si la loi de S n'est pas diffuse, il existe un réel a tel que $\mathbb{P}(S \in a + C) = 1$.

4 °) S'il existe un Borélien N de mesure de Lebesgue nulle tel que $\mathbb{P}(S \in N) > 0$, montrer qu'il existe un Borélien M de mesure de Lebesgue nulle tel que $\mathbb{P}(S \in M) = 1$.

5 °) Prouver le Théorème de Wintner (ou Théorème de pureté) ci-après:

Théorème: Soit la loi de $S = \Sigma X_i$, les X_i indépendantes et de lois discrètes. Alors cette loi est ***pure***, c'est-à-dire que:

-Soit la loi est discrète.

-Soit la loi est absolument continue.

-Soit la loi est singulière.

D. *Construction de lois singulières.*

On se donne dans cette partie une suite $\{\varepsilon_i\}$ de v.a.r. indépendantes et de même loi: $\mathbb{P}(\varepsilon_i = 1) = \mathbb{P}(\varepsilon_i = -1) = 1/2$, qu'on appellera "signes". On se donne un réel ξ de $]0, 1[$ et on considère la v.a.r.

$$S = \Sigma_{i>0} \varepsilon_i \xi^i. \tag{6}$$

Montrer que la série converge sûrement!

Le but de cette partie est de prouver l'assertion suivante:

(7) Si $1/\xi$ est un nombre de Pisot différent de 2, la loi de S est singulière.

Les deux premières questions établissent des propriétés de $\mathcal{S}$ utiles dans la suite du problème .

1 °) a)Prouver que si θ est un entier algébrique, racine du Polynôme A de $\mathbb{Q}(X)$, alors ses conjugués sont aussi racines de A.

En déduire que, pour m entier positif:

b) Si $\theta^m = 2$, sauf si $m = 1$ et $\theta = 2$, θ ne peut être élément de $\mathcal{S}$.

c) Si $\theta^m = h + 1/2$ où h appartient à $\mathbb{Z}$, θ ne peut être élément de $\mathcal{S}$.

2 °) En utilisant les relations entre coefficients et racines d'un Polynôme, montrer que, si $\theta \in S$, alors il existe deux réels C et ρ avec $0 < \rho < 1$ tels que: pour tout n de $\mathbb{N}$ il existe k de $\mathbb{Z}$ avec $|\theta^n - k| \leq C\rho^n$.

3 °) Vérifier que si f est l'indicatrice de l'intervalle $[a, b]$ avec $-\infty < a < b < \infty$, sa transformée de Fourier $\widehat{f}(t)$ tend vers 0 quand $|t|$ tend vers l'infini. Par un argument de densité, vérifier le *Lemme de Riemann-Lebesgue*: Si f est Lebesgue-intégrable, alors $\lim_{|t|\to\infty} |\widehat{f}(t)| = 0$.

4 °) Soient θ un nombre de Pisot avec $0 < \xi = 1/\theta < 1$, θ différent de 2, et φ la fonction caractéristique de la v.a.r. S définie par (6). Justifier que φ s'écrit sous forme d'un produit infini convergent. Montrer que la suite γ_n définie par $\gamma_n = |\varphi(\theta^n \pi)|$ a une limite non nulle (on suggère d'étudier séparément

$$A_n = \Pi_{k<n}|\cos(\pi\theta^k)| \text{ et } B = |\Pi_{0\leq k}\cos(\pi\theta^{-k})|).$$

5 °) En combinant ces résultats avec les Théorèmes précédents prouver l'assertion (7).

6 °) Décrire la loi de S quand $\xi = 1/2$.

E. *Etude des supports topologiques.*

Cette partie a pour but d'étudier le support topologique des Probabilités introduites dans la partie **D** dont on reprend les notations. Soit S_n la v.a.r. somme des n premiers termes: $S_n = \Sigma_{0<i\leq n}\varepsilon_i\xi^i$.

La loi de S_n accorde la masse 2^{-n} à chacun des nombres $\Sigma_{0<i\leq n} \pm \xi^i$ (qui ne sont pas nécéssairement distincts). On note A_n l'ensemble de ces valeurs possibles. Dans ce qui suit, on se donne une suite de v.a.r. auxiliaires $\{U_n\}$, indépendante de la suite $\{\varepsilon_i\}$. On suppose U_n de loi uniforme sur l'intervalle J_n centré en 0 et de longueur $2\xi^{n+1}/(1-\xi)$. On définit les v.a.r. $T_n = S_n + U_n$. On note C_n l'ensemble $C_n = \cup(a + J_n | a \in A_n)$.

E.1 *Le cas* $\xi < 1/2$.

Dans ce paragraphe, ξ est un réel tel que $0 < \xi < 1/2$.

1 °) Soit a et a' deux points distincts de A_n. Montrer que

$$|a' - a| \geq 2\xi^n.$$

En déduire que C_n est composé de 2^n intervalles disjoints, que $C_{n+1} \subset C_n$ et que T_n a une densité constante sur C_n et nulle en dehors.

2 °) Montrer que T_n tend en loi vers S, et que $\mathbb{P}(S \in C_n) = 1$.

3 °) Soit $C_\xi = \cap_n C_n$. Montrer que C_ξ est un ensemble fermé, de mesure de Lebesgue nulle et que $\mathbb{P}(S \in C_\xi) = 1$. Montrer que C_ξ est un ensemble *parfait*, c'est-à-dire que tout point α de C_ξ est limite d'une suite $\{\alpha_n\}$ telle que: a) $\alpha_n \in C_\xi$; b) $\alpha_n \neq \alpha$.

4 °) Construire la suite $\{F_n\}$ des fonctions de répartition des variables T_n et vérifier qu'elle converge uniformément.

5 °) Conclure des quatre questions précédentes une preuve directe de ce que, quand $0 < \xi < 1/2$, la construction (6) donne une loi singulière dont le support topologique est de mesure de Lebesgue nulle.

E.2 *Le cas* $1/2 < \xi < 1$.

Soit J_ξ l'intervalle $[-\xi/(1-\xi), \xi/(1-\xi)]$. On se propose de prouver que le support topologique de la loi de S est J_ξ. Soit x vérifiant $0 < x < \xi/(1-\xi)$.

6 °) Montrer qu'il existe un entier ℓ_1 tel que

$$0 \leq \Sigma_{0<i<\ell_1} \xi^i < x \leq \Sigma_{0<i\leq\ell_1} \xi^i < \xi/(1-\xi).$$

7 °) Construire par récurrence une suite croissante d'entiers distincts ℓ_k et un choix de signes e_i tels que si $w_k = \Sigma_{0<i\leq\ell_k} e_i \xi^i$ on ait simultanément

a) $|x - w_k| \leq \xi^{\ell_k}$.

b) $\forall t \geq 0$, $w_{2t} \leq x \leq w_{2t+1}$

c) $\mathbb{P}(w_k - \xi^{\ell_k+1}/(1-\xi) \leq S \leq w_k + \xi^{\ell_k+1}/(1-\xi)) \geq 2^{-\ell_k}$

(On notera que les w_k et les e_i, non aléatoires, sont fonction de x).

8 °) En déduire que la loi de S donne une Probabilité strictement positive à tout ouvert (non vide) de J_ξ.

9 °) Le *nombre d'or* est le nombre $\theta_o = (1+\sqrt{5})/2$. Soit ξ_o son inverse. Montrer que la loi de la variable S définie par la formule (6) où l'on porte $\xi = \xi_o$ a les propriétés suivantes:

- Le support topologique est un intervalle (d'intérieur non vide).
- Cependant il existe un Borélien N de mesure de Lebesgue nulle tel que $\mathbb{P}(S \in N) = 1$.
- Cette loi est diffuse.
- La fonction caractéristique φ_S ne tend pas vers 0 à l'infini.

MATHÉMATIQUES DE L'INFORMATIQUE

Dans tout ce problème, nous désignerons par K un corps quelconque, par p un nombre premier, et par $\mathbb{F}_p$ le corps à p éléments dont on écrira les éléments $0, 1, \ldots, p-1$ sans distinction avec les nombres entiers naturels.

Dans un anneau $\mathcal{A}$, on appelle unité, un élément inversible. (Lorsque $\mathcal{A} = \mathbb{Z}[X]$, les unités sont $+1$ et -1, lorsque $\mathcal{A} = K[X]$, les unités sont les éléments de K sauf 0).

Soient a et b deux éléments de $\mathcal{A}$, on dit que a divise b s'il existe $c \in \mathcal{A}$ tel que $b = ac$. La congruence dans $\mathcal{A}$

$$a \equiv b \bmod c$$

signifie "c divise $a - b$".

Si P et Q sont deux polynômes de $K[X]$, on notera $P \bmod Q$ le reste dans la division euclidienne de P par Q, et $\text{pgcd}(P, Q)$ le polynôme unitaire (ce qui veut dire que le coefficient du monôme de plus haut degré vaut 1) de degré maximum qui divise simultanément P et Q.

On dira qu'un polynôme P à coefficients dans $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{C}$ est sans facteurs carrés si toutes les racines de P dans $\mathbb{C}$ sont simples.

Enfin dans un anneau $\mathcal{A}$ on dit que $a \in \mathcal{A}$ est irréductible si l'égalité $a = bc$ avec b et c dans $\mathcal{A}$ implique que b ou c est une unité. Tout polynôme unitaire de $K[X]$ s'écrit de façon unique comme produit de polynômes unitaires irréductibles dans $K[X]$. On rappelle également que tout polynôme de $\mathbb{Z}[X]$ à coefficient dominant positif s'écrit de façon unique comme produit de polynômes irréductibles de $\mathbb{Z}[X]$ à coefficient dominant positif. Factoriser un polynôme consiste à déterminer ses facteurs irréductibles.

- I -

1) a) Factoriser le polynôme $x^5 + x + 1$ sur $\mathbb{F}_2[X]$.

b) Combien y a-t-il de polynômes irréductibles de degré $1, 2, 3, 4$ dans $\mathbb{F}_2[X]$?

2) a) Soient A et B deux polynômes de $K[X]$ de degrés m et n. Montrer que la division euclidienne de A par B peut s'effectuer avec $(m - n + 1)(2n + 3)$ opérations de K si $m \geqslant n$.

b) Montrer que le pgcd de A et B peut se calculer en $O(mn)$ opérations de K.

3) a) Soit la matrice

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

à coefficients dans $\mathbf{F}_2$, et I la matrice unité de même taille. Quel est le rang de $M - I$? Montrer que 1 est valeur propre de M, et trouver les vecteurs propres correspondants.

b) Soient n et r deux entiers naturels vérifiant $1 \leqslant r \leqslant n$. Parmi les 2^{nr} familles de r vecteurs de $\mathbf{F}_2^n$, combien y en a-t-il qui sont des familles linéairement indépendantes ?

4) a) Montrer que pour tout $F \in \mathbf{Q}[X]$, le polynôme

$$G = F/\operatorname{pgcd}(F, F')$$

est sans facteurs carrés et est à coefficients dans $\mathbf{Q}$.

b) On considère la procédure suivante qui, à partir de $F \in \mathbf{Q}[X]$ calcule l'entier k et le tableau de polynômes $P = P_1, P_2, \ldots, P_k$.

Procédure poly(F, k, P) ;
$C_1 := \operatorname{pgcd}(F, F')$;
$D_1 := F/C_1$; $i := 1$;
tantque $C_i \neq 1$ faire
  $C_{i+1} := \operatorname{pgcd}(C_i, C_i')$;
  $D_{i+1} := C_i/C_{i+1}$;
  $P_i := D_i/D_{i+1}$;
  $i := i + 1$;
fin tantque ;
$k := i$; $P_k := D_k$;

Exécuter cette procédure lorsque F est sans facteurs carrés, puis lorsque $F(x) = x^3(x^2 - 1)(x^4 - 1)$.

Montrer que tout polynôme $F \in \mathbf{Q}[X]$ peut s'écrire comme un produit de polynômes à coefficients dans $\mathbf{Q}$ et sans facteurs carrés.

5) Soient m et n deux entiers naturels non nuls et U et V deux polynômes de degré n et m dans $K[X]$ où K est un corps :

$$U = \sum_{i=0}^{n} u_i x^i \; ; \qquad V = \sum_{i=0}^{m} v_i x^i .$$

a) On suppose U et V premiers entre eux et on considère $S \in K[X]$ de degré $< m + n$. Montrer qu'il existe A et B dans $K[X]$ avec $d^0 A < m$, $d^0 B < n$ tels que

$$AU + BV = S$$

et ceci de façon unique.

Application numérique : $K = \mathbb{Q}$, $U = 1 + x + x^2 + x^3$, $V = 1 + x + x^2$, calculer A et B lorsque $S = 1$, puis lorsque $S = s_0 + s_1 x$.

b) Soit $R = R(U, V)$ la matrice carrée à $m + n$ lignes définie par :

$$\begin{aligned} &\text{pour } 1 \leqslant j \leqslant m, && r_{i,j} = u_{n+j-i} \\ &\text{pour } m+1 \leqslant j \leqslant m+n, && r_{i,j} = v_{j-i}. \end{aligned}$$

Par convention on pose $u_i = 0$ pour $i < 0$ et $i > n$ et de même $v_i = 0$ pour $i < 0$ et $i > m$.

Montrer que R est inversible si et seulement si U et V sont premiers entre eux.

Montrer que les polynômes A et B de 5)a) peuvent se calculer à partir de R^{-1} et de S.

Application numérique : $U(x) = 2x^3 + x^2 + x + 1$, $V(x) = 6x^2 + x + 1$. On a $R = R(U, V)$:

$$R = \begin{pmatrix} 2 & 0 & 6 & 0 & 0 \\ 1 & 2 & 1 & 6 & 0 \\ 1 & 1 & 1 & 1 & 6 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \quad \text{et} \quad R^{-1} = \frac{1}{164} \begin{pmatrix} 7 & -30 & -12 & 192 & -120 \\ 5 & 2 & -32 & 20 & 172 \\ 25 & 10 & 4 & -64 & 40 \\ -7 & 30 & 12 & -28 & -44 \\ -5 & -2 & 32 & -20 & -8 \end{pmatrix}$$

Calculer A et B tels que $AU + BV = S$ lorsque

$$S = 8x^4 + 8x^3 + 20x^2 + 10x + 7.$$

6) Soit $U \in \mathbb{C}[X]$ avec

$$U(x) = \sum_{i=0}^{n} u_i x^i$$

et $u_n \neq 0$. On pose

$$N(U) = \left(\sum_{i=0}^{n} |u_i|^2 \right)^{1/2}.$$

a) Soient $\alpha \in \mathbb{C}$, et $\bar{\alpha}$ son conjugué. On pose

$$g(x) = (x - \alpha)U(x) \quad \text{et} \quad h(x) = (\bar{\alpha}x - 1)U(x).$$

Montrer que $N(g) = N(h)$.

b) Soient $x_1, x_2, \ldots, x_n$ les racines de U dans $\mathbb{C}$. On pose

$$M(U) = |u_n| \prod_{1 \leqslant i \leqslant n} \max(1, |x_i|).$$

Montrer que

$$M(U) \leqslant N(U)$$

et que

$$|u_j| \leqslant \binom{n}{j} M(U), \quad \text{avec } \binom{n}{j} = \frac{n!}{j!(n-j)!}.$$

c) On suppose maintenant que $U \in \mathbb{Z}[X]$ et que V est un diviseur de U dans $\mathbb{Z}[X]$, de degré d :

$$V(x) = \sum_{i=0}^{d} v_i x^i.$$

Montrer que pour $0 \leqslant i \leqslant d$, on a :

$$|v_i| \leqslant \binom{d}{[d/2]} N(U).$$

Application numérique : donner une majoration des coefficients des diviseurs éventuels de $U(x) = x^5 + 2x^4 - 22x^3 + 53x^2 - 28x + 6$ dans $\mathbb{Z}[X]$.

- II -

1) Soient K un corps, et $U_1, \ldots, U_r$ des polynômes de $K[X]$ premiers entre eux deux à deux. Soit $A_1, \ldots A_r$ des polynômes quelconques de $K[X]$. Montrer qu'il existe un et un seul polynôme $F \in K[X]$ satisfaisant

$$d^0 F < \sum_{i=1}^{r} d^0 U_i$$

et

$$F \equiv A_i \bmod U_i \qquad 1 \leqslant i \leqslant r.$$

Donner un algorithme de calcul de F.

2) Soient p un nombre premier, et $U(x)$ un polynôme unitaire de $\mathbb{F}_p[X]$. On suppose que $n = d^0 U$, $n \geqslant 1$,

$$U = \prod_{i=1}^{r} U_i$$

où les U_i sont unitaires, irréductibles et distincts dans $\mathbb{F}_p[X]$ et de degré $\geqslant 1$. Montrer que le nombre de polynômes unitaires $V \in \mathbb{F}_p[X]$ vérifiant

$$d^0 V \leqslant n - 1$$

et

$$V(x)^p \equiv V(x) \mod U$$

est égal à p^r.

Application numérique : trouver les polynômes $V(x)$ lorsque $p = 5$, et

$$U(x) = (1 + x + x^2)(1 + x + x^2 + x^3).$$

3) Le polynôme U vérifie les mêmes hypothèses qu'à la question précédente. Soit $\mathbf{F}_p^{(n-1)}[X]$ l'ensemble des polynômes de degré $\leqslant n - 1$ de $\mathbf{F}_p[X]$. Montrer que l'application

$$\Phi : \mathbf{F}_p^{(n-1)}[X] \to \mathbf{F}_p^{(n-1)}[X]$$
$$V(x) \mapsto V(x^p) \bmod U$$

est linéaire sur le corps $\mathbf{F}_p$. Soit M la matrice de Φ dans la base canonique $1, X, \ldots, X^{n-1}$ de $\mathbf{F}_p^{(n-1)}[X]$. Donner une méthode de calcul de cette matrice. Montrer que 1 est valeur propre de M, et que la dimension du sous-espace propre correspondant est égale à r.

Application numérique : calculer M lorsque $p = 2$ et $U(x) = x^5 + x + 1$.

4) Le polynôme U vérifie toujours les hypothèses de II.2). Soit $V_1, V_2, \ldots, V_r$ une base du sous-espace propre de Φ, pour la valeur propre 1. On considère la procédure suivante qui, à partir de U, fournit k, et le tableau de polynômes $W = W_1, \ldots, W_k$.

```
Procédure    Facteur (U, k, W) ;
k := 1 ;
W_1 := U ;
Pour i de 1 à r faire
   Pour s de 0 à p − 1 faire
      ℓ := k ;
      Pour j de 1 à k faire
         D := pgcd(W_j, V_i − s) ;
         Si D ≠ 1 et D ≠ W_j alors
            ℓ := ℓ + 1 ;
            W_ℓ := D ;
            W_j := W_j / D
         finsi
      finpour
      k := ℓ ;
   finpour
finpour.
```

Montrer que les polynômes W_j, $1 \leqslant j \leqslant k$, retournés par cette procédure sont des diviseurs de U, et que, à l'ordre près, ils sont égaux à $U_1, \ldots, U_r$ (et donc $k = r$).

5) Soient maintenant $U \in \mathbb{Z}[X]$, unitaire, et p un nombre premier. On suppose qu'il existe deux polynômes f_1 et g_1 de $\mathbb{Z}[X]$, unitaires, premiers entre eux dans $\mathbb{F}_p[X]$ tels que dans $\mathbb{Z}[X]$, on ait :

$$U \equiv f_1 g_1 \mod p.$$

Montrer qu'il existe deux suites de polynômes unitaires f_n, g_n de $\mathbb{Z}[X]$ vérifiant $d^0 f_n = d^0 f_1$, $d^0 g_n = d^0 g_1$ et les congruences dans $\mathbb{Z}[X]$:

$$f_n \equiv f_1 \bmod p \; ; \qquad g_n \equiv g_1 \bmod p$$

et

$$U \equiv f_n g_n \bmod p^n.$$

Application numérique : $U(x) = x^5 + 2x^4 - 22x^3 + 53x^2 - 28x + 6$, $p = 5$, $f_1(x) = x^3 + x^2 + x + 1$; $g_1(x) = x^2 + x + 1$. Trouver f_3 et g_3.

6) Soit $U \in \mathbb{Z}[X]$ unitaire. On suppose que dans $\mathbb{Q}[X]$, $\operatorname{pgcd}(U, U') = 1$. Montrer qu'il existe un nombre premier p tel que dans $\mathbb{F}_p[X]$, $\operatorname{pgcd}(U, U') = 1$.

Déduire des questions précédentes un algorithme de décomposition de U en facteurs irréductibles dans $\mathbb{Z}[X]$.

Application : décomposer le polynôme $U(x)$ de la question précédente en facteurs irréductibles sur $\mathbb{Z}[X]$.

7) Soit $U(x) = u_n x^n + \cdots + u_0 \in \mathbb{Z}[X]$ un polynôme sans facteurs carrés. Montrer que, si U s'écrit comme le produit de deux polynômes de $\mathbb{Z}[X]$, alors $u_n U$ peut s'écrire comme le produit de deux polynômes de $\mathbb{Z}[X]$ dont les coefficients dominants sont égaux à u_n. En déduire un algorithme de décomposition de U en facteurs irréductibles.

- III -

Soit $V \in \mathbb{Z}[X]$, $V = \sum_{i=0}^{m} v_i x^i$. On appelle contenu de V le pgcd des coefficients $v_0, \ldots, v_m$ de V. Un polynôme de $\mathbb{Z}[X]$ est dit primitif si son contenu est égal à 1.

On pourra utiliser les théorèmes suivants :

THÉORÈME 1. — *Le produit de polynômes primitifs est primitif. Le contenu d'un produit de polynômes est égal au produit des contenus.*

THÉORÈME 2. — *Tout $V \in \mathbb{Z}[X]$ peut s'écrire de façon unique*

$$V = \Omega F_1^{e_1} \ldots F_k^{e_k}$$

où les F_i sont des polynômes distincts de $\mathbb{Z}[X]$, irréductibles, primitifs, à coefficient dominant positif, de degré $\geqslant 1$, les e_i des entiers naturels $\geqslant 1$, et $\Omega \in \mathbb{Z}$.

THÉORÈME 3. — *Soit $F \in \mathbb{Z}[X]$ un polynôme irréductible dans $\mathbb{Z}[X]$, alors il est irréductible dans $\mathbb{Q}[X]$.*

1) a) Soient $P \in \mathbb{Z}[X]$, $a \in \mathbb{Z}$ tel que $b = P(a) \neq 0$, $c \in \mathbb{N}$, $c \neq 0$. Montrer que $\frac{1}{b}P(a + bc)$ est un entier premier avec c.

b) Montrer que l'ensemble des nombres premiers p qui divisent $P(n)$ pour au moins une valeur de $n \in \mathbb{Z}$ est infini, si P est de degré $\geqslant 1$.

c) Soit F_1 et F_2 deux polynômes irréductibles distincts de $\mathbb{Z}[X]$. Montrer qu'il existe un entier N et deux polynômes G_1 et G_2 de $\mathbb{Z}[X]$ tels que

$$F_1G_1 + F_2G_2 = N.$$

2) a) Soit $V \in \mathbb{Z}[X]$. On suppose que l'on connaît Ω, $F_1, \ldots, F_k$, $e_1, \ldots, e_k$ décrits dans le théorème 2 ci-dessus tels que

$$V = \Omega F_1^{e_1} \ldots F_k^{e_k}.$$

Montrer qu'il existe $y_0 \in \mathbb{Z}$ et des entiers $d_1, d_2, \ldots, d_k$ tels que

(*i*) $$V(y_0) \neq 0$$

(ii) $d_i \geqslant 2$, d_i divise $F_i(y_0)$ et $\text{pgcd}(d_i, \Omega) = 1$ pour $1 \leqslant i \leqslant k$

(iii) $\text{pgcd}(d_i, F_j(y_0)) = 1$ pour $i \neq j$, $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant k$.

b) Ecrire un algorithme qui, à partir de V, Ω, $F_1, \ldots, F_k$ et y_0, retourne une variable booléenne B et des entiers $d_1, \ldots, d_k$. Si B est vraie, alors les conditions (i), (ii), et (iii) sont vérifiées. Si B n'est pas vrai, alors il n'existe pas d'entiers $d_1, \ldots, d_k$ vérifiant (i), (ii) et (iii).

Application numérique : $V(y) = y^3 + y^2$, $y_0 = 2$.

c) On suppose que l'on connaît $y_0, d_1, \ldots, d_k$ vérifiant (i), (ii) et (iii) ci-dessus, et que l'on a :

$$V = H_1 H_2 \ldots H_r$$

où $H_1, \ldots, H_r$ sont dans $\mathbb{Z}[X]$. Montrer que, si l'on connaît $\alpha_i = H_i(y_0)$ pour $1 \leqslant i \leqslant r$, on peut déterminer les polynômes $H_1, \ldots, H_r$.

Application numérique : $V(y) = y^3 + y^2$, $y_0 = 2$, $r = 2$, $\alpha_1 = 6$, $\alpha_2 = 2$.

3) a) Soit $U \in \mathbb{Z}[X, Y]$. On écrit

$$U(x, y) = V_n(y)x^n + V_{n-1}(y)x^{n-1} + \cdots + V_1(y)x + V_0(y)$$

où les $V_i \in \mathbb{Z}[Y]$, et $V_n(y) \neq 0$.

On suppose que les polynômes V_i, $0 \leqslant i \leqslant n$, sont premiers entre eux dans leur ensemble dans $\mathbb{Z}[Y]$, c'est-à-dire que si $D \in \mathbb{Z}[Y]$ divise simultanément $V_0, V_1, \ldots, V_n$, on a $D = \pm 1$.

Soit la matrice à coefficients dans $\mathbb{Z}[Y]$ que nous noterons $R = R(U, \frac{\partial U}{\partial x})$ par analogie avec I.5)b), à $2n-1$ lignes et $2n-1$ colonnes, et définie par :

$$1 \leqslant j \leqslant n-1, \qquad r_{i,j} = V_{n+j-i}(y)$$
$$n \leqslant j \leqslant 2n-1, \qquad r_{i,j} = (j-i+1)V_{j-i+1}(y).$$

Nous supposerons que le déterminant de R, qui est un polynôme en y, n'est pas le polynôme nul.

On pose $V = V_n$, et on suppose connue la factorisation de V :

$$V = \Omega F_1^{e_1} \dots F_k^{e_k}$$

comme précédemment. Montrer qu'il existe $y_0 \in \mathbb{Z}$ et $d_1, \dots, d_k \in \mathbb{Z}$ vérifiant (i), (ii) et (iii) du 2)b) et de plus :

(iv) $U(x, y_0)$ est sans facteurs carrés

(v) d_i est premier avec le contenu de $U(x, y_0)$, $1 \leqslant i \leqslant k$.

b) On suppose de plus que U s'écrit comme produit de deux polynômes inconnus A et $B \in \mathbb{Z}[X, Y]$.

$$A(x, y) = A_k(y)x^k + \dots + A_0(y)$$
$$B(x, y) = B_\ell(y)x^\ell + \dots + B_0(y)$$

et que l'on connaît y_0, $d_1, \dots, d_k$ vérifiant (i) – (v), et $A(x, y_0)$ et $B(x, y_0)$.

Montrer que les termes de plus haut degré en x de A et B, à savoir $A_k(y)$ et $B_\ell(y)$ peuvent être déterminés.

Montrer que l'on peut écrire

$$A(x, y) - A_k(y)x^k = S_0(x) + S_1(x)(y - y_0) + \dots + S_s(x)(y - y_0)^s$$
$$B(x, y) - B_\ell(y)x^\ell = T_0(x) + T_1(x)(y - y_0) + \dots + T_t(x)(y - y_0)^t$$

et que les polynômes $S_0, \dots, S_s, T_0, \dots, T_t$ peuvent être déterminés.

Application numérique :

$$U(x, y) = (y^3 + y^2)x^5 + (y^3 + y^2 - 2y)x^4 + (4y^2 - 2y - 3)x^3$$
$$+ (y^3 + 3y^2 + y - 14)x^2 + (y^3 - y^2 + 2y - 6)x + 2y^3 - y^2 - 13y + 15.$$

$y_0 = 2$, $A(x, y_0) = 2x^3 + x^2 + x + 1$; $B(x, y_0) = 6x^2 + x + 1$.

Calculer la valeur en y_0 de $\frac{\partial U}{\partial y}$ et $\frac{\partial^2 U}{\partial y^2}$ et déterminer $A(x, y)$ et $B(x, y)$.

c) Donner une méthode de décomposition en facteurs irréductibles d'un polynôme $U \in \mathbb{Z}[X, Y]$ et satisfaisant les hypothèses de 3)a).