

Composition de Mathématiques D – (U)

(Durée : 6 heures)

L'utilisation des calculatrices n'est pas autorisée pour cette épreuve.

Sujet saisi par Michel Quercia (michel.quercia@prepas.org) d'après l'original. Les parties en caractères penchés ont été ajoutées pour rectifier les erreurs de langage que comportait l'énoncé d'origine.

Notations et objectifs du sujet

Dans tout ce problème, I désigne un intervalle de \mathbb{R} de la forme $I = [a, b]$ avec $a < b$. On note $\mathcal{C}^0(I, \mathbb{R})$ l'espace vectoriel des fonctions continues $f : I \rightarrow \mathbb{R}$. On munit cet espace de la norme $\| \cdot \|_I$ définie par $\|f\|_I = \sup\{|f(x)|, x \in I\}$. Si A est une partie de $\mathcal{C}^0(I, \mathbb{R})$ et si $f \in \mathcal{C}^0(I, \mathbb{R})$, on dit que f est une limite uniforme d'éléments de A s'il existe une suite $(f_n)_{n \geq 1}$ d'éléments de A telle que $\|f - f_n\|_I \rightarrow 0$ quand $n \rightarrow +\infty$.

On note \mathbb{N} l'ensemble des entiers positifs (ou nuls). On note $\mathbb{R}[X]$ l'espace vectoriel des polynômes à coefficients réels et si $n \in \mathbb{N}$, on note $\mathbb{R}_n[X]$ le sous-espace des polynômes de degré au plus n . On dit qu'un polynôme $p \in \mathbb{R}[X]$ est unitaire si $p(X) = 1$ ou bien s'il existe un entier $n \geq 1$ et un polynôme $r \in \mathbb{R}_{n-1}[X]$ tels que $p(X) = X^n + r(X)$.

La restriction à I permet de voir $\mathbb{R}[X]$ comme un sous-espace vectoriel de $\mathcal{C}^0(I, \mathbb{R})$, ce que nous faisons. Nous munissons alors $\mathbb{R}_n[X]$ et $\mathbb{R}[X]$ de la norme $\| \cdot \|_I$. On rappelle le théorème de Weierstrass.

Théorème. Toute fonction $f \in \mathcal{C}^0(I, \mathbb{R})$ est limite uniforme d'éléments de $\mathbb{R}[X]$.

L'essentiel du problème (les parties 3 à 7) est inspiré par la question suivante : quelles fonctions continues sur I sont limites uniformes de polynômes à coefficients entiers ? Le problème comporte sept parties. Les résultats des questions 2.4 à 2.8 ne sont pas utilisés dans la suite. La partie 5 n'utilise pas les résultats des parties précédentes.

1. Existence et unicité d'une meilleure approximation

Soit $n \in \mathbb{N}$ et soit $f \in \mathcal{C}^0(I, \mathbb{R})$. On pose $m = \inf\{\|f - p\|_I, p \in \mathbb{R}_n[X]\}$.

- 1.1. Montrer que l'ensemble C des $g \in \mathbb{R}_n[X]$ tel que $\|f - g\|_I \leq 1 + m$ est un compact non vide de $\mathbb{R}_n[X]$.
- 1.2. Montrer qu'il existe un élément $p \in \mathbb{R}_n[X]$ tel que $\|f - p\|_I = m$. En déduire que si $m = 0$, on a alors $f \in \mathbb{R}_n[X]$.

On suppose dans la suite de cette partie que $m > 0$.

- 1.3. Soit k le nombre de solutions dans I de l'équation $|f(x) - p(x)| = m$; on suppose que $k \leq n + 1$ et on note ces solutions $x_1 < \dots < x_k$, avec $x_i \in I$. Montrer qu'il existe un polynôme $q \in \mathbb{R}_n[X]$ tel que $q(x_i) = f(x_i)$ pour tout $i \in \{1, \dots, k\}$.
- 1.4. Pour $\delta > 0$, on pose $U_\delta = \{x \in I \mid \exists i \in \{1, \dots, k\} \mid |x - x_i| < \delta\}$. Soit $\varepsilon > 0$. Montrer qu'il existe $\delta > 0$ tel que $|f(x) - q(x)| < \varepsilon$ pour tout $x \in U_\delta$.
- 1.5. Soit $\ell = \|p - q\|_I$ et soit $\varepsilon > 0$, à ajuster ensuite. Soit δ comme à la question 1.4. Pour $t \in]0, 1[$, on pose $p_t = (1 - t)p + tq$. Montrer que pour tout $x \in I$, on a

$$|f(x) - p_t(x)| \leq \begin{cases} (1 - t)m + t\varepsilon & \text{si } x \in U_\delta ; \\ t\ell + \sup\{|f(y) - p(y)|, y \in I \setminus U_\delta\} & \text{si } x \in I \setminus U_\delta. \end{cases}$$

- 1.6. Montrer que pour un choix convenable de $\varepsilon > 0$, il existe $t \in]0, 1[$ tel que $\|f - p_t\|_I < m$. En déduire que l'équation $|f(x) - p(x)| = m$ admet au moins $n + 2$ solutions distinctes dans I .
- 1.7. On suppose qu'il existe $p_1, p_2 \in \mathbb{R}_n[X]$ tels que $\|f - p_1\|_I = \|f - p_2\|_I = m$. Montrer que $p_1 = p_2$ (on pourra appliquer la question 1.6 à $(p_1 + p_2)/2$).

2. Capacité d'un compact

Soit K une partie compacte de \mathbb{R} . Si $f \in \mathcal{C}^0(K, \mathbb{R})$, on pose $\|f\|_K = \sup\{|f(x)|, x \in K\}$. On suppose que K est un ensemble infini.

- 2.1. Montrer que si $n \geq 1$ est un entier, il existe un polynôme $q \in \mathbb{R}[X]$, unitaire de degré n , tel que $\|q\|_K = \inf_p \{\|p\|_K\}$ où p parcourt l'ensemble des polynômes unitaires de degré n à coefficients dans \mathbb{R} . On pose $t_n = \|q\|_K = \inf_p \{\|p\|_K\}$. Montrer que si $a < b$ et $K = [a, b]$, un tel polynôme q est unique. On le note T_n^K .
- 2.2. Soit $(\ell_n)_{n \geq 1}$ une suite de réels telle que pour tous $m, n \geq 1$, on a $\ell_{m+n} \leq \frac{n}{m+n} \ell_n + \frac{m}{m+n} \ell_m$. Soit $\ell = \inf\{\ell_n, n \geq 1\} \in \{-\infty\} \cup \mathbb{R}$. Montrer que $\ell_n \rightarrow \ell$ quand $n \rightarrow +\infty$.
- 2.3. Montrer que la suite $(t_n^{1/n})_{n \geq 1}$ admet une limite, notée $d_1(K)$.
- 2.4. On pose $w_1 = 1$ et, pour tout $n \geq 2$, on pose $w_n = \sup\{\prod_{1 \leq i < j \leq n} |x_i - x_j|, x_1, \dots, x_n \in K\}$. Montrer que la suite $(w_n^{2/(n(n-1))})_{n \geq 2}$ est décroissante. En déduire qu'elle converge ; on notera $d_2(K)$ sa limite.
- 2.5. Montrer que pour tout entier $n \geq 1$, on a $t_n \leq w_{n+1}/w_n$. On pourra montrer qu'il existe $x_1, \dots, x_n \in K$ tels que $w_n = \prod_{1 \leq i < j \leq n} |x_i - x_j|$, puis considérer $p(X) = (X - x_1) \dots (X - x_n)$ et choisir judicieusement $x_{n+1} \in K$.
- 2.6. Montrer qu'il existe $x_1, \dots, x_{n+1} \in K$ tels que pour tout polynôme unitaire $p \in \mathbb{R}[X]$ de degré n , on a

$$w_{n+1} = \left| \det \begin{pmatrix} 1 & \cdots & x_1^{n-1} & p(x_1) \\ \vdots & \ddots & \vdots & \vdots \\ 1 & \cdots & x_{n+1}^{n-1} & p(x_{n+1}) \end{pmatrix} \right|.$$

En déduire que $w_{n+1} \leq (n+1)w_n t_n$.

- 2.7. Soit $(u_n)_{n \geq 1}$ une suite de réels qui converge vers une limite u . Pour $n \geq 1$, on pose $z_n = (u_1 + \dots + u_n)/n$. Montrer que $z_n \rightarrow u$ quand $n \rightarrow +\infty$.
- 2.8. Montrer que $d_1(K) = d_2(K)$.

Remarque. Cette limite commune est appelée la *capacité* de K .

3. Polynômes de Tchebychev

Dans toute cette partie, n est un entier strictement positif.

- 3.1. Montrer qu'il existe un et un seul polynôme T_n tel que $T_n(\cos \theta) = \cos(n\theta)$ pour tout $\theta \in \mathbb{R}$. Quel est son degré ?
- 3.2. Montrer que $2^{1-n} T_n$ est un polynôme unitaire qui admet $n+1$ *extremums* dans l'intervalle $[-1, 1]$.
- 3.3. Soit $I = [-1, 1]$, soit f la fonction définie par $f(x) = x^n$ et soit q un élément de $\mathbb{R}_{n-1}[X]$ tel que $\|f - q\|_I = \inf\{\|f - p\|_I, p \in \mathbb{R}_{n-1}[X]\}$ (cf. la question 1.2). On suppose que $\|f - q\|_I < 2^{1-n}$. Montrer que le polynôme $2^{1-n} T_n - (f - q)$ a au moins n racines distinctes dans I . En déduire que si $I = [-1, 1]$, alors $T_n^I = 2^{1-n} T_n$ (le polynôme T_n^I est défini à la question 2.1).
- 3.4. Calculer $T_n^{[a,b]}$ et en déduire que $\|T_n^{[a,b]}\|_{[a,b]} = 2\left(\frac{b-a}{4}\right)^n$ puis que $d_1([a, b]) = \frac{b-a}{4}$ (où d_1 est défini à la question 2.3).
- 3.5. Montrer que si $I = [a, b]$ avec $b - a \geq 4$, et si p est un polynôme non constant à coefficients entiers, alors $\|p\|_I \geq 2$.
- 3.6. En déduire que si $b - a \geq 4$, une fonction $f \in \mathcal{C}^0([a, b], \mathbb{R})$ est une limite uniforme de polynômes à coefficients entiers si et seulement si f est elle-même un polynôme à coefficients entiers.

4. L'approximation par des polynômes à coefficients entiers

On suppose dans le reste du problème que $I = [a, b]$ avec $b - a < 4$.

- 4.1. Montrer qu'il existe un polynôme unitaire non constant $p \in \mathbb{R}[X]$ tel que $\|p\|_I < 1$.
- 4.2. Soit $r \in \mathbb{R}[X]$ un polynôme de degré $d \geq 1$. Montrer que si $s \in \mathbb{R}[X]$, il existe $n \geq 0$ et $b_0, \dots, b_n \in \mathbb{R}_{d-1}[X]$ tels que $s(X) = b_0(X) + b_1(X)r(X) + \dots + b_n(X)r(X)^n$.
- 4.3. Soit d le degré du polynôme p construit à la question 4.1 et soient $\ell_0 \geq 1$ et $k \geq \ell_0$ des entiers ; on pose $m = \ell_0 d$. Montrer qu'il existe des réels $b_{i,\ell,k} \in [0, 1]$ pour $0 \leq i \leq d - 1$ et pour $\ell \geq \ell_0$, tels que l'on puisse écrire $p(X)^k = r_k(X) + z_k(X) + p_k(X)$, où

$$r_k(X) = \sum_{\substack{0 \leq i \leq d-1 \\ \ell \geq \ell_0}} b_{i,\ell,k} X^i p(X)^\ell,$$

où z_k est un polynôme unitaire de degré kd à coefficients entiers et où p_k est un polynôme de degré au plus $m - 1$ et à coefficients dans $[0, 1]$.

- 4.4. Choisir soigneusement ℓ_0 et montrer qu'il existe alors deux entiers $k' > k$ tels que $q = z_{k'} - z_k$ est un polynôme unitaire non constant à coefficients entiers vérifiant $\|q\|_I < 1$.

Définition. Soit $J(I)$ l'ensemble des $x \in I$ tels que $p(x) = 0$ pour tout polynôme p à coefficients entiers vérifiant $\|p\|_I < 1$. Par la question 4.4, l'ensemble $J(I)$ est fini.

- 4.5. Déterminer $J(I)$ lorsque $I = [a, b]$ avec $-1 < a < b < 1$, puis lorsque $I = [-1, 1]$.
- 4.6. Soit $f \in C^0(I, \mathbb{R})$ une fonction qui est une limite uniforme de polynômes à coefficients entiers. Montrer qu'il existe un polynôme p à coefficients entiers tel que $f(x) = p(x)$ pour tout $x \in J(I)$.
- 4.7. Montrer qu'il existe un polynôme unitaire q à coefficients entiers tel que $\|q\|_I < 1$ et que, si $x \in I$ vérifie $q(x) = 0$, alors $x \in J(I)$.

Notation. Dans le reste de cette partie, q désigne un tel polynôme et n son degré.

- 4.8. Montrer qu'il existe une constante $M > 0$ telle que pour tout $p \in \mathbb{R}[X]$, il existe $\tilde{p} \in \mathbb{Z}[X]$ vérifiant $\|p - \tilde{p}\|_I \leq M$. On pourra utiliser la question 4.2.
- 4.9. Soit $f \in C^0(I, \mathbb{R})$ une fonction telle que pour tout $x \in I$ vérifiant $q(x) = 0$, il existe $\delta > 0$ tel que $f(y) = 0$ pour tout $y \in I$ vérifiant $|x - y| < \delta$. Soit $\varepsilon > 0$. En appliquant le théorème de Weierstrass (rappelé dans l'introduction) à f/q^k pour k grand, montrer qu'il existe un polynôme p à coefficients entiers tel que $\|f - p\|_I < \varepsilon$.
- 4.10. Soit $f \in C^0(I, \mathbb{R})$ une fonction telle que pour tout $x \in I$ vérifiant $q(x) = 0$, on a $f(x) = 0$. Montrer que f est une limite uniforme de polynômes à coefficients entiers.
- 4.11. Montrer qu'une fonction $f \in C^0(I, \mathbb{R})$ est une limite uniforme de polynômes à coefficients entiers si et seulement s'il existe un polynôme p à coefficients entiers tel que $f(x) = p(x)$ pour tout $x \in J(I)$.
- 4.12. Montrer qu'une fonction $f \in C^0([-1, 1], \mathbb{R})$ est une limite uniforme de polynômes à coefficients entiers si et seulement si $f(-1) \in \mathbb{Z}$, $f(0) \in \mathbb{Z}$, $f(1) \in \mathbb{Z}$ et $f(-1)$ et $f(1)$ sont de même parité.

5. Polynômes symétriques

Définitions. Soit $n \geq 1$. On considère des polynômes en les n variables T_1, \dots, T_n à coefficients dans \mathbb{Z} , c'est-à-dire

$$p(T_1, \dots, T_n) = \sum_{i_1, \dots, i_n \geq 0} a_{i_1, \dots, i_n} T_1^{i_1} \dots T_n^{i_n}$$

avec $a_{i_1, \dots, i_n} \in \mathbb{Z}$, la somme étant presque nulle. L'ensemble de ces polynômes est noté $\mathbb{Z}[T_1, \dots, T_n]$ et forme un anneau. Un monôme est un polynôme de la forme $a_{i_1, \dots, i_n} T_1^{i_1} \dots T_n^{i_n}$ avec $a_{i_1, \dots, i_n} \neq 0$. Son degré est le n -uplet $\underline{i} = (i_1, \dots, i_n) \in \mathbb{N}^n$. Nous dirons qu'un n -uplet $\underline{i} \in \mathbb{N}^n$ est *plus petit* qu'un n -uplet $\underline{j} \in \mathbb{N}^n$ si $\sum_k i_k < \sum_k j_k$ ou bien si $\sum_k i_k = \sum_k j_k$ et il existe k tel que $i_1 = j_1, \dots, i_{k-1} = j_{k-1}$ et $i_k < j_k$.

- 5.1. Montrer que si $\underline{i} \in \mathbb{N}^n$ et $\underline{j} \in \mathbb{N}^n$ sont des n -uplets avec $\underline{i} \neq \underline{j}$, alors soit \underline{i} est plus petit que \underline{j} , soit \underline{j} est plus petit que \underline{i} .

5.2. Montrer que si l'on se donne un n -uplet $\underline{i} \in \mathbb{N}^n$, l'ensemble des n -uplets $\underline{j} \in \mathbb{N}^n$ qui sont plus petits que \underline{i} est fini.

Définitions. Si $p(T_1, \dots, T_n) = \sum_{i_1, \dots, i_n \geq 0} a_{i_1, \dots, i_n} T_1^{i_1} \dots T_n^{i_n}$ est un polynôme non nul, on note $\text{dom}(p)$ le coefficient a_{i_1, \dots, i_n} du monôme $a_{i_1, \dots, i_n} T_1^{i_1} \dots T_n^{i_n}$, où (i_1, \dots, i_n) est le plus grand des degrés pour lesquels $a_{i_1, \dots, i_n} \neq 0$. Le degré (i_1, \dots, i_n) correspondant est le *degré* de p , noté $\text{deg}(p)$.

Si π est une permutation de l'ensemble $\{1, \dots, n\}$ et si $p \in \mathbb{Z}[T_1, \dots, T_n]$, on note p^π le polynôme $P(T_{\pi(1)}, \dots, T_{\pi(n)})$. On dit que p est un *polynôme symétrique* si $p^\pi = p$ pour toute permutation π . Les éléments S_1, \dots, S_n de $\mathbb{Z}[T_1, \dots, T_n]$ sont définis par la formule

$$\prod_{i=1}^n (X - T_i) = X^n - S_1 X^{n-1} + \dots + (-1)^{n-1} S_{n-1} X + (-1)^n S_n.$$

Ce sont donc des polynômes symétriques. On a $S_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} T_{i_1} \dots T_{i_k}$.

5.3. Soit $p \in \mathbb{Z}[T_1, \dots, T_n]$ un polynôme symétrique non nul et soit (i_1, \dots, i_n) le degré de p . Montrer que $i_1 \geq i_2 \geq \dots \geq i_n$.

5.4. Soit p un polynôme comme dans la question précédente. On pose

$$d_1 = i_1 - i_2, \quad d_2 = i_2 - i_3, \quad \dots, \quad d_{n-1} = i_{n-1} - i_n, \quad d_n = i_n.$$

Montrer que

- ou bien $p = \text{dom}(p) S_1^{d_1} \dots S_n^{d_n}$;
- ou bien $\text{deg}(p - \text{dom}(p) S_1^{d_1} \dots S_n^{d_n})$ est plus petit que $\text{deg}(p)$.

5.5. Montrer que si $p \in \mathbb{Z}[T_1, \dots, T_n]$ est un polynôme symétrique, il existe un polynôme $q \in \mathbb{Z}[T_1, \dots, T_n]$ tel que $p = q(S_1, \dots, S_n)$.

6. Entiers algébriques

Définition. On dit qu'un nombre complexe x est un *entier algébrique* s'il existe un polynôme unitaire (non nul) à coefficients entiers $p \in \mathbb{Z}[X]$ tel que $p(x) = 0$.

6.1. Montrer que si $x \in \mathbb{Q}$ alors x est un entier algébrique si et seulement si $x \in \mathbb{Z}$.

6.2. Si $a(X) = a_0 + a_1 X + \dots + a_n X^n \in \mathbb{Z}[X]$, on note $c(a)$ le pgcd de a_0, \dots, a_n . Montrer que si $a, b \in \mathbb{Z}[X]$, on a alors $c(ab) = c(a)c(b)$. On pourra montrer que si un nombre premier divise $c(ab)$ alors il divise $c(a)$ ou $c(b)$.

6.3. Montrer que si x est un entier algébrique, il existe un et un seul polynôme $p_x \in \mathbb{Z}[X]$ unitaire tel que $p_x(x) = 0$ et tel que p_x est irréductible dans $\mathbb{Q}[X]$. Montrer que p_x est à racines simples dans \mathbb{C} .

Définition. Dans les notations de 6.3, les racines x_1, \dots, x_n de p_x dans \mathbb{C} (y compris x lui-même) sont appelées les conjugués de x . On a alors $p_x(X) = (X - x_1) \dots (X - x_n)$.

6.4. Dans les notations ci-dessus, soit r un élément de $\mathbb{Q}[X]$ tel qu'il existe i vérifiant $r(x_i) = 0$. Montrer que p_x divise r dans $\mathbb{Q}[X]$.

6.5. Soient x et y des entiers algébriques et soient y_1, \dots, y_m les conjugués de y . Montrer (par exemple en utilisant la question 5.5) que les coefficients du polynôme $p_x(X - y_1) \dots p_x(X - y_m)$ sont dans \mathbb{Z} . En déduire que $x + y$ est un entier algébrique.

6.6. Montrer que si x et y sont des entiers algébriques, alors xy est un entier algébrique.

Définition. Soit $I = [a, b]$ et soit $F(I)$ l'ensemble des $x \in I$ qui sont des entiers algébriques dont tous les conjugués appartiennent aussi à I . Cet ensemble est appelé le noyau de Fekete de I .

6.7. Soit q un polynôme à coefficients entiers tel que $\|q\|_I < 1$, soit x un élément de $F(I)$ et soient x_1, x_2, \dots, x_n ses conjugués. Montrer que $\prod_{i=1}^n q(x_i)$ est un élément de \mathbb{Z} , puis que $q(x) = 0$. En déduire $F(I) \subset J(I)$.

6.8. En considérant par exemple le polynôme $X(X^2 - 1)(X^2 - 2)$, calculer $J(I)$ pour tout intervalle $I = [-a, a]$ avec $a \leq \frac{3}{2}$.

7. Le noyau de Fekete

Le but de cette partie est de montrer que pour tout intervalle $I = [a, b]$ de longueur $b - a < 4$, on a en fait $F(I) = J(I)$.

Définition. Un pavé est une partie P de \mathbb{R}^n de la forme

$$P = \{\lambda_1 v_1 + \dots + \lambda_n v_n, \lambda_1, \dots, \lambda_n \in [-1, 1]\},$$

où $v_1, \dots, v_n \in \mathbb{R}^n$. Le volume de P est alors $\text{vol}(P) = 2^n |\det(V)|$, où V est la matrice de v_1, \dots, v_n dans la base canonique de \mathbb{R}^n . Pour $h \in \mathbb{R}^n$ on note $h + P = \{h + v, v \in P\}$. Soit \mathbb{Z}^n l'ensemble des vecteurs de \mathbb{R}^n dont toutes les coordonnées sont entières.

- 7.1.** Montrer que si P est un pavé tel que $\text{vol}(P) > 1$, il existe $w \neq w'$ dans P tels que $w - w' \in \mathbb{Z}^n$. On pourra observer que dans le cas contraire, $h + P$ et $h' + P$ sont disjoints pour tous $h \neq h'$ dans \mathbb{Z}^n .
- 7.2.** Soit $x \in \mathbb{R}$ un entier algébrique et soient $x_1 = x, x_2, \dots, x_m$ ses conjugués. On suppose que $m \geq 2$ et qu'il existe $n \in \{2, \dots, m\}$ tel que $x_1, \dots, x_{n-1} \in \mathbb{R}$. On considère la matrice

$$M = \begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \dots & x_{n-1}^{n-1} \\ 1 & 1 & 1 & \dots & 1 \end{pmatrix}$$

et on note $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ l'application linéaire correspondante. Si $r > 0$, on note $B(r)$ l'ensemble des $a \in \mathbb{R}^n$ tels que $|a_n| \leq r$ et que $|a_i| \leq \frac{1}{2}$ pour tout $i \in \{1, \dots, n-1\}$. Montrer que si r est assez grand, il existe $h \in \mathbb{Z}^n \setminus \{0\}$ tel que $h \in f^{-1}(B(r))$.

- 7.3.** Soit $h \in \mathbb{Z}^n \setminus \{0\}$ comme à la question précédente. On pose $s(X) = h_1 + h_2 X + \dots + h_n X^{n-1}$, où h_1, \dots, h_n sont les coordonnées de h . Montrer que pour tout $i \in \{1, \dots, n-1\}$, on a $|s(x_i)| \leq \frac{1}{2}$ et $s(x_i) \neq 0$.
- 7.4.** On conserve les notations de la question 7.2. Soit $\varepsilon > 0$. Montrer que si $y_1, \dots, y_{n-1} \in \mathbb{R}$, il existe $p \in \mathbb{Z}[X]$ tel que $|p(x_i) - y_i| < \varepsilon$ pour tout $i \in \{1, \dots, n-1\}$ (on pourra s'inspirer des questions 4.8 et 4.9).
- 7.5.** Soit à présent $S = \{x_1, \dots, x_n\}$ un ensemble de réels deux à deux distincts tel que, pour tout $1 \leq i \leq n$, le réel x_i est un entier algébrique qui admet au moins un conjugué qui n'est pas dans S . Montrer que si $y_1, \dots, y_n \in \mathbb{R}$, il existe $p \in \mathbb{Z}[X]$ tel que $|p(x_i) - y_i| < \varepsilon$ pour tout $i \in \{1, \dots, n\}$.
- 7.6.** Soit $I = [a, b]$ avec $b - a < 4$ et soit q un polynôme unitaire à coefficients entiers tel que $\|q\|_I < 1$. En écrivant l'ensemble des racines de q dans I comme union disjointe $F(I) \cup S$, montrer qu'une fonction $f \in C^0(I, \mathbb{R})$ telle que $f(x) = 0$ pour tout $x \in F(I)$ est une limite uniforme de polynômes à coefficients entiers.
- 7.7.** Montrer que $F(I) = J(I)$.

Fin du problème

Corrigé

1. Existence et unicité d'une meilleure approximation

- 1.1. C est l'intersection de la boule fermée de centre f , rayon $1 + m$ et du sous-espace $\mathbb{R}_n[X]$ qui est lui aussi fermé car de dimension finie. Ainsi C est fermé et borné dans un espace de dimension finie ; il est compact. Si l'on avait $C = \emptyset$ alors on aurait $\|f - g\|_I > 1 + m$ pour tout $g \in \mathbb{R}_n[X]$, en contradiction avec la définition de m .
- 1.2. L'application $g \mapsto \|f - g\|_I$ est continue sur C donc elle admet un minimum atteint en $p \in C$. Pour $g \in \mathbb{R}_n[X]$, on a $\|f - g\|_I \geq \|f - p\|_I$ si $g \in C$ et $\|f - g\|_I \geq 1 + m \geq \|f - p\|_I$ si $g \notin C$. Ainsi, $\|f - p\|_I$ est le minimum de $\|f - g\|_I$ sur $\mathbb{R}_n[X]$, soit : $\|f - p\|_I = m$. Le cas $m = 0$ est immédiat.
- 1.3. On remarque déjà que $k \geq 1$ car la fonction continue $|f - p|$ admet un maximum sur le compact $[a, b]$. L'existence de q est une conséquence du théorème d'interpolation de Lagrange.
- 1.4. Par continuité de $f - q$ en x_i , il existe $\delta_i > 0$ tel que $|f(x) - q(x)| < \varepsilon$ pour tout $x \in]x_i - \delta_i, x_i + \delta_i[\cap I$. $\delta = \min\{\delta_1, \dots, \delta_k\}$ convient alors.
- 1.5. Pour $x \in U_\delta$ on a $|f(x) - p_t(x)| = |(1-t)(f(x) - p(x)) + t(f(x) - q(x))| \leq (1-t)m + t\varepsilon$. Pour $x \in I \setminus U_\delta$ on a $|f(x) - p_t(x)| = |(f(x) - p(x)) + t(p(x) - q(x))| \leq \sup_{I \setminus U_\delta} |f - p| + t\ell$.
- 1.6. Il s'agit de choisir ε et t de sorte que les deux majorants obtenus à la question précédente soient strictement inférieurs à m .

On impose $0 < \varepsilon < m$. Ainsi, pour tout $t \in]0, 1[$, on a $(1-t)m + t\varepsilon < m$.

$I \setminus U_\delta$ est compact car fermé dans I compact. S'il est non vide, alors $|f - p|$ admet un maximum m' sur ce compact et $m' < m$ car la valeur m ne peut être atteinte par construction de U_δ . Alors, pour t suffisamment proche de 0^+ on a $t\ell + m' < m$. Lorsque $I \setminus U_\delta = \emptyset$, le deuxième majorant n'a pas lieu d'être considéré.

En conclusion, l'existence de q , et donc le fait que $k \leq n + 1$ ont permis de trouver un polynôme $p_t \in \mathbb{R}_n[X]$ strictement plus proche de f que ne l'est p , en contradiction avec la définition de p . Par négation d'une conclusion absurde, il vient $k \geq n + 2$ (éventuellement $k = \infty$).

- 1.7. $p_3 = (p_1 + p_2)/2 \in \mathbb{R}_n[X]$ et $\|f - p_3\|_I \leq \frac{1}{2}(\|f - p_1\|_I + \|f - p_2\|_I) = m$. Ainsi $\|f - p_3\|_I = m$ et il existe au moins $n + 2$ points x_1, \dots, x_{n+2} distincts pour lesquels $|f(x_i) - p_3(x_i)| = m$. On a aussi $|f(x_i) - p_3(x_i)| \leq \frac{1}{2}(|f(x_i) - p_1(x_i)| + |f(x_i) - p_2(x_i)|) \leq m$, d'où $|f(x_i) - p_1(x_i)| = |f(x_i) - p_2(x_i)| = m$ et de plus $f(x_i) - p_1(x_i)$ et $f(x_i) - p_2(x_i)$ ont même signe (sans quoi $f(x_i) - p_3(x_i) = 0$). Il vient $f(x_i) - p_1(x_i) = f(x_i) - p_2(x_i)$ puis $p_1(x_i) = p_2(x_i)$. Par conséquent $p_1 - p_2 \in \mathbb{R}_n[X]$ a au moins $n + 2$ racines distinctes ; c'est le polynôme nul.

2. Capacité d'un compact

- 2.1. Remarquons déjà que l'hypothèse « K est infini» implique que $\|\cdot\|_K$ est une norme sur $\mathbb{R}[X]$. En écrivant $p = X^n + r$ avec $\deg(r) < n$, on voit qu'il s'agit de trouver un polynôme $r \in \mathbb{R}_{n-1}[X]$ de meilleure approximation pour la fonction définie par $f(x) = -x^n$. Un tel polynôme existe et est unique d'après la première partie où l'on n'a pas fait usage de l'hypothèse supplémentaire « I est un intervalle», et où l'on a bien $m > 0$ car $f \notin \mathbb{R}_{n-1}[X]$.
- 2.2. Cas $\ell \in \mathbb{R}$: soit $\varepsilon > 0$ et $m \geq 1$ tel que $\ell_m \leq \ell + \varepsilon$. Pour $n \geq 1$, on écrit la division euclidienne de n par m : $n = qm + r$ et n choisit une valeur arbitraire pour ℓ_0 de façon à simplifier le raisonnement qui suit. Partant de l'inégalité $(x + m)\ell_{x+m} \leq x\ell_x + m\ell_m$, on obtient de proche en proche : $(r + qm)\ell_{r+qm} \leq r\ell_r + qm\ell_m$, soit $n\ell_n \leq r\ell_r + (n - r)\ell_m \leq M + n(\ell + \varepsilon)$ où $M = \max\{x(\ell_x - \ell_m), 0 \leq x < m\}$ (quantité indépendante de n). Ainsi, pour tout entier $n \geq 1$, on a $\ell_n \leq \frac{M}{n} + \ell + \varepsilon$ et ce majorant est inférieur ou égal à $\ell + 2\varepsilon$ si n est suffisamment grand. Il est ainsi prouvé que $\ell_n \rightarrow \ell$ quand $n \rightarrow +\infty$. Le cas $\ell = -\infty$ se traite par adaptation immédiate.
- 2.3. Posons $\ell_n = \ln(t_n)/n$ (quantité bien définie car $t_n > 0$ en tant que minimum). Le polynôme $p = T_m^K T_n^K$ est unitaire de degré $m+n$, donc $t_{m+n} \leq \|p\|_K \leq \|T_m^K\|_K \|T_n^K\|_K \leq t_m t_n$, d'où $(m+n)\ell_{m+n} \leq m\ell_m + n\ell_n$. Avec la question précédente, la suite (ℓ_n) converge ou diverge vers $-\infty$, donc la suite $(t_n^{1/n}) = (\exp(\ell_n))$ converge vers une limite finie, positive ou nulle.

- 2.4. Le nombre w_n est bien défini car K est borné non vide. Pour $x_1, \dots, x_{n+1} \in K$ et $p \in \{1, \dots, n+1\}$ on a $\prod_{1 \leq i < j \leq n+1, i, j \neq p} |x_i - x_j| \leq w_n$. En multipliant ces inégalités pour $p = 1, \dots, p = n+1$ il vient $\prod_{1 \leq i < j \leq n+1} |x_i - x_j|^{n-1} \leq w_n^{n+1}$ (l'exposant $n-1$ vient du fait qu'un même couple (i, j) apparaît dans tous les produits où $p \neq i$ et $p \neq j$ et seulement dans ceux-là). En prenant la borne supérieure sur x_1, \dots, x_{n+1} , on obtient $w_{n+1}^{n-1} \leq w_n^{n+1}$, ce qui donne la décroissance de la suite de terme général $w_n^{2/(n(n-1))}$. Étant minorée par 0, elle converge.
- 2.5. La borne supérieure définissant w_n est atteinte par compacité de K . Le polynôme p donné dans l'énoncé est un polynôme unitaire de degré n donc $\|p\|_K \geq t_n$. En prenant pour x_{n+1} un point de K où $|p|$ atteint son maximum, on obtient $w_{n+1} \geq \prod_{1 \leq i < j \leq n+1} |x_i - x_j| \geq w_n t_n$.
- 2.6. Le déterminant proposé est inchangé si l'on ajoute à p un polynôme r quelconque de degré au plus $n-1$ car la colonne $(r(x_1) \dots r(x_{n+1}))$ est combinaison linéaire des premières colonnes. Il suffit donc de choisir x_1, \dots, x_{n+1} de sorte que l'égalité soit valide dans le cas particulier $p(X) = X^n$. Or dans ce cas, on reconnaît le déterminant de Vandermonde, égal à $\prod_{1 \leq i < j \leq n+1} (x_j - x_i)$. On obtient l'égalité en valeur absolue en choisissant $x_1, \dots, x_{n+1} \in K$ tels que $\prod_{1 \leq i < j \leq n+1} |x_i - x_j| = w_{n+1}$, ce qui est possible par compacité de K .
- En développant le déterminant selon la dernière colonne, on obtient une combinaison linéaire des valeurs $p(x_1), \dots, p(x_{n+1})$ dont les coefficients sont au signe près des déterminants de Vandermonde associés à un arrangement de n termes parmi x_1, \dots, x_{n+1} . Chacun de ces déterminants est majoré en valeur absolue par w_n , tandis que $|p(x_i)| \leq \|p\|_K$. En conséquence, $w_{n+1} \leq (n+1)w_n \|p\|_K$. En choisissant alors $p = T_n^K$, on a $\|p\|_K = t_n$, d'où $w_{n+1} \leq (n+1)w_n t_n$.
- 2.7. C'est le lemme de Césaro, valide aussi bien si la limite u est finie ou infinie.
- 2.8. D'après les questions 2.5 et 2.6, on a par itération : $x_n = t_1 \dots t_{n-1} \leq w_n \leq n! x_n$.

Avec la formule de Stirling, $\ln(n!) \sim n \ln(n)$, donc $(n!)^{2/(n(n-1))} \rightarrow 1$ quand n tend vers l'infini. Ainsi les suites de termes généraux $w_n^{2/(n(n-1))}$ et $x_n^{2/(n(n-1))}$ ont même limite, $d_2(K)$.

Dans le cas $d_1(K) \neq 0$, on a $\frac{1}{n} \ln(t_n) = \ln(d_1(K)) + o(1)$, soit $\ln(t_n) - n \ln(d_1(K)) = o(n)$. Comme la série de terme général n est à termes réels positifs et diverge, par sommation de cette relation de comparaison il vient $\ln(t_1) + \dots + \ln(t_{n-1}) - (1 + \dots + (n-1)) \ln(d_1(K)) = o(1 + \dots + (n-1))$. Soit $\ln(x_n) = \frac{n(n-1)}{2} \ln(d_1(K)) + o(\frac{n(n-1)}{2})$ et ainsi $x_n^{2/(n(n-1))} \rightarrow d_1(K)$ quand $n \rightarrow +\infty$ puis $d_2(K) = d_1(K)$.

Dans le cas $d_2(K) = 0$, on a de même $1 = o(\frac{1}{n} \ln(t_n))$, soit $n = o(-\ln(t_n))$. Puisque $t_n^{1/n} \rightarrow 0$, on a $-\ln(t_n) \geq 0$ pour n assez grand et on peut encore appliquer le principe de sommation des relations de comparaison. La série de terme général $-\ln(t_n)$ est nécessairement divergente (sans quoi la série de terme général n serait convergente), d'où $\frac{n(n-1)}{2} = o(-\ln(x_n))$ puis $1 = o(-\ln(x_n^{2/(n(n-1))}))$ et enfin $x_n^{2/(n(n-1))} \rightarrow 0$ quand $n \rightarrow +\infty$. Dans ce cas encore, $d_2(K) = d_1(K)$.

Autre solution, proposée par Denis Choimet.

On déduit des questions 2.5 et 2.6 l'encadrement $t_n^{1/n} \leq (w_{n+1}/w_n)^{1/n} \leq (n+1)^{1/n} t_n^{1/n}$, ce qui montre que $(w_{n+1}/w_n)^{1/n} \xrightarrow[n \rightarrow \infty]{} d_1(K)$, et donc $\frac{\ln(w_{n+1}) - \ln(w_n)}{n} \xrightarrow[n \rightarrow \infty]{} \ln(d_1(K))$ avec par convention $\ln(0) = -\infty$. Appliquons le lemme de Césaro :

$$\sum_{k=1}^n \frac{\ln(w_{k+1}) - \ln(w_k)}{nk} \xrightarrow[n \rightarrow \infty]{} \ln(d_1(K)).$$

Par ailleurs,

$$\begin{aligned} \sum_{k=1}^n \frac{\ln(w_{k+1}) - \ln(w_k)}{nk} &= \sum_{k=1}^n \frac{\ln(w_{k+1})}{nk} - \sum_{k=1}^n \frac{\ln(w_k)}{nk} \\ &= \sum_{k=2}^{n+1} \frac{\ln(w_k)}{n(k-1)} - \sum_{k=1}^n \frac{\ln(w_k)}{nk} \\ &= \sum_{k=2}^n \frac{\ln(w_k)}{nk(k-1)} + \frac{\ln(w_{n+1})}{n^2} - \frac{\ln(w_1)}{n}. \end{aligned}$$

Ayant $\frac{\ln(w_n)}{n(n-1)} \xrightarrow{n \rightarrow \infty} \frac{1}{2} \ln(d_2(K))$, avec une nouvelle application du lemme de Césaro, on obtient

$$\sum_{k=2}^n \frac{\ln(w_k)}{nk(k-1)} + \frac{\ln(w_{n+1})}{n^2} - \frac{\ln(w_1)}{n} \xrightarrow{n \rightarrow \infty} \frac{1}{2} \ln(d_2(K)) + \frac{1}{2} \ln(d_2(K)) - 0 = \ln(d_2(K)).$$

Ainsi, $\ln(d_1(K)) = \ln(d_2(K))$.

3. Polynômes de Tchebychev

- 3.1. Question classique. On trouve $\deg(T_n) = n$.
- 3.2. Question classique. les valeurs extrêmes $\pm 2^{1-n}$ sont atteintes aux nœuds de Tchebychev : $\cos(k\frac{\pi}{n})$, $0 \leq k \leq n$.
- 3.3. Notons $x_k = \cos(k\frac{\pi}{n})$. Puisque $\|f - q\|_I < 2^{1-n} = |2^{1-n}T_n(x_k)|$, le polynôme $r = 2^{1-n}T_n - (f - q)$ prend en x_k une valeur non nulle du signe de $T_n(x_k)$, soit $(-1)^k$. La suite (x_0, \dots, x_n) est strictement décroissante dans I et délimite n intervalles aux bornes desquels r prend des valeurs de signes opposés. Ainsi r admet au moins une racine dans chaque intervalle ouvert délimité par deux x_k successifs, soit au moins n racines distinctes dans I .

Mais $\deg(r) < n$ puisque les termes de degré n se compensent entre $2^{1-n}T_n$ et f . En conséquence, $r = 0$ et $f - q = 2^{1-n}T_n$, ce qui est contraire à l'hypothèse « $\|f - q\|_I < 2^{1-n}$ ».

Ainsi, $\|f - q\|_I \geq 2^{1-n}$ et comme $f - 2^{1-n}T_n \in \mathbb{R}_{n-1}[X]$ vérifie $\|f - (f - 2^{1-n}T_n)\|_I = 2^{1-n}$, par unicité, $T_n^I = 2^{1-n}T_n$.

- 3.4. Le changement de variable $\varphi : x \mapsto \frac{a+b}{2} + x\frac{b-a}{2} = t$ envoie bijectivement l'intervalle $[-1, 1]$ sur l'intervalle $[a, b]$ et par composition envoie bijectivement l'ensemble des fonctions polynomiales sur $[-1, 1]$ sur l'ensemble des fonctions polynomiales sur $[a, b]$. Plus précisément, pour $p \in \mathbb{R}[X]$ considéré comme une fonction de $x \in [-1, 1]$ et $p' = p \circ \varphi^{-1}$ considéré comme une fonction de $t \in [a, b]$, on a :

$$\deg(p) = \deg(p') ;$$

$$\text{coefficient dominant}(p) = \left(\frac{b-a}{2}\right)^{\deg(p)} \text{coefficient dominant}(p') ;$$

$$\|p\|_{[-1,1]} = \|p'\|_{[a,b]}.$$

Il en résulte que l'image du polynôme unitaire de degré n de plus petite norme $\| \cdot \|_{[-1,1]}$ est le polynôme de degré n de coefficient dominant $\left(\frac{b-a}{2}\right)^n$ de plus petite norme $\| \cdot \|_{[a,b]}$ parmi ceux de degré n ayant ce coefficient dominant. Par homogénéité, il vient $T_n^{[a,b]} = \left(\frac{b-a}{2}\right)^n (T_n^{[-1,1]})'$, soit

$$T_n^{[a,b]}(t) = 2\left(\frac{b-a}{4}\right)^n \cos(n \arccos(\frac{2t-a-b}{b-a})).$$

On a alors $\|T_n^{[a,b]}\|_{[a,b]} = t_n = 2\left(\frac{b-a}{4}\right)^n$ et $d_1([a,b]) = \lim_{n \rightarrow \infty} (t_n^{1/n}) = \frac{b-a}{4}$.

- 3.5. Si p est un tel polynôme, de degré n et de coefficient dominant c alors p/c est unitaire de degré n donc $\|p/c\|_{[a,b]} \geq t_n = 2\left(\frac{b-a}{4}\right)^n \geq 2$, puis $\|p\|_{[a,b]} = |c| \|p/c\|_{[a,b]} \geq 2|c| \geq 2$.
- 3.6. Le sens indirect est évident. Pour le sens direct, si (p_n) est une suite de polynômes à coefficients entiers convergeant uniformément vers f sur $[a, b]$ alors la suite $(p_{n+1} - p_n)$ converge uniformément vers la fonction nulle et est constituée de polynômes à coefficients entiers. D'après la question précédente, le polynôme $p_{n+1} - p_n$ est donc constant à partir d'un certain rang que l'on note N . Soit c_n le coefficient constant de p_n : pour $n \geq N$, $p_{n+1} - p_n = c_{n+1} - c_n$ et la série télescopique de terme général $p_{n+1} - p_n$ étant uniformément convergente sur $[a, b]$ il en est de même pour la série télescopique de terme général $c_{n+1} - c_n$. Autrement dit, la suite (c_n) admet une limite finie notée $c \in \mathbb{Z}$. Enfin, $f = p_N + \sum_{k=N}^{\infty} (p_{k+1} - p_k) = p_N + c - c_N$ est un polynôme à coefficients entiers.

4. L'approximation par des polynômes à coefficients entiers

- 4.1. Prendre $p = T_n^{[a,b]}$ avec n suffisamment grand pour que $\|p\|_I = 2(\frac{b-a}{4})^n < 1$.
- 4.2. On procède par récurrence forte sur $\deg(s)$. Si $\deg(s) < d$, $n = 0$ et $b_0 = s$ conviennent. Sinon, on écrit la division euclidienne de s par r : $s = b_0 + r \times s_1$ avec $\deg(b_0) < d$ et $\deg(s_1) = \deg(s) - d$. Par hypothèse de récurrence, s_1 s'écrit $s_1 = b_1 + rb_2 + \dots + r^n b_{n+1}$ avec $\deg(b_i) < d$ et l'on obtient $s = b_0 + rb_1 + \dots + r^{n+1} b_{n+1}$. L'unicité de cette décomposition (non demandée) peut aussi facilement être établie par récurrence forte sur $\deg(s)$.
- 4.3. Montrons d'abord que tout polynôme $q \in \mathbb{R}[X]$ s'écrit sous la forme suivante :

$$q = z + \sum_{\substack{0 \leq i \leq d-1 \\ \ell \geq 0}} b_{i,\ell} X^i p(X)^\ell$$

où les coefficients $b_{i,\ell}$ appartiennent à $[0, 1[$ et z est un polynôme à coefficients entiers. On procède par récurrence forte sur $n = \deg(q)$.

Pour $n < d$, on place dans z les parties entières des coefficients de q et on place les parties fractionnaires dans $\sum_{0 \leq i \leq d-1} b_{i,0} X^i$. Les coefficients $b_{i,\ell}$ avec $\ell \geq 1$ sont posés nuls.

Pour $n \geq d$, on écrit

$$q = a_n X^n + \dots$$

où \dots désigne la somme des termes de degré inférieur à n . Puis $a_n = [a_n] + \{a_n\}$ (partie entière, partie fractionnaire), soit

$$q = [a_n] X^n + \{a_n\} X^n + \dots = [a_n] X^n + \{a_n\} X^{\ell d + i} + \dots$$

où $n = \ell d + i$ est la division euclidienne de n par d . Ensuite, $X^{\ell d} = p^\ell + \dots$ où \dots désigne la somme des termes de degré inférieur à ℓd . Il vient

$$q = [a_n] X^n + \{a_n\} X^i p^\ell + q'$$

avec $\deg(q') < n$. Il ne reste plus qu'à décomposer q' qui relève de l'hypothèse de récurrence. Par construction, le terme $X^i p^\ell$ étant de degré n ne sera pas modifié par la décomposition de q' , ce qui termine la récurrence.

En décomposant de cette manière le polynôme $q = p^k$, on obtient $p^k = z_k + \sum_{\substack{0 \leq i \leq d-1 \\ \ell \geq 0}} b_{i,\ell,k} X^i p(X)^\ell$

avec z_k à coefficients entiers et $b_{i,\ell,k} \in [0, 1[$. Comme $\deg(p^k) = kd$ et p^k est unitaire, l'algorithme de décomposition exposé ci-dessus montre que z_k est unitaire de degré kd et $b_{i,\ell,k} = 0$ si $\ell \geq k$. Il ne reste plus qu'à reprendre le polynôme $\sum_{\substack{0 \leq i \leq d-1 \\ 0 \leq \ell < \ell_0}} b_{i,\ell,k} X^i p(X)^\ell$, qui a un degré au plus $d(\ell_0 - 1) + d - 1 = m - 1$,

et à le réécrire comme combinaison linéaire de $1, X, \dots, X^{m-1}$. On place les parties fractionnaires des coefficients dans p_k et on incorpore les parties entières au polynôme z_k .

Remarque : l'énoncé original demandait $r_k(X) = \sum_{\substack{0 \leq i \leq d-1 \\ \ell \geq \ell_0}} b_{i,\ell,k} X^i p(X)^\ell$, pouvant laisser penser que r_k ne dépendait pas de k . Vu le caractère inintelligible de la question – avec ou sans rectification – on peut penser que cette faute typographique n'a gêné aucun candidat.

- 4.4. $z_{k'} - z_k = p^{k'} - p^k - (r_{k'} - r_k) - (p_{k'} - p_k)$ est un polynôme unitaire de degré $k'd$, donc non constant.

On a $\|p\|_I < 1$ et $\|\cdot\|_I$ est sous-multiplicative, donc la suite (p^k) converge vers le polynôme nul pour $\|\cdot\|_I$. En particulier, il existe $k_0 \in \mathbb{N}$ tel que pour tous k, k' vérifiant $k' > k \geq k_0$, on a $\|p^{k'} - p^k\|_I < \frac{1}{3}$.

Par ailleurs, $\|r_{k'} - r_k\|_I \leq \sum_{\substack{0 \leq i \leq d-1 \\ \ell \geq \ell_0}} |b_{i,\ell,k'} - b_{i,\ell,k}| \|X\|_I^i \|p\|_I^\ell \leq M \|p\|_I^{\ell_0}$ où M est une constante ne dépendant que de p . En choisissant soigneusement ℓ_0 , on obtient $\|r_{k'} - r_k\|_I < \frac{1}{3}$ pour tous $k' > k$.

ℓ_0 étant désormais fixé, m l'est aussi et la suite (p_k) est à valeurs dans un espace de dimension finie $(\mathbb{R}_{m-1}[X])$ et à coefficients dans la base canonique de $\mathbb{R}_{m-1}[X]$ bornés. Elle contient une sous-suite

convergente pour n'importe quelle norme sur $\mathbb{R}_{m-1}[X]$, en particulier pour $\|\cdot\|_I$. On peut donc trouver $k' > k \geq k_0$ tels que $\|p_{k'} - p_k\|_I < \frac{1}{3}$.

En conclusion, on peut trouver $k' > k$ tels que $q = z_{k'} - z_k$ vérifie toutes les conditions de l'énoncé.

- 4.5. Je dis que si I est un intervalle quelconque inclus dans $[-1, 1]$ alors $J(I) = I \cap \{-1, 0, 1\}$. En effet, le polynôme $p(X) = X(X^2 - 1)$ est à coefficients entiers, et par étude de fonction on a $|p(x)| \leq \frac{2}{3\sqrt{3}}$ pour tout $x \in [-1, 1]$ donc $\|p\|_I \leq \frac{2}{3\sqrt{3}} < 1$. Ainsi $I \cap \{-1, 0, 1\} \subset J(I)$. L'inclusion réciproque résulte du fait que tout polynôme $p \in \mathbb{Z}[X]$ vérifiant $\|p\|_I < 1$ doit s'annuler sur $I \cap \mathbb{Z} = I \cap \{-1, 0, 1\}$.
- 4.6. Si (p_n) est une suite de polynômes à coefficients entiers convergeant uniformément vers f sur I alors on a $\|p_{n+1} - p_n\|_I < 1$ pour tout n suffisamment grand et donc pour $x \in J(I)$, la suite $(p_n(x))$ est stationnaire et la valeur de stationnement est $f(x)$. On prend pour p l'un des p_n avec n assez grand.
- 4.7. On considère $p \in \mathbb{Z}[X]$ unitaire vérifiant $\|p\|_I < 1$: tous les éléments de $J(I)$ sont racines de p et si la réciproque est vraie, alors $q = p$ convient.

Sinon, soit a une racine de p qui n'appartient pas à $J(I)$. Il existe donc un polynôme $r \in \mathbb{Z}[X]$ vérifiant $\|r\|_I < 1$ et $r(a) \neq 0$. Pour $n > \deg(r)$, le polynôme $p_1 = p^{2^n} + r^2$ est à coefficients entiers, unitaire, et l'ensemble des racines de p_1 est inclus dans l'ensemble des racines de p privé de a . En itérant, on élimine une à une toutes les racines de p n'appartenant pas à $J(I)$.

- 4.8. On choisit dans 4.2 un polynôme $r \in \mathbb{Z}[X]$ tel que $\|r\|_I < 1$. Soit $p \in \mathbb{R}[X]$ que l'on décompose sous la forme : $p = b_0 + b_1 r + \dots + b_n r^n$. On décompose ensuite chaque coefficient de chaque b_i en partie entière et partie fractionnaire. Il vient :

$$p = (c_0 + \dots + c_n r^n) + (d_0 + \dots + d_n r^n)$$

où les c_i sont des polynômes à coefficients entiers et les d_i sont des polynômes à coefficients dans $[0, 1[$. On pose enfin $\tilde{p} = c_0 + \dots + c_n r^n$. Il vient

$$\|p - \tilde{p}\|_I = \|d_0 + \dots + d_n r^n\|_I \leq \sum_{0 \leq i < d, \ell \geq 0} \|X^i\|_I \|r\|_I^\ell = M$$

où $d = \deg(r)$ et M sont indépendants de p .

- 4.9. Soient $\varepsilon > 0$ et $k \geq 1$ tel que $\|q\|_I^k M \leq \varepsilon/2$. La fonction f/q^k est prolongeable par continuité aux racines de q car f est identiquement nulle sur un voisinage relatif de chacune de ces racines. On peut trouver un polynôme $r \in \mathbb{R}[X]$ tel que $\|f/q^k - r\|_I \leq \varepsilon/2$ et avec la question précédente, on peut décomposer $r = \tilde{r} + s$ avec $\tilde{r} \in \mathbb{Z}[X]$ et $\|s\|_I \leq M$. Soit $p = q^k \tilde{r}$. Il vient

$$\|f - p\|_I \leq \|q\|_I^k \|f/q^k - \tilde{r}\|_I \leq \|q\|_I^k (\varepsilon/2 + M) \leq \varepsilon/2 + \|q\|_I^k M \leq \varepsilon.$$

- 4.10. Si f est identiquement nulle sur un voisinage relatif de chaque racine de q , la question précédente permet de conclure. Dans le cas général, il suffit de prouver que si f est une fonction continue sur I nulle en chaque racine de q et si $\varepsilon > 0$, on peut trouver $g \in \mathcal{C}^0(I, \mathbb{R})$ nulle sur un voisinage relatif de chaque racine de q telle que $\|f - g\|_I \leq \varepsilon$. Pour ce faire, considérons la fonction $\varphi : \mathbb{R} \rightarrow \mathbb{R}$ définie par $\varphi(x) = x + \varepsilon$ si $x < -\varepsilon$, $\varphi(x) = 0$ si $-\varepsilon \leq x \leq \varepsilon$ et $\varphi(x) = x - \varepsilon$ si $x > \varepsilon$: φ est continue et on a $|\varphi(x) - x| \leq \varepsilon$ pour tout $x \in \mathbb{R}$. Alors la fonction $g = \varphi \circ f$ convient.
- 4.11. S'il existe un tel p alors $f - p$ relève de la question précédente donc $f - p$ est limite uniforme d'une suite de polynômes à coefficients entiers et f aussi. La réciproque a été vue en 4.6.
- 4.12. Tout polynôme $p \in \mathbb{Z}[X]$ vérifie ces conditions. Réciproquement, si $a, b, c \in \mathbb{Z}$ et si a et c ont même parité, le polynôme p suivant est à coefficients entiers et vérifie $p(-1) = a$, $p(0) = b$, $p(1) = c$:

$$p(X) = a \frac{X(X-1)}{2} + b \frac{(X-1)(X+1)}{-1} + c \frac{X(X+1)}{2} = \left(\frac{a+c}{2} - b\right)X^2 + \frac{c-a}{2}X + b.$$

5. Polynômes symétriques

- 5.1. Dans le cas contraire on aurait $\sum_k i_k = \sum_k j_k$ et $(i_1, \dots, i_k) = (j_1, \dots, j_k)$ pour tout k , ce qui est exclu car $i_j \neq j_j$.
- 5.2. On doit avoir $\sum_k j_k \leq \sum_k i_k$ et en particulier $0 \leq j_1, \dots, j_n \leq \sum_k i_k$. S'agissant d'entiers, j_1, \dots, j_n ne peuvent prendre qu'un nombre fini de valeurs.
- 5.3. On remarque d'abord que les notions de degré et de coefficient dominant sont bien définies car la relation «est plus petit» induit un ordre total sur \mathbb{N}^n d'après la question 5.1.

p étant symétrique, pour toute permutation π , p contient un terme de degré $(i_{\pi(1)}, \dots, i_{\pi(n)})$ qui est donc égal ou plus petit que (i_1, \dots, i_n) . Comme $\sum_k i_{\pi(k)} = \sum_k i_k$, on en déduit $i_1 \geq i_{\pi(1)}$ et en particulier $i_1 \geq i_2$. De même, en se limitant aux permutations π telles que $\pi(1) = 1$, on voit que $i_2 \geq i_3$ et ainsi de suite.

- 5.4. On remarque que la relation «est plus petit ou égal» est compatible avec l'addition dans \mathbb{N}^n et il en résulte que si $p, q \in \mathbb{Z}[T_1, \dots, T_n] \setminus \{0\}$ alors $\deg(pq) = \deg(p) + \deg(q)$. En conséquence,

$$\begin{aligned} \deg(S_1^{d_1} \dots S_n^{d_n}) &= d_1 \deg(S_1) + \dots + d_n \deg(S_n) \\ &= (d_1, 0, \dots, 0) + (d_2, d_2, 0, \dots, 0) + \dots + (d_n, \dots, d_n) \\ &= (i_1, i_2, \dots, i_n). \end{aligned}$$

De plus, le coefficient dominant de $S_1^{d_1} \dots S_n^{d_n}$ est égal à 1 donc les termes de plus haut degré se compensent dans la différence $p - \text{dom}(p)S_1^{d_1} \dots S_n^{d_n}$. Ceci suffit à conclure.

- 5.5. La question précédente montre comment éliminer le terme de plus haut degré dans p en lui retranchant un monôme en S_1, \dots, S_n , ce qui conserve le caractère symétrique du polynôme initial. En itérant, on élimine tous les monômes de degré inférieur à ce plus haut degré (ils sont en nombre fini). Il reste après un nombre fini d'étapes : $p - (\text{un polynôme en } S_1, \dots, S_n) = 0$.

6. Entiers algébriques

- 6.1. Si $x \in \mathbb{Z}$ alors le polynôme $p(X) = X - x$ répond à la définition et x est entier algébrique. Si $x \in \mathbb{Q} \setminus \mathbb{Z}$, $x = a/b$ avec $a \wedge b = 1$ et $b \geq 2$ et si $p \in \mathbb{Z}[X]$ est un polynôme non nul tel que $p(x) = 0$ alors en écrivant $p(X) = a_0 + a_1X + \dots + a_nX^n$ où $a_n \in \mathbb{Z} \setminus \{0\}$, on a

$$0 = p(x) = \frac{a_n a^n + a_{n-1} a^{n-1} b + \dots + a_0 b^n}{b^n},$$

donc $a_n a^n$ est un multiple non nul de b . Ayant $a \wedge b = 1$, il vient $b \mid a_n$ et en particulier $a_n \neq 1$. Donc x n'est pas un entier algébrique.

- 6.2. Il s'agit du classique lemme de Gauss que l'on expédie en quelques lignes de la manière suivante : soit π un nombre premier. Pour tout polynôme $a \in \mathbb{Z}[X]$, on note $a^\pi \in \mathbb{Z}/\pi\mathbb{Z}[X]$ le polynôme obtenu en remplaçant les coefficients de a par leurs classes de congruence modulo π . L'application $a \mapsto a^\pi$ est clairement un morphisme d'anneaux et π étant premier, $\mathbb{Z}/\pi\mathbb{Z}$ est un corps donc $\mathbb{Z}/\pi\mathbb{Z}[X]$ est un anneau intègre. Soient alors $a, b \in \mathbb{Z}[X]$. On a

$$\pi \mid c(ab) \Leftrightarrow (ab)^\pi = 0 \Leftrightarrow (a^\pi = 0 \text{ ou } b^\pi = 0) \Leftrightarrow (\pi \mid c(a) \text{ ou } \pi \mid c(b)) \Leftrightarrow \pi \mid c(a)c(b).$$

Ainsi $c(ab)$ et $c(a)c(b)$ ont les mêmes diviseurs premiers. En particulier $c(ab) = 1 = c(a)c(b)$ lorsque $c(a) = c(b) = 1$ et le cas général s'en déduit par mise en facteur.

- 6.3. Soit I l'ensemble des polynômes $p \in \mathbb{Q}[X]$ tels que $p(x) = 0$. C'est un idéal de $\mathbb{Q}[X]$, non nul car x est algébrique, donc engendré par un polynôme $h \in \mathbb{Q}[X] \setminus \{0\}$ unique à un coefficient multiplicatif près. En jouant sur ce coefficient multiplicatif, on peut imposer que h soit à coefficients entiers, premiers entre eux dans leur ensemble, c'est-à-dire :

$$h \in \mathbb{Z}[X], \quad c(h) = 1, \quad \forall p \in \mathbb{Q}[X], (p(x) = 0) \Leftrightarrow (h \mid p \text{ dans } \mathbb{Q}[X]).$$

h est alors unique au signe près et on peut imposer au coefficient dominant de h d'être strictement positif, ce qui le rend unique.

h est unitaire : soit $p \in \mathbb{Z}[X]$ unitaire tel que $p(x) = 0$. Donc h divise p dans $\mathbb{Q}[X]$, et après réduction au même dénominateur des coefficients du quotient, il existe $d \in \mathbb{N}^*$ et $q \in \mathbb{Z}[X] \setminus \{0\}$ tels que $qh = dp$. Avec le lemme de Gauss, $c(q) = c(qh) = c(dp) = d$ donc tous les coefficients de q sont divisibles par d et le produit des coefficients dominants de q et de h est égal au coefficient dominant de dp , soit d . Ainsi le coefficient dominant de h divise 1 et est positif ; il vaut 1.

h est irréductible dans $\mathbb{Q}[X]$: sinon $h = h_1 h_2$ avec $\deg(h_1) < \deg(h)$ et $\deg(h_2) < \deg(h)$. Alors h_1 et h_2 sont deux polynômes non nuls non éléments de I donc tels que $h_1(x) \neq 0$ et $h_2(x) \neq 0$ ce qui contredit $h(x) = 0$.

h est à racines simples dans \mathbb{C} : sinon h et son polynôme dérivé h' ont un pgcd non constant dans $\mathbb{C}[X]$ donc aussi dans $\mathbb{Q}[X]$ (le pgcd est invariant par extension du corps d'après l'algorithme d'Euclide) et ceci contredit le caractère irréductible de h car ce pgcd, divisant h' , ne saurait être un multiple de h .

En résumé, $p_x = h$ convient.

Si $k \in \mathbb{Z}[X]$ est un polynôme unitaire irréductible dans $\mathbb{Q}[X]$ tel que $k(x) = 0$ alors h divise k dans $\mathbb{Q}[X]$ et par irréductibilité de ces deux polynômes, ils sont égaux à un facteur multiplicatif près. Ledit facteur multiplicatif vaut 1 puisque h et k sont unitaires.

En résumé, p_x est unique.

6.4. x_i est un entier algébrique en tant que racine de p_x donc p_{x_i} divise dans $\mathbb{Q}[X]$ tout polynôme nul en x_i . En particulier p_{x_i} divise p_x et r . Mais p_{x_i} et p_x sont unitaires irréductibles, ils sont égaux. Ainsi p_x divise r .

6.5. Ces coefficients sont des polynômes en y_1, \dots, y_m symétriques et à coefficients entiers. Ce sont donc des polynômes à coefficients entiers en les fonctions symétriques élémentaires $s_k = \sum_{1 \leq i_1 < \dots < i_k \leq m} y_{i_1} \dots y_{i_k}$ et $(-1)^{m-k} s_k$ est un coefficient de p_y donc est entier.

Le polynôme $p_x(X - y_1) \dots p_x(X - y_m)$ est unitaire à coefficients entiers donc ses racines sont entiers algébriques, et $x + y$ est l'une de ces racines.

6.6. Soient x_1, \dots, x_n les conjugués de x et y_1, \dots, y_m ceux de y . Le polynôme à deux variables

$$p(X, T) = \prod_{i=1}^n (X - Tx_i)$$

à coefficients des polynômes symétriques en x_1, \dots, x_n à coefficients entiers donc c'est un polynôme en X, T à coefficients entiers. De plus, en tant que polynôme en X à coefficients polynômes en T , c'est un polynôme unitaire. De même, pour X, T_1, \dots, T_m variables indépendantes,

$$p(X, T_1, \dots, T_m) = \prod_{j=1}^m \left(\prod_{i=1}^n (X - T_j x_i) \right) \in \mathbb{Z}[T_1, \dots, T_m][X]$$

et c'est un polynôme unitaire en X dont les coefficients sont des polynômes en T_1, \dots, T_m symétriques et à coefficients entiers. En conséquence ce polynôme appartient à $\mathbb{Z}[S_1, \dots, S_m][X]$ où S_1, \dots, S_m sont les polynômes symétriques élémentaires en T_1, \dots, T_m . De plus, c'est un polynôme unitaire en X dans cet anneau. Lorsqu'on substitue (y_1, \dots, y_m) à (T_1, \dots, T_m) , les polynômes S_1, \dots, S_m prennent des valeurs entières (les coefficients de p_y ou leurs opposés). Ainsi, $p(X, y_1, \dots, y_m) \in \mathbb{Z}[X]$ et c'est toujours un polynôme unitaire ... qui a tous les $x_i y_j$ pour racine, en particulier xy .

6.7. $\prod_{i=1}^n q(x_i)$ est un polynôme en x_1, \dots, x_n symétrique et à coefficients entiers. C'est un entier. De plus, c'est le produit de n valeurs de q avec $\|q\|_1 < 1$ donc sa valeur absolue est strictement inférieure à 1, c'est 0. Ainsi il existe i tel que $q(x_i) = 0$ et comme x_1, \dots, x_n ont les mêmes polynômes annulateurs dans $\mathbb{Q}[X]$ (question 6.4), on a aussi $q(x) = 0$. L'inclusion $F(I) \subset J(I)$ résulte alors de la définition de $J(I)$.

6.8. On a vu $|x(x^2 - 1)| \leq \frac{2}{3\sqrt{3}}$ pour tout $x \in [-1, 1]$ donc $|x(x^2 - 1)(x^2 - 2)| \leq \frac{4}{3\sqrt{3}}$ pour tout $x \in [-1, 1]$. Par ailleurs, $|(x - 1)(x - 2)| \leq \frac{5}{16}$ pour tout $x \in [1, \frac{9}{4}]$ donc $|(x^2 - 1)(x^2 - 2)| \leq \frac{5}{16}$ pour tout x tel

que $1 \leq |x| \leq \frac{3}{2}$ et $|x(x^2 - 1)(x^2 - 2)| \leq \frac{15}{32} < \frac{4}{3\sqrt{3}} < 1$ dans les mêmes conditions. Ainsi, le polynôme $p(X) = X(X^2 - 1)(X^2 - 2)$ est unitaire à coefficients entiers et vérifie $\|p\|_I < 1$.

Il est stable par opposé, donc par conjugué s'agissant des racines de p , on en déduit

$$I \cap \{0, \pm 1, \pm\sqrt{2}\} \subset F(I) \subset J(I) \subset I \cap \{0, \pm 1, \pm\sqrt{2}\}.$$

Ces ensembles sont égaux.

7. Le noyau de Fekete

7.1. Il s'agit du théorème de Minkowski, qui résulte des propriétés de la mesure de Lebesgue sur \mathbb{R}^n (hors programme). J'admets la propriété suivante extraite de la théorie de la mesure :

si P et Q sont deux pavés tels que Q contienne N translatés de P deux à deux disjoints, alors $\text{vol}(Q) \geq N \text{vol}(P)$.

Supposons les translatés $h + P$ deux à deux disjoints lorsque h décrit \mathbb{Z}^n et soit M un majorant des valeurs absolues de toutes les coordonnées de tous les v_i dans la base canonique de \mathbb{R}^n . Pour $k \in \mathbb{N}$, les translatés $h + P$ avec $h \in \llbracket -k, k \rrbracket^n$ sont deux à deux disjoints, au nombre de $(2k+1)^n$ et tous inclus dans le pavé $Q = \llbracket -k - M, k + M \rrbracket^n$. Avec la propriété admise, il vient $\text{vol}(P) \leq \left(\frac{2k+2M}{2k+1}\right)^n$ puis $\text{vol}(P) \leq 1$ en faisant tendre k vers l'infini.

7.2. $B(r)$ est un pavé de volume $2r$ donc $f^{-1}(\frac{1}{2}B(r))$ est un pavé de volume $r/(2^{n-1}|\det(M)|)$ avec $\det(M) \neq 0$ (déterminant de Vandermonde, les x_i sont distincts et distincts de 1 qui n'est pas algébrique de degré m). Avec le théorème de Minkowski, si ce volume dépasse 1 alors $f^{-1}(\frac{1}{2}B(r))$ contient deux points distincts w, w' tels que $h = w - w' \in \mathbb{Z}^n$. On a alors $f(h) = f(w) - f(w') \in B(r)$, soit $h \in f^{-1}(B(r))$ et par construction $h \in \mathbb{Z}^n \setminus \{0\}$.

7.3. $|s(x_i)| \leq \frac{1}{2}$ résulte du fait que $f(h) \in B(r)$.

$s(x_i) \neq 0$ car le polynôme minimal des x_i est de degré $m > \deg(s)$.

7.4. Supposons dans un premier temps que les nombres $s(x_i)$ sont distincts. Soit $f \in C^0([-1, 1], \mathbb{R})$ telle que $f(s(x_i)) = y_i$ pour $i \in \{1, \dots, n-1\}$ et $f(0) = f(1) = f(-1) = 0$. D'après la question 4.12, il existe un polynôme $q \in \mathbb{Z}[X]$ tel que $\|f - q\|_{[-1, 1]} < \varepsilon$. Alors le polynôme $p = q \circ s$ convient.

Lorsque la suite $(s(x_1), \dots, s(x_{n-1}))$ comporte des répétitions, on remplace s dans le raisonnement précédent par $s_k(X) = Xs(X)^k$ où $k \in \mathbb{N}$ est un entier à choisir. Pour chaque i on peut trouver un rang à partir duquel $|s_k(x_i)| \leq \frac{1}{2}$ et $s_k(x_i) \neq 0$ ($x_i \neq 0$ par algébricité de degré m). Par ailleurs, si $s_k(x_i) = s_k(x_j)$ pour deux indices $i \neq j$ alors $k \ln(|s(x_i)/s(x_j)|) = \ln(|x_j/x_i|)$ donc il n'y a qu'un nombre fini de valeurs de k ne convenant pas.

7.5. La différence avec la situation de la question précédente est le fait que les x_i ne sont pas tous conjugués d'un même x . On imite la construction de Lagrange : mettons par exemple x_1, x_2, x_3 sont conjugués de a et x_4, x_5 sont conjugués de $b \neq a$. On trouve p envoyant x_1, x_2, x_3 près de y_1, y_2, y_3 et q envoyant x_4, x_5 près de y_4, y_5 . Alors le polynôme $p(X)p_b(X) + q(X)p_a(X)$ envoie chaque x_i près de $y_i p_a(x_i)$ ou $y_i p_b(x_i)$ selon les cas. Ces valeurs sont tout aussi arbitraires que y_1, \dots, y_5 car p_a et p_b n'ont pas de racine en commun.

7.6. Par définition, l'ensemble $F(I)$ est constitué d'entiers algébriques et il est stable par conjugaison. Donc le polynôme $p = \prod_{x \in F(I)} p_x$ est un polynôme unitaire à coefficients entiers dont l'ensemble des racines est exactement $F(I)$. En particulier, pour tout $x \in S$ on a $p(x) \neq 0$. Avec la question précédente, pour $\varepsilon > 0$ on peut trouver un polynôme $r \in \mathbb{Z}[X]$ tel que pour tout $x \in S$: $|r(x) - f(x)/p(x)| < \varepsilon$. Il vient :

$$\forall x \in F(I) \cup S, |f(x) - p(x)r(x)| \leq \varepsilon \|p\|_I.$$

Soit φ définie comme en 4.10 avec $\varepsilon \|p\|_I$ à la place de ε et $g(x) = \varphi(f(x) - p(x)r(x))$. g est continue sur I et s'annule sur $F(I) \cup S$ qui est l'ensemble des racines de q donc g est limite uniforme de polynômes à coefficients entiers et on peut trouver un tel polynôme s tel que $\|g - s\|_I \leq \varepsilon$. En conséquence, $\|f - pr - s\|_I \leq \|(f - pr) - g\|_I + \|g - s\|_I \leq \varepsilon(\|p\|_I + 1)$. On a trouvé un polynôme à coefficients entiers arbitrairement proche de f .

7.7. Si $a \in J(I) \setminus F(I)$ alors on peut facilement construire une fonction $f \in \mathcal{C}^0(I, \mathbb{R})$ telle que $f(x) = 0$ pour tout $x \in F(I)$, $f(a) = \frac{1}{2}$ et $\|f\|_I < 1$. Si p est un polynôme à coefficients entiers suffisamment proche de f alors on a $p(a) \neq 0$ et $\|p\|_I < 1$ en contradiction avec l'hypothèse « $a \in J(I)$ ». Ainsi $J(I) \subset F(I)$ et l'inclusion réciproque a été établie en **6.7**.

Fin du corrigé