ENS PARIS MI

Groupe C/S

PREMIÈRE COMPOSITION DE MATHÉMATIQUES

DURÉE : 6 heures

NOTATIONS:

On note $\mathbf{C}$ (resp. $\mathbf{R}$, resp. $\mathbf{Q}$) le corps des nombres complexes (resp. réels, resp. rationnels), et $\mathbf{Z}$ l'anneau des entiers relatifs.

Pour tout élément $z \in \mathbf{C}$, on note $|z|$ le module de z. On désigne par $\mathbf{C}[X]$ l'anneau des polynômes à une variable à coefficients dans $\mathbf{C}$.

On note $\mathbf{Q}[X]$ (resp. $\mathbf{Z}[X]$) le sous-anneau de $\mathbf{C}[X]$ formé des polynômes à coefficients dans $\mathbf{Q}$ (resp. $\mathbf{Z}$).

On dit qu'un polynôme est *unitaire* si le coefficient de son terme de plus haut degré est égal à 1.

Pour tout $f \in \mathbf{C}[X]$, on note $\deg f$ le degré de f.

Si a et b sont deux éléments de $\mathbf{R}$, on note $\sup(a,b)$ le plus grand des deux nombres a et b.

Si $f(X) = \sum_{i=0}^{n} a_i X^i$ est un élément de $\mathbf{C}[X]$, on note $|f|$ le plus grand élément de l'ensemble $\{|a_i|, \quad 0 \leq i \leq n\}$. En particulier, si f est unitaire, on a $|f| \geq 1$.

Pour tout entier $k \geq 0$, et pour tout $f \in \mathbf{C}[X]$, on note $f^{(k)}$ le polynôme égal à la dérivée k-ième de f.

Pour tout $x \in \mathbf{R}$, on note $E(x)$ la partie entière de x, c'est-à-dire l'entier m tel que $m \leq x < m+1$.

PARTIE I

I.1.a Montrer que, pour tout couple (f,g) d'éléments de $\mathbf{C}[X]$, et tout élément $z \in \mathbf{C}$, on a

$$|f+g| \leq |f| + |g|, \quad |zf| = |z||f|.$$

I.1.b Soit k un entier ≥ 0. Montrer que

$$|\frac{1}{k!} f^{(k)}| \leq 2^{\deg f} |f|.$$

I.1.c Montrer que, si $f \in \mathbf{Z}[X]$, on a

$$\frac{1}{k!} f^{(k)} \in \mathbf{Z}[X].$$

I.2.a Soient d un entier > 0, et d éléments de $\mathbf{C}$, α_i $(1 \leq i \leq d)$. Soit f l'élément de $\mathbf{C}[X]$ défini par

$$f(x) = \prod_{i=1}^{d} (X - \alpha_i).$$

Tournez la page S.V.P.

Montrer que

$$2^{-d}\prod_{i=1}^{d}\sup(1,|\alpha_i|) \leq |f| \leq 2^d\prod_{i=1}^{d}\sup(1,|\alpha_i|).$$

(Pour prouver l'inégalité de gauche, on pourra procéder par récurrence sur le nombre des α_i de module ≥ 2.)

I.2.b En déduire que, si f et g sont des éléments de $\mathbf{C}[X]$ tels que $\deg(fg) = d$, on a

$$4^{-d}|fg| \leq |f||g| \leq 4^d|fg|.$$

I.3 Soient n et m deux entiers tels que $1 \leq m < n$, et

$$\begin{cases} \sum_{i=1}^{n} a_{i,1}x_i = 0 \\ \dots \\ \sum_{i=1}^{n} a_{i,m}x_i = 0 \end{cases} \tag{1}$$

un système de m équations à n inconnues $(x_1, \dots, x_n)$, où les $a_{i,j}$ sont des éléments de $\mathbf{Z}$.

On pose

$$A_j = \sum_{i=1}^{n} |a_{i,j}|.$$

On suppose que, pour tout j, $1 \leq j \leq m$, on a $A_j \neq 0$.

Montrer qu'il existe une solution $(x_1, \dots, x_n) \neq (0, \dots, 0)$ du système (1), où les x_i sont des éléments de $\mathbf{Z}$ tels que

$$|x_i| \leq \left(\prod_{j=1}^{m} A_j\right)^{1/(n-m)},$$

pour $1 \leq i \leq n$.

(On pourra montrer que, si M est un nombre réel ≥ 0, lorsque $(x_1, \dots, x_n)$ parcourt les vecteurs à coordonnées dans $\mathbf{Z}$ telles que, pour tout i, $0 \leq x_i \leq M$, la quantité $\sum_i a_{i,j}x_i$ prend au plus $1 + A_jE(M)$ valeurs.)

Partie II.

Dans toute cette partie, F est un polynôme irréductible de $\mathbf{Q}[X]$, unitaire, à coefficients dans $\mathbf{Z}$, de degré $r \geq 3$, qui admet une racine réelle ρ.

II.1 Montrer que, pour tout entier $n \geq 0$, il existe un unique polynôme $F_n \in \mathbf{Z}[X]$, de degré $\leq r - 1$, tel que

$$\rho^n = F_n(\rho).$$

Montrer qu'il existe une constante c_1, indépendante de n (mais dépendant du polynôme F) telle que

$$|F_n| \leq c_1^n.$$

ENS PARIS C|S MI

II.2 Soient ε un nombre réel tel que $0 < \varepsilon < r/2$, n un entier > 0, et m un entier $\geq E(n(\varepsilon - 1 + \frac{r}{2}))$.

II.2.a Montrer qu'il existe des éléments P et Q non nuls de $\mathbf{Z}[X]$, de degré $\leq n+m$, tels que le polynôme $P - \rho Q$ soit divisible par $(X-\rho)^n$, et tels que $|P|$ et $|Q|$ soient majorés par

$$c_2^{(n+m)\frac{r}{2\varepsilon}},$$

où c_2 est une constante ne dépendant que de F (donc indépendante de n, m et ε.)

(On pourra remarquer que le fait que $(X-\rho)^n$ divise $P - \rho Q$ équivaut à $P^{(k)}(\rho) - \rho Q^{(k)}(\rho) = 0$ pour $0 \leq k \leq n-1$, et qu'on est ainsi ramené à la résolution d'un système d'équations linéaires à coefficients dans $\mathbf{Z}$.)

II.2.b Montrer qu'il existe une constante c_3, ne dépendant que de F, telle que, pour tout entier k tel que $0 \leq k \leq n$, il existe un polynôme $G_k \in \mathbf{C}[X]$ tel que

$$\frac{1}{k!}(P^{(k)} - \rho Q^{(k)})(X) = (X-\rho)^{n-k} G_k(X),$$

avec

$$|G_k| \leq c_3^{(n+m)\frac{r}{2\varepsilon}}.$$

II.3 Soient p et q deux éléments de $\mathbf{Z}$, avec $q > 0$, tels que

$$|p - \rho q| < 1.$$

Soit k un entier tel que $0 \leq k \leq n$. On pose

$$A = \frac{1}{k!} q^{m+n-k} P^{(k)}(p/q)$$

et

$$B = \frac{1}{k!} q^{m+n-k} Q^{(k)}(p/q).$$

Montrer que A et B sont des éléments de $\mathbf{Z}$, et qu'il existe une constante c_4 ne dépendant que de F (et donc indépendante de $n, p, q, k, m, \varepsilon$) telle que

$$|A| \leq c_4^{(n+m)\frac{r}{2\varepsilon}} q^{n+m}, \quad |B| \leq c_4^{(n+m)\frac{r}{2\varepsilon}} q^{n+m}, \quad |A - \rho B| \leq c_4^{(n+m)\frac{r}{2\varepsilon}} q^m |p - q\rho|^{n-k}.$$

II.4 On suppose désormais que l'on a $m < n(r-1)$, et l'on pose

$$\gamma = 2m - (n-1)(r-2).$$

II.4.a Soit f un élément de $\mathbf{Q}[X]$, et k un entier. Montrer que, si $(X-\rho)^k$ divise f, alors F^k divise f.

II.4.b En déduire qu'il existe $W \in \mathbf{Q}[X]$, non nul, de degré $\leq \gamma$, tel que

$$P'Q - PQ' = F^{n-1}W.$$

II.4.c Soient p et q deux éléments de $\mathbf{Z}$, avec $q \neq 0$.
Montrer que le polynôme $(X - p/q)^{\gamma+1}$ ne divise pas $P'Q - PQ'$.
En déduire qu'il existe deux entiers a, b, avec $0 \leq a \leq b \leq \gamma + 1$

$$(P^{(a)}Q^{(b)} - P^{(b)}Q^{(a)})(p/q) \neq 0.$$

II.5 Montrer qu'il existe un constante c_5, ne dépendant que de F, telle que, pour tout couple (p, q) d'éléments de $\mathbf{Z}$, $q > 0$, vérifiant $|p - \rho q| < 1$, pour tout couple (p_1, q_1) d'éléments de $\mathbf{Z}$, tel que $q_1 \neq 0$, pour tout entier $n > 0$ et tout nombre réel ε tel que $0 < \varepsilon < r/2$, il existe deux éléments A et B de $\mathbf{Z}$ tels que

i) $Bp_1 - Aq_1 \neq 0$,
ii) $|B| \leq c_5^{n(\varepsilon+r/2)r/(2\varepsilon)} q^{n(\varepsilon+r/2)}$,
iii) $|A - B\rho| \leq c_5^{n(\varepsilon+r/2)r/(2\varepsilon)} q^{n(\varepsilon-1+r/2)} |p - q\rho|^{n(1-2\varepsilon)-(r-1)}$

II.6 En déduire que, si c et h sont deux nombres réels > 0, il n'existe qu'un nombre fini de couples (p, q) d'éléments de $\mathbf{Z}$, $q > 0$, tels que

$$|p - q\rho| < \frac{c}{q^{r/2+h}}. \tag{2}$$

(On utilisera la question II.5, en montrant que, si ε est choisi suffisamment petit, et si (p, q) et (p_1, q_1) sont deux solutions de (2) avec q et q_1 assez grands, il existe $n > 0$ tel que les entiers A et B construits en II.5 sont tels que $|B||p_1 - q_1\rho|$ et $|q_1||A - B\rho|$ sont $< 1/2$, d'où l'on déduira une contradiction avec la condition i) de II.5).

Partie III.

III.1 Soit $f \in \mathbf{Q}[X]$ un élément irréductible de $\mathbf{Q}[X]$ de degré $r \geq 3$, et ρ une racine de f. Montrer que, si c et h sont deux nombre réels > 0, il n'existe qu'un nombre fini de couples (p, q) d'éléments de $\mathbf{Z}$, $q \neq 0$, tels que l'on ait

$$|p - q\rho| < \frac{c}{q^{r/2+h}}.$$

III.2 Soit $f \in \mathbf{Q}[X]$ un élément irréductible de $\mathbf{Q}[X]$ de degré $r \geq 3$, et m un élément de $\mathbf{Q}$. Montrer que l'équation

$$f(x/y)y^r = m$$

n'admet qu'un nombre fini de solutions (x, y), avec $x, y \in \mathbf{Z}$. (On pourra remarquer que, s'il existait une infinité de $(x, y) \in \mathbf{Z}^2$ solutions d'une telle équation, on pourrait en extraire une suite (x_n, y_n) telle que x_n/y_n tende vers une racine de f.)

III.3.a Montrer que l'équation

$$x^3 - 2x^2y + 5xy^2 - 2y^3 = 11$$

n'a qu'un nombre fini de solutions (x, y), avec $x, y \in \mathbf{Z}$.

III.3.b Montrer que l'équation

$$x^4 - x^3y + 3x^2y^2 + 3xy^3 - 2y^4 = 15$$

n'a qu'un nombre fini de solutions (x, y), avec $x, y \in \mathbf{Z}$.