Préparation à l'agrégation interne de mathématiques - Année 2011
Devoir 1 - Mercredi 6 juillet 2011

Durée : 2 heures 30 minutes

- Ce sujet comporte 3 pages.
- Les parties A et B sont indépendantes.
- La partie A traite de certaines propriétés des racines d'un polynôme à coefficients réels ou complexes. Les trois questions composant cette partie sont indépendantes.
- La partie B étudie la factorisation d'un polynôme particulier dans l'anneau des polynômes à coefficients dans le corps fini à p éléments. La question 1 traite quelques cas particuliers. Les questions 3 et 4 utilisent un résultat démontré dans la question 2.

Partie A. Localisation des racines d'un polynôme à coefficients complexes

1. Racines d'un polynôme particulier et de ses polynômes dérivés

On considère dans toute cette question le polynôme $P = X^4 + \frac{2}{3}X^3 - X - \frac{2}{3}$ appartenant à l'algèbre $\mathbb{C}[X]$ des polynômes à coefficients dans le corps $\mathbb{C}$ des nombres complexes.

(a) Vérifier que le polynôme $X^3 - 1$ divise P dans $\mathbb{C}[X]$ puis en déduire les racines complexes de P.

(b) Vérifier que $P'\left(\frac{1}{2}\right) = 0$ puis déterminer les racines complexes de P'.

(c) Sur un graphique représentant le plan complexe (unité : 6 cm), représenter les polygones convexes $\mathcal{P}_0$ (respectivement $\mathcal{P}_1$) de sommets les racines de P (respectivement P').

(d) Déterminer les racines des polynômes dérivés $P^{(2)}$ et $P^{(3)}$ et les indiquer sur le graphique.

2. Une majoration de Cauchy du module des racines

On désigne par P le polynôme unitaire de degré n (n entier, $n \geqslant 2$)

$$P = X^n + \sum_{k=0}^{n-1} a_k X^k = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$$

dont les coefficients $a_0, \ldots, a_{n-1}$ sont des nombres complexes.
On suppose qu'au moins un des coefficients a_k est non nul et on note $A = \max\limits_{k=0,\ldots,n-1} |a_k|$ le maximum des modules des coefficients $a_0, \ldots, a_{n-1}$ de P.
On souhaite établir la majoration suivante du module des racines du polynôme P :

$$|z| < 1 + A \quad \text{pour toute racine } z \text{ de } P. \qquad (\star)$$

On note f la fonction rationnelle réelle définie par

$$f(x) = \frac{1}{x^n} \sum_{k=0}^{n-1} |a_k|\, x^k = \frac{|a_{n-1}|}{x} + \ldots + \frac{|a_0|}{x^n}.$$

(a) Justifier que f est strictement décroissante sur $]0;+\infty[$ et que l'équation $f(x) = 1$ admet une unique solution sur $]0;+\infty[$.
Cette solution sera notée r dans la suite.

(b) Montrer que, pour tout nombre complexe non nul z :

$$|P(z) - z^n| \leqslant |z|^n f(|z|)$$

puis en déduire que toute racine complexe z de P vérifie $|z| \leqslant r$.

(c) Justifier successivement les inégalités

$$f(x) \leqslant A \times \frac{1-\dfrac{1}{x^n}}{x-1} \quad \text{pour tout réel } x > 1$$
$$\text{et} \quad f(1+A) < 1.$$

(d) Déduire de ce qui précède la majoration $(\star)$.

3. Enveloppe convexe et racines des polynômes dérivés

On conserve ici les notations de la question 2 :

$$P = X^n + \sum_{k=0}^{n-1} a_k X^k = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$$

est un polynôme de degré n, $n \geqslant 2$, à coefficients complexes.
On note $z_1, \ldots, z_n$ ses racines dans $\mathbb{C}$ (comptées avec multiplicité).

(a) (i) Justifier que le barycentre du système pondéré $\{(z_1;1), \ldots, (z_n;1)\}$ est le nombre complexe $\omega = \frac{-a_{n-1}}{n}$.

(ii) Montrer que, pour tout entier k, $0 \leqslant k \leqslant n-1$, l'isobarycentre de l'ensemble des racines (comptées avec multiplicité) du polynôme dérivé $P^{(k)}$ est le nombre ω.

(b) Montrer, par récurrence sur n, que

$$P' = \sum_{k=1}^{n} \prod_{\substack{j=1 \\ j\neq k}}^{n} (X - z_j)$$

puis en déduire que

$$\frac{P'}{P} = \sum_{k=1}^{n} \frac{1}{X - z_k}.$$

(c) Soit a une racine du polynôme dérivé P'. Démontrer que

$$P(a) = 0 \quad \text{ou} \quad \sum_{k=1}^{n} \frac{a - z_k}{|a - z_k|^2} = 0.$$

(d) Montrer que toute racine du polynôme P' appartient à l'enveloppe convexe (l'ensemble des barycentres à coefficients positifs) des racines de P.

Partie B. Factorisation d'un polynôme sur le corps à p éléments

Dans cette partie, la lettre p désigne un entier naturel premier.
On note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z} = \{0, \ldots, p-1\}$ à p éléments.
L'objectif de cette partie est d'établir une factorisation dans l'anneau $\mathbb{F}_p[X]$ du polynôme

$$Q = X^4 + 1.$$

On pourra utiliser la version suivante du petit théorème de Fermat. Dans le corps $\mathbb{F}_p$, pour tout élément x non nul :

$$x^{p-1} = 1.$$

1. Exemples de factorisation

(a) Justifier qu'un nombre premier p différent de 2 vérifie $p \equiv 1 \pmod 4$ ou $p \equiv 3 \pmod 4$.

(b) On suppose ici $p = 2$. Justifier que $Q = (X+1)^4$ est la factorisation en produit de facteurs irréductibles du polynôme Q dans $\mathbb{F}_2[X]$.

(c) On suppose ici $p = 3$. Vérifier que $Q = (X^2+X-1)(X^2-X-1)$ dans $\mathbb{F}_3[X]$ et que Q n'admet pas de racine dans $\mathbb{F}_3$.

(d) On suppose ici $p = 5$. Vérifier que $Q = (X^2+2)(X^2-2)$ dans $\mathbb{F}_5[X]$ et que Q n'admet pas de racine dans $\mathbb{F}_5$.

2. Caractérisation des carrés dans $\mathbb{F}_p$ si $p > 2$

On suppose dans toute la suite que p est strictement supérieur à 2.
On note $\mathcal{C}_p$ l'ensemble des éléments de $\mathbb{F}_p$ qui sont des carrés : $\mathcal{C}_p = \{x^2 : x \in \mathbb{F}_p\}$.
On note $\mathcal{C}_p^*$ l'ensemble des éléments non nuls de $\mathcal{C}_p$: $\mathcal{C}_p^* = \{x^2 : x \in \mathbb{F}_p, x \neq 0\}$.
Le but de cette question est de démontrer la caractérisation suivante. Pour tout x dans $\mathbb{F}_p$:

$$x \in \mathcal{C}_p^* \iff x^{\frac{p-1}{2}} = 1. \qquad (\star\star)$$

(a) Justifier l'équivalence

$$x^2 = y^2 \text{ dans } \mathbb{F}_p \iff x = \pm y \text{ dans } \mathbb{F}_p.$$

(b) En utilisant le nombre d'antécédents de chaque image par l'application

$$\mathbb{F}_p \longrightarrow \mathcal{C}_p \ : \ x \longmapsto x^2,$$

justifier que l'ensemble $\mathcal{C}_p^*$ contient exactement $\frac{p-1}{2}$ éléments.

(c) On note R le polynôme $R = X^{\frac{p-1}{2}} - 1$ dans $\mathbb{F}_p[X]$.
Justifier que tout élement de $\mathcal{C}_p^*$ est une racine de R.

(d) En utilisant le nombre de racines de R, démontrer l'équivalence $(\star\star)$.

3. Le cas $p = 4m+1$

On suppose ici que p est un entier de la forme $4m+1$ avec m entier naturel.

(a) Justifier que -1 appartient à l'ensemble $\mathcal{C}_p^*$.

(b) En déduire qu'il existe un élément a dans $\mathbb{F}_p$ tel que

$$Q = (X^2+a)(X^2-a).$$

(c) Démontrer que $Q = X^4+1$ admet une racine dans $\mathbb{F}_p$ si et seulement si l'entier m est pair.

4. Le cas $p = 4m+3$

On suppose ici que p est un entier de la forme $4m+3$ avec m entier naturel.

(a) Vérifier que tout élément x de $\mathbb{F}_p^*$ vérifie

$$x^{\frac{p-1}{2}} = 1 \quad \text{ou} \quad x^{\frac{p-1}{2}} = -1.$$

(b) Justifier l'équivalence

$$2 \in \mathcal{C}_p^* \iff -2 \notin \mathcal{C}_p^*.$$

(c) En déduire qu'il existe un élément a dans $\mathbb{F}_p$ tel que

$$Q = (X^2+aX+1)(X^2-aX+1) \quad \text{ou} \quad X^4+1 = (X^2+aX-1)(X^2-aX-1).$$

(d) Démontrer que $Q = X^4+1$ n'admet aucune racine dans $\mathbb{F}_p$.