Préparation à l'agrégation interne de mathématiques - Année 2011
Éléments de correction du Devoir 1 - juillet 2011

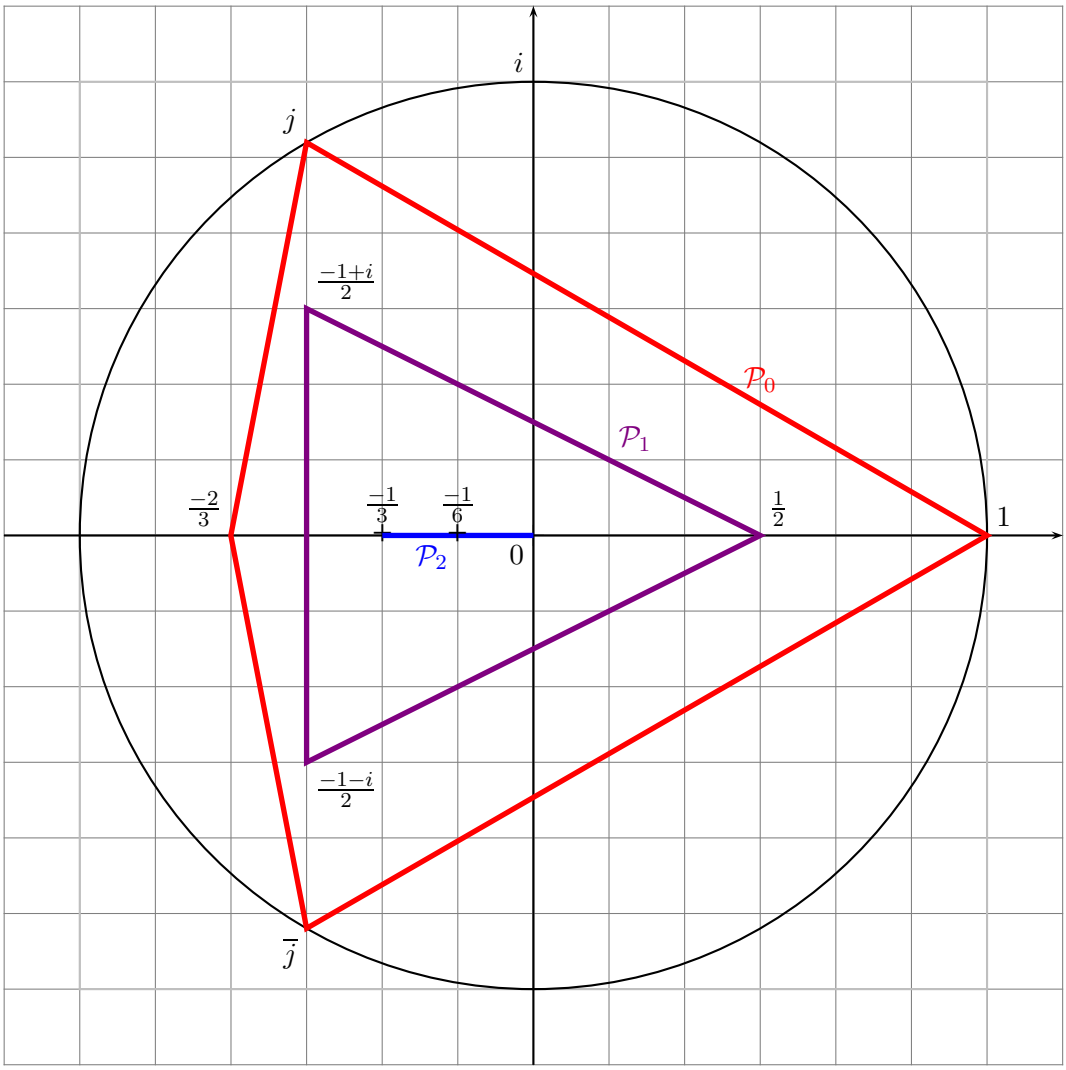
Partie A. Localisation des racines d'un polynôme à coefficients complexes

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

(a) $P = X^4+\frac{2}{3}X^3-X-\frac{2}{3} = (X^3-1)\left(X+\frac{2}{3}\right)$ donc l'ensemble des racines de P est $\left\{-\frac{2}{3}; 1; j = e^{i\frac{2\pi}{3}}; \overline{j}\right\}$

(b) $P'\left(\frac{1}{2}\right) = 4\left(\frac{1}{2}\right)^3 + 2\left(\frac{1}{2}\right)^2 - 1 = \frac{1}{2}+\frac{1}{2}-1 = 0$ donc P' est divisible par $X-\frac{1}{2}$:
$P' = 4\left(X-\frac{1}{2}\right)\left(X^2+X+\frac{1}{2}\right)$ donc l'ensemble des racines de P' est $\left\{\frac{1}{2}; \frac{-1\pm i}{2}\right\}$.

(c) Graphique



(d) Les racines de $P^{(2)} = 12X^2+4X$ sont 0 et $\frac{-1}{3}$ et la racine de $P^{(3)} = 24X+4$ est $\frac{-1}{6}$.

2. Une majoration de Cauchy du module des racines

(a) Sur $]0;+\infty[$, les fonctions $x \mapsto \frac{|a_{n-k}|}{x^k}$ sont strictement décroissantes (si $a_{n-k} \neq 0$) ou constantes (si $a_{n-k} = 0$) et l'une au moins d'entre elles est strictement décroissante. Donc leur somme f est une fonction strictement décroissante.

La fonction f est continue sur cet intervalle et vérifie $\lim\limits_{\substack{x\to 0\\ x>0}} f(x) = +\infty$ et $\lim\limits_{x\to+\infty} f(x) = 0$ donc 1 admet un unique antécédent r par f sur $]0;+\infty[$.

(b) Pour tout nombre complexe non nul z :

$$|P(z) - z^n| = \left|\sum_{k=0}^{n-1} a_k z^k\right| \leqslant \sum_{k=0}^{n-1} \left|a_k z^k\right| = \sum_{k=0}^{n-1} |a_k| \,.|z|^k = |z|^n f\left(|z|\right).$$

Si z est une racine non nulle de P, alors $|P(z) - z^n| = |z^n|$ donc $|z|^n \leqslant |z|^n f\left(|z|\right)$ ou encore $f\left(|z|\right) \geqslant 1$ donc $|z| \leqslant r$ puisque f est strictement décroissante et $f(r) = 1$.

(c) Pour tout réel $x > 1$:

$$f(x) = \frac{|a_{n-1}|}{x} + \ldots + \frac{|a_0|}{x^n} \leqslant A\left(\frac{1}{x} + \ldots + \frac{1}{x^n}\right) = \frac{A}{x} \times \frac{1 - \left(\frac{1}{x}\right)^n}{1 - \frac{1}{x}} = A \times \frac{1 - \frac{1}{x^n}}{x - 1}.$$

Puis (avec $x = 1 + A > 1$) : $f(1+A) \leqslant A \times \frac{1 - \frac{1}{x^n}}{A} = 1 - \frac{1}{(1+A)^n} < 1$.

(d) Si z est une racine non nulle de P, on a $|z| \leqslant r$. Or $f(1+A) < 1 = f(r)$ donc $1 + A > r$ (toujours la (stricte) décroissance de f). D'où l'inégalité $|z| < 1 + A$.

3. Enveloppe convexe et racines des polynômes dérivés

(a) (i) Le barycentre du système pondéré $\{(z_1;1), \ldots, (z_n;1)\}$ est (avec la notation habituelle sur la somme des racines) le nombre $\dfrac{1}{n}\sum\limits_{k=1}^{n} z_k = \dfrac{1}{n}\sigma_1 = \dfrac{1}{n} \times \dfrac{-a_{n-1}}{1} = \omega$.

(ii) Le raisonnement précédent montre que l'isobarycentre de l'ensemble des $n-1$ racines du polynôme dérivé $P' = nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \ldots + a_1$ est le nombre $\frac{1}{n-1} \times \frac{-(n-1)a_{n-1}}{n} = \omega$. Une récurrence sur k permet de conclure.

(b) On dérive le produit $P = \prod\limits_{k=1}^{n} (X - z_k)$ des n facteurs $X - z_k$. On a alors

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

(c) Soit a une racine du polynôme dérivé P'. Si a est une racine de P, alors $P(a) = 0$. Sinon a est un zéro de la fraction rationnelle $\frac{P'}{P}$:

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

d'où la conclusion par conjugaison complexe.

(d) Une racine a du polynôme P', qui n'est pas racine de P, vérifie $c_k = \frac{1}{|a - z_k|^2} > 0$ pour tout k. Donc

$$a = \frac{\sum_{k=1}^{n} c_k z_k}{\sum_{k=1}^{n} c_k}$$

ce qui exprime a comme barycentre à coefficients positifs des racines de P.

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

1. Exemples de factorisation

(a) Un nombre premier p différent de 2 est impair donc vérifie $p \equiv 1 \pmod 4$ ou $p \equiv 3 \pmod 4$.

(b) Dans $\mathbb{F}_2[X]$, on a $(X+1)^4 = X^4 + 4X^3 + 6X^2 + 4X + 1 = X^4 + 1 = Q$ et le polynôme $X+1$ est irréductible (car de degré 1).

(c) Dans $\mathbb{F}_3[X]$, on a $(X^2+X-1)(X^2-X-1) = X^4 - 3X^2 + 1 = X^4 + 1 = Q$ et aucun des deux facteurs ne s'annule sur $\mathbb{F}_3$.

(d) Dans $\mathbb{F}_5[X]$, on a $(X^2+2)(X^2-2) = X^4 - 4 = X^4 + 1 = Q$ et aucun nombre dans $\mathbb{F}_5$ n'admet -2 ou 2 comme carré.

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

(a) $x^2 = y^2 \Leftrightarrow (x+y)(x-y) = 0 \Leftrightarrow x + y = 0$ ou $x - y = 0$

(b) L'application indiquée est surjective. Le nombre 0 admet un unique antécédent (0) et les éléments de $\mathcal{C}_p^*$ admettent exactement deux antécédents d'après ce qui précède ($x \neq -x$ car $p \neq 2$). Il y a $p-1$ éléments non nuls dans $\mathbb{F}_p$ donc $\frac{p-1}{2}$ éléments dans $\mathcal{C}_p^*$.

(c) $y \in \mathcal{C}_p^* \Rightarrow y = x^2 \Rightarrow y^{\frac{p-1}{2}} = x^{p-1} = 1$ donc $\tilde{R}(y) = 0$.

(d) Le nombre de racines de R dans $\mathbb{F}_p$ est inférieur ou égal au degré $\frac{p-1}{2}$. Donc toute racine de R est un élément de $\mathcal{C}_p^*$ et les racines de R sont les éléments de $\mathbb{F}_p$ vérifiant $x^{\frac{p-1}{2}} = 1$.

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

(a) On a $\frac{p-1}{2} = 2m$ donc $(-1)^{\frac{p-1}{2}} = (-1)^{2m} = 1$ donc $-1 \in \mathcal{C}_p^*$.

(b) Soit a dans $\mathbb{F}_p$ tel que $a^2 = -1$ (l'existence vient de ce qui précède). Alors

$$(X^2 + a)(X^2 - a) = X^4 + (a-a)X^2 - a^2 = X^4 + 1 = Q.$$

(c) Les racines de Q sont les solutions de $x^2 = a$ ou de $x^2 = -a$ avec $a^2 = -1$.
Un tel nombre existe si et seulement si $a \in \mathcal{C}_p^*$ ou $-a \in \mathcal{C}_p^*$ (a est non nul).
Or $(\pm a)^{\frac{p-1}{2}} = (\pm a)^{2m} = \big((\pm a)^2\big)^m = (-1)^m$ est égal à 1 si et seulement si l'entier m est pair.

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

(a) Pour tout élément x de $\mathbb{F}_p^*$, le nombre $y = x^{\frac{p-1}{2}}$ vérifie $y^2 = \left(x^{\frac{p-1}{2}}\right)^2 = x^{p-1} = 1$ donc $y = \pm 1$.

(b) L'entier $\frac{p-1}{2} = 2m+1$ est impair donc $(-x)^{\frac{p-1}{2}} = (-x)^{2m+1} = -x^{2m+1}$. En appliquant le résultat précédent à $x = 2$, on sait que $2^{\frac{p-1}{2}} = 1$ ou $2^{\frac{p-1}{2}} = -1$ une possibilité excluant l'autre. Donc

$$2 \in \mathcal{C}_p^* \Longleftrightarrow 2^{2m+1} = 1 \Longleftrightarrow 2^{2m+1} \neq -1 \Longleftrightarrow (-2)^{2m+1} \neq 1 \Longleftrightarrow -2 \notin \mathcal{C}_p^*.$$

(c) Si $2 \in \mathcal{C}_p^*$, alors il existe a dans $\mathbb{F}_p$ tel que $a^2 = 2$ et dans ce cas

$$(X^2 + aX + 1)(X^2 - aX + 1) = X^4 + (2 - a^2)X^2 + 1 = X^4 + 1 = Q.$$

Sinon,$-2 \in \mathcal{C}_p^*$ et il existe a dans $\mathbb{F}_p$ tel que $a^2 = -2$ et

$$(X^2 + aX - 1)(X^2 - aX - 1) = X^4 - (2 + a^2)X^2 + 1 = X^4 + 1 = Q.$$

(d) Il suffit de montrer que les facteurs de Q de degré 2 ne possèdent pas de racine dans $\mathbb{F}_p$.
- Si $a^2 = 2$, $Q = (X^2 + aX + 1)(X^2 - aX + 1)$ et chacun des facteurs a pour discriminant (commun) $\Delta = (\pm a)^2 - 4 = a^2 - 4 = -2 \notin \mathcal{C}_p^*$ donc n'admet pas de racine.
- De même, si $a^2 = -2$, $Q = (X^2 + aX - 1)(X^2 - aX - 1)$ et chacun des facteurs a pour discriminant (commun) $\Delta' = (\pm a)^2 + 4 = a^2 + 4 = 2 \notin \mathcal{C}_p^*$ donc n'admet pas de racine.

1.	a) $P = (X^3-1)\left(X+\frac{2}{3}\right)$ racines de P : $\left\{-\frac{2}{3}; 1; j = e^{i\frac{2\pi}{3}}; \overline{j}\right\}$	1 1	
1.	b) $P'\left(\frac{1}{2}\right) = 0$ racines de P' : $\left\{\frac{1}{2}; \frac{-1\pm i}{2}\right\}$	1 1	
1.	c) graphique, $\mathcal{P}_0$, $\mathcal{P}_1$	1	
1.	d) racines de $P^{(2)}$: $\left\{0; \frac{-1}{3}\right\}$; racine de $P^{(3)}$: $\frac{-1}{6}$	1	
2.	a) f strict. décroissante, continue, TVI	2	
2.	b) $\lvert P(z) - z^n\rvert \leqslant \lvert z\rvert^n f(\lvert z\rvert)$ Si $z \neq 0$ racine, alors $f(\lvert z\rvert) \geqslant 1$ donc $\lvert z\rvert \leqslant r$	1 1	
2.	c) $f(x) \leqslant A \times \frac{1-1/x^n}{x-1}$ $f(1+A) < 1$	1 1	
2.	d) $\lvert z\rvert \leqslant r$ et $f(1+A) < 1 = f(r) \Rightarrow 1+A > r$	1	
3.	a) i) $\frac{\sigma_1}{n} = \frac{-a_{n-1}}{n} = \omega$	1	
3.	a) ii) isobarycentre des racines de P' récurrence	2	
3.	b) polynôme dérivé de P expression de P'/P	1 1	
3.	c) $P(a) = 0$ ou $\sum \frac{a-z_k}{\lvert a-z_k\rvert^2} = 0$	2	
3.	d) a barycentre à coefficients positifs	1	
	Total Partie A	**21**	

1.	a) p premier différent de 2 donc impair	1	
1.	b) $(X+1)^4 = X^4+4X^3+6X^2+4X+1 = X^4+1 = Q$ $X+1$ est irréductible	1 1	
1.	c) $(X^2+X-1)(X^2-X-1) = X^4-3X^2+1 = Q$ pas de racine sur $\mathbb{F}_3$	1 1	
1.	d) $(X^2+2)(X^2-2) = X^4-4 = X^4+1 = Q$ pas de racine sur $\mathbb{F}_5$	1 1	
2.	a) $x^2 = y^2 \Leftrightarrow x+y = 0$ ou $x-y = 0$	1	
2.	b) $\frac{p-1}{2}$ éléments dans $\mathcal{C}_p^*$	1	
2.	c) $y \in \mathcal{C}_p^* \Rightarrow \tilde{R}(y) = 0$	1	
2.	d) nombre de racines de $R \leqslant \frac{p-1}{2} = card(\mathcal{C}_p^*)$	1	
3.	a) $(-1)^{\frac{p-1}{2}} = (-1)^{2m} = 1$	1	
3.	b) $a^2 = -1 \Rightarrow (X^2+a)(X^2-a) = X^4-a^2 = Q$	1	
3.	c) $(\pm a)^{\frac{p-1}{2}} = (-1)^m = 1 \Leftrightarrow m$ pair	1	
4.	a) $y = x^{\frac{p-1}{2}}$ vérifie $y^2 = 1$	1	
4.	b) $2 \in \mathcal{C}_p^* \Longleftrightarrow -2 \notin \mathcal{C}_p^*$	1	
4.	c) $a^2 = 2 \Rightarrow (X^2+aX+1)(X^2-aX+1) = Q$ $a^2 = -2 \Rightarrow (X^2+aX-1)(X^2-aX-1) = Q$	2	
4.	d) pas de racine dans $\mathbb{F}_p$	1	
	Total Partie B	**19**	

Total : . . . . + ... /**40**