Université Gustave Eiffel
Préparation à l'Agrégation Interne de Mathématiques 2025-26

Composition 2025-26-3–énoncé – Alain Tissier.

samedi 11 octobre 2025.

Arithmétique des polynômes, composition de polynômes.

Dans le problème, les polynômes sont des éléments de $\mathbb{C}[X]$. On dira que ce sont des polynômes complexes.

Soit P un polynôme complexe non nul. On note $\deg(P)$ son degré, $\mathrm{Rac}(P)$ l'ensemble des racines de P et $\rho(P)$ le cardinal de $\mathrm{Rac}(P)$.

Pour tout complexe z on note $\mu_P(z)$ la multiplicité de z comme racine de P. *En particulier* $\mu_P(z) = 0$ *si* z *n'est pas racine de* P.

Le PGCD des polynômes non nuls $P_1, P_2, \ldots, P_r$ est l'unique polynôme *unitaire* divisant chaque P_i et dont le degré est maximal pour cette propriété. On note en particulier $P \wedge Q$ le PGCD de P et Q.

On dit que les polynômes $P_1, P_2, \ldots, P_r$ sont premiers entre eux *dans leur ensemble* si leur PGCD vaut 1. On dit qu'ils sont *deux à deux* premiers entre eux si $P_i \wedge P_j = 1$ pour tous i, j tels que $1 \leqslant i < j \leqslant r$.

Soit f une fonction de $\mathbb{C}$ dans $\mathbb{N}$ telle que le support de f, soit l'ensemble I des z tels que $f(z) \neq 0$, est fini. Dans ce cas la notation $\sum\limits_{z \in J} f(z)$ est admise pour toute partie J de $\mathbb{C}$ finie ou non ; par définition c'est $\sum\limits_{z \in I \cap J} f(z)$. Exemple : $\sum\limits_{z \in \mathbb{C}} f(z) = \sum\limits_{z \in I} f(z)$.

*****

Questions préliminaires.

1) Soit P un polynôme complexe non constant.

a) Justifier $1 \leqslant \rho(P) \leqslant \deg(P)$. Que dire de P si $\rho(P) = 1$? si $\rho(P) = \deg(P)$?

b) Justifier la relation $\deg(P) = \sum\limits_{z \in \mathbb{C}} \mu_P(z)$.

2) Soit (P, Q) un couple de polynômes complexes non constants. Comparer les propriétés (i) et (ii) :
(i) P et Q sont premiers entre eux ;
(ii) $\mathrm{Rac}(P) \cap \mathrm{Rac}(Q) = \emptyset$.

3) Donner un exemple de triplet (P, Q, R) de polynômes complexes non constants dont le PGCD vaut 1 alors que P et Q ne sont pas premiers entre eux, Q et R non plus et R et P non plus.

*****

Partie I. Inégalité de Mason

Pour tout entier $d \geqslant 1$, on note $\mathcal{T}_d$ l'ensemble des triplets (A, B, C) de polynômes complexes *non nuls* vérifiant :

- $A + B + C = 0$;
- A, B et C sont premiers entre eux dans leur ensemble.
- $\max(\deg(A), \deg(B), \deg(C)) = d$.

Le but de cette partie est de montrer l'inégalité de Mason :

$$\text{(R)} \qquad \rho(A) + \rho(B) + \rho(C) \geqslant 1 + d$$

pour tout (A, B, C) de $\mathcal{T}_d$.

Jusqu'à la fin de cette partie on se donne un entier $d \geqslant 1$ et un élément (A, B, C) de $\mathcal{T}_d$. On note :

$$D = AB' - BA'.$$

1)a) Montrer que A, B et C sont deux à deux premiers entre eux.

b) Montrer que $\mathrm{Rac}(A)$, $\mathrm{Rac}(B)$ et $\mathrm{Rac}(C)$ constituent une partition de $\mathrm{Rac}(ABC)$.

2)a) Montrer : $D = BC' - CB' = CA' - AC'$.

b) Montrer que D n'est pas nul.

Quitte à changer l'ordre de (A, B, C), ce qui ne modifie pas l'appartenance à $\mathcal{T}_d$, on imposera désormais la condition :

$$\deg(A) \geqslant \deg(B) \geqslant \deg(C)$$

et on notera d' le degré de C.

3)a) Montrer : $\deg(B) = \deg(A) = d$.

b) Montrer : $\deg(D) \leqslant d + d' - 2$ si $d' = d$ et $\deg(D) = d + d' - 1$ si $d' < d$.

4)a) Soit z une racine de P où P est l'un des polynômes A, B, C.
Montrer : $\mu_D(z) = \mu_P(z) - 1$.

b) Montrer : $\deg(D) \geqslant 2d + d' - (\rho(A) + \rho(B) + \rho(C))$.

5) Montrer l'inégalité (R).

6) Montrer que l'égalité $\rho(A) + \rho(B) + \rho(C) = 1 + d$ équivaut à ((i) et (ii)) :
(i) toute racine de D est racine de A, de B ou de C ;
(ii) $d' < d$.

*****

Partie II. Cas d'égalité dans l'inégalité de Mason. Exemples

On garde les notations de la partie précédente.

Le but de cette partie est d'exprimer dans certains cas, pour $d \geqslant 1$, les triplets (A, B, C) de $\mathcal{T}_d$ vérifiant la condition :

$$\text{(E)} \qquad d+1 = \rho(A)+\rho(B)+\rho(C)$$

On imposera toujours la condition $\deg(A) = \deg(B) = d \geqslant \deg(C)$.

D'après le **6)** de la partie I, on a $d' = \deg(C) < d$.

Quitte à échanger A et B *on imposera de plus la condition* $\rho(A) \leqslant \rho(B)$.

Quitte à remplacer (A, B, C) par $(\lambda A, \lambda B, \lambda C)$ pour un certain λ non nul, ce qui ne change pas l'appartenance à $\mathcal{T}_d$ et conserve l'éventuelle propriété (E), *on supposera que le polynôme A est unitaire*; le terme directeur de A est donc X^d.

Dans toutes les questions de cette partie la notation (A, B, C) désigne un élément de $\mathcal{T}_d$ vérifiant les condtions du préambule. On notera si besoin $\alpha_1, \alpha_2 \ldots$ les racines de A, α s'il n'y en a qu'une; idem pour B et C avec les lettres β et γ.

1) Montrer que $-X^d$ est le terme directeur de B.

2) Exprimer les (A, B, C) vérifiant (E) pour $d = 1$.

3) Soit un entier $d \geqslant 2$ quelconque.
Prouver que si $\rho(A) = 1$ et $d' = 0$ alors (A, B, C) vérifie (E).

4) Soit un entier $d \geqslant 2$ quelconque.
Prouver que si $\rho(A) = 1$ et $\rho(B) = 1$ alors (A, B, C) vérifie (E).

5) Exprimer les (A, B, C) vérifiant (E) pour $d = 2$.

6) On suppose dans cette question $d \geqslant 3$, $d' = 1$ et $\rho(A) = 1$.

a) Montrer qu'il existe des complexes distincts α et γ et un complexe non nul λ tels que $A = (X-\alpha)^d$ et $C = \lambda(X-\gamma)$.

b) Montrer que (A, B, C) vérifie (E) si et seulement si B admet une racine double β à exprimer en fonction de α et γ.

7) On suppose dans cette question $d = 3$, $d' = 0$ et $\rho(A) = 2$.

a) Montrer que (A, B, C) vérifie (E) si et seulement s'il existe des complexes distincts α_1, α_2, β_1, β_2 tels que $A = (X-\alpha_1)^2(X-\alpha_2)$,
$B = -(X-\beta_1)^2(X-\beta_2)$ et un complexe non nul λ tel que $C = \lambda$.

b) On pose $\mu = \frac{\alpha_1+\beta_1}{2}$ et $\delta = \frac{\alpha_1-\beta_1}{2}$, $\alpha_2 = \mu+\alpha'$ et $\beta_2 = \mu+\beta'$. Calculer α', β' et λ en fonction de δ.

c) Exprimer les (A, B, C) vérifiant (E) dans ce cas.

8) Montrer qu'on a obtenu tous les (A, B, C) vérifiant (E) pour $d = 3$.

*****

Partie III. Une application

On considère l'équation

$$(\mathrm{F}) \qquad A^m + B^m + C^m = 0$$

où (A, B, C) est un triplet de polynômes non nuls et m est un entier *au moins égal à* 3. Une solution de (F) est dite *triviale* s'il existe un triplet (λ, μ, ν) de complexes non nuls et un polynôme non nul P tels que $A = \lambda P$, $B = \mu P$, $C = \nu P$ et $\lambda^m + \mu^m + \nu^m = 0$.

1) Montrer, en utilisant l'inégalité de Mason que (F) n'a aucune solution non triviale où A, B, C sont premiers entre eux dans leur ensemble.

2) Montrer que (F) n'a aucune solution non triviale.

*****

Partie IV. Points d'ordre fini pour un polynôme complexe.

Soit un polynôme $P = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_0$ où les a_i sont complexes. Soit Q un polynôme complexe. On définit le composé $P \circ Q$:

$$P \circ Q = a_d Q^d + a_{d-1} Q^{d-1} + \cdots + a_0.$$

1) Montrer que $P \circ Q$ est l'unique polynôme R tel que

$$\forall z \in \mathbb{C}\ ,\ R(z) = P(Q(z)).$$

2) Montrer que le polynôme X est élément neutre pour la loi $\circ$ c'est-à-dire : $X \circ P = P \circ X = P$.

3) Montrer : $(P \circ Q) \circ R = P \circ (Q \circ R)$ pour tous polynômes P, Q, R.

***

Pour tout polynôme complexe non nul P, on définit par récurrence le polynôme P_n pour tout entier $n \geqslant 0$:

$$P_0 = X\,;\ P_1 = P\,;\ \forall n \geqslant 0, P_{n+1} = P \circ P_n$$

***

4) Montrer $P_n \circ P_m = P_{n+m}$ pour tous entiers m et n.

5)a) Exprimer le degré de $P \circ Q$ en fonction de ceux de P et de Q.
b) Exprimer le degré de P_n en fonction de celui de P.

***

Définitions.
Soit P un polynôme complexe de degré $d \geqslant 2$.
Un complexe z tel que $P(z) = z$ est appelé *point fixe* de P.
Un complexe z est dit *d'ordre fini* pour P s'il existe au moins un entier $n \geqslant 1$ tel que z est un point fixe de P_n. Le plus petit de ces entiers n s'appelle l'*ordre* de z pour P et on le note $O(z, P)$.

***

6) Soit z un point d'ordre fini pour P. On note $m = O(z,P)$.

a) Montrer que z est un point fixe de P_n si et seulement si m divise n.

b) Montrer que la suite de terme général $(P_k(z))_{k\in\mathbb{N}}$ est périodique de plus petite période m.

7) Montrer que P possède au moins un point d'ordre 1.

8) On traite l'exemple $P = X^2 - a$ où a est un paramètre complexe.

a) Montrer que P possède exactement deux points fixes sauf pour une valeur de a à préciser.

b) Prouver que sauf pour une valeur a_0 de a à préciser, le système :

$$P(u) = v\,;\ P(v) = u\,;\ v \neq u$$

admet un couple (u,v) solution unique à l'ordre près tandis pour $a = a_0$ il n'a pas de solution.

Que peut-on en conclure sur l'existence de points d'ordre 2 pour P ?

*****

Partie V. Existence de points d'ordre n pour un polynôme complexe.

Pour tout entier $n \geqslant 2$ on note $\pi(n)$ l'ensemble des nombres premiers p divisant n.

Pour tous entiers $d \geqslant 2$ et $n \geqslant 2$, on note

$$\sigma(d,n) = \sum_{p\in\pi(n)} d^{n/p}.$$

Dans cette partie on prouve le théorème de Baker :

Théorème. *Pour tout polynôme P de degré $d \geqslant 2$, l'ensemble des entiers $n \geqslant 2$ tels qu'il n'existe aucun z tel que $O(z,P) = n$ est ou bien vide ou bien réduit à un seul élément.*

On établit d'abord une conséquence de la partie I.

1) Soit (U,V) un couple de polynômes complexes non nuls et premiers entre eux. On suppose $\deg(U) > \deg(V)$. Montrer, en utilisant l'inégalité de Mason :

$$\rho(U) + \rho(U-V) \geqslant 1 + \deg(U) - \deg(V).$$

On se donne maintenant un polynôme complexe P non nul de degré $d \geqslant 2$.

2) Soit un entier $n \geqslant 2$ et soit z un point fixe de P_n. Montrer l'équivalence de (i),(ii),(iii).

(i) z est d'ordre n pour P ;
(ii) n ne possède aucun diviseur strict q tel que $P_q(z) = z$;
(iii) il n'existe aucun nombre premier p tel que $P_{n/p}(z) = z$.

3) Soit un entier $n \geqslant 2$. On suppose que P ne possède aucun point d'ordre n.

a) Montrer : $\rho(P_n - X) \leqslant \sum_{p \in \pi(n)} \rho(P_{n/p} - X)$.

b) Montrer : $\rho(P_n - X) \leqslant \sigma(d, n)$.

Dans la suite on raisonne par l'absurde en supposant faux pour P l'énoncé du théorème de Baker. On suppose donc l'existence de deux entiers m et n tels que $2 \leqslant m < n$ et pour lesquels P ne possède ni point d'ordre m ni point d'ordre n. On pose :

$$U = \frac{P_n - X}{R} \text{ et } V = \frac{P_{n-m} - X}{R} \text{ où } R = (P_n - X) \wedge (P_{n-m} - X).$$

4) Montrer à l'aide du **1)** : $\rho(U) + \rho(U - V) \geqslant 1 + d^n - d^{n-m}$.

5) Montrer : $\rho(U) \leqslant \sigma(d, n)$.

6)a) Soit z un élément de $\mathrm{Rac}(P_n - P_{n-m})$. On pose $w = P_{n-m}(z)$.
Montrer : $P_m(w) = w$.

b) Montrer : $\rho(P_n - P_{n-m}) \leqslant d^{n-m}\sigma(d, m)$.

c) Montrer : $\rho(U - V) \leqslant d^{n-m}\sigma(d, m)$.

7) Soit un entier $q \geqslant 2$. On montre dans cette question :

$$\sigma(d, q) \leqslant \begin{cases} d^{q-1} & \text{si} \quad q = 2 \\ d^{q-2} & \text{si} \quad q \geqslant 3 \end{cases}.$$

a) Résoudre le cas $q = 2$.

b) Résoudre les cas $3 \leqslant q \leqslant 5$.

On suppose désormais $q \geqslant 6$.

c) Montrer que l'application $p \mapsto q/p$ est une injection de $\pi(q)$ dans $[1, q/2]$.

d) En déduire : $\sigma(d, q) \leqslant \sum_{0 \leqslant i \leqslant q/2} d^i$.

e) Terminer la preuve.

8) Montrer : $\rho(U) \leqslant d^{n-2}$ et $\rho(U - V) \leqslant d^{n-1}$.

9) Terminer la preuve du théorème de Baker.

*****

FIN