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

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

samedi 11 octobre 2025.

L'énoncé provient dans une très large part du livre :
« Problèmes clefs pour mathématiques supérieures »
Problème 19 p.142 ; année 2009
auteurs : Hervé Gianella, Romain Krust, Franck Taïeb, Nicolas Tosel ,
éditeur : Calvage et Mounet .

*****

Questions préliminaires

1)a) Puisque $\mathbb{C}$ est algébriquement clos, P admet au moins une racine, donc : $\rho(P) \geqslant 1$.

Puisque le produit Q des $X - z$, où z est racine de P, divise P, on a : $\rho(P) \leqslant \deg(P)$.

On a : $\rho(P) = 1$ si et seulement si P est proportionnel à $(X - z)^d$ où $d = \deg(P)$.

On a $\rho(P) = \deg(P)$ si et seulement si P est proportionnel à Q, c'est-à-dire que toutes les racines de P sont simples.

1)b) Puisque tout polynôme est scindé sur $\mathbb{C}$, P est proportionnel au polynôme $\prod_{z \in \mathrm{Rac}(P)} (X-z)^{\mu_P(z)}$. Ainsi $\deg(P) = \sum_{z \in \mathrm{Rac}(P)} \mu_P(z) = \sum_{z \in \mathbb{C}} \mu_P(z)$, puisque $\mu_P(z) = 0$ pour tout z qui n'est pas racine de P.

2) Si $\mathrm{Rac}(P) \cap \mathrm{Rac}(Q)$ n'est pas vide alors il existe z tel $P(z) = 0$ et $Q(z) = 0$; le polynôme $X - z$ divise P et Q donc P et Q ne sont pas premiers entre eux.

Réciproquement si P et Q ne sont pas premiers entre eux alors $P \wedge Q$ n'est pas constant donc possède au moins une racine z puisque le corps de base est $\mathbb{C}$. Alors z est dans $\mathrm{Rac}(P) \cap \mathrm{Rac}(Q)$ qui n'est donc pas vide.

On a prouvé par contraposition les deux implications.

3) Il suffit de considérer trois nombres complexes distincts α, β, γ et $P = (X - \alpha)(X - \beta)$, $Q = (X - \beta)(X - \gamma)$, $R = (X - \gamma)(X - \alpha)$.

*****

Partie I. Inégalité de Mason

1)a) Dire que A et B sont premiers entre eux revient à dire qu'il n'ont aucune racine commune. Mais si z est racine de A et de B, z est aussi racine de C puisque $C(z) = -A(z) - B(z)$, ce qui est contraire à l'hypothèse. Donc A et B sont premiers entre eux. Il en est de même de A et C et de B et C.

1)b) D'après **2a)** les ensembles $\mathrm{Rac}(A)$, $\mathrm{Rac}(B)$ et $\mathrm{Rac}(C)$ sont deux à deux disjoints. Chacun d'eux est inclus dans $\mathrm{Rac}(ABC)$.

Réciproquement si $(ABC)(z) = 0$ le produit $A(z)B(z)C(z)$ est nul donc l'un des termes de ce produit est nul. C'est dire que $\mathrm{Rac}(ABC)$ est inclus dans $\mathrm{Rac}(A) \cup \mathrm{Rac}(B) \cup \mathrm{Rac}(C)$.

2)a) On a $D = AB' - BA' = (-B - C)B' - B(-B' - C') = BC' - CB'$,
puis $BC' - CB' = (-A - C)C' - C(-A' - C') = CA' - AC'$.

2)b) Supposons par l'absurde $D = 0$. Alors $AB' = A'B$.

Puisque A est premier avec B, d'après le théorème de Gauss, il divise A' ce qui n'est possible que si A' est nul donc A est constant. De même B et C sont constants donc $d = 0$ ce qui est contraire à l'hypothèse.

3)a) D'après l'ordre imposé sur (A, B, C), $\deg(A) = d$.

Puisque $A = -(B + C)$, on a $\deg(B + C) = \deg(A) = d$.

D'une part on a $\deg B \leqslant d$; d'autre part, comme $\deg(C) \leqslant \deg(B)$, on a $d = \deg(B + C) \leqslant \deg(B)$; donc $\deg(B) = d$.

3)b) Notons aX^d le terme directeur de A et $cX^{d'}$ celui de C ; a et c sont des complexes non nuls. Alors $D = CA' - AC' = ac(d - d')X^{d+d'-1} + \cdots$.

Si $d' < d$, alors $ac(d - d')$ n'est pas nul et le degré de D est $d + d' - 1$.

Si $d' = d$, alors $ac(d - d') = 0$ et le coefficient de $X^{d+d'-1}$ dans D est nul ; donc le degré de D est au plus $d + d' - 2$.

4)a) Par exemple $A(z) = 0$. Posons $k = \mu_A(z)$. Par hypothèse $k \geqslant 1$.

Par définition $A = (X - z)^k A_1$ où A_1 est un polynôme tel que $A_1(z) \neq 0$.

Puis $D = AB' - BA' = (X - z)^k A_1 B' - (X - z)^k BA_1' - k(X - z)^{k-1} BA_1$.

Ainsi $D = (X - z)^{k-1} D_1$ où $D_1 = -kBA_1 + (X - z)(A_1 B' - BA_1')$.

Comme z n'est racine ni de A_1 ni de B, $D_1(z)$ n'est pas nul.

Donc $\mu_D(z) = \mu_A(z) - 1$.

La preuve est identique pour B et C.

4)b) Notons Z le complémentaire dans $\mathbb{C}$ de $\mathrm{Rac}(ABC)$.

On a $\deg(D) = \sum_{z\in\mathbb{C}} \mu_D(z) = \sum_{z\in Z} \mu_D(z) + \sum_{z\in\mathrm{Rac}(ABC)} \mu_D(z)$.

D'abord $\sum_{z\in Z} \mu_D(z)$ est positif et est nul si et seulement si D ne possède aucune racine autre que celles de A, B ou C.

D'après **1)b)**, on a : $\sum_{z\in\mathrm{Rac}(ABC)} \mu_D(z) = \sum_{z\in\mathrm{Rac}(A)} \mu_D(z) + \sum_{z\in\mathrm{Rac}(B)} \mu_D(z) + \sum_{z\in\mathrm{Rac}(C)} \mu_D(z)$.

Soit P l'un des trois polynômes A, B ou C.

D'après **a)**, on a : $\sum_{z\in\mathrm{Rac}(P)} \mu_D(z) = \sum_{z\in\mathrm{Rac}(P)} (\mu_P(z) - 1) = \deg(P) - \rho(P)$.

Ainsi $\sum_{z\in\mathrm{Rac}(ABC)} \mu_D(z) = 2d + d' - (\rho(A) + \rho(B) + \rho(C))$.

Donc $\deg(D) \geqslant 2d + d' - (\rho(A) + \rho(B) + 1\rho(C))$.

5) En réunissant les résultats de **3)b)** et **4)b)** il vient : $\rho(A)+\rho(B)+\rho(C) \geqslant 2 + d$ si $d' = d$, $1 + d$ si $d' < d$. Donc l'inégalité (R) est toujours vérifiée.

6) Dans la preuve du **4)b)**, on voit que $\deg(D) = 2d + d' - (\rho(A) + \rho(B) + \rho(C))$ si et seulement si D ne possède aucune racine autre que celles de A, B ou C. D'après **3c)** on voit que $\deg(D) = d + d' - 1$ si et seulement si $d' < d$. Ces deux condtions sont nécessaires et suffisantes pour que l'inégalité (R) soit une égalité.

*****

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

1) C'est une conséquence de : $\deg(A + B) < d$.

2) Nécessairement : $A = X - \alpha$ et $B = \beta - X$ où α et β sont distincts puisque A et B n'ont pas de racine commune. Puis $C = \alpha - \beta$.

Réciproquement on a bien ainsi : $d = 1$, $\rho(A) + \rho(B) + \rho(C) = 2 = 1 + d$.

3) On a $A = (X-\alpha)^d$ pour un certain complexe α et $C = \lambda$ pour un certain complexe non nul λ. Donc $B = -(X - \alpha)^d - \lambda$.

Ainsi construits, A, B et C sont premiers entre eux. Donc $1 + d \leqslant \rho(A) + \rho(B) + \rho(C)$.

Mais comme $\rho(B) \leqslant d$, on a $\rho(B) = d$.

On en déduit sans calcul que les racines de B sont simples.

Les solutions sont $((X - \alpha)^d, -(X - \alpha)^d - \lambda, \lambda)$.

4) On a $A = (X-\alpha)^d$ et $B = -(X-\beta)^d$ pour certains α et β distincts.
Donc $C = (X-\beta)^d - (X-\alpha)^d$.
Ainsi construits, A, B et C sont premiers entre eux.
Donc $1+d \leqslant \rho(A)+\rho(B)+\rho(C)$, donc $\rho(C) \leqslant d-1$, mais comme $\deg(C) \leqslant d-1$ on a $\rho(C) = d-1$.
On en déduit sans calcul que les racines de C sont simples.
Les solutions sont $((X-\alpha)^d, -(X-\beta)^d, (X-\beta)^d - (X-\alpha)^d)$.

5) Si $d = 2$ il faut $\rho(A)+\rho(B)+\rho(C) = 3$, donc :

- ou bien $\rho(A) = \rho(B) = \rho(C) = 1$ et on retrouve le **4)** : $(A = (X-\alpha)^2, B = -(X-\beta)^2, C = (X-\beta)^2 - (X-\alpha)^2)(\alpha \neq \beta)$;
- ou bien, puisque $\rho(A) \leqslant \rho(B)$, $\rho(A) = 1$, $\rho(B) = 2, \rho(C) = 0$ et on retrouve le **3)** : $(A = (X-\alpha)^2, B = -(X-\alpha)^2 - \lambda, \lambda)$; $(\lambda \neq 0)$.

6)a) On a $\deg(C) = 1$ donc $\rho(C) = 1$ et il existe un complexe γ et un complexe non nul λ tel que $C = \lambda(X-\gamma)$.
Il existe un complexe α différent de γ tel que $A = (X-\alpha)^d$.
Donc $-B = (X-\alpha)^d + \lambda(X-\gamma)$.

6)b) On a $\rho(B) = d-1$. Donc B admet une racine double β autre que α et γ et $d-2$ racines simples autres que α, β et γ.
Calculons β ; on a $B(\beta) = 0$ et $B'(\beta) = 0$.
Donc : $(\beta-\alpha)^d = -\lambda(\beta-\gamma)$ et $d(\beta-\alpha)^{d-1} = -\lambda$, puis : $\beta = \frac{d\gamma-\alpha}{d-1}$.
On vérifie bien que $\beta \neq \alpha$ et que $\beta \neq \gamma$. En effet : $\beta-\alpha = \frac{d(\gamma-\alpha)}{d-1}$ et $\beta = \frac{\gamma-\alpha}{d-1}$.

6)c) Ainsi $A = (X-\alpha)^d$, $C = \lambda(X-\gamma)$, $B = -A-C = -\left(X - \frac{d\gamma-\alpha}{d-1}\right)^2 B_1$ où B_1 est unitaire et toutes les racines de B_1 sont simples.

7)a) On a $\rho(A)+\rho(B)+\rho(C) = 4$, $\rho(A) = 2$, $\rho(C) = 0$, donc $\rho(B) = 2$.
Donc pour certains α_1, α_2, β_1, β_2 distincts on a $A = (X-\alpha_1)^2(X-\alpha_2)$ et $B = -(X-\beta_1)^2(X-\beta_2)$ et $C = \lambda$ pour un certain $\lambda \neq 0$.

7)b) On a $A = (X-\mu-\delta)^2(X-\mu-\alpha')$ et $B = -(X-\mu+\delta)^2(X-\mu-\beta')$.
On développe :
$A+B = (X-\mu)^2(\beta'-\alpha'-4\delta) + 2\delta(\alpha'+\beta')(X-\mu) + \delta^2(\beta'-\alpha') = -\lambda$.
On en tire : $\beta'-\alpha'-4\delta = 0$, $\beta'+\alpha' = 0$ (car $\delta \neq 0$) et $\lambda = -\delta^2(\beta'-\alpha')$.
Finalement $\beta' = 2\delta$, $\alpha' = -2\delta$, et $\lambda = -4\delta^3$.

7)c) On obtient les solutions :
$A = (X-\mu-\delta)^2(X-\mu+2\delta)$, $B = -(X-\mu+\delta)^2(X-\mu-2\delta)$, $C = -4\delta^3$, où $\delta \neq 0$.

8) On a $\rho(A)+\rho(B)+\rho(C)=4$.
Nous avons quatre possibilités :

- $(\rho(A),\rho(B),\rho(C))=(1,3,0)$: on retrouve le **3** ;
- $(\rho(A),\rho(B),\rho(C))=(1,1,2)$: on retrouve le **4** ;
- $(\rho(A),\rho(B),\rho(C))=(1,2,1)$: on retrouve le **6** ;
- $(\rho(A),\rho(B),\rho(C))=(2,2,0)$: on retrouve le **7**.

*****

Partie III. Une application

1) On raisonne par l'absurde et on se donne une solution (A,B,C) non triviale où (A,B,C) sont premiers entre eux dans leur ensemble. Notons $d=\max(\deg(A),\deg(B),\deg(C)$. Si $d=0$, alors (A,B,C) est une solution triviale de (F) ce qui est contraire à l'hypothèse.

On a $\rho(P^m)=\rho(P)$ pour tout polynôme P non constant.

Comme A, B et C n'ont aucune racine commune, il en est de même pour A^m, B^m et C^m. On a : $\max(\deg(A^m),\deg(B^m),\deg(C^m))=md$.

Ainsi le triplet (A^m,B^m,C^m) est un élément de $\mathcal{T}_{md}$. D'après l'inégalité de Mason, $\rho(A)+\rho(B)+\rho(C)\geqslant 1+md$.

A fortiori, puisque $\rho(P)\leqslant d$ si P est l'un de A, B ou C, on a $3d\geqslant 1+md$ puis $3>m$. C'est contradictoire.

2) On se ramène au cas précédent. Soit (A,B,C) une solution non triviale de (E). Notons R le PGCD de A, B, C. On a $A=RA_1$, $B=RB_1$, $C=RC_1$ où A_1, B_1, C_1 sont premiers entre eux dans leur ensemble et vérifient $A_1+B_1+C_1=0$. D'après le **1)** nécessairement A_1, B_1 et C_1 sont des constantes non nulles λ, μ et ν et $A=\lambda R$, $B=\mu R$, $C=\nu R$, donc (A,B,C) est une solution triviale de (E), ce qui est contraire à l'hypothèse.

*****

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

1) On a pour tout z de $\mathbb{C}$: $(P\circ Q)(z)=\sum_{j=1}^{n}a_jQ(z)^j=P(Q(z)$.

Si R est un polynôme tel que $R(z)=P(Q(z))$ pour tout z alors $R-P\circ Q$ admet une infinité de racines et est donc le polynôme nul.

2) D'après la définition donnée en préambule : $X\circ Q=Q$ et $P\circ X=P$.

3) Pour tout z de $\mathbb{C}$, on a : $((P\circ Q)\circ R)(z)=(P\circ Q)(R(z))=P(Q(R(z)))$
et : $(P(Q\circ R))(z)=P((Q\circ R)(z))=P(Q(R(z)))$,
donc $(P\circ Q)\circ R=P\circ(Q\circ R)$.

4) On a : $P_0 \circ P_m = P_m$; $P_1 \circ P_m = P_{m+1}$. Soit $n \geqslant 1$; supposons établi $P_n \circ P_m = P_{n+m}$. Il vient :

$P_{n+1} \circ P_m = (P_1 \circ P_n) \circ P_m = P_1 \circ (P_n \circ P_m) = P_1 \circ (P_{n+m}) = P_{n+m+1}$.

5)a) Les termes directeurs de P et Q étant respectivement aX^d et $a'X^{d'}$ celui de $P \circ Q$ est $a(a')^d X^{dd'}$. Donc le degré de $P \circ Q$ est le produit de ceux de P et de Q.

5)b) De **a)** on déduit par récurrence $\deg(P_n) = d^n$ où $d = \deg(P)$.

6)a) On montre par récurrence sur l'entier $k \geqslant 0$ que $P_{km}(z) = z$ pour tout k. C'est vrai pour $k = 1$. Si c'est vrai pour un $k \geqslant 1$ alors $P_{(k+1)m}(z) = P_m(P_{km}(z)) = P_m(z) = z$. Donc si m divise n, z est un point fixe de P_n.

Réciproquement soit un entier n positif. Supposons que z soit un point fixe de P_n. Effectuons la division euclidienne de n par m : $n = km + r$ où $0 \leqslant r < m$. Puis $z = P_n(z) = P_r(P_{km}(z)) = P_r(z)$. Ainsi z est un point fixe de P_r, donc $r = 0$ d'après la définition de $O(z, P)$. Ainsi m divise n.

6)b) On a pour tout n : $P_{n+m}(z) = P_n(P_m(z)) = P_n(z)$. Donc m est une période de la suite $(P_n(z))$. Si q est une période de la suite $(P_n(z)$, alors $P_q(z) = z$ donc m divise q.

7) Puisque $\deg(P) = d \geqslant 2$, $P - X$ admet au moins une racine z qui est un point d'ordre 1.

8a) Les points fixes de P sont les z tels que $z^2 - z - a = 0$. Il y en a deux distincts sauf si le discriminant $1 + 4a$ est nul, c'est-à-dire $a = -1/4$, et dans ce cas le point fixe est $1/2$.

8b) On cherche les solutions de

$$u^2 - a = v\,;\; v^2 - a = u\,;\; v \neq u.$$

Par différence puis division par $v - u$ il vient :

$$u + v = -1$$

et u et v sont les racines de $X^2 + X - a - 1$. Pour $a \neq -5/4$ le système en question admet deux solutions (u, v) et (v, u). Pour $a = -5/4$ ce système n'admet aucune solution car $X^2 + X + \frac{1}{4}$ admet une racine unique $-1/2$.

La seule valeur de a pour laquelle P n'admet aucun point d'ordre deux est $a_0 = -5/4$.

*****

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

1) On a $A+B+C=0$ où $A=U-V$, $B=-U$, $C=V$. Toute racine commune à (A,B,C) est racine de U et de V donc A,B,C sont premiers entre eux dans leur ensemble. De plus $d=\deg(U)>\deg(V)=d'\geqslant 0$. On en déduit $\deg(U)=\deg(U-V)=d$. On a d'après l'inégalité de Mason : $\rho(U)+\rho(U-V)\geqslant 1+d-\rho(V)$ et puisque $\rho(V)\leqslant\deg(V)$ on a a fortiori : $\rho(U)+\rho(U-V)\geqslant 1+\deg(U)-\deg(V)$.

2) Posons $m=O(z,n)$. Ou bien $m=n$ ou bien m est un diviseur strict de n tel que $P_m(z)=z$. Donc (i) équivaut à (ii).

Si p est un nombre premier tel que $P_{n/p}(z)=z$ alors $q=n/p$ est un diviseur strict de n tel que $P_q(z)=z$, donc (ii) implique (iii).

Si q est un diviseur strict de n tel que $P_q(z)=z$ alors n/q est un entier strictement supérieur à 1 ; il possède donc un diviseur premier p et n/p est un diviseur strict de n tel que $P_{n/p}(z)=z$, donc (iii) implique (ii).

3a) Soit z une racine de P_n-X. D'après le **2)**, puisque z n'est pas d'ordre n pour P, il existe un nombre premier p tel que z est une racine de $P_{n/p}-X$. Donc $\mathrm{Rac}(P_n-X)$ est inclus dans la réunion des $\mathrm{Rac}(P_{n/p}-X)$ où p parcourt l'ensemble $\pi(n)$ des nombres premiers divisant n. Il en résulte que $\rho(P_n-X)$ est majoré par $\sum_{p\in\pi(n)}\rho(P_{n/p}-X)$.

3b) $\rho(P_{n/p}-X)\leqslant\deg(P_{n/p}-X)=\deg(P_{n/p})=d^{n/p}$.
Donc $\rho(P_n-X)\leqslant\sigma(d,n)$.

4) On a $\deg(U)=d^n-\deg(\Delta)$; $\deg(V)=d^{n-m}-\deg(\Delta)<\deg(U)$. Le **1)** s'applique et donne : $\rho(U)+\rho(U-V)\geqslant 1+d^n-d^{n-m}$.

5) On a $\mathrm{Rac}(U)\subset\mathrm{Rac}(P_n-X)$ donc $\rho(U)\leqslant\rho(P_n-X)$ et on applique le **3)b** .

6)a) On a : $P_n(z)=P_{n-m}(z)=w$, et $P_n(z)=P_m(P_{n-m}(z))=P_m(w)$ donc $P_m(w)=w$.

6)b) Puisque P n'a pas d'élément d'ordre m on a : $\rho(P_m-X)\leqslant\sigma(d,m)$. Il y a donc au plus $\sigma(d,m)$ complexes w tels que $P_m(w)=w$. Pour tout w il y a au plus d^{n-m} complexes z tels que $P_{n-m}(z)=w$. Donc : $\rho(P_n-P_{n-m})\leqslant d^{n-m}\sigma(d,m)$.

6)c) On a $\mathrm{Rac}(U-V)\subset\mathrm{Rac}P_n-P_{n-m})$ donc $\rho(U-V)\leqslant\rho(P_n-P_{n-m})$ et on applique le **b)** : $\rho(U-V)\leqslant d^{n-m}\sigma(d,m)$.

7a) $\sigma(d,2)=d^{2/2}=d^{2-1}\leqslant d^{2-1}$.

7)b) $\sigma(d,3) = d^{3/3} = d \leqslant d^{3-2}$.
$\sigma(d,4) = d^{4/2} = d^2 \leqslant d^{4-2}$.
$\sigma(d,5) = d^{5/5} = d^1 \leqslant d^{5-2}$.

7)c) Tous les q/p où $p \in \pi(n)$ sont des entiers distincts compris entre 1 et $q/2$.

7)d) C'est une conséquence immédiate de ce qui précède.

7)e) Soit q_1 la partie entière de $q/2$. On majore $\sigma(d,q)$ par $\frac{d^{q_1+1}-1}{d-1} < d^{q_1+1} \leqslant d^{q/2+1}$. Mais $q/2+1 \leqslant q-2$ si $q \geqslant 6$. La preuve est complète.

8) Comme $n > m \geqslant 2$, $n \geqslant 3$ donc $\sigma(d,n) \leqslant d^{n-2}$, donc, d'après **5)**, $\rho(U) \leqslant d^{n-2}$.
Comme $m \geqslant 2$ on a $\sigma(d,m) \leqslant d^{m-1}$ donc d'après **6)**, $\rho(U-V) \leqslant d^{n-1}$.

9) D'après **8)** et **4)**,
on a : $1 + d^n - d^{n-m} \leqslant \rho(U) + \rho(U-V) \leqslant d^{n-1} + d^{n-2}$,
donc : $1 + d^n \leqslant d^{n-1} + d^{n-2} + d^{n-m}$,
puis : $1 + d^n \leqslant d^{n-1} + 2d^{n-2} \leqslant 2d^{n-1} \leqslant d^n$.

Contradiction.

*****

FIN