SESSION 2020

Concours commun Centrale

MATHÉMATIQUES 1. FILIERE MP

I - Quelques résultats utiles

I.A - Propriétés générales de la loi $*$

Q 1. Soit $f \in \mathbb{A}$. Pour $n \in \mathbb{N}^*$, puisque 1 divise n,

$$\delta * f(n) = \sum_{d|n} \delta(d) f\left(\frac{n}{d}\right) = \delta(1) f\left(\frac{n}{1}\right) = f(n)$$

et donc $\delta * f = f$. De même, pour $n \in \mathbb{N}^*$, puisque n divise n,

$$f * \delta(n) = \sum_{d|n} f(d) \delta\left(\frac{n}{d}\right) = f(n)\delta\left(\frac{n}{n}\right) = f(n)$$

et donc $f * \delta = f$. On a montré que δ est élément neutre de $\mathbb{A}$ pour $*$.

Q 2. Soit $(f, g) \in \mathbb{A}^2$. Pour $n \in \mathbb{N}^*$, en posant $d_2 = \dfrac{d_1}{n}$, on obtient

$$f * g(n) = \sum_{\substack{d_1=1 \\ d_1|n}}^{n} f(d_1) g\left(\frac{n}{d_1}\right) = \sum_{(d_1,d_2) \in (\mathbb{N}^*)^2,\ d_1 d_2 = n} f(d_1) g(d_2) = \sum_{(d_1,d_2) \in \mathscr{C}_n} f(d_1) g(d_2).$$

Q 3. Soit $(f, g) \in \mathbb{A}^2$. Pour $n \in \mathbb{N}^*$, en posant $d_1' = d_2$ et $d_2' = d_1$ de sorte que (d_1, d_2) décrit $\mathscr{C}_n$ si et seulement si (d_1', d_2') décrit $\mathscr{C}_n$,

$$f * g(n) = \sum_{(d_1,d_2) \in \mathscr{C}_n} f(d_1) g(d_2) = \sum_{(d_1',d_2') \in \mathscr{C}_n} g(d_1') f(d_2') = g * f(n)$$

et donc $f * g = g * f$. Donc, $*$ est commutative dans $\mathbb{A}$.

Q 4. Soit $(f, g, h) \in \mathbb{A}^3$. Pour $n \in \mathbb{N}^*$,

$$\begin{aligned}
((f * g) * h)(n) &= \sum_{(d,d_3) \in (\mathbb{N}^*)^2,\ d d_3 = n} (f * g)(d) h(d_3) = \sum_{(d,d_3) \in (\mathbb{N}^*)^2,\ d d_3 = n} \left(\sum_{(d_1,d_2) \in (\mathbb{N}^*)^2,\ d_1 d_2 = d} f(d_1) g(d_2) \right) h(d_3) \\
&= \sum_{(d_1,d_2,d_3) \in (\mathbb{N}^*)^3,\ d_1 d_2 d_3 = n} f(d_1) g(d_2) h(d_3) = \sum_{(d_1,d_2,d_3) \in \mathscr{C}_n'} f(d_1) g(d_2) h(d_3).
\end{aligned}$$

Cette égalité étant vraie pour tout $(f, g, h) \in \mathbb{A}^3$ et tout $n \in \mathbb{N}^*$ et la loi $*$ étant commutative, on a aussi

$$\begin{aligned}
(f * (g * h))(n) = ((g * h) * f)(n) &= \sum_{(d_1,d_2,d_3) \in \mathscr{C}_n'} g(d_1) h(d_2) f(d_3) = \sum_{(d_1',d_2',d_3') \in \mathscr{C}_n'} f(d_1') g(d_2') h(d_3') \\
&= ((f * g) * h)(n).
\end{aligned}$$

Ainsi, pour tout $(f, g, h) \in \mathbb{A}^3$, $(f * g) * h = f * (g * h)$. $*$ est associative dans $\mathbb{A}$.

Q 5. On sait que $(\mathbb{A}, +, .)$ est un $\mathbb{C}$-espace vectoriel. En particulier, $(\mathbb{A}, +)$ est un groupe commutatif. Ensuite, $*$ est une loi interne dans $\mathbb{A}$, $*$ est associative et possède un élément neutre à savoir δ.

Vérifions que $*$ est distributive sur $+$. Soit $(f, g, h) \in \mathbb{A}^3$. Pour $n \in \mathbb{N}^*$,

$$\begin{aligned}((f+g)*h)(n) &= \sum_{(d_1,d_2)\in\mathscr{C}_n} (f+g)(d_1)\,h(d_2) = \sum_{(d_1,d_2)\in\mathscr{C}_n} f(d_1)\,h(d_2) + \sum_{(d_1,d_2)\in\mathscr{C}_n} g(d_1)\,h(d_2)\\ &= (f*h+g*h)(n)\end{aligned}$$

et donc $(f+g)*h = f*h+g*h$. Puisque $*$ est commutative, cette égalité valable pour tout $(f,g,h)\in\mathbb{A}^3$, suffit pour prouver que $*$ est distributive sur $+$. Donc, $(\mathbb{A},+,*)$ est un anneau. Enfin, puisque $*$ est commutative, $(\mathbb{A},+,*)$ est un anneau commutatif.

I.B - Groupe des fonctions multiplicatives

Q 6. Soient f et g deux fonctions multiplicatives telles que : $\forall p\in\mathscr{P}$, $\forall k\in\mathbb{N}^*$, $f\left(p^k\right)=g\left(p^k\right)$.

$1\wedge 1=1$ et donc $f(1)=f(1\times 1)=f(1)\times f(1)$ puis $f(1)=1$ car $f(1)\neq 0$. De même, $g(1)=1$ et finalement, $f(1)=g(1)=1$.

Soit $n\geqslant 2$. D'après le théorème fondamental de l'arithmétique, n s'écrit de manière unique sous la forme $n=p_1^{\alpha_1}\dots p_k^{\alpha_k}$ où les p_i, $1\leqslant i\leqslant k$, sont des éléments deux à deux distincts de $\mathscr{P}$ et les α_i, $1\leqslant i\leqslant k$, sont des entiers naturels non nuls (décomposition primaire de n). Si $k\geqslant 2$, puisque f est multiplicative et que $\left(p_1^{\alpha_1}\dots p_{k-1}^{\alpha_{k-1}}\right)\wedge p_k^{\alpha_k}=1$ (car ces deux entiers sont sans facteurs premiers commun), $f\left(p_1^{\alpha_1}\dots p_{k-1}^{\alpha_{k-1}}p_k^{\alpha_k}\right)=f\left(p_1^{\alpha_1}\dots p_{k-1}^{\alpha_{k-1}}\right)f\left(p_k^{\alpha_k}\right)$ puis, par récurrence sur k,

$$f(n)=f\left(p_1^{\alpha_1}\dots p_k^{\alpha_k}\right)=\prod_{i=1}^{k} f\left(p_i^{\alpha_i}\right)$$

ce qui reste vrai quand $k=1$. Mais alors, pour tout $n\geqslant 2$,

$$f(n)=\prod_{i=1}^{k} f\left(p_i^{\alpha_i}\right)=\prod_{i=1}^{k} g\left(p_i^{\alpha_i}\right)=g(n)$$

et donc $f=g$. Ainsi, deux fonctions multiplicatives qui coïncident sur l'ensemble des nombres primaires sont égales.

Q 7. Soient n et m deux entiers naturels non nuls et premiers entre eux.

Soit $(d_1,d_2)\in\mathscr{D}_n\times\mathscr{D}_m$. Donc, il existe $(q_1,q_2)\in(\mathbb{N}^*)^2$ tel que $n=q_1d_1$ et $m=q_2d_2$. Mais alors, $nm=(q_1q_2)(d_1d_2)$ avec $(q_1q_2)\in\mathbb{N}^*$. Donc, $d_1d_2\in\mathscr{D}_{nm}$. Ceci montre que π est bien une application de $\mathscr{D}_n\times\mathscr{D}_m$ vers $\mathscr{D}_{nm}$.

Vérifions que π est injective. Soit $((d_1,d_2),(d_1',d_2'))\in(\mathscr{D}_n\times\mathscr{D}_m)^2$ tel que $\pi(d_1,d_2)=\pi(d_1',d_2')$ ou encore tel que $d_1d_2=d_1'd_2'$. d_1 divise n, d_2' divise m et n et m sont premiers entre eux. Donc, d_1 et d_2' sont premiers entre eux. Ainsi, d_1 divise $d_1d_2=d_1'd_2'$ et d_1 est premier à d_2'. D'après le théorème de Gauss, d_1 divise d_1'. De même, d_1' divise d_1. Puisque d_1 et d_1' sont des entiers naturels, on en déduit que $d_1=d_1'$ puis, après simplification, que $d_2=d_2'$. En résumé, pour tout $((d_1,d_2),(d_1',d_2'))\in(\mathscr{D}_n\times\mathscr{D}_m)^2$, $\pi(d_1,d_2)=\pi(d_1',d_2')\Rightarrow(d_1,d_2)=(d_1',d_2')$. Ceci montre que π est injective.

Vérifions que π est surjective. Soit d un diviseur de nm. Si $d=1$, alors $d=1\times 1=\pi(1,1)$ où on a bien $(1,1)\in\mathscr{D}_n\times\mathscr{D}_m$. Si $n=1$, d est un diviseur de m puis $d=\pi(1,d)$ où on a bien $(1,d)\in\mathscr{D}_n\times\mathscr{D}_m$. De même, si $m=1$, $d=\pi(d,1)$. Dorénavant, $d\geqslant 2$, $n\geqslant 2$ et $m\geqslant 2$. d s'écrit sous la forme $d=p_1^{\alpha_1}\dots p_k^{\alpha}$ où les p_i sont des nombres premiers deux à deux distincts et les α_i sont des entiers naturels non nuls. Chaque nombre premier p_i divise nm et donc divise n ou m. Puisque n et m sont sans facteur premier commun, on peut écrire $[\![1,k]\!]=I\cup J$ où $I=\{i\in[\![1,k]\!]/\ p_i|n\}$ et $J=\{i\in[\![1,k]\!]/\ p_i|m\}$ avec $I\cap J=\varnothing$ (et $I\neq\varnothing$ et $J\neq\varnothing$). $d_1=\prod_{i\in I}p_i^{\alpha_i}$ divise d et donc nm et est premier à m. Donc, d_1 divise n. De même, $d_2=\prod_{i\in J}p_i^{\alpha_i}$ divise m. Enfin, $d_1d_2=d$. Ainsi, pour tout $d\in\mathscr{D}_{nm}$, il existe $(d_1,d_2)\in\mathscr{D}_n\times\mathscr{D}_m$ tel que $\pi(d_1,d_2)=d$. Ceci montre que π est surjective.

Finalement, π est une bijection de $\mathscr{D}_n\times\mathscr{D}_m$ sur $\mathscr{D}_{nm}$.

Q 8. Soient f et g deux fonctions multiplicatives. $f*g(1)=\sum_{d|1}f(d)g\left(\dfrac{1}{d}\right)=f(1)g(1)\neq 0$. Soit alors $(n,m)\in(\mathbb{N}^*)^2$ tel que $n\wedge m=1$.

$$\begin{aligned}
f*g(mn) &= \sum_{(d,d')\in\mathscr{C}_{nm}} f(d)\,g(d') \\
&= \sum_{\substack{((d_1,d_2),(d'_1,d'_2))\in(\mathscr{D}_n\times\mathscr{D}_m)^2,\\ d_1d_2d'_1d'_2=nm}} f(d_1d_2)\,g(d'_1d'_2)\ \text{(car } \pi \text{ est bijective)} \\
&= \sum_{\substack{((d_1,d_2),(d'_1,d'_2))\in(\mathscr{D}_n\times\mathscr{D}_m)^2,\\ d_1d_2d'_1d'_2=nm}} f(d_1)\,f(d_2)\,g(d'_1)\,(d'_2)\ \text{(car } d_1\wedge d_2=1 \text{ et } d'_1\wedge d'_2=1).
\end{aligned}$$

Maintenant, si $d_1d_2d'_1d'_2 = nm$, alors $d_1d'_1$ divise nm et est premier à m (car d_1 et d'_1 sont des diviseurs de n et $n\wedge m = 1$). Donc, $d_1d'_1$ divise n et de même $d_2d'_2$ divise m. En posant $n = d_1d'_1q_1$ et $m = d_2d'_2q_2$ où $(q_1, q_2) \in (\mathbb{N}^*)^2$, on a

$$nm = d_1d'_1q_1d_2d'_2q_2 = nmq_1q_2$$

puis $q_1q_2 = 1$. On sait que ceci impose $q_1 = q_2 = 1$ et donc $d_1d'_1 = n$ et $d_2d'_2 = m$. Ainsi,

$$\begin{aligned}
f*g(mn) &= \sum_{((d_1,d'_1),(d_2,d'_2))\in\mathscr{C}_n\times\mathscr{C}_m} f(d_1)\,f(d_2)\,g(d'_1)\,(d'_2) \\
&= \left(\sum_{(d_1,d'_1)\in\mathscr{C}_n} f(d_1)\,g(d'_1)\right)\left(\sum_{(d_2,d'_2)\in\mathscr{C}_m} f(d_2)\,g(d'_2)\right) \\
&= ((f*g)(m))\times((f*g)(n)).
\end{aligned}$$

Donc, $f*g$ est multiplicative.

Q 9. Les égalités de l'énoncé définissent par récurrence une fonction g sur l'ensemble des nombres primaires p^k, $p\in\mathscr{P}$, $k\in\mathbb{N}^*$. On pose de plus $g(1) = 1$ et pour $n \geqslant 2$, si la décomposition primaire de n s'écrit $n = p_1^{\alpha_1}\dots p_k^{\alpha_k}$, on pose $g(n) = \prod_{i=1}^{k} g(p_i^{\alpha_i})$. On obtient une fonction g de $\mathbb{N}^*$ dans $\mathbb{C}$.
Soient alors n et m deux entiers naturels premiers entre eux. Si $n = 1$, $g(nm) = g(1\times m) = g(m) = g(1)g(m) = g(n)g(m)$.
De même, si $m = 1$, $g(nm) = g(n)g(m)$.
Si $n \geqslant 2$ et $m \geqslant 2$, on peut considérer les décompositions primaires de n et m : $n = p_1^{\alpha_1}\dots p_k^{\alpha_k}$ et $m = q_1^{\beta_1}\dots q_l^{\beta_l}$. Puisque n et m sont premiers entre eux, $\{p_1,\dots,p_k\}\cap\{q_1,\dots,q_l\} = \varnothing$. Par suite,

$$g(nm) = g(p_1^{\alpha_1})\dots g(p_k^{\alpha_k})\,g\left(q_1^{\beta_1}\right)\dots g\left(q_l^{\beta_l}\right) = g(n)g(m).$$

La fonction g ainsi définie est multiplicative.

Ensuite, $f*g(1) = \sum_{d|1} f(d)g\left(\dfrac{d}{1}\right) = f(1)g(1) = 1$. Soit maintenant $p\in\mathscr{P}$. Montrons que pour tout $k\in\mathbb{N}^*$, $(f*g)\left(p^k\right) = 0$.

Soit $k \geqslant 1$. Les diviseurs de p^k sont les p^i, $0 \leqslant i \leqslant k$. Donc

$$\begin{aligned}
(f*g)\left(p^k\right) &= \sum_{i=0}^{k} f\left(p^i\right) g\left(p^{k-i}\right) = g\left(p^k\right) + \sum_{i=1}^{k} f\left(p^i\right) g\left(p^{k-i}\right) \\
&= -\sum_{i=1}^{k} f\left(p^i\right) g\left(p^{k-i}\right) + \sum_{i=1}^{k} f\left(p^i\right) g\left(p^{k-i}\right) = 0.
\end{aligned}$$

On a montré que pour tout $k\in\mathbb{N}^*$, $(f*g)\left(p^k\right) = 0 = \delta\left(p^k\right)$.

On sait que la fonction $f*g$ est multiplicative d'après la question Q8. Vérifions que δ est multiplicative. On a déjà $\delta(1) = 1$.

Soient n et m deux entiers naturels non nuls. Si $n = m = 1$, $\delta(nm) = 1 = \delta(n)\delta(m)$ et si $n \geqslant 2$ ou $m \geqslant 2$, alors $nm \geqslant 2$ puis $\delta(nm) = 0 = \delta(n)\delta(m)$. Donc, pour tout $(n, m) \in (\mathbb{N}^*)^2$, $\delta(nm) = \delta(n)\delta(m)$. En particulier, la fonction δ est multiplicative.

Ainsi, $f * g$ et δ sont deux fonctions multiplicatives coïncidant sur l'ensemble des nombres primaires. D'après la question Q6, $f * g = \delta$.

Q 10. La question Q8 montre que $*$ est une loi interne dans $\mathbb{M}$. Les questions Q2 et Q3 montrent que $*$ est commutative et associative dans $\mathbb{M}$. Puisque $\delta \in \mathbb{M}$, la question Q1 montre que δ est élément neutre pour $*$ dans $\mathbb{M}$. Enfin, la question précédente montre que tout élément de $\mathbb{M}$ admet un symétrique pour $*$ dans $\mathbb{M}$. Finalement, $(\mathbb{M}, *)$ est un groupe commutatif.

I.C - La fonction de MÖBIUS

Q 11. On a déjà $\mu(1) = 1$. Soient n et m deux entiers naturels non nuls et premiers entre eux.
Si $n = 1$, on a $\mu(nm) = \mu(m) = \mu(n)\mu(m)$. De même, si $m = 1$, on a $\mu(nm) = \mu(n)\mu(m)$. Si n et m sont tous deux supérieurs ou égaux à 2, on peut considérer les décompositions primaires de n et m : $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ et $m = q_1^{\beta_1} \dots q_l^{\beta_l}$ avec $\{p_1, \dots, p_k\} \cap \{q_1, \dots, q_l\} = \varnothing$.
Si n et m sont sans facteur carré ($\alpha_1 = \dots = \alpha_k = \beta_1 = \dots = \beta_l = 1$),

$$\mu(mn) = \mu(p_1 \dots p_k q_1 \dots q_l) = (-1)^{k+l} = (-1)^k (-1)^l = \mu(n)\mu(m).$$

Si n ou m contient un facteur carré (l'un des α_i ou l'un des β_j est supérieur ou égal à 2), il en est de même de nm et dans ce cas,

$$\mu(nm) = 0 = \mu(n)\mu(m).$$

On a montré que la fonction μ est multiplicative.

Q 12. $(\mu * 1)(1) = \mu(1) = 1$. Ensuite, pour $n \geqslant 2$, en considérant la décomposition primaire de n : $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $(\mu * 1)(n) = \sum_{d|n} \mu(d)$. Dans cette somme, si d contient au moins un facteur carré, le terme correspondant est nul. Il ne reste que les termes $\mu(1)$ et les $\mu(p_{i_1} \dots p_{i_l}) = (-1)^l$ avec $1 \leqslant l \leqslant k$ et $1 \leqslant i_1 < \dots < i_l \leqslant k$. Pour $l \in [\![1, k]\!]$, il y a $\binom{k}{l}$ parties à l éléments de $[\![1, k]\!]$ ou encore $\binom{k}{l}$ l-uplets $(i_1, \dots, i_l)$ tels que $i_1 < \dots < i_l$. Donc, d'après la formule du binôme de NEWTON,

$$(\mu * 1)(n) = 1 + \sum_{l=1}^{k} \binom{k}{l} (-1)^l = (1 - 1)^k = 0 \text{ (car } k \geqslant 1).$$

On a montré que $\mu * 1 = \delta$. Ceci montre que le symétrique de 1 pour $*$ est μ.

Q 13.

$$\forall n \in \mathbb{N}^*,\ F(n) = \sum_{d|n} f(d) \Leftrightarrow F = f * 1 \Leftrightarrow F * \mu = f \text{ (car } (\mathbb{M}, *) \text{ est un groupe)}$$
$$\Leftrightarrow \forall n \in \mathbb{N}^*,\ f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Q 14. Pour tout $n \in \mathbb{N}^*$, $(\varphi * 1)(n) = \sum_{d|n} \varphi(d) = n$ (formule connue) et donc $\varphi * 1 = I$. Mais alors, $\varphi = \mu * I$ puisque $(\mathbb{M}, *)$ est un groupe et que μ est le symétrique de 1 pour $*$.

I.D - Déterminant de SMITH

Q 15. Soit $(i, j) \in [\![1, n]\!]^2$. Le coefficient ligne i, colonne j, de $M'D^T$ est

$$\sum_{k=1}^{n} m'_{i,k} d_{j,k} = \sum_{d|j} m'_{i,d}.$$

Dans cette somme, si d ne divise pas i, $m'_{i,d} = 0$ et si i divise d, $m'_{i,d} = g(d)$. Puisque les diviseurs communs aux entiers i et j sont les diviseurs de leur PGCD $i \wedge j$, le coefficient ligne i, colonne j, de $M'D^T$ est

$$\sum_{d|i\wedge j} g(d) = (g * 1)(i \wedge j) = f(i \wedge j) = m_{i,j},$$

car $g = f * \mu \Leftrightarrow f = g * 1$. On a montré que $M = M'D^T$.

Q 16. Donc, $\det(M) = \det(M') \times \det\left(D^T\right)$.

$\det(M') = \displaystyle\sum_{\sigma\in\mathscr{S}_n} \varepsilon(\sigma) m_{\sigma(1),1} \dots m_{\sigma(n),n}$. Dans cette somme, un terme est nul si et seulement si il existe $i \in [\![1, n]\!]$ tel que i ne divise pas $\sigma(i)$. Il ne reste donc que les termes tels que pour tout $i \in [\![1, n]\!]$, i divise $\sigma(i)$ et en particulier $i \leqslant \sigma(i)$. Ceci impose par récurrence descendante sur i que pour tout $i \in [\![1, n]\!]$, $\sigma(i) = i$ et donc $\sigma = Id_{[\![1,n]\!]}$. Il reste

$$\det(M') = \varepsilon(Id) m_{1,1} \dots m_{n,n} = \prod_{k=1}^{n} g(k).$$

Avec le même raisonnement,

$$\det\left(D^T\right) = \det(D) = d_{1,1} \dots d_{n,n} = 1.$$

Finalement,

$$\det(M) = \prod_{k=1}^{n} g(k).$$

***I.E - Séries de* DIRICHLET**

Q 17. Soit $s > A_c(f)$. Il existe $s' \in \left\{t \in \mathbb{R}/ \text{ la série } \sum \dfrac{f(k)}{k^t} \text{ converge absolument}\right\}$ tel que $A_c(f) \leqslant s' < s$. Pour tout $k \in \mathbb{N}^*$, on a $k^{s'} \leqslant k^s$ puis

$$\left|\frac{f(k)}{k^s}\right| = \frac{|f(k)|}{k^s} \leqslant \frac{|f(k)|}{k^{s'}} = \left|\frac{f(k)}{k^{s'}}\right|.$$

Puisque la série numérique de terme général $\dfrac{f(k)}{k^{s'}}$, $k \in \mathbb{N}^*$, converge absolument, il en est de même de la série de terme général $\dfrac{f(k)}{k^s}$, $k \in \mathbb{N}^*$.

Q 18. Posons $h = g - f$ de sorte que L_h est définie et nulle sur $]\text{Max}\left(A_c(f), A_c(g)\right), +\infty[$. Il s'agit de montrer que h est nulle sur $]\text{Max}\left(A_c(f), A_c(g)\right), +\infty[$. Supposons par l'absurde qu'il existe $k \in \mathbb{N}^*$ tel que $h(k) = f(k) - g(k) \neq 0$.

Soit $k_0 = \text{Min}\{k \in \mathbb{N}^*/\ h(k) \neq 0\}$. Par définition de k_0, pour tout $s > \text{Max}\left(A_c(f), A_c(g)\right)$, $\displaystyle\sum_{k=k_0}^{+\infty} \frac{h(k)}{k^s} = 0$ puis $\displaystyle\sum_{k=k_0}^{+\infty} \frac{h(k)k_0^s}{k^s} = 0$ et donc

$$\lim_{s\to+\infty} \sum_{k=k_0}^{+\infty} \frac{h(k)k_0^s}{k^s} = 0.$$

Soit $s_0 > \text{Max}\left(A_c(f), A_c(g)\right)$. Pour $s \geqslant s_0$, posons $u_k(s) = \dfrac{h(k)k_0^s}{k^s}$. Chaque fonction u_k, $k \geqslant k_0$, a une limite ℓ_k quand s tend vers $+\infty$ à savoir $\ell_k = \begin{cases} h\left(k_0\right) \text{ si } k = k_0 \\ 0 \text{ si } k \geqslant k_0 + 1 \end{cases}$. Ensuite, pour $k \geqslant k_0$ et $s \geqslant s_0$,

$$|u_k(s)| = |h(k)| \left|\frac{k_0}{k}\right|^s \leqslant |h(k)| \left|\frac{k_0}{k}\right|^{s_0} = k_0^{s_0} \left|\frac{h(k)}{k^{s_0}}\right|,$$

puis $\|u_k\|_{\infty,[s_0,+\infty[} \leqslant k_0^{s_0} \left|\dfrac{h(k)}{k^{s_0}}\right|$. La série numérique de terme général $k_0^{s_0} \left|\dfrac{h(k)}{k^{s_0}}\right|$ converge d'après la question Q17 et donc la série de terme général u_k converge normalement et en particulier uniformément sur $[s_0, +\infty[$.

D'après le théorème d'interversion des limites

- (la fonction $\sum_{k=k_0}^{+\infty} u_k$ a une limite ℓ en $+\infty$)
- (la série numérique de terme général ℓ_k, $k \geqslant k_0$, converge)
- $\ell = \sum_{k=k_0}^{+\infty} \ell_k$,

ce qui fournit explicitement

$$0 = \ell = \sum_{k=k_0}^{+\infty} \ell_k = h(k_0).$$

Ceci contredit la définition de k_0 et donc pour tout $k \in \mathbb{N}^*$, $f(k) = g(k)$ puis $f = g$.

Q 19. Soit $s > \text{Max}(A_c(f), A_c(g))$. Vérifions que la famille $\left(\dfrac{f(i)\,g(j)}{i^s j^s}\right)_{(i,j)\in(\mathbb{N}^*)^2} = (u_{i,j})_{(i,j)\in\mathbb{N}^*}$ est sommable.

- Pour $i \in \mathbb{N}^*$, $\sum_{j=1}^{+\infty} |u_{i,j}| = \left|\dfrac{f(i)}{i^s}\right| \sum_{j=1}^{+\infty} \left|\dfrac{g(j)}{j^s}\right| < +\infty$ puis
- $\sum_{i=1}^{+\infty}\left(\sum_{j=1}^{+\infty} |u_{i,j}|\right) = \left(\sum_{i=1}^{+\infty}\left|\dfrac{f(i)}{i^s}\right|\right)\left(\sum_{j=1}^{+\infty}\left|\dfrac{g(j)}{j^s}\right|\right) < +\infty.$

Ceci montre que la suite $(u_{i,j})_{(i,j)\in(\mathbb{N}^*)^2}$ est sommable. Maintenant, la famille $(\mathscr{C}_k)_{k\in\mathbb{N}^*}$ est une partition de $(\mathbb{N}^*)^2$ (notation de la question Q1). D'après un cas particulier du théorème de sommation par paquets

$$\begin{aligned} L_f(s)L_g(s) &= \left(\sum_{i=1}^{+\infty} \frac{f(i)}{i^s}\right)\left(\sum_{j=1}^{+\infty} \frac{g(j)}{j^s}\right) = \sum_{k=1}^{+\infty}\left(\sum_{(i,j)\in\mathscr{C}_k} \frac{f(i)}{i^s}\frac{g(j)}{j^s}\right) = \sum_{k=1}^{+\infty}\left(\sum_{(i,j)\in\mathscr{C}_k} f(i)g(j)\right)\frac{1}{k^s} \\ &= \sum_{k=1}^{+\infty} \frac{(f*g)(k)}{k^s} = L_{f*g}(s). \end{aligned}$$

On note qu'il n'est pas nécessaire que f et g soient multiplicatives.

II - Matrices et endomorphismes de permutation

II.A - Similitude de deux matrices de permutation

Q 20. Soit $(\rho, \rho') \in (\mathscr{S}_n)^2$. Posons $P_\rho = (p_{k,l})_{1\leqslant k,l\leqslant n}$ et $P_{\rho'} = (p'_{k,l})_{1\leqslant k,l\leqslant n}$. Soit $(i,j) \in [\![1,n]\!]^2$. Le coefficient ligne i, colonne j, de $P_\rho \times P_{\rho'}$ est

$$\sum_{k=1}^{n} p_{i,k}p'_{k,j} = \sum_{k=1}^{n} \delta_{i,\rho(k)}\delta_{k,\rho'(j)} = \delta_{i,\rho(\rho'(j))} \text{ (obtenu pour } k = \rho'(j)).$$

$\delta_{i,\rho\circ\rho'(j)}$ est aussi le coefficient ligne i, colonne j, de $P_{\rho\rho'}$. Ceci étant vrai pour tout $(i,j) \in [\![1,n]\!]^2$, on a montré que $P_{\rho\rho'} = P_\rho P_{\rho'}$.

En particulier, $P_\rho P_{\rho^{-1}} = P_{\rho\rho^{-1}} = P_{\mathrm{Id}_{[\![1,n]\!]}} = (\delta_{i,j})_{1\leqslant i,j\leqslant n} = I_n$. Ceci montre que P_ρ est inversible, d'inverse $(P_\rho)^{-1} = P_{\rho^{-1}}$.

Soit $(\sigma, \tau) \in (\mathscr{S}_n)^2$ tel que σ et τ soient conjuguées. Il existe $\rho \in \mathscr{S}_n$ telle que $\tau = \rho\sigma\rho^{-1}$. Par suite,

$$P_\tau = P_\rho \times P_\sigma \times P_{\rho^{-1}} = P_\rho \times P_\sigma \times (P_\rho)^{-1}.$$

Les matrices P_σ et P_τ sont donc semblables.

Q 21. $\rho\gamma_1\rho^{-1}(2) = \rho\gamma_1(1) = \rho(3) = 6 = \gamma_2(2)$, $\rho\gamma_1\rho^{-1}(6) = \rho\gamma_1(3) = \rho(7) = 4 = \gamma_2(6)$ et $\rho\gamma_1\rho^{-1}(4) = \rho\gamma_1(7) = \rho(1) = 2 = \gamma_2(4)$. D'autre part, si $x \notin \{2,4,6\}$, $\rho^{-1}(x) \notin \{1,3,7\}$ puis $\gamma_1\rho^{-1}(x) = \rho^{-1}(x)$ et donc $\rho\gamma_1\rho^{-1}(x) = x = \gamma_2(x)$.

Finalement, pour tout $x \in [\![1,7]\!]$, $\rho\gamma_1\rho^{-1}(x) = \gamma_2(x)$ et donc $\rho\gamma_1\rho^{-1} = \gamma_2$.

Q 22. Soit $\gamma = (a_1, \dots, a_\ell)$ et $\gamma' = (a'_1, \dots, a'_\ell)$ deux cycles de même longueur $\ell \in [\![2,n]\!]$. Soit ρ un élément de $\mathscr{S}_n$ tel que pour tout $i \in [\![1,\ell]\!]$, $\rho(a_i) = a'_i$.

Soit $i \in [\![1, \ell-1]\!]$. $\rho\gamma\rho^{-1}(a'_i) = \rho\gamma(a_i) = \rho(a_{i+1}) = a'_{i+1} = \gamma'(a_i)$ et d'autre part $\rho\gamma\rho^{-1}(a'_\ell) = \rho\gamma(a_\ell) = \rho(a_1) = a'_1 = \gamma'(a_\ell)$.
Enfin, si $x \notin \{a'_1, \ldots, a'_\ell\}$, $\rho^{-1}(x) \notin \{a_1, \ldots, a_\ell\}$ puis $\gamma\rho^{-1}(x) = \rho^{-1}(x)$ puis $\rho\gamma\rho^{-1}(x) = \rho\rho^{-1}(x) = x = \gamma'(x)$. Finalement, $\rho\gamma_1\rho^{-1} = \gamma_2$.

On a montré que deux cycles de même longueur sont conjugués.

Q 23. Réciproquement, soient γ et γ' deux cycles conjugués de longueur respectives ℓ et ℓ' et soit $\rho \in \mathscr{S}_n$ tel que $\gamma' = \rho\gamma\rho^{-1}$. Le plus petit entier $k \in \mathbb{N}^*$ tel que $\gamma^k = \mathrm{Id}_{[\![1,n]\!]}$ (resp. $\gamma'^k = \mathrm{Id}_{[\![1,n]\!]}$) est ℓ (resp. ℓ') (l'ordre d'un cycle est sa longueur). De plus, pour tout $k \in \mathbb{N}^*$, $\gamma'^k = \rho\gamma^k\rho^{-1}$ et donc $\gamma^k = \mathrm{Id}_{[\![1,n]\!]} \Leftrightarrow \gamma'^k = \mathrm{Id}_{[\![1,n]\!]}$. Ceci montre que $\ell = \ell'$. En résumé, deux cycles sont conjugués si et seulement si ils ont même longueur.

Soit maintenant $(\sigma, \tau) \in (\mathscr{S}_n)^2$ tel que $\forall \ell \in [\![1, n]\!]$, $c_\ell(\sigma) = c_\ell(\tau)$. On peut associer de manière bijective chaque cycle de longueur $\ell \geqslant 2$ apparaissant dans la décomposition de σ à un cycle de longueur ℓ dans la décomposition de τ. On commence par définir ρ par ses restrictions aux supports des différents cycles de σ de la même façon que dans la question Q22. Enfin, si $a_1, \ldots, a_t$ sont les éventuels points fixes de σ et $a'_1, \ldots, a'_t$, ceux de τ (on rappelle que $c_1(\sigma) = c_1(\tau)$), pour chaque i on pose (éventuellement) $\rho(a_i) = a'_i$. Puisque les supports des différents cycles et les points fixes constituent une partition de $[\![1, n]\!]$, on vient de définir un élément ρ de $\mathscr{S}_n$.
Si a'_i est un (éventuel) point fixe de τ, $\rho\sigma\rho^{-1}(a'_i) = \rho\sigma(a_i) = \rho(a_i) = a'_i = \tau(a'_i)$.
Si x n'est pas un point fixe de τ et donc est élément du support d'un et un seul des supports des cycles γ' apparaissant (éventuellement) dans τ, $\rho^{-1}(x)$ n'est modifié que par γ et $\gamma\rho^{-1}(x)$ reste un élément du support de γ. Le calcul de la question Q22 montre que $\rho\sigma\rho^{-1}(x) = \tau(x)$.

Finalement, ρ est un élément de $\mathscr{S}_n$ tel que $\rho\sigma\rho^{-1} = \tau$. Donc, σ et τ sont conjugués.

Inversement, supposons σ et τ conjuguées. Soit $\rho \in \mathscr{S}_n$ tel que $\rho\sigma\rho^{-1} = \tau$. Soit $\gamma = (a'_1, \ldots, a'_\ell)$, $\ell \geqslant 2$, un (éventuel) cycle de longueur ℓ apparaissant dans τ. Alors, pour tout $i \in [\![1, \ell-1]\!]$, $\rho^{-1}\left(a'_{i+1}\right) = \rho^{-1}\tau(a'_i) = \sigma\rho^{-1}(a'_i)$ et de même, $\rho^{-1}(a'_1) = \sigma\rho^{-1}(a'_\ell)$. Ceci montre que $\left(\rho^{-1}(a'_1), \ldots, r^{-1}(a'_\ell)\right)$ est un cycle de longueur ℓ apparaissant dans σ. De même, si x est un point fixe de τ, alors $\rho^{-1}(x)$ est un point fixe de σ et réciproquement.

Ainsi, ρ^{-1} associe de manière bijective chaque cycle de longueur $\ell \geqslant 2$ dans τ à un cycle de longueur ℓ dans σ et chaque point fixe de τ à un point fixe de σ. Ceci montre en particulier que $(c_1(\sigma), \ldots, c_n(\sigma)) = (c_1(\tau), \ldots, c_n(\tau))$.

Q 24. Soient $\ell \in [\![2, n]\!]$ puis $\gamma \in \mathscr{S}_\ell$ un cycle de longueur ℓ de $[\![1, \ell]\!]$. γ a même longueur que le cycle $\gamma' = (1\ 2\ \ldots\ \ell)$ et donc P_γ est semblable à P'_γ puis

$$\chi_\gamma(X) = \chi_{\gamma'}(X) = \det(XI_\ell - \Gamma_\ell) = \begin{vmatrix} X & 0 & \ldots & \ldots & 0 & -1 \\ -1 & X & \ldots & \ldots & \ldots & 0 \\ 0 & -1 & \ddots & & \vdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & -1 & X & 0 \\ 0 & \ldots & \ldots & 0 & -1 & X \end{vmatrix}.$$

On développe ce déterminant suivant sa première ligne. On obtient $\chi_\gamma(X) = X \times \Delta_1 + (-1) \times (-1)^{\ell+1}\Delta_2$ où Δ_1 est un déterminant triangulaire inférieur égal à $X^{\ell-1}$ et Δ_2 est un déterminant triangulaire supérieur égal à $(-1)^{\ell-1}$. Donc,

$$\chi_\gamma(X) = X \times X^{\ell-1} + (-1)^{\ell+2} \times (-1)^{\ell-1} = X^\ell + (-1)^{2\ell-1} = X^\ell - 1.$$

Q 25. Soit $\sigma \in \mathscr{S}_n$. Soit f l'endomorphisme de $\mathbb{C}^n$ de matrice P_σ dans la base canonique $\mathscr{B} = (e_1, \ldots, e_n)$ (donc, pour tout $j \in [\![1, n]\!]$, $f(e_j) = e_{\sigma(j)}$). On réordonne les vecteurs de cette base en mettant en premier les vecteurs dont le numéro est un point fixe de σ puis les vecteurs dont le numéro appartient au support d'un cycle de longueur 2 et ceci pour chaque cycle de longueur 2, puis les vecteurs dont le numéro appartient au support d'un cycle de longueur 3 ... On obtient ainsi une nouvelle base $\mathscr{B}'$ de $\mathbb{C}^n$ (car obtenue par permutation des vecteurs de $\mathscr{B}$) dans laquelle la matrice de f est diagonale par blocs, les blocs diagonaux étant du type Γ_l, $\ell \geqslant 1$. P_σ est donc semblable à une matrice de ce type.

Le format d'un bloc Γ_ℓ, $\ell \geqslant 2$, est la longueur du cycle correspondant. Il y a donc $c_\ell(\sigma)$ blocs Γ_ℓ où $\ell \geqslant 2$. D'autre part, chaque bloc Γ_1 correspond à un point fixe de σ. Il y a $c_1(\sigma)$ blocs Γ_1. Puisque $\chi_{\Gamma_1} = X - 1$, un calcul par blocs fournit

$$\chi_\sigma(X) = \prod_{\ell=1}^{n} (\det(\Gamma_\ell))^{c_\ell(\sigma)} = \prod_{\ell=1}^{n} \left(X^\ell - 1\right)^{c_\ell(\sigma)},$$

(avec la convention $(\det(\Gamma_\ell))^{c_\ell(\sigma)} = \left(X^\ell - 1\right)^{c_\ell(\sigma)} = 1$ quand $c_\ell(\sigma) = 0$).

Q 26. Soit $q \in [\![1,n]\!]$. Pour $\ell \in [\![1,n]\!]$, le nombre $e^{\frac{2i\pi}{q}}$ est racine de $X^\ell - 1$ si et seulement si q divise ℓ. Puisque chaque $X^\ell - 1$ est à racines simples dans $\mathbb{C}$ (car sans racine commune avec sa dérivée), pour $\ell \in [\![1,n]\!]$, le nombre $e^{\frac{2i\pi}{q}}$ est racine de $\left(X^\ell - 1\right)^{c_\ell(\sigma)}$ d'ordre $c_\ell(\sigma)$ (y compris si $e^{\frac{2i\pi}{q}}$ n'est pas racine de $\left(X^\ell - 1\right)^{c_\ell(\sigma)}$). Finalement, le nombre $e^{\frac{2i\pi}{q}}$ est racine de χ_σ d'ordre $\displaystyle\sum_{\substack{\ell=1\\ q|\ell}}^{n} c_\ell(\sigma)$. De même, le nombre $e^{\frac{2i\pi}{q}}$ est racine de χ_τ d'ordre $\displaystyle\sum_{\substack{\ell=1\\ q|\ell}}^{n} c_\ell(\tau)$.

Puisque P_σ et P_τ sont semblables, $\chi_\sigma = \chi_\tau$ et en particulier, les deux ordres de multiplicité ci-dessus sont les mêmes :

$$\forall q \in [\![1,n]\!],\ \sum_{\substack{\ell=1\\ q|\ell}}^{n} c_\ell(\sigma) = \sum_{\substack{\ell=1\\ q|\ell}}^{n} c_\ell(\tau).$$

Q 27. Soit $q \in [\![1,n]\!]$. Le q-ème coefficient de $T_\sigma D$ est

$$\sum_{\ell=1}^{n} c_\ell(\sigma) d_{\ell,q} = \sum_{1 \leqslant \ell \leqslant n,\ q|\ell} c_\ell(\sigma).$$

D'après la question précédente, ce coefficient est aussi le q-ème coefficient de $T_\tau D$.

Ainsi, $T_\sigma D = T_\tau D$. D'après la question Q16, $\det(D) = 1 \neq 0$ et donc D est inversible. On en déduit que $T_\sigma = T_\tau$ puis que σ et τ sont conjuguées d'après la question Q23. En résumé, σ et τ sont conjuguées si et seulement si P_σ et P_τ sont semblables.

II.B - Endomorphismes de permutation

Q 28. Soit u un endomorphisme de permutation de E. Il existe une base $\mathscr{B} = (e_1, \dots, e_n)$ base de E et $\sigma \in \mathscr{S}_n$ telles que $\forall j \in [\![1,n]\!]$, $u(e_j) = e_{\sigma(j)}$.
Pour $(i,j) \in [\![1,n]\!]^2$, le coefficient ligne i, colonne j, de $\mathrm{Mat}_{\mathscr{B}}(u)$ est $\delta_{i,\sigma(j)}$ (symbole de KRONECKER) et donc $\mathrm{Mat}_{\mathscr{B}}(f) = P_\sigma$. Inversement, s'il existe $\mathscr{B} = (e_1, \dots, e_n)$ base de E et $\sigma \in \mathscr{S}_n$ telles que $\mathrm{Mat}_{\mathscr{B}}(f) = P_\sigma$, alors pour tout $j \in [\![1,n]\!]$, $u(e_j) = e_{\sigma(j)}$ et donc u est un endomorphisme de permutation.

Q 29. Soit u un endomorphisme de permutation de E. Soient $\mathscr{B} = (e_1, \dots, e_n)$ base de E et $\sigma \in \mathscr{S}_n$ telles que $\mathrm{Mat}_{\mathscr{B}}(f) = P_\sigma$. Le coefficient ligne i, colonne i de P_σ est i si $\sigma(i) = i$ et 0 si $\sigma(i) \neq i$. Donc,

$$\mathrm{Tr}(u) = \mathrm{Tr}(P_\sigma) = c_1(\sigma) \in [\![0,n]\!].$$

Ensuite, P_σ est semblable à une matrice diagonale par blocs Γ, chaque bloc étant du type Γ_ℓ, $\ell \geqslant 1$. Soit $\ell \geqslant 1$. Le polynôme caractéristique de Γ_ℓ, à savoir $\chi_{\Gamma_\ell} = X^\ell - 1$, est à racines simples dans $\mathbb{C}$. Donc, chaque bloc Γ_ℓ, $\ell \geqslant 1$, est diagonalisable dans $\mathscr{M}_\ell(\mathbb{C})$. Un calcul par blocs montre alors que Γ est diagonalisable dans $\mathscr{M}_n(\mathbb{C})$ et il en est de même de P_σ. Mais alors u est diagonalisable.

Q 30. Si A et B sont semblables, on sait que A et B ont même polynôme caractéristique.
Inversement, soient A et B deux matrices ayant même polynôme caractéristique $(X - \lambda_1) \dots (X - \lambda_n)$. Si de plus A et B sont diagonalisables, alors A et B sont toutes deux semblables à $D = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$. Par transitivité, A et B sont semblables.

Q 31. Si u est un endomorphisme de permutation, $\mathrm{Tr}(u)$ est un entier naturel d'après la question Q29.

Inversement, soit u un endomorphisme de E tel que $u^2 = \mathrm{Id}_E$ et $\mathrm{Tr}(u) \in \mathbb{N}$. u est une symétrie et donc, il existe une base $\mathscr{B}$ telle que $\mathrm{Mat}_{\mathscr{B}}(u) = \mathrm{diag}(\underbrace{1,\dots,1}_{p}, \underbrace{-1,\dots,-1}_{q})$. De plus, $p - q = \mathrm{Tr}(u) \geqslant 0$ et donc $p \geqslant q$. Le polynôme caractéristique de u est donc $(X-1)^p(X+1)^q = (X-1)^{p-q}\left(X^2-1\right)^q$. Maintenant, la matrice Γ diagonale par blocs comportant sur sa diagonale $p - q$ blocs Γ_1 et q blocs Γ_2 a aussi pour polynôme caractéristique $(X-1)^{p-q}\left(X^2-1\right)^q$ et est diagonalisable. D'après la question précédente, $\mathrm{Mat}_{\mathscr{B}}(u)$ est semblable à la matrice de permutation Γ et donc il existe une base de E dans laquelle la matrice de u est une matrice de permutation. On en déduit que u est un endomorphisme de permutation de E.

Q 32. Si u est un endomorphisme de permutation de E tel que $u^3 = \mathrm{Id}_E$, alors comme à la question précédente, $\mathrm{Tr}(u) = c_1(\sigma) \in [\![0,n]\!]$.

Réciproquement, soit u un endomorphisme de E tel que $u^3 = \mathrm{Id}_E$ et $\mathrm{Tr}(u) \in \mathbb{N}$. Le polynôme $X^3 - 1 = (X-1)(X-j)\left(X-j^2\right)$ est à racines simples dans $\mathbb{C}$ et annulateur de u. Donc, u est diagonalisable. Il existe une base $\mathscr{B}$ de E telle que $\mathrm{Mat}_{\mathscr{B}}(u) = \mathrm{diag}(\underbrace{1,\dots,1}_{p}, \underbrace{j,\dots,j}_{q}, \underbrace{j^2,\dots,j^2}_{r})$.

Si par exemple $q > r$, $\text{Tr}(u) = p + qj + rj^2 = p - r + (q - r)j \notin \mathbb{R}$ (car $j + j^2 = -1$ et $j \notin \mathbb{R}$). De même, $q < r$ est impossible et donc $q = r$. Par suite, $\text{Tr}(u) = p + qj + qj^2 = p - q$ et comme à la question précédente, $p \geqslant q$. Ainsi, le polynôme caractéristique de u est $(X-1)^{p-q}(X-1)^q(X-j)^q\left(X-j^2\right)^q = (X-1)^{p-q}\left(X^3-1\right)^q$. Comme à la question précédente, $\text{Mat}_{\mathscr{B}}(u)$ est semblable à la matrice de permutation Γ, diagonale par blocs comportant sur sa diagonale $p - q$ blocs Γ_1 et q blocs Γ_3. Donc, u est un endomorphisme de permutation de E.

Soit u l'endomorphisme de $E = \mathbb{C}^2$ canoniquement associé à la matrice $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. $\chi_A = X^2 + 1$ puis, d'après le théorème de Cayley-Hamilton, $A^2 = -I_2$ puis $A^4 = I_2$ puis $u^4 = \text{Id}_E$. De plus, $\text{Tr}(u) = 0 \in \mathbb{N}$.
Il n'existe que deux matrices de permutations de format 2 : $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. A n'est semblable ni à I (car alors $A = I$ ce qui est faux), ni à J (car alors $A^2 = I$ ce qui est faux). Donc, u n'est pas un endomorphisme de permutation. Ainsi, la condition $\text{Tr}(u) \in \mathbb{N}$ n'est pas suffisante pour que u soit un endormorphisme de permutation dans le cas $k = 4$.

Q 33. Soit u un endomorphisme de permutation de E. Soient $\mathscr{B} = (e_1, \ldots, e_n)$ une base de E et $\sigma \in \mathscr{S}_n$ telles que pour tout $j \in [\![1, n]\!]$, $u(e_j) = e_{\sigma(j)}$. La permutation σ se décompose en produit de cycles à supports disjoints : $\sigma = \gamma_1 \ldots \gamma_r$ (on suppose que le résultat de cours rappelé par l'énoncé est vrai également avec $\sigma = \text{Id}$ en prenant conventionnellement $r = 0$ (produit vide)). En notant ℓ_i la longueur de γ_i pour chaque $i \in [\![1, r]\!]$, on a $\gamma_i^{\ell_i} = \text{Id}_{[\![1,n]\!]}$.
Soit $N = \text{PPCM}(\ell_1, \ldots, \ell_r)$. Pour chaque $i \in [\![1, r]\!]$, $\gamma_i^N = \text{Id}_{[\![1,n]\!]}$ puis, des cycles à supports disjoints commutant deux à deux,

$$\sigma^N = \gamma_1^N \ldots \gamma_r^N = \text{Id}_{[\![1,n]\!]}.$$

Mais alors, $(P_\sigma)^n = P_{\sigma^N} = P_{\text{Id}} = I_n$ puis $u^N = \text{Id}_E$. Donc (b) est vrai. D'autre part, (a) est vrai d'après la question Q25.

Réciproquement, soit u un endomorphisme de E tel que (a) et (b) soient vrais. Puisque le polynôme $X^N - 1$ est annulateur de u et à racines simples, u est diagonalisable. D'autre part, si $\mathscr{B}$ est une base donnée de E et $M = \text{Mat}_{\mathscr{B}}(u)$, M a le même polynôme caractéristique que la matrice de permutation Γ, diagonale par blocs, ayant sur sa diagonale c_1 blocs Γ_1, c_2 blocs Γ_2, ..., c_n blocs Γ_n. Puisque les matrices M et Γ sont diagonalisables et ont même polynôme caractéristique, ces matrices sont semblables d'après la question Q30 et donc u est un endomorphisme de permutation.

Q 34. Posons $\chi_u = \displaystyle\prod_{i=1}^{r} (X - \lambda_i)^{\alpha_i}$ où les λ_i sont les valeurs propres deux à deux distinctes de u et les α_i sont leurs ordres de multiplicités respectifs. Posons de même $\chi_v = \displaystyle\prod_{i=1}^{s} (X - \mu_i)^{\beta_i}$ où les μ_i sont les valeurs propres deux à deux distinctes de v et les β_i leurs ordres de multiplicités respectifs.
On sait que pour tout $k \in \mathbb{N}$, $\text{Sp}\left(u^k\right) = (\underbrace{\lambda_1^k, \ldots, \lambda_1^k}_{\alpha_1}, \ldots, \underbrace{\lambda_r^k, \ldots, \lambda_r^k}_{\alpha_r})$ et donc $\text{Tr}\left(u^k\right) = \displaystyle\sum_{i=1}^{r} \alpha_i \lambda_i^k$. De même, pour tout $k \in \mathbb{N}$, $\text{Tr}\left(v^k\right) = \displaystyle\sum_{i=1}^{s} \beta_i \mu_i^k$.

Par hypothèse, pour tout $k \in \mathbb{N}$, $\displaystyle\sum_{i=1}^{r} \alpha_i \lambda_i^k = \sum_{i=1}^{s} \beta_i \mu_i^k$. Soit R un réel strictement positif inférieur ou égal à tous les $\left|\dfrac{1}{\lambda}\right|$, $\lambda \in \text{Sp}(u) \setminus \{0\}$ et à tous les $\left|\dfrac{1}{\mu}\right|$, $\mu \in \text{Sp}(v) \setminus \{0\}$ (s'il existe au moins une valeur propre non nulle et sinon on prend $R = 1$ par exemple). Pour tout $x \in]-R, R[$, chaque série de terme général $(\lambda_i x)^k$ converge et chaque série de terme général $(\mu_i x)^k$ converge (y compris si $\lambda_i = 0$ ou $\mu_i = 0$). De plus, pour $x \in]-R, R[$ et $i \in [\![1, r]\!]$,

$$\sum_{k=0}^{+\infty} (\lambda_i x)^k = \frac{1}{1 - \lambda_i x}.$$

On en déduit que pour $x \in]-R, R[$,

$$\sum_{k=0}^{+\infty} \text{Tr}\left(u^k\right) x^k = \frac{\alpha_1}{1 - \lambda_1 x} + \ldots + \frac{\alpha_r}{1 - \lambda_r x}.$$

De même, pour $x \in]-R, R[$, $\displaystyle\sum_{k=0}^{+\infty} \text{Tr}\left(v^k\right) x^k = \frac{\beta_1}{1 - \mu_1 x} + \ldots + \frac{\beta_s}{1 - \mu_s x}$. On a donc,

$$\forall x \in]-R,R[,\ \frac{\alpha_1}{1-\lambda_1 x}+\ldots+\frac{\alpha_r}{1-\lambda_r x}=\frac{\beta_1}{1-\mu_1 x}+\ldots+\frac{\beta_s}{1-\mu_s x}.$$

Puisque $]-R,R[$ est infini, on en déduit encore que $\dfrac{\alpha_1}{1-\lambda_1 X}+\ldots+\dfrac{\alpha_r}{1-\lambda_r X}=\dfrac{\beta_1}{1-\mu_1 X}+\ldots+\dfrac{\mu_s}{1-\beta_s X}$. L'unicité de la décomposition en éléments simples permet alors d'affirmer que $r=s$ puis que u et v ont les mêmes valeurs propres avec même ordre de multiplicité. Finalement, u et v ont même polynôme caractéristique.

Q 35. Si u est un endomorphisme de permutation, on pose $(c_1,\ldots,c_n)=(c_1(\sigma),\ldots,c_n(\sigma))$ où σ est associée à u. Il existe une base de E dans laquelle la matrice Γ de u est une matrice diagonale par blocs, ayant sur sa diagonale c_1 blocs Γ_1, c_2 blocs Γ_2, ..., c_n blocs Γ_n. Donc,

$$\forall k \in \mathbb{N}^*,\ \mathrm{Tr}\left(u^k\right)=\sum_{\ell=1}^{n} c_\ell \mathrm{Tr}\left(\Gamma_\ell^k\right).$$

Maintenant, pour $\ell \in [\![1,n]\!]$, si k n'est pas multiple de ℓ, les coefficients diagonaux de Γ_ℓ^k sont nuls et donc $\mathrm{Tr}\left(\Gamma_\ell^k\right)=0$ et si k est multiple de ℓ, $\Gamma_\ell^k=I_\ell$ et donc $\mathrm{Tr}\left(\Gamma_\ell^k\right)=\ell$. On en déduit que

$$\forall k \in \mathbb{N}^*,\ \mathrm{Tr}\left(u^k\right)=\sum_{\substack{\ell=1\\ \ell|k}}^{n} \ell c_\ell.$$

Enfin, puisque $\chi_u=\displaystyle\prod_{\ell=1}^{n}\left(X^\ell-1\right)^{c_\ell}$, on a

$$\sum_{\substack{\ell=1\\ \ell|0}}^{n} \ell c_\ell=\sum_{\ell=1}^{n} \ell c_\ell=\deg\left(\chi_u\right)=n=\mathrm{Tr}\left(\mathrm{Id}_E\right)=\mathrm{Tr}\left(u^0\right).$$

En résumé, il existe des entiers naturels non nuls c_1, ..., c_n, tels que $\forall k \in \mathbb{N}$, $\mathrm{Tr}\left(u^k\right)=\displaystyle\sum_{\substack{\ell=1\\ \ell|k}}^{n} c_\ell \mathrm{Tr}\left(\Gamma_\ell^k\right)$.

Réciproquement, supposons qu'il existe des entiers naturels non nuls c_1, ..., c_n, tels que $\forall k \in \mathbb{N}$, $\mathrm{Tr}\left(u^k\right)=\displaystyle\sum_{\substack{\ell=1\\ \ell|k}}^{n} \ell c_\ell$. Soit v l'endomorphisme de permutation de E dont la matrice dans une certaine base $\mathscr{B}$ est la matrice Γ définie ci-dessus. On a donc : $\forall k \in \mathbb{N}$, $\mathrm{Tr}\left(u^k\right)=\mathrm{Tr}\left(v^k\right)$. D'après la question précédente, u et v ont même polynôme caractéristique et donc

$$\chi_u=\prod_{\ell=1}^{n}\left(X^\ell-1\right)^{c_\ell} \quad \text{(a)}.$$

On en déduit que les valeurs propres de u sont des nombres de la forme $\lambda=e^{\frac{2ik\pi}{\ell}}$, où $\ell \in [\![1,n]\!]$ et $k \in [\![0,\ell-1]\!]$. Soit $N=n!$. Pour tout $\lambda \in \mathrm{Sp}(u)$, $\lambda^N=1$ et donc $\mathrm{Sp}\left(u^N\right)=(1,\ldots,1)$. Puisque u est diagonalisable, il en est de même de u^N et donc il existe une base $(e_1,\ldots,e_n)$ de E telle que, pour tout $i \in [\![1,n]\!]$, $u^N(e_i)=e_i$. Les endomorphismes u^N et Id_E coïncident sur une base de E et donc $u^N=\mathrm{Id}_E$ (b).

D'après la question Q33, u est un endomorphisme de permutation.

III - Valeurs propres de la matrice de Redheffer

Q 36. La matrice A_n est triangulaire supérieure puis $\det(A_n)=\mu(1)\times 1\times\ldots\times 1=1$. Donc,

$$\det(H_n)=\det(A_n)\det(H_n)=\det(A_nH_n)=\det(C_n).$$

Posons $C_n=(c_{i,j})_{1\leqslant i,j\leqslant n}$. $c_{1,1}=\displaystyle\sum_{k=1}^{n} a_{1,k}h_{k,1}=\sum_{k=1}^{n}\mu(k)=M(n)$.

Ensuite, pour $i \in [\![2,n]\!]$, $c_{i,1}=\displaystyle\sum_{k=1}^{n} a_{i,k}h_{k,1}=a_{i,i}=1$. Ensuite, si $(i,j) \in [\![2,n]\!]^2$,

$$c_{i,j}=\sum_{k=1}^{n} a_{i,k}h_{k,j}=a_{i,i}h_{i,j}=\begin{cases} 1 \text{ si } i|j \\ 0 \text{ sinon}\end{cases}.$$

En particulier, si $2 \leqslant j < i \leqslant n$, $c_{i,j} = 0$ et si $2 \leqslant i \leqslant n$, $c_{i,i} = 1$. Enfin, si $j \in [\![2, n]\!]$,

$$c_{1,j} = \sum_{k=1}^{n} a_{1,k} h_{k,j} = \sum_{\substack{k=1 \\ k|j}}^{n} \mu(k) = \sum_{\substack{k=1 \\ k|j}}^{j} \mu(k) = \mu * 1(j) = \delta(j) = 0.$$

En développant $\det(C_n)$ suivant sa première ligne, on obtient $\det(C_n) = M(n) \times \Delta_{n-1}$ où Δ_{n-1} est un déterminant triangulaire supérieur dont les coefficients diagonaux sont égaux à 1 et donc Δ_{n-1} est égal à 1. Finalement,

$$\det(H_n) = M(n) = \sum_{k=1}^{n} \mu(k).$$

Q 37. Le coefficient ligne 1, colonne 1, de $B_n(\lambda)(\lambda I_n - H_n)$ est $(\lambda - 1)b(1) - \sum_{j=2}^{n} b(j) = (\lambda - 1) - \sum_{j=2}^{n} b(j)$.

Si $j \geqslant 2$, le coefficient ligne 1, colonne j, de $B_n(\lambda)(\lambda I_n - H_n)$ est

$$-\sum_{k=1,\ k \neq j}^{n} b(k) h_{k,j} + b(j)(\lambda - h_{i,i}) = (\lambda - 1)b(j) - \sum_{d|j}^{b}(d) = 0.$$

Ensuite, si $i \geqslant 2$ et $j \geqslant 2$, le coefficient ligne i, colonne j, de $B_n(\lambda)(\lambda I_n - H_n)$ est

$$-\sum_{k=1\ k \neq j}^{n} b_{i,k} h_{k,j} + b_{i,j}(\lambda - h_{j,j}).$$

Si $i = j$, cette somme est égale à $-0 + b_{i,i}(\lambda - h_{i,i}) = \lambda - 1$. Si $i \neq j$, cette somme est égale à $-b_{i,i}h_{i,j} + 0 = -h_{i,j}$. En particulier, si $2 \leqslant j < i \leqslant n$, ce coefficient est nul et donc le mineur correspondant est triangulaire supérieur. Ce mineur est égal à $(\lambda - 1)^{n-1}$.

En développant $\det(B_n(\lambda)(\lambda I_n - H_n))$ suivant sa première ligne, on obtient

$$\det(B_n(\lambda)(\lambda I_n - H_n)) = \left((\lambda - 1) - \sum_{j=2}^{n} b(j)\right)(\lambda - 1)^{n-1} = (\lambda - 1)^n - (\lambda - 1)^{n-1} \sum_{j=2}^{n} b(j).$$

D'autre part, $B_n(\lambda)$ est triangulaire supérieure, à coefficients diagonaux tous égaux à 1 et donc $\det(B_n(\lambda)) = 1$. Par suite,

$$\chi_n = \det(\lambda I_n - H_n) = \det(B_n(\lambda)(\lambda I_n - H_n)) = (\lambda - 1)^n - (\lambda - 1)^{n-1} \sum_{j=2}^{n} b(j).$$

Q 38. $f * b = (1 + w)\delta * b - w1 * b = (1 + w)b - w1 * b$. Ensuite, $w(1 * b)(1) = w \times 1 \times b(1) = w$ et pour $j \geqslant 2$,

$$w(1 * b)(j) = w \sum_{d|j}^{b}(d) = w \sum_{d|j,\ d \neq j}^{b}(d) + wb(j) = b(j) + wb(j) = (w + 1)b(j).$$

Mais alors, $(f * b)(1) = (1 + w) - w = 1 = \delta(1)$ et pour $j \geqslant 2$, $(f * b)(j) = (1 + w)b(j) - (1 + w)b(j) = 0 = \delta(j)$. Finalement, $f * b = \delta$.

Q 39. Pour tout réel s, $L_\delta(s) = \sum_{k=1}^{+\infty} \frac{\delta(k)}{k^s} = 1$ et pour tout $s > 1$, $L_1(s) = \sum_{k=1}^{+\infty} \frac{1}{k^s}$ (fonction ζ de Riemann). Donc,

$$\forall s > 1,\ L_f(s) = (1 + w)L_\delta(s) - wL_1(s) = 1 + w - wL_1(s).$$

Q 40. Soit g la fonction arithmétique définie par : $g(1) = 1$ et $\forall m \geqslant 2$, $g(m) = \sum_{k=1}^{\lfloor \log_2(m) \rfloor} w^k D_k(m)$.

Tout d'abord, pour $m \geqslant 2$, si il existe $d_1, \ldots, d_k$, $(k \in \mathbb{N}^*)$, tels que $m = d_1 \ldots d_k$ et $\forall i \in [\![1, k]\!]$, $d_i \geqslant 2$, alors $m \geqslant 2^k$ puis $k \leqslant \log_2(m)$ puis $k \leqslant \lfloor \log_2(m) \rfloor$. Donc, si $k > \lfloor \log_2(m) \rfloor$, $D_k(m) = 0$. Ceci permet d'écrire pour tout $m \geqslant 2$, $g(m) = \sum_{k=1}^{+\infty} w^k D_k(m)$.

Pour tout $m \geqslant 1$, $(f*g)(m) = (1+w)(\delta*g)(m) - w(1*g)(m) = (1+w)g(m) - w(1*g)(m)$. Déjà, $(f*g)(1) = 1+w-w = 1$. Soit alors $m \geqslant 2$.

$$\begin{aligned}
w(1*g)(m) &= w\sum_{d|m} g(d) = wg(1) + wg(m) + \sum_{\substack{d|m\\ d\neq 1,\ d\neq m}} g(d) = (1+w)g(m) + w\sum_{\substack{d|m\\ d\neq 1,\ d\neq m}} g(d)\\
&= w + wg(m) + w\sum_{\substack{d|m\\ d\neq 1,\ d\neq m}}\left(\sum_{k=1}^{+\infty} w^k D_k(d)\right)\\
&= w + wg(m) + \sum_{k=1}^{+\infty} w^{k+1}\left(\sum_{\substack{d|m\\ d\neq 1,\ d\neq m}} D_k(d)\right) \text{ (toutes les sommes sont finies).}
\end{aligned}$$

Maintenant, pour $m \geqslant 2$, les décompositions de m en $k+1$ facteurs supérieurs ou égaux à 2 s'écrivent $m = d_1 \dots d_k d_{k+1} = dd_{k+1}$ où d est un diviseur de m distinct de 1 et m. Ces ensembles de décomposition étant deux à deux disjoints, on en déduit que $\displaystyle\sum_{\substack{d|m\\ d\neq 1,\ d\neq m}} D_k(d) = D_{k+1}(m)$. Par suite,

$$\begin{aligned}
w(1*g)(m) &= (1+w)g(m) + \sum_{k=1}^{+\infty} w^{k+1}D_{k+1}(m) = w + g(m) + \sum_{k=2}^{+\infty} w^k D_k(m) = w + wg(m) + g(m) - wD_1(m)\\
&= (1+w)g(m),
\end{aligned}$$

et donc, $(f*g)(m) = (1+w)g(m) - (1+w)g(m) = 0$. Ceci montre que $f*g = \delta$.

On admet la convergence de la série de somme $L_g(s)$ pour s suffisamment grand. D'après la question Q19, pour s suffisamment grand,

$$1 = L_\delta(s) = L_{f*g}(s) = L_f(s)L_g(s)$$

et donc $\displaystyle\frac{1}{L_f(s)} = 1 + \sum_{m=2}^{+\infty}\frac{1}{m^s}\left(\sum_{k=1}^{\lfloor \log_2(m)\rfloor} w^k D_k(m)\right)$.

Q 41. On a aussi $f*b = \delta$. On admet la convergence de la série de somme $L_b(s)$ pour s suffisamment grand. Pour s suffisamment grand, $L_f(s)L_b(s) = L_{f*b}(s) = L_f(s)L_g(s)$ et donc $L_b(s) = L_g(s)$. D'après la question Q18, $b = g$ ou encore $b(1) = 1$ et pour tout $m \geqslant 2$, $b(m) = \displaystyle\sum_{k=1}^{\lfloor \log_2(m)\rfloor} w^k D_k(m)$.

Soit $m \geqslant 2$.

$$\begin{aligned}
\sum_{m=2}^{n} b(m) &= \sum_{m=2}^{n}\left(\sum_{k=1}^{\lfloor \log_2(m)\rfloor} w^k D_k(m)\right) = \sum_{m=2}^{n}\left(\sum_{k=1}^{\lfloor \log_2(n)\rfloor} w^k D_k(m)\right) \text{ (car, pour } k > \lfloor \log_2(m)\rfloor,\ D_k(m) = 0)\\
&= \sum_{k=1}^{\lfloor \log_2(n)\rfloor} w^k\left(\sum_{m=2}^{n} D_k(m)\right) = \sum_{k=1}^{\lfloor \log_2(n)\rfloor} w^k S_k(m).
\end{aligned}$$

D'après la question Q37, pour $\lambda \neq 1$,

$$\chi_n(\lambda) = (\lambda-1)^n - (\lambda-1)^{n-1}\sum_{k=1}^{\lfloor \log_2(n)\rfloor} w^k S_k(m) = (\lambda-1)^n - \sum_{k=1}^{\lfloor \log_2(n)\rfloor}(\lambda-1)^{n-k-1}S_k(m).$$

Ainsi, pour tout $\lambda \neq 1$, $\chi_n(\lambda) = (\lambda-1)^n - \displaystyle\sum_{k=1}^{\lfloor \log_2(n)\rfloor}(\lambda-1)^{n-k-1}S_k(m)$. Cette égalité reste vraie pour $\lambda = 1$ car deux polynômes qui coïncident en une infinité de valeurs sont égaux.

Q 42. Le résultat est faux quand $n = 2$ car $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ et donc $\chi_2 = X(X-2)$. Ensuite, $H_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ puis en développant suivant la première colonne,

$$\chi_3 = \begin{vmatrix} X-1 & -1 & -1 \\ -1 & X-1 & 0 \\ -1 & 0 & X-1 \end{vmatrix} = (X-1)^3 - (X-1) - (X-1) = (X-1)\left((X-1)^2 - 2\right).$$

Donc, 1 est valeur propre d'ordre 1 de H_3. Puisque $3 - \lfloor \log_2(3) \rfloor - 1 = 3 - 1 - 1 = 1$, le résultat est vrai quand $n = 3$. Dorénavant, $n \geqslant 4$. $\chi_n(\lambda) = (\lambda - 1)^{n - \lfloor \log_2(n) \rfloor - 1} Q_n(\lambda)$ où $Q_n(\lambda) = (\lambda - 1)^{\lfloor \log_2(n) \rfloor + 1} - \displaystyle\sum_{k=1}^{\lfloor \log_2(n) \rfloor} (\lambda - 1)^{\lfloor \log_2(n) \rfloor - k} S_k(n)$ de sorte que $Q_n(1) = -S_{\lfloor \log_2(n) \rfloor}(n)$.

Pour $k \in \mathbb{N}$, $k = \lfloor \log_2(n) \rfloor \Leftrightarrow k \leqslant \log_2(n) < k + 1 \Leftrightarrow 2^k \leqslant n < 2^{k+1}$. Puisque $n \geqslant 4$, alors $k \geqslant 2$ puis $2^k = (1+1)^k \geqslant 1 + k + \dfrac{k(k-1)}{2} \geqslant k + 2$ puis

$$n - \lfloor \log_2(n) \rfloor - 1 = n - k - 1 \geqslant 1 > 0.$$

Ainsi, pour tout $n \geqslant 3$, $n - \lfloor \log_2(n) \rfloor - 1 > 0$ et donc 1 est effectivement valeur propre de H_n. Ensuite, si $k = \lfloor \log_2(n) \rfloor$, alors $2 \leqslant 2^k \leqslant n$ (car $n \geqslant 4$) et donc

$$-Q_n(1) = S_k(n) = \sum_{m=2}^{n} D_k(m) \geqslant D_k(2^k) > 0,$$

car l'entier $2^k = 2 \times \ldots \times 2$ admet au moins une décomposition en produit de k facteurs supérieurs ou égaux à 2. Ainsi, $Q_n(1) \neq 0$ et donc 1 est valeur propre de H_n d'ordre $n - \lfloor \log_2(n) \rfloor - 1$ exactement.

