# Centrale-Supélec 2020 [1]
# MP - Mathématiques 1

On rappelle qu'un produit vide vaut 1 par convention.

## I. Quelques résultats utiles

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

1. Soit $f \in \mathbb{A}$. Soit $n \in \mathbb{N}^*$. Alors $(f*\delta)(n) = \sum_{d|n} f(d)\delta(\frac{n}{d}) = f(n)$ car tous les termes $\delta(\frac{n}{k})$ sont nuls sauf quand $d = n$ où il vaut 1. De même, $(\delta * f)(n) = \sum_{d|n} \delta(d) f(\frac{n}{d}) = f(n)$ car tous les termes sont nuls sauf quand $d = 1$. Vrai pour tout $n \in \mathbb{N}^*$, donc $f*\delta = \delta * f = f$.

La fonction $\delta$ est le neutre de la loi $*$.

2. Soit $n \in \mathbb{N}^*$. Si $(d_1, d_2) \in \mathcal{C}_n$ alors $d_1$ divise $n$ et $d_2 = \frac{n}{d_1}$ d'où $\mathcal{C}_n \subset \{(d, \frac{n}{d}) : d \in \mathcal{D}_n\}$. Réciproquement, si $d \in \mathbb{N}$ divise $n$, alors $(d, \frac{n}{d}) \in \mathcal{C}_n$. D'où $\mathcal{C}_n = \{(d, \frac{n}{d}) : d \in \mathcal{D}_n\}$ et $(f*g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}) = \sum_{(d_1,d_2)\in\mathcal{C}_n} f(d_1)g(d_2)$.

Pour tout $n \in \mathbb{N}^*$, $(f*g)(n) = \displaystyle\sum_{(d_1,d_2)\in\mathcal{C}_n} f(d_1)g(d_2)$.

3. Soient $f, g \in \mathbb{A}$ et $n \in \mathbb{N}^*$. D'après la question précédente, $(f*g)(n) = \sum_{(d_1,d_2)\in\mathcal{C}_n} f(d_1)g(d_2)$. Or $(d_1, d_2) \in \mathcal{C}_n$ si et seulement si $(d_2, d_1) \in \mathcal{C}_n$ donc $(f*g)(n) = \sum_{(d_2,d_1)\in\mathcal{C}_n} f(d_1)g(d_2) = (g*f)(n)$. Vrai pour tout $n \in \mathbb{N}^*$, donc $f*g = g*f$. Vrai pour toutes fonctions $f, g \in \mathbb{A}$, donc

La loi $*$ est commutative.

4. Soient $f, g, h \in \mathbb{A}$ et $n \in \mathbb{N}^*$. On a :

$$\begin{aligned}
(f*(g*h))(n) &= \sum_{(a,b)\in\mathcal{C}_n} f(a)(g*h)(b) \\
&= \sum_{(a,b)\in\mathcal{C}_n} f(a) \sum_{(c,d)\in\mathcal{C}_b} g(c)h(d) \\
&= \sum_{(a,c,d)\in\mathcal{C}'_n} f(a)g(c)h(d) \\
&= \sum_{(b,d)\in\mathcal{C}_n} \left( \sum_{(a,c)\in\mathcal{C}_b} f(a)g(c) \right) h(d) \\
&= \sum_{(b,d)\in\mathcal{C}_n} (f*g)(b)h(d) \\
&= ((f*g)*h)(n).
\end{aligned}$$

En effet, $(c, d) \in \mathcal{C}_b$ et $(a, b) \in \mathcal{C}_n$ si seulement si $ab = n$ et $cd = b$ *i.e* $acd = n$ soit $(a, c, d) \in \mathcal{C}'_n$. Vrai pour tout $n \in \mathbb{N}^*$ donc $f*(g*h) = (f*g)*h$. Vrai pour tous $f, g, h \in \mathbb{A}$ donc

La loi $*$ est associative.

1. Vous pouvez envoyez vos remarques ainsi que les irréductibles erreurs et fautes de frappes qui se seront glissées dans ce document à l'adresse suivante pierre-amaury.monard@laposte.net. L'auteur vous en sera reconnaissant.

5. L'ensemble $(\mathbb{A}, +)$ est un groupe abélien car $(\mathbb{C}^{\mathbb{N}^*}, +, \cdot)$ est un $\mathbb{C}$-espace vectoriel. La loi de composition interne $\delta$ sur $\mathbb{A}$ est associative, commutative et admet un élément neutre. Vérifions qu'elle est distributive par rapport à $+$. Soient $f, g, h \in \mathbb{A}$ et $n \in \mathbb{N}^*$. On a $((f+g)*h)(n) = \sum_{d|n}(f+g)(d)h(\frac{n}{d}) = \sum_{d|n} f(d)h(\frac{n}{d}) + \sum_{d|n} g(d)h(\frac{n}{d}) = (f*h)(n) + (g*h)(n)$. Vrai pour tout $n \in \mathbb{N}^*$ donc $(f+g)*h = f*h + g*h$. Donc $*$ est distributive à gauche par rapport à $+$ et comme $*$ est commutative, elle est aussi distributive à droite. En conclusion,

$(\mathbb{A}, +, *)$ est un anneau commutatif.

## I.B. Groupe des fonctions multiplicatives

6. Soient $f, g \in \mathbb{M}$ deux fonctions multiplicatives. Commençons par montrer que $f(1) = g(1) = 1$. Comme 1 et 1 sont premiers entre eux, on a $f(1.1) = f(1)f(1)$ d'où $f(1) = 0$ ou $f(1) = 1$. Or $f(1) \neq 0$ par définition d'une fonction multiplicative, donc $f(1) = 1$. Ceci est vrai pour toute fonction multiplicative, donc $g(1) = 1$ aussi.

   Soit $n \geqslant 2$. D'après le théorème fondamental de l'arithmétique, il existe $p_1, \dots, p_r \in \mathcal{P}$ des nombres premiers distincts et $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$ des entiers non nuls tels que $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. On a alors $f(p_1^{\alpha_1}) = g(p_1^{\alpha_1})$ par hypothèse sur $f$ et $g$. Si $f(p_1^{\alpha_1} \dots p_k^{\alpha_k}) = g(p_1^{\alpha_1} \dots p_k^{\alpha_k})$ pour un certain $k \in \{1, \dots, r-1\}$ alors comme $p_1^{\alpha_1} \dots p_k^{\alpha_k}$ et $p_{k+1}^{\alpha_{k+1}}$ sont premiers entre eux, on a

$$\begin{aligned} f(p_1^{\alpha_1} \dots p_{k+1}^{\alpha_{k+1}}) &= f(p_1^{\alpha_1} \dots p_k^{\alpha_k}) f(p_1^{\alpha_1}) \\ &= g(p_1^{\alpha_1} \dots p_k^{\alpha_k}) g(p_1^{\alpha_1}) \\ &= g(p_1^{\alpha_1} \dots p_{k+1}^{\alpha_{k+1}}). \end{aligned}$$

   Donc, par récurrence finie sur $k = 1, \dots, r$ on a bien $f(p_1^{\alpha_1} \dots p_k^{\alpha_k}) = g(p_1^{\alpha_1} \dots p_k^{\alpha_k})$. En particulier, pour $k = r$ on tombe bien sur $f(n) = g(n)$. Vrai pour tout $n \geqslant 2$ (et $n = 1$), donc $f = g$.

   Si $f$ et $g$ multiplicatives coïncident sur les puissances des nombres premiers, alors $f = g$.

   Remarque : si $(a_{p,k})$ est une famille d'entiers indexée par $\mathcal{P} \times \mathbb{N}^*$ alors il existe une unique fonction multiplicative $f$ telle que $f(p^k) = a_{p,k}$. C'est celle définie par $f(p_1^{\alpha_1} \dots p_r^{\alpha_r}) = a_{p_1,\alpha_1} \dots a_{p_r,\alpha_r}$.

7. Écrivons $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ et $m = q_1^{\beta_1} \dots q_s^{\beta_s}$ la décomposition en facteurs premiers de $n$ et $m$. Remarquons que $s$ et $r$ peuvent être éventuellement nuls si $n$ ou $m$ vaut 1 ; ce n'est pas un problème. Puisque $n$ et $m$ sont premiers entre eux, les facteurs premiers de $n$ et de $m$ sont disjoints. Autrement dit, les nombres $p_1, \dots p_r, q_1, \dots q_s$ sont distincts deux à deux.

   L'ensemble $\mathcal{D}_n$ (resp. $\mathcal{D}_m$) des diviseurs de $n$ (resp. $m$) est l'ensemble des nombres de la forme $p_1^{\gamma_1} \dots p_r^{\gamma_r}$ où $\gamma_i \leqslant \alpha_i$ (resp. $q_1^{\gamma_1} \dots q_s^{\gamma_s}$ et $\gamma_i \leqslant \beta_i$) pour tout $i$. La décomposition en facteurs premiers de $nm$ étant, $p_1^{\alpha_1} \dots p_r^{\alpha_r} q_1^{\beta_1} \dots q_s^{\beta_s}$, l'ensemble $\mathcal{D}_{nm}$ des diviseurs de $nm$ est l'ensemble des entiers de la forme $p_1^{\gamma_1} \dots p_r^{\gamma_r} q_1^{\delta_1} \dots q_s^{\delta_s}$ où $\gamma_i \leqslant \alpha_i$ et $\delta_i \leqslant \beta_i$. L'application $\pi : \mathcal{D}_n \times D_m \to \mathcal{D}_{nm}$ est donc bien définie. L'écriture $\ell = p_1^{\gamma_1} \dots p_r^{\gamma_r} q_1^{\delta_1} \dots q_s^{\delta_s}$ fait naturellement apparaître une décomposition $\ell = d_1 d_2$ où $d_1 | n$ et $d_2 | m$ (il suffit de séparer les $p_i$ des $q_j$ ce qui montre la surjectivité de $\pi$. L'injectivité de $\pi$ découle de l'unicité de la décomposition en facteur premiers. (On peut aussi invoquer l'égalité des cardinaux des ensembles de départ et d'arrivée de $\pi$).

   La fonction $\pi : \mathcal{D}_n \times D_m \to \mathcal{D}_{nm}$ est bijective si l'on sait dénombrer $\mathcal{D}_n$ en fonction de la décomposition en

8. Soient $n, m \in \mathbb{N}^*$ premiers entre eux. Alors,

$$\begin{aligned} (f*g)(nm) &= \sum_{d \in \mathcal{D}_{nm}} f(d) g(\frac{nm}{d}) \\ &= \sum_{a \in \mathcal{D}_n, b \in \mathcal{D}_m} f(ab) g(\frac{nm}{ab}) \end{aligned}$$

d'après la question précédente,

$$= \sum_{a\in\mathcal{D}_n} \sum_{b\in\mathcal{D}_m} f(a)f(b)g(\frac{n}{a})g(\frac{m}{b})$$

car $a \wedge b = 1$ et $\frac{n}{a} \wedge \frac{m}{b} = 1$ car $n$ et $m$ sont premiers entre eux,

$$= \left(\sum_{a\in\mathcal{D}_n} f(a)g(\frac{n}{a})\right)\left(\sum_{b\in\mathcal{D}_m} f(b)g(\frac{m}{b})\right)$$
$$= (f*g)(n)(f*g)(m).$$

Donc $f * g$ est multiplicative.

L'ensemble $\mathbb{M}$ des fonctions multiplicatives est stable par $*$.

9. Soit $f \in \mathbb{A}$.
Commençons par l'unicité. Supposons qu'une telle fonction multiplicative $g$ existe. Montrons alors que $f * g = \delta$. Soit $p \in \mathcal{P}$ et $k \in \mathbb{N}^*$. Alors $(f*g)(p^k) = f(1)g(p^k) + \sum_1^k f(p^i)g(p^{k-i}) = 0$. Donc $f * g$ est multiplicative d'après la question précédente et elle coïncide avec $\delta$ sur les puissances de nombres premiers, donc d'après la question 6, $f * g = \delta$. Comme $*$ est commutative, on as aussi $g * f = \delta$. Donc $f$ admet un inverse pour la loi $*$ et $f^{-1} = g$. Par unicité de l'inverse, $g$ est unique.
Pour l'existence, nous allons construire $g$ à la main. Commençons par poser $g(1) = 1$. Soit $p \in \mathcal{P}$ un nombre premier. On a déjà défini $g(p^0)$. On défini $g(p^k)$ par récurrence en posant $g(p^k) = -\sum_1^k f(p^i)g(p^{k-i})$ une fois $g(p^0), g(p^1), \ldots, g(p^{k-1})$ construits. Soit $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ un entier où les $p_i$ sont des nombres premiers distincts. On définit $g(n)$ par $g(n) := g(p_1^{\alpha_1}) \ldots g(p_r^{\alpha_r})$. Cette définition assure que $g$ est multiplicative d'après la remarque faite à la question 6. De plus $g$ vérifie bien la l'égalité souhaitée.

Tout élément de $\mathbb{M}$ admet un inverse dans $\mathbb{M}$ pour la loi $*$.

10. D'après la question 8, $*$ est une LCI sur $\mathbb{M}$. Puisque $\delta$ est multiplicative, cette loi possède un élément neutre. D'après la question précédente,tout élément de $\mathbb{M}$ admet un inverse pour la loi $*$. La loi $*$ est donc une loi de composition interne, admettant un élément neutre et telle que tout élément admet un inverse. Elle est de plus associative et commutative d'après la partie **I**.

$(\mathbb{M}, *)$ est un groupe abélien.

## I.C. La fonction de Möbius

11. On remarque tout d'abord que $\mu(1) \neq 0$. Soient $n, m$ premiers entre eux. Si $n$ ou $m$ est divisible par le carré d'un nombre premier, alors $nm$ aussi est divisible par le carré d'un nombre premier donc $\mu(n)\mu(m) = 0 = \mu(nm)$. Sinon, on écrit $n = p_1 \ldots p_r$ et $m = q_1 \ldots q_s$ où les $p,q_j$ sont des nombres premiers, les $p_i$ étant distincts, les $q_j$ étant distincts. On a alors $\mu(n) = (-1)^r$ et $\mu(m) = (-1)^s$ y compris si $r = 0$ ou $s = 0$. Puisque $n$ et $m$ sont premiers entre eux, les $p_i$ sont distincts des $q_j$, et $nm = p_1 \ldots p_r q_1 \ldots q_s$ est un produit de $r + s$ nombres premiers distincts. Donc $\mu(nm) = (-1)^{r+s} = \mu(n)\mu(m)$. Vrai pour tout $n, m$ premiers entre eux, donc

$\mu$ est multiplicative.

12. Soit $n \in \mathbb{N}^*$. Écrivons $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ sa décomposition en facteurs premiers, toujours avec $r = 0$ si $n = 1$. Alors,

$$(\mu * \mathbf{1})(n) = \sum_{d|n} \mu(d)\mathbf{1}(\frac{n}{d}).$$

Puisque $\mu(d) = 0$ dès qu'un facteur carré apparaît dans la décomposition en facteurs premiers de $d$, on ne garde dans la somme que les diviseurs de $n$ de la forme $p_1^{\epsilon_1} \dots p_r^{\epsilon_r}$ où $\epsilon_i \in \{0, 1\}$ pour tout $i = 1, \dots, r$.

$$\begin{aligned}
&= \sum_{\epsilon_1, \dots \epsilon_r} \mu(p_1^{\epsilon_1} \dots p_r^{\epsilon_r}) \\
&= \sum_{\epsilon_1, \dots \epsilon_r} (-1)^{\epsilon_1 + \dots + \epsilon_r} \\
&= \sum_{k=0}^{r} \sum_{I \subset \{1, \dots, r\}, |I| = k} (-1)^{|I|}
\end{aligned}$$

en faisant une disjonction de cas sur $k$ le nombre d'indices $i$ tels que $\epsilon_i = 1$,

$$\begin{aligned}
&= \sum_{0}^{r} \binom{r}{k} (-1)^k \\
&= (1 - 1)^r \\
&= 0^r \\
&= \delta_{0,r}
\end{aligned}$$

Or $r = 0$ si et seulement si $n = 1$. Autrement dit, $(\mu * \mathbf{1})(n) = \delta(n)$.

$$\boxed{\mu * \mathbf{1} = \delta.}$$

13. D'après la façon dont $F$ est définie, on a $F = f * \mathbf{1}$. Multiplions cette égalité par $\mu$ : $F * \mu = f * \mathbf{1} * \mu = f * \delta = f$ car $\mu$ est l'inverse de $\mathbf{1}$ pour la loi $*$. Ainsi, on peut « inverser » la formule et exprimer $f$ en fonction de $F$ : $f(n) = (F * \mu)(n) = \sum_{d|n} F(d)\mu(\frac{n}{d})$.

$$\boxed{\text{Pour tout } n \in \mathbb{N}^*,\ f(n) = (F * \mu)(n) = \textstyle\sum_{d|n} F(d)\mu(\frac{n}{d}).}$$

14. Soit $n \in \mathbb{N}^*$. Considérons la liste de rationnels suivantes : $\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$. Il y a $n$ termes. Chaque fraction $\frac{k}{n}$ s'écrit de manière unique sous la forme $\frac{l}{d}$ où $l$ et $d$ sont des entiers naturels premiers entre eux. De l'égalité $\frac{k}{n} = \frac{l}{d}$ on tire $kd = nl$ donc $d$ divise $nl$. Or $d \wedge l = 1$ donc $d$ divise $n$ d'après le lemme de Gauss. De plus, $\frac{k}{n} \leqslant 1$ donc $l \leqslant d$. Réciproquement, toute fraction de la forme $\frac{l}{d}$ avec $d|n$, $l \wedge d = 1$ et $l \leqslant d$ peut se mettre sous la forme $\frac{k}{n}$ en posant simplement $k = \frac{ln}{d} \in \{1, \dots, n\}$. Pour chaque diviseur $d$ de $n$ il y a $\varphi(d)$ entiers $l \leqslant d$ premiers avec $d$ d'où $n = \sum_{d|n} \varphi(d)$.
Ainsi, $\mathbf{I} = \varphi * \mathbf{1}$. D'après la question précédente, $\varphi = \mathbf{I} * \mu$.

$$\boxed{\varphi = \mu * \mathbf{I}.}$$

## I.D. Déterminant de Smith

15. Soient $i, j \in [\![1, n]\!]$.

$$\begin{aligned}(M'^t D)_{ij} &= \sum_{k=1}^{n} m'_{ik} d_{jk} \\ &= \sum_{k=1}^{n} g(k) \mathbf{1}_{k|i} \mathbf{1}_{k|j} \\ &= \sum_{k|i\wedge j} g(k)\end{aligned}$$

car un entier $k$ divise $i$ et $j$ si et seulement si il divise $i \wedge j$,

$$= (g * \mathbf{1})(i \wedge j)$$

car $g * \mathbf{1} = f$

$$\begin{aligned}&= f(i \wedge j) \\ &= M_{ij}.\end{aligned}$$

$$\boxed{M = M'^t D.}$$

16. Prenons le déterminant de l'égalité matricielle que nous venons d'obtenir : $\det(M) = \det(M')\det(D)$. Or $M'$ et $D$ sont des matrices triangulaires inférieures car $j$ ne peut diviser $i$ si $i < j$. Donc $\det(M') = m_{11} \dots m_{nn} = g(1) \dots g(n)$ et $\det(D) = d_{11} \dots d_{nn} = 1$ car $d_{ii} = 1$.

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

## I.E. Séries de Dirichlet

17. Soit $s > A_c(f)$. Alors il existe $t < s$ tel que $\sum \frac{f(k)}{k^t}$ converge absolument par définition de la borne inférieure. Mais alors $k^t < k^s$ pour tout entier naturel $k$ non nul. D'où $\left|\frac{f(k)}{k^s}\right| \leqslant \left|\frac{f(k)}{k^t}\right|$ pour tout $k \geqslant 1$ et la série $\sum \frac{f(k)}{k^s}$ converge absolument par comparaison à une série absolument convergente.

$$\boxed{\text{La série } \sum \frac{f(k)}{k^s} \text{ converge absolument.}}$$

18. Soit $t > \max(A_c(f), A_c(g))$ un réel que l'on fixe. Par l'absurde, si $f \neq g$ alors on peut poser $k_0 := \min\{k \in \mathbb{N}^* : \ f(k) \neq g(k)\}$ puisqu'il s'agit du minimum d'une partie non vide de $\mathbb{N}^*$. Soit $s > t$. Alors $L_f(s) = L_g(s)$ d'où $f(k_0) - g(k_0) + k_0^s \sum_{k_0+1}^{\infty} \frac{f(k)-g(k)}{k^s} = 0$. Posons $h(s) := k_0^s \sum_{k_0+1}^{\infty} \frac{f(k)-g(k)}{k^s}$ et montrons que $h(s) \to 0$ quand $s$ tend vers $+\infty$. On a : $|h(s)| \leqslant k_0^s \sum_{k_0+1}^{\infty} \frac{|f(k)|+|g(k)|}{k^t} \cdot \frac{1}{k^{s-t}} \leqslant k_0^s C_t \frac{1}{(k_0+1)^{s-t}}$ où $C_t := \sum_{k_0+1}^{\infty} \frac{|f(k)|+|g(k)|}{k^t} < +\infty$ est finie par hypothèse sur $t$. D'où $|h(s)| \leqslant (k_0+1)^t C_t \left(\frac{k_0}{k_0+1}\right)^s \to 0$ quand $s \to +\infty$ car $\left|\frac{k_0}{k_0+1}\right| < 1$. Un passage à la limite dans l'égalité $f(k_0) - g(k_0) + h(s) = 0$ montre que $f(k_0) = g(k_0)$ ce qui est ABSURDE. Donc $f = g$.

$$\boxed{\text{Si } L_f(s) = L_g(s) \text{ pour } s \text{ assez grand alors } f = g}$$

19. Soit $s > \max(A_c(f), A_c(g))$. Les séries $\sum \frac{f(k)}{k^s}$ et $\sum \frac{g(k)}{k^s}$ étant absolument convergente, la série double $\sum a_{k,l}$ où $a_{k,l} := \frac{f(k)g(l)}{k^s l^s}$ est sommable sur $(\mathbb{N}^*)^2$ :

$$\begin{aligned} L_f(s)L_g(s) &= \left(\sum_1^{+\infty} \frac{f(k)}{k^s}\right)\left(\sum_1^{+\infty} \frac{g(k)}{k^s}\right) \\ &= \sum_{k,l\geqslant 1} \frac{f(k)g(l)}{k^s l^s} \\ &= \sum_{n\geqslant 1} \sum_{(k,l)\in\mathcal{C}_n} \frac{f(k)g(l)}{(kl)^s} \end{aligned}$$

puisque les ensembles $\mathcal{C}_n$ pour $n \geqslant 1$ forment une partition dénombrable de $(\mathbb{N}^*)^2$,

$$\begin{aligned} &= \sum_1^{\infty} \left(\sum_{(k,l)\in\mathcal{C}_n} f(k)g(l)\right) \frac{1}{n^s} \\ &= \sum_1^{\infty} \frac{(f*g)(n)}{n^s} \\ &= L_{f*g}(s). \end{aligned}$$

Pour $s$ assez grand, $L_{f*g}(s) = L_f(s)L_g(s)$.

# II. Matrices et endomorphismes de permutation

## II.A. Similitude de deux matrices de permutation

20. Soient $\sigma, \tau \in \mathfrak{S}_n$ des permutations. La matrice $P_\sigma P_\tau$ a pour terme général $(P_\sigma P_\tau)_{ij} = \sum_{k=1}^n (P_\sigma)_{ik}(P_\tau)_{kj} = \sum_{k=1}^n \delta_{i,\sigma(k)}\delta_{k,\tau(j)} = \delta_{i,\sigma\tau(j)} = (P_{\sigma\tau})_{ij}$. Donc les matrices $P_\sigma P_\tau$ et $P_{\sigma\tau}$ sont égales.

$P_\sigma P_\tau = P_{\sigma\tau}$.

En particuliers, $P_\sigma P_{\sigma^{-1}} = P_{id} = I_n$ donc les matrices de permutations sont inversibles et de plus $(P_\sigma)^{-1} = P_{\sigma^{-1}}$. On a ainsi montré que $P : \mathfrak{S}_n \to GL_n(\mathbb{R})$ défini par $\sigma \mapsto P_\sigma$ est un morphisme de groupe.
Si $\sigma$ et $\tau$ sont conjugués, il existe $\gamma \in \mathfrak{S}_n$ tel que $\sigma = \gamma\tau\gamma^{-1}$. D'où, $P_\sigma = P_\gamma P_\tau P_{\gamma^{-1}}$ et les matrices $P_\sigma$ et $P_\tau$ sont semblables via la matrice de passage $P_\gamma$.

Si $\sigma$ et $\tau$ sont conjugués alors $P_\sigma$ et $P_\tau$ sont semblables.

21. Montrons le résultat suivant : si $\gamma = (a_1 \dots a_r)$ est un $r$-cycle de $\mathfrak{S}_n$ et $\sigma \in \mathfrak{S}_n$ alors $\sigma\gamma\sigma^{-1} = (\sigma(a_1)\,\sigma(a_2)\dots\sigma(a_r))$. En effet, avec la convention $a_{r+1} = a_1$, on a $\sigma\gamma\sigma^{-1}(\sigma(a_i)) = \sigma\gamma(a_i) = \sigma(a_{i+1})$ et pour $x \notin \{\sigma(a_1), \dots, \sigma(a_r)\}$ on a $\sigma^{-1}(x) \notin \{a_1, \dots, a_r\}$ et donc $\gamma\sigma^{-1}(x) = \sigma^{-1}x$ d'où $\sigma\gamma\sigma^{-1}(x) = x$ ce qui prouve bien que $\sigma\gamma\sigma^{-1} = (\sigma(a_1)\dots\sigma(a_r))$.

Pour $\gamma_1 = (1\ 3\ 7)$ et $\rho$ qui envoie 1 sur 2, 3 sur 6 et 7 sur 4 on a $\rho\gamma\rho^{-1} = (2\ 6\ 4) = \gamma_2$.

$\rho\gamma_1\rho^{-1} = \gamma_2$.

22. Soient $(a_1 \dots a_r)$ et $(b_1 \dots b_r)$ deux cycles de même longueur de $\mathfrak{S}_n$. D'après le lemme montré à la question précédente, il suffit de montrer qu'il existe $\sigma \in \mathfrak{S}_n$ tel que $\sigma(a_i) = b_i$ pour tout $i = 1, \dots, r$ pour montrer que ces deux cycles sont conjugués car alors $\sigma(a_1 \dots a_r)\sigma^{-1} = (b_1 \dots b_r)$. Une telle permutation existe toujours car les $a_i$ sont disjoints et de même pour les $b_i$.

Dans $\mathfrak{S}_n$, deux cycles de même longueur sont conjugués.

23. Notons $\sigma = \gamma_1 \dots \gamma_s$ la décomposition en cycles à supports disjoints en incluant les cycles de longueur 1 (qui correspondent aux points fixes de $\sigma$). Alors, pour $\rho \in \mathfrak{S}_n$, $\rho\sigma\rho^{-1} = \rho\gamma_1 \dots \gamma_s\rho^{-1} = \rho\gamma_1\rho^{-1}\rho\gamma_2\rho^{-1} \dots \rho\gamma_s\rho^{-1}$. Mais d'après le lemme de la question 21, $\rho\gamma_i\rho^{-1}$ est un cycle de même longueur que $\gamma_i$. De plus, les cycles $\rho\gamma_i\rho^{-1}$ sont à supports disjoints par injectivité de $\rho$. Ainsi, si $\tau = \rho\sigma\rho^{-1}$, alors $\rho\gamma_1\rho^{-1} \dots \rho\gamma_s\rho^{-1}$ est la décomposition en cycles à supports disjoints de $\tau$. Et puisque la conjugaison préserve la longueur des cycles, $c_\ell(\sigma) = c_\ell(\tau)$ pour tout $l = 1, \dots, n$.

Réciproquement si $\sigma$ et $\tau$ ont le même type cyclique *i.e* $c_\ell(\sigma) = c_\ell(\tau)$ pour tout $l = 1, \dots, n$ alors on peut écrire $\sigma = \gamma_1 \dots \gamma_r$, $\tau = \delta_1 \dots \delta_r$ les décomposition en cycles à supports disjoints de $\sigma$ et $\tau$ tel que les cycles $\gamma_i$ et $\delta_i$ sont de même longueur $k_i \in [\![1, n]\!]$ et $k_1 + \dots + k_r = n$. Cette dernière condition revient à inclure les points fixes dans la décomposition. Écrivons $\gamma_i = (a_{i1} \dots a_{ik_i})$ et $\delta_i = (b_{i1} \dots b_{ik_i})$. On dispose alors des égalités ensemblistes suivantes : $[\![1, n]\!] = \{a_{11}, \dots, a_{rk_r}\} = \{b_{11}, \dots b_{rk_r}\}$. Soit $\rho \in \mathfrak{S}_n$ l'unique permutation de $[\![1, n]\!]$ qui envoie $a_{ij}$ sur $b_{ij}$ pour tout $i = 1, \dots, r$ et $1 \leqslant j \leqslant k_j$. Alors $\rho\gamma_i\rho^{-1} = \delta_i$ et $\rho\sigma\rho^{-1} = \tau$ ce qui montre que $\sigma$ et $\tau$ sont conjugués.

$\sigma$ et $\tau$ sont conjugués si et seulement si ils ont le même type cyclique.

24. Soit $\gamma \in \mathfrak{S}_\ell$ un cycle de longueur $\ell$. Alors $\gamma$ est conjugué au cycle $\gamma_0 = (1\ 2 \dots \ell)$ d'après la question 22. Les matrices $P_\gamma$ et $P_{\gamma_0}$ sont donc semblables. Le polynôme caractéristique étant un invariant de similitude, $\chi_\gamma = \chi_{\gamma_0}$. Il suffit donc de calculer $\chi_{\gamma_0}$. La matrice $P_{\gamma_0}$ est la matrice $\Gamma_\ell$ donnée par l'énoncé. Il s'agit de la matrice compagnon associée au polynôme $X^\ell - 1$ donc $\chi_{\gamma_0} = \chi_{\Gamma_\ell} = X^\ell - 1$ ce qui conclut.

$\chi_\gamma(X) = X^\ell - 1.$

25. Si $\ell = 1$ alors $\Gamma_\ell = (1)$ et $\chi_\ell = X - 1$.
Soit $\sigma = \gamma_1 \dots \gamma_r$ la décomposition de $\sigma$ en cycles à supports disjoints en incluant les points fixes. Deux cycles à supports disjoints commutant, on peut supposer que les $\gamma_i$ sont rangés par longueur croissante. Quitte à conjuguer $\sigma$ par la permutation qui « réarrange » les entiers par ordre croissant, on peut supposer $\sigma = (1\ 2 \dots, k_1)(k_1{+}1\ \dots k_1{+}k_2) \dots (\dots n{-}1\ n)$ où $k_i$ est la longueur du cycle $\gamma_i$. La matrice $P_\sigma$ est donc la matrice diagonale par bloc $D = \mathrm{Diag}(\Gamma_{k_1}, \dots, \Gamma_{k_r})$. La matrice $\Gamma_\ell$ apparaît autant de fois qu'il y a de cycles de longueur $\ell$ dans la décomposition en cycles de $\sigma$ *i.e* $c_\ell(\sigma)$ fois. Donc $\chi_\sigma(X) = \prod_1^n \chi_\ell(X)^{c_\ell(\sigma)}$.

$\chi_\sigma(X) = \prod_1^n (X^\ell - 1)^{c_\ell(\sigma)}.$

26. Si $P_\sigma$ et $P_\tau$ sont semblables, elles ont le même polynôme caractéristique. D'où $\prod_1^n (X^\ell - 1)^{c_\ell(\sigma)} = \prod_1^n (X^\ell - 1)^{c_\ell(\tau)}$. Notons $T$ ce polynôme. Soit $q \in [\![1, n]\!]$. On s'intéresse à la multiplicité de $\omega_q := \mathrm{e}^{\frac{2\pi i}{q}}$ en tant que racine de $T$. Exceptionnellement, on dira que $\omega_q$ est racine de $T$ de multiplicité 0 si $\omega_q$ n'est pas une racine de $P$.
Si $\lambda \in \mathbb{C}$ est de multiplicité $\alpha$ dans $R$ et $\beta$ dans $S$ alors il est de multiplicité $\alpha + \beta$ dans $RS$. Donc $\omega_q$ est de multiplicité $\sum_{\ell=1}^n c_\ell(\sigma) m_\ell$ dans $T$ où $m_\ell$ est la multiplicité de $\omega_q$ dans $X^\ell - 1$. Or, $\omega_q$ est racine de $X^\ell - 1$ si et seulement si $\mathrm{e}^{\frac{2\pi i \ell}{q}} = 1$ si et seulement si $\frac{\ell}{n}$ est un entier *ie* $q$ divise $\ell$. Donc $m_\ell = \mathbf{1}_{q|\ell}$. Ainsi, $\omega_q$ est de multiplicité $\sum_{q|\ell} c_\ell(\sigma)$ dans $T$. Mais puisque $\chi_\sigma = \chi_\tau$, $\omega_q$ est également de multiplicité $\sum_{q|\ell} c_\ell(\tau)$ dans $T$ d'où l'égalité recherchée.

$$\boxed{\text{Pour tout } q = 1, \dots, n, \sum_{q|\ell} c_\ell(\sigma) = \sum_{q|\ell} c_\ell(\tau).}$$

27. Suivons l'indication de l'énoncé et calculons $T_\sigma D$ qui est une matrice ligne de longueur $n$. Soit $q \in [\![1, n]\!]$. On a : $(T_\sigma D)_{1,q} = \sum_{\ell=1}^n (T_\sigma)_{1,\ell} D_{\ell,q} = \sum_{\ell=1}^n c_\ell(\sigma) \mathbf{1}_{q|\ell}$. Ainsi, si $P_\sigma$ et $P_\tau$ sont semblables, les matrices $T_\sigma D$ et $T_\tau D$ sont égales d'après la question précédente. Or $D$ est inversible (triangulaire avec aucun zéro sur la diagonale) donc $T_\sigma = T_\tau$. Ainsi, les permutations $\sigma$ et $\tau$ sont de même type cyclique donc sont conjuguées d'après la question 23. Ceci prouve la réciproque à la question 20.

$$\boxed{\sigma \text{ et } \tau \text{ sont conjugués si et seulement si } P_\sigma \text{ et } P_\tau \text{ sont semblables.}}$$

## II.B. Endomorphismes de permutation

28. Soit $u \in \mathcal{L}(E)$ un endomorphisme de permutation. Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de $E$ et $\sigma \in \mathfrak{S}_n$ tels que $u(e_j) = e_{\sigma(j)}$. Alors $u(e_j) = \sum_{i=1}^n \delta_{i,\sigma(j)} e_i$. La matrice de $u$ dans la base $\mathcal{B}$ a pour terme général $\delta_{i,\sigma(j)}$...c'est donc $P_\sigma$.

    Réciproquement, si $mat_\mathcal{B}(u) = P_\sigma$ pour une certaine base $\mathcal{B} = (e_1, \dots, e_n)$ de $E$ et un certain $\sigma \in \mathfrak{S}_n$. Alors $u(e_j) = \sum_{i=1}^n \delta_{i,\sigma(j)} e_i = e_{\sigma(j)}$ pour tout $j = 1, \dots, n$. L'endomorphisme $u$ est alors un endomorphisme de permutation.

    $$\boxed{u \text{ est de permutation ssi } mat_\mathcal{B}(u) = P_\sigma \text{ pour une certaine base } \mathcal{B} \text{ et } \sigma \in \mathfrak{S}_n.}$$

29. Soit $\sigma \in \mathfrak{S}_n$ tel que $mat_\mathcal{B}(u) = P_\sigma$ pour une certaine base $\mathcal{B}$ de $E$. Le groupe $\mathfrak{S}_n$ étant fini, il existe un entier $k$ tel que $\sigma^k = \mathrm{id}_{[\![1,n]\!]}$. Alors, $(P_\sigma)^k = P_{\mathrm{id}_{[\![1,n]\!]}} = I_n$. Ainsi, le polynôme $X^k - 1$ annule la matrice $P_\sigma$. Or $X^k - 1$ est scindé à racine simple sur $\mathbb{C}$. L'endomorphisme $u$ est donc annulé par un polynôme scindé à racines simples ; il est donc diagonalisable.

    $$\boxed{\text{L'endomorphisme } u \text{ est diagonalisable.}}$$

    De plus, $\mathrm{Tr}(u)$ est la somme des coefficients diagonaux de $P_\sigma$. La matrice $P_\sigma$ ne contient que des 0 et des 1 donc sa trace est le nombre de 1 sur sa diagonale ; il s'agit donc d'un entier compris entre 0 et $n$.

    $$\boxed{\mathrm{Tr}(u) \in [\![0, n]\!].}$$

    En fait, la trace de $u$ est le nombre de points fixes de $\sigma$.

30. Si $A$ et $B$ sont semblables alors elles ont le même polynôme caractéristique.

    Réciproquement, supposons que $\chi_A = \chi_B$. Notons $P = \prod_1^r (X - \lambda_i)^{m_i}$ ce polynôme commun. Commençons par remarquer que $A$ et $B$ partagent le même spectre à savoir $\{\lambda_1, \dots, \lambda_r\}$. Puisque $A$ est diagonalisable, $A$ est semblable à la matrice diagonale par blocs $D = \mathrm{Diag}(\lambda_1 I_{m_1}, \dots, \lambda_r I_{m_r})$. En effet, pour une matrice diagonalisable, la multiplicité algébrique d'une valeur propre (nombre de fois où elle apparaît dans une base de diagonalisation) est égale à sa multiplicité algébrique (multiplicité en tant que racine du polynôme caractéristique). Il en va de même pour $B$. Donc $A$ et $B$ sont semblables à une même matrice $D$ donc sont semblables.

    $$\boxed{A \text{ et } B \text{ diagonalisables sont semblables si et seulement si } \chi_A = \chi_B.}$$

31. On a déjà vu à la question 29 que si $u$ est de permutation, alors sa trace est un entier naturel.

Réciproquement, supposons que $\mathrm{Tr}(u)$ soit un entier naturel. Puisque $u$ est une symétrie, on dispose de la décomposition $E = E_1(u) \oplus E_{-1}(u)$. Dans une base adaptée à cette décomposition la matrice de $u$ est $\mathrm{Diag}(I_{n-r}, I_r)$ où $r = \dim E_{-1}(u)$. La trace de $u$ est alors $(n-r)-r$. Puisque $\mathrm{Tr}(u)$ est un entier **naturel** on en déduit $r \leqslant n-r$. On pose $k = n-r$. Soit $(e_1, \dots, e_r, e_{r+1}, \dots, e_k)$ une base de $E_1(u)$ et $(f_1, \dots, f_r)$ une base de $E_{-1}(u)$. On a $u(e_i) = +e_i$ et $u(f_i) = -f_i$. Posons $v_i := e_i + f_i$ et $w_i = e_i - f_i$ pour tout $i \in [\![1, r]\!]$. On considère la famille $\mathcal{B} = (v_1, w_1, \dots, v_r, w_r, e_{r+1}, \dots, e_k)$. Montrons que c'est une base de $E$. Elle est de cardinal $2r + (k-r) = n$. De plus, la famille $(e_1, \dots, e_k, f_1, \dots, f_r)$ est une base de $E$ et chacun de ses vecteurs est combinaison linéaire de vecteurs de la famille $\mathcal{B}$. La famille $\mathcal{B}$ est donc génératrice et c'est une base de $E$. Dans la base $\mathcal{B}$, la matrice de $u$ est $P_\sigma$ où $\sigma = (1\ 2)(3\ 4)\dots(2r-1\ 2r)(2r+1)\dots(n)$. L'endomorphisme $u$ est bien de permutation.

Une symétrie $u$ est de permutation si et seulement si $\mathrm{Tr}(u) \in \mathbb{N}$.

32. Le sens gauche directe de l'équivalence précédente est toujours vérifiée.

Pour $k = 3$. L'endomorphisme $u$ est annulé par le polynôme $X^3 - 1$ scindé à racine simple sur $\mathbb{C}$ donc est diagonalisable et $E = E_1(u) \oplus E_j(u) \oplus E_{j^2}(u)$. Notons $a, b, c$ les multiplicités de $1, j, j^2$. Alors $\mathrm{Tr}(u) = a + bj + cj^2$. Si $\mathrm{Tr}(u)$ est un entier naturel, alors en particulier elle est réelle et $b = c$. Elle est de plus positive, donc $a + bj + bj^2 = a - b \geqslant 0$. On note $r := \dim E_j(u) = \dim E_{j^2}(u)$ et $k := n - 2r = \dim E_1(u)$. Soient $(e_1, \dots, e_k)$ une base de $E_1(u)$, $(f_1, \dots, f_r)$ une base de $E_j(u)$ et $(g_1, \dots, g_r)$ une base de $E_{j^2}(u)$. On pose $v_i := e_1 + f_i + g_i$, $w_i := e_i + jf_i + j^2 g_i$ et $z_i := e_i + j^2 f_i + j g_i$ pour tout $i = 1, \dots, r$. Alors, on vérifie rapidement que $u(v_i) = w_i$, $u(w_i) = z_i$ et $u(z_i) = v_i$. On considère la famille $\mathcal{B} = (v_1, w_1, z_1, \dots, v_r, w_r, z_r, e_{r+1}, \dots, e_k)$ de $E$. Elle est de cardinal $3r + (k-r) = n$. De plus chaque vecteur $e_i$, $f_i$ et $g_i$ peut s'écrire comme combinaison linéaire de vecteurs de $\mathcal{B}$. Donc $\mathcal{B}$ engendre $E_1(u), E_j(u)$ et $E_{j^2}(u)$ donc $E$ et c'est une base. Dans la base $\mathcal{B}$, la matrice de $u$ est $P_\sigma$ où $\sigma = (123)(456)\dots(3r-2\ 3r-1\ 3r)(3r+1)\dots(n)$. Donc $u$ est un endomorphisme de permutation.

Pour $k = 4$ la réciproque est fausse pour $n = 2$ (et $n \geqslant 2$ en adaptant le contre-exemple). Considérons l'endomorphisme $u$ de $\mathbb{R}^2$ dont la matrice dans la base canonique est $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$. On a bien $u^4 = \mathrm{id}_{\mathbb{R}^2}$. De plus, $\chi_u(X) = (X-i)(X+i) = X^2 + 1$. Or, pour $n = 2$, il n'existe que deux permutations : $\mathrm{id}_{[\![1,2]\!]}$ et $(12)$ dont les polynômes caractéristiques sont respectivement $(X-1)^2$ et $X^2 - 1$. Ainsi, $u$ ne peut être un endomorphisme de permutation. Pour $n = 1$, $u$ est de la forme $u = \lambda\,\mathrm{id}_E$ avec $\lambda \in \mathbb{N}$ tel que $\lambda^4 = 1$ donc $\lambda = 1$. Donc $u = \mathrm{id}_{\mathbb{R}^2}$ et est un endomorphisme de permutation.

Pour $k = 4$ le sens indirect n'est plus vrai si $n \geqslant 2$.

33. Soit $u$ un endomorphisme de permutation. Alors $\chi_u = \chi_\sigma$. Or on a vu à la question 25 que $\chi_\sigma(X) = \prod_1^n (X^\ell - 1)^{c_\ell(\sigma)}$. La condition $(a)$ est vérifiée avec $c_\ell = c_\ell(\sigma)$. De plus la réponse à la question 29 a montré l'existence intervenir un polynôme annulateur de $u$ de la forme $X^k - 1$ (prendre $k$ l'ordre de $\sigma$ dans $\mathfrak{S}_n$). La condition $(b)$ est alors vérifiée avec $N = k$.

Réciproquement, supposons les conditions $(a)$ et $(b)$ vérifiées. L'endomorphisme $u$ est annulé par le polynôme $X^N - 1$ qui est scindé à racines simples dans $\mathbb{C}$ donc $u$ est diagonalisable. Le degré de $\chi_u$ vaut $n = \sum_1^n \ell c_\ell$. Soit $\sigma \in \mathfrak{S}_n$ une permutation telle que sa décomposition en cycles à supports disjoints fait intervenir exactement $c_\ell$ cycles de longueur $\ell$ pour tout $\ell \in [\![1, n]\!]$. L'existence d'un tel $\sigma$ est assurée par la condition $\sum_1^n \ell c_\ell = n$. La matrice $P_\sigma$ et la matrice de $u$ dans une base quelconque de $E$ ont toutes deux pour polynôme caractéristique $\prod_1^n (X^\ell - 1)^{c_\ell}$. D'après la question 30 ces deux matrices sont semblables car elles sont de plus diagonalisables. Il existe une base de $E$ dans laquelle la matrice de $u$ est de la forme $P_\sigma$ et $u$ est de permutation.

$u$ est de permutation si et seulement si il vérifie $(a)$ et $(b)$.

34. Dans $\mathbb{C}[X]$ tout polynôme est scindé d'après le théorème de D'Alembert-Gauss. Écrivons $\chi_u = \prod_1^r (X-\lambda_i)_i^n$ et $\chi_v = \prod_1^s (X-\mu_i)_i^m$. Nous voulons montrer que $r=s$, $\lambda_i = \mu_i$ et $n_i = m_i$ pour tout $i = 1, \dots, r$. Les endomorphismes $u$ et $v$ sont annulés par leur polynômes caractéristiques d'après le théorème de Cayley-Hamilton qui sont scindés donc $u$ et $v$ sont trigonalisables. Dans une base de trigonalisation, $u$ est triangulaire supérieure avec comme coefficients diagonaux $\lambda_1, \dots, \lambda_r$. La valeur propre $\lambda_i$ apparaît $n_i$ fois. La trace de $u^k$ est donc $\mathrm{Tr}(u^k) = \sum_1^r n_i \lambda_i^k$. De même $\mathrm{Tr}(v^k) = \sum_1^s m_i \mu_i^k$.

    Soit $P \in \mathbb{C}[X]$. Par linéarité de la trace, on a $\mathrm{Tr}(P(u)) = \sum_1^r n_i P(\lambda_i)$. Puisque $\mathrm{Tr}(u^k) = \mathrm{Tr}(v^k)$ pour tout $k \geqslant 0$ alors $\mathrm{Tr}(P(u)) = \mathrm{Tr}(P(v))$. Supposons par l'absurde que $\{\lambda_1, \dots, \lambda_r\} \neq \{\mu_1, \dots, \mu_s\}$. Supposons par symétrie que que $\{\mu_1, \dots, \mu_s\} \not\subset \{\lambda_1, \dots, \lambda_r\}$. Il existe alors $j \in [\![1, s]\!]$ tel que $\mu_j \notin \{\lambda_1, \dots, \lambda_r\}$. Choisissons $P \in \mathbb{C}[X]$ tel que $P(\mu_j) = 1$ et $P$ est nul sur $\lambda_1, \dots, \lambda_r, \mu_1, \dots, \mu_{j-1}, \mu_{j+1}, \dots, \mu_s$. Un tel polynôme existe bien grâce à l'hypothèse faite sur $\mu_j$ (prendre un polynôme interpolateur de Lagrange). Mais alors, $\mathrm{Tr}(P(u)) = 0$ mais $\mathrm{Tr}(P(v)) = m_j.1$ ce qui est contradictoire. Donc $\{\lambda_1, \dots, \lambda_r\} = \{\mu_1, \dots, \mu_s\}$. Quitte à renommer les valeurs propres, on peut supposer $\lambda_i = \mu_i$ pour tout $i = 1, \dots, r$. Prenons maintenant $P_i \in \mathbb{C}[X]$ tel que $P(\lambda_i) = 1$ et $P(\lambda_j) = 0$ pour $j \neq i$ où $i \in [\![1, r]\!]$. Alors $n_i = \mathrm{Tr}(P_i(u)) = \mathrm{Tr}(P(v_i)) = m_i$ ce qui montre que $\chi_u = \chi_v$.

    Si $\mathrm{Tr}(u^k) = \mathrm{Tr}(v^k)$ pour tout $k \geqslant 0$, alors $\chi_u = \chi_v$.

35. Si $u$ est un endomorphisme de permutation. Il existe $\sigma \in \mathfrak{S}_n$ et une base base $\mathcal{B}$ de $E$ dans laquelle la matrice de $u$ est diagonale par blocs, de blocs $\Gamma_1, \dots, \Gamma_n$. Le bloc $\Gamma_\ell$ apparaît $c_\ell(\sigma)$ fois pour tout $\ell = 1, \dots, n$. Pour tout $k \geqslant 0$, $\mathrm{Tr}(u^k) = \sum_{\ell=1}^n c_\ell(\sigma) \mathrm{Tr}(\Gamma_\ell^k)$. Or $\Gamma_\ell$ est la matrice de permutation associée à $\gamma_0 = (1\,2 \dots \ell) \in \mathfrak{S}_\ell$. Donc $\mathrm{Tr}(\Gamma_\ell^k)$ est le nombre de points fixes de $\gamma_0^k$. La permutation $\gamma_0^k$ est la permutation identité si $\ell$ divise $k$ et sinon c'est un $\ell$-cycle de $\mathfrak{S}_\ell$ donc qui a 0 point fixe. Ainsi, $\mathrm{Tr}(\Gamma_\ell^k) = \ell \mathbf{1}_{\ell|k}$. D'où : $\mathrm{Tr}(u^k) = \sum_{\ell=1, \ell|k}^n \ell c_\ell(\sigma)$ pour tout $k \geqslant 0$.

    Réciproquement, supposons qu'il existe des entiers $c_1, \dots, c_n$ tels que $\mathrm{Tr}(u^k) = \sum_{\ell=1, \ell|k}^n \ell c_\ell$. En particulier, pour $k = 0$ on obtient : $\mathrm{Tr}(u^0) = n = \sum_{\ell=1}^n \ell c_\ell$ car tout entier divise 0. Donc il existe $\sigma \in \mathfrak{S}_n$ tel que $c_\ell(\sigma) = c_\ell$ pour tout $\ell = 1, \dots, n$. Soit $\mathcal{B}$ une base de $E$ et $v$ l'endomorphisme de $E$ défini par $v(e_i) = e_{\sigma(i)}$. Alors $v$ est un endomorphisme de permutation et d'après ce qui vient d'être dit, $\mathrm{Tr}(v^k) = \sum_{\ell=1, \ell|k}^n \ell c_\ell(\sigma)$. Donc $\mathrm{Tr}(u^k) = \mathrm{Tr}(v^k)$ pour tout $k \geqslant 0$ et $u$ et $v$ ont le même polynôme caractéristique d'après la question précédente. Or $u$ est diagonalisable par hypothèse et $v$ est diagonalisable d'après la question 29 donc les matrices de $u$ et de $v$ dans n'importe quelle base sont semblables d'après la question 30. Mais alors la matrice de $u$ dans une bonne base est $P_\sigma$ et $u$ est de permutation.

    $u \in \mathcal{L}(E)$ diagonalisable est de permutation ssi $\mathrm{Tr}(u^k) = \displaystyle\sum_{\ell=1, \ell|k}^n \ell c_\ell$ pour des entiers $c_1, \dots, c_n$.

## III. Valeurs propres de la matrice de Redheffer

36. Suivons l'indication de l'énoncé. $(C_n)_{11} = \sum_{k=1}^n a_{1k} h_{k1} = \sum_{k=1}^n \mu(k).1 = M(n)$. Pour $i > 1$, $(C_n)_{i1} = \sum_{k=1}^n a_{ik} h_{k1} = \sum_{k=1}^n \delta_{i,k}.h_{k1} = h_{i1} = 0$. Pour $i > 1$ et $j > 1$, $(C_n)_{ij} = \sum_{k=1}^n a_{ik} h_{kj} = \sum_{k=1}^n \delta_{i,k} \mathbf{1}_{k|j} = \mathbf{1}_{i|j}$. En particulier, $(C_n)_{ij} = 0$ dès que $i > j$. Donc $C_n$ est triangulaire supérieure et les coefficients sur sa diagonale sont $M(n), 1, \dots, 1$. D'où $\det C_n = M(n)$.
    Par ailleurs, $\det C_n = \det A_n \det H_n$ donc $M(n) = \det A_n \det H_n = \det H_n$ puisque $\det A_n = 1$ ($A_n$ est triangulaire supérieure avec des 1 sur la diagonale).

$$\boxed{\det H_n = M(n).}$$

37. La matrice $B_n(\lambda)$ est triangulaire avec pour coefficients diagonaux $\mathbf{b}(1), 1, \dots, 1$ donc $\det B_n(\lambda) = \mathbf{b}(1) = 1$. Donc $\chi_n(\lambda) = \det(\lambda I_n - H) = \det(B_n(\lambda)(\lambda I_n - H))$. Posons $T = (t_{ij})_{1\leqslant i,j\leqslant n} = B_n(\lambda)(\lambda I_n - H)$.
Pour $i = j = 1$, on a $t_{11} = \sum_1^n b_{1k}(\lambda\delta_{k1} - h_{k1}) = (\lambda - 1) - \sum_2^n \mathbf{b}(k)$.
Pour $i > 1, j > 1$, on a $t_{ij} = \sum_1^n b_{ik}(\lambda\delta_{k,j} - h_{k,j}) = \lambda\delta_{i,j} - \mathbf{1}_{i|j}$. En particulier, $t_{ij} = 0$ si $i > j > 1$ et $t_{ij} = \lambda - 1$ si $i = j > 1$.
Pour $i = 1$ et $j > 1$, on a $t_{1j} = \sum_{k=1}^n b_{1k}(\lambda\delta_{k,j} - h_{kj}) = \sum_{k=1}^n b_{1k}\mathbf{b}(k)(\lambda\delta_{k,j} - \mathbf{1}_{k|j}) = (\lambda - 1)\mathbf{b}(j) - \sum_{k|j,k\neq j} \mathbf{b}(k) = 0$.
Donc la première ligne de $T$ est $((\lambda - 1) - \sum_2^n \mathbf{b}(k), 0, \dots, 0)$. Un développement par rapport à la première ligne donne : $\det T = ((\lambda - 1) - \sum_2^n \mathbf{b}(k)) \det([T]_{11})$ où $[T]_{11}$ est la matrice obtenue à partir de $T$ en rayant la première ligne et la première colonne. Il s'agit d'une matrice triangulaire supérieure avec les coefficients $\lambda - 1$ sur la diagonale. D'où $\det([T]_{11}) = (\lambda - 1)^{n-1}$ et $\det T = (\lambda - 1)^n - (\lambda - 1)^{n-1} \sum_2^n \mathbf{b}(k)$.

$$\boxed{\text{Pour } \lambda \neq 1,\ \chi_n(\lambda) = (\lambda - 1)^n - (\lambda - 1)^{n-1} \sum_{k=2}^{n} b(k).}$$

38. Commençons par calculer $\mathbf{1} * \mathbf{b}$. On a $(\mathbf{1} * \mathbf{b})(1) = \mathbf{1}(1)\mathbf{b}(1) = 1$ et pour $n \geqslant 2, (\mathbf{1} * \mathbf{b})(n) = \sum_{k|n,k\neq n} \mathbf{b}(k) + \mathbf{b}(n) = (\lambda - 1)\mathbf{b}(n) + \mathbf{b}(n) = \lambda\mathbf{b}(n)$. Ainsi $\mathbf{1} * \mathbf{b} = \lambda\mathbf{b} + (1 - \lambda)\delta$.

On a $\mathbf{f} * \mathbf{b} = ((1 + w)\delta - w\mathbf{1}) * \mathbf{b} = (1 + w)\mathbf{b} - w\lambda\mathbf{b} - w(1 - \lambda)\delta = [1 - w(\lambda - 1)]\mathbf{b} + w(\lambda - 1)\delta = \delta$ par définition de $w$.

$$\boxed{\mathbf{f} * \mathbf{b} = \delta.}$$

39. Pour $k \geqslant 2$ et $s \in \mathbb{R}$, $\frac{\mathbf{f}(k)}{k^s} = \frac{-w}{k^s}$. Donc la série $\sum \frac{\mathbf{f}(k)}{k^s}$ converge si et seulement si $s > 1$. Soit $s > 1$. On a $L_{\mathbf{f}}(s) = (1 + w)L_\delta(s) - wL_{\mathbf{1}}(s)$. La fonction $L_\delta$ est constante égale à 1.

$$\boxed{\text{Pour } s > 1,\ L_{\mathbf{f}}(s) = 1 + w - wL_{\mathbf{1}}(s).}$$

40. En admettant que $L_{\mathbf{b}}$ a une abscisse de convergence finie. Soit $s > \max(1, \Lambda_c(\mathbf{b}))$. La formule prouvée à la question 19 montre que $L_{\mathbf{f}}(s)L_{\mathbf{b}}(s) = L_\delta(s) = 1$. Donc $L_{\mathbf{f}}(s)$ est non nul et $\frac{1}{L_{\mathbf{f}}(s)} = L_{\mathbf{b}}(s) = 1 + \sum_{m=2}^{+\infty} m^{-s}\mathbf{b}(m)$. Posons $\mathbf{c}(m) = \sum_{k=1}^{+\infty} w^k D_k(m)$ pour tout $m \geqslant 2$.
Commençons par remarquer que pour $m \geqslant 2$ et $k \geqslant 1$, si $D_k(m)$ est non nul, alors il existe une décomposition de $m$ en $k$ facteurs plus grand que 2 d'où $2^k \leqslant m$ et $k \leqslant \log_2(m)$. Or $k$ est un entier donc $k \leqslant \lfloor \log_2(m) \rfloor$. Ainsi, $D_k(m) = 0$ si $k > \lfloor \log_2(m) \rfloor$ et $\mathbf{c}(m) = \sum_{k=1}^{\lfloor \log_2(m) \rfloor} w^k D_k(m)$ pour tout $m \geqslant 2$ ce qui prouve que $\mathbf{c}$ est bien définie (c'est heureux). Pour prouver l'égalité voulue, il suffit de prouver que $\mathbf{b}(m) = \mathbf{c}(m)$ pour tout $m \geqslant 2$. Montrons ce résultat par récurrence forte sur $m \geqslant 2$.
Pour $m = 2$. On a $\mathbf{b}(2) = \frac{1}{\lambda - 1}\mathbf{b}(1) = w$ et $\mathbf{c}(2) = \sum_{k=1}^1 w^k D_1(2) = w$ car $\log_2(2) = 1$ et $D_1(m) = 1$ pour tout $m \geqslant 2$.
Supposons le résultat vrai pour tout $2 \leqslant d < m$. Alors

$$\begin{aligned}
\mathbf{b}(m) &= \frac{1}{\lambda-1}\sum_{d|m,d\neq m}\mathbf{b}(d)\\
&= w\left(\sum_{d|m,1<d<m}\mathbf{c}(d)+1\right) \quad \text{par hypothèse de récurrence,}\\
&= w + w\sum_{d|m,1<d<m}\sum_{k=1}^{+\infty} w^k D_k(d)\\
&= w + \sum_{k=1}^{+\infty} w^{k+1}\sum_{d|m,1<d<m} D_k(d)
\end{aligned}$$

car les sommes infinies sont des sommes finies donc on peut inverser l'ordre de sommation sans problème,

$$= w + \sum_{k=2}^{+\infty} w^{k}\sum_{d|m,1<d<m} D_{k-1}(d)$$

Or, pour tout diviseur $1<d<m$ de $m$, l'écriture $m = d.\frac{m}{d}$ donne une factorisation de $m$ en $k$ entiers plus grand que 2 à partir d'une factorisation de $\frac{m}{d}$ en $k-1$ entiers plus grand que 2. Réciproquement si $m = n_1\dots n_k$ où les $k_i$ sont des entiers plus grand que 2 alors $1<n_1<m$ et $n_1$ divise $m$ et $n_2\dots n_k$ est une factorisation de $\frac{m}{k_1}$. Donc $D_k(m) = \sum_{d|m,1<d<m} D_{k-1}(\frac{m}{d}) = \sum_{d'|m,1<d'<m} D_{k-1}(d')$.

$$\begin{aligned}
&= w + \sum_{k=2}^{+\infty} w^k D_k(m)\\
&= \sum_{k=1}^{+\infty} w^k D_k(m)\\
&= \mathbf{c}(m).
\end{aligned}$$

Ceci conclut la récurrence.
D'où $\frac{1}{L_{\mathbf{f}}(s)} = 1 + \sum_{m=2}^{+\infty} m^{-s}\mathbf{c}(m) = 1 + \sum_{m=2}^{+\infty} m^{-s}\sum_{k=1}^{\lfloor \log_2(m)\rfloor} w^k D_k(m)$.

Pour $s$ assez grand, $\frac{1}{L_{\mathbf{f}}(s)} = 1 + \sum_{m=2}^{+\infty} m^{-s}\sum_{k=1}^{+\infty} w^k D_k(m)$.

41. On a

$$\begin{aligned}
\sum_{2}^{n}\mathbf{b}(m) &= \sum_{2}^{n}\mathbf{c}(m)\\
&= \sum_{2}^{n}\sum_{1}^{+\infty} w^k D_k(m)\\
&= \sum_{1}^{+\infty} w^k \sum_{2}^{n} D_k(m)\\
&= \sum_{1}^{+\infty} w^k S_k(n)
\end{aligned}$$

Or, pour $k > \lfloor \log_2(n) \rfloor$ et tout $m \in [\![1, n]\!]$, on a $D_k(m) = 0$ donc $S_k(n) = 0$ d'où $\sum_2^n \mathbf{b}(m) = \sum_1^{\lfloor \log_2(n) \rfloor} w^k S_k(n)$. Donc, $\chi_n(\lambda) = (\lambda-1)^n - (\lambda-1)^{n-1} \sum_2^n \mathbf{b}(j) = (\lambda-1)^n - (\lambda-1)^{n-1} \sum_1^{\lfloor \log_2(n) \rfloor} (\lambda-1)^{-k} S_k(n)$.

$$\text{Pour tout } \lambda \neq 1,\ \chi_n(\lambda) = (\lambda-1)^n - \sum_1^{\lfloor \log_2(n) \rfloor} (\lambda-1)^{n-k-1} S_k(n).$$

42. Soit $n \geqslant 2$. Considérons la fonction $g : x \mapsto x - 1 - \log_2 x$ définie sur $\mathbb{R}_+^*$. La fonction $g$ est dérivable de dérivée $g'(x) = 1 - \frac{1}{x \ln 2}$. Donc $g$ est strictement croissante sur $[2, +\infty)$ car $\frac{1}{\ln 2} \leqslant 2$. Donc $g(n) \geqslant g(2) = 0$ et $n - k - 1$ est un entier naturel pour tout $1 \leqslant k \leqslant \lfloor \log_2(n) \rfloor$.

Les polynômes $\chi_n(X)$ et $(X-1)^n - \sum_1^{\lfloor \log_2(n) \rfloor} (X-1)^{n-k-1} S_k(n)$ coïncident sur $\mathbb{R}\backslash\{1\}$ qui est une partie infinie de $\mathbb{R}$ donc sont égaux. On écrit $\chi_n(X) = (X-1)^{n-\lfloor \log_2(n) \rfloor - 1} Q$ où $Q = (X-1)^{\lfloor \log_2(n) \rfloor + 1} - \sum_1^{\lfloor \log_2(n) \rfloor} (X-1)^{\lfloor \log_2(n) \rfloor - k} S_k(n)$. Comme $Q(1) = 0 - \sum_1^{\lfloor \log_2(n) \rfloor - 1} 0 - S_{\lfloor \log_2(n) \rfloor}(n) \leqslant D_{\lfloor \log_2(n) \rfloor}(2^{\lfloor \log_2(n) \rfloor}) = -1$, $Q(1)$ est non nul et 1 est racine de $\chi_n$ de multiplicité $n - \lfloor \log_2(n) \rfloor - 1$.

$$\text{Pour } n \geqslant 2,\ 1 \text{ est valeur propre de } H_n \text{ de multiplicité } n - \lfloor \log_2(n) \rfloor - 1.$$

Pour $n = 1$ le résultat est faux. En effet, 1 est racine de multiplicité 1 de $H_1 = (1)$, mais $1 - \lfloor \log_2(1) \rfloor - 1 = 0$.

---

• • • FIN • • •

---