Corrigé du DS03 du 04/10/2025 (4h)
Sujet A (MPI*)

Le sujet se compose de 3 exercices indépendants.
Calculatrice interdite.

* * *

Exercice 1 : Inégalité de Knopp

Q 1. On utilise le théorème de convergence des sommes de Riemann, avec par exemple la méthode des rectangles à gauche : puisque f est continue sur le segment $[a,b]$, on a

$$\int_a^b f = \lim_{n\to+\infty} \frac{b-a}{n} \sum_{k=0}^{n-1} f\left(a + \frac{k(b-a)}{n}\right),$$

et de même

$$\int_a^b \varphi\circ f = \lim_{n\to+\infty} \frac{b-a}{n} \sum_{k=0}^{n-1} (\varphi\circ f)\left(a + \frac{k(b-a)}{n}\right).$$

En outre, par convexité de φ, on a l'inégalité de Jensen avec les coefficients $(\lambda_k)_{0\leq k\leq n-1} = (1/n)_{0\leq k\leq n-1}$ (positifs et de somme 1) :

$$\forall n\in\mathbb{N}^*, \qquad \varphi\left(\frac{1}{n}\sum_{k=0}^{n-1} f\left(a+\frac{k(b-a)}{n}\right)\right) \leq \frac{1}{n}\sum_{k=0}^{n-1} \varphi\left(f\left(a+\frac{k(b-a)}{n}\right)\right).$$

En faisant tendre $n\to+\infty$, on obtient par continuité de φ :

$$\varphi\left(\frac{1}{n}\sum_{k=0}^{n-1} f\left(a+\frac{k(b-a)}{n}\right)\right) \underset{n\to+\infty}{\longrightarrow} \varphi\left(\frac{1}{b-a}\int_a^b f\right).$$

En outre :

$$\frac{1}{n}\sum_{k=0}^{n-1} \varphi\left(f\left(a+\frac{k(b-a)}{n}\right)\right) \underset{n\to+\infty}{\longrightarrow} \frac{1}{b-a}\int_a^b \varphi\circ f,$$

donc par passage à la limite dans l'inégalité précédente, on obtient l'inégalité de Jensen intégrale :

$$\varphi\left(\frac{1}{b-a}\int_a^b f\right) \leq \frac{1}{b-a}\int_a^b \varphi\circ f.$$

Q 2. La fonction $t\mapsto tf(t)$ est continue sur $\mathbb{R}^+$, donc la fonction $H : x\mapsto \displaystyle\int_0^x tf(t)dt$ est de classe $\mathcal{C}^1$ sur $\mathbb{R}^+$ avec $H' : x\mapsto xf(x)$. On en déduit que pour $x>0$:

$$g(x) = \frac{H(x)}{x} = \frac{H(x)-H(0)}{x-0} \underset{x\to0^+}{\longrightarrow} H'(0) = 0\times f(0) = 0.$$

Q 3. Notons $F : x\mapsto \int_0^x f$, il s'agit d'une primitive $\mathcal{C}^1$ de f sur $\mathbb{R}^+$ et elle est nulle en 0. En intégrant par parties, on obtient

$$\forall x>0, \qquad g(x) = \frac{1}{x}\int_0^x tf(t)dt = \frac{1}{x}\left([tF(t)]_0^x - \int_0^x F(t)dt\right) = F(x) - \frac{1}{x}\int_0^x F(t)dt.$$

Passons maintenant à la limite lorsque $x\to+\infty$: puisque f est intégrable sur $\mathbb{R}^+$, l'intégrale $\int_0^{+\infty} f$ converge, donc la primitive F possède une limite finie $\ell\in\mathbb{R}$ en $+\infty$. Donc la "moyenne de Cesàro continue" $x\mapsto \dfrac{1}{x}\displaystyle\int_0^x F(t)$ possède la même limite que F en $+\infty$ (exercice classique, déjà fait dans le TD2 et dans le DS2A !). Ainsi :

$$g(x) \underset{x\to+\infty}{\longrightarrow} \ell - \ell = 0$$

Q 4. En reprenant les notations précédentes, la fonction $h : x \mapsto \frac{H(x)}{x^2}$ est continue sur $]0, +\infty[$. En effectuant une IPP généralisée, on a :

$$\int_0^{+\infty} h(x)dx = \int_0^{+\infty} \frac{H(x)}{x^2}dx = \Big[-\frac{H(x)}{x}\Big]_0^{+\infty} + \int_0^{+\infty} \frac{H'(x)}{x}dx = [-g(x)]_0^{+\infty} + \int_0^{+\infty} f(x)dx$$

(sous réserve de convergence du crochet et des intégrales). Or, le crochet converge et vaut 0 car g a des limites nulles en 0^+ et $+\infty$ (d'après Q2. et Q3.), et l'intégrale $\int_0^{+\infty} f$ converge par hypothèse d'intégrabilité de f. Donc l'intégrale $\int_0^{+\infty} h$ converge et l'IPP donne

$$\int_0^{+\infty} h(x)dx = \int_0^{+\infty} f(x)dx.$$

Q 5. Fixons $x > 0$. Conformément à l'indication, décomposons :

$$\forall t \in]0, x], \qquad \ln(f(t)) = \ln(tf(t)) - \ln(t)$$

(ces expressions sont bien définies car $f > 0$ par hypothèse). On sait que $t \mapsto \ln(t)$ est intégrable sur $]0, x]$ (exemple de référence), et $t \mapsto \ln(f(t))$ est intégrable sur $]0, x]$ (car en fait continue sur le segment $[0, x]$ étant donné que $f(t) > 0$ pour tout $t \in \mathbb{R}^+$). Donc $t \mapsto \ln(tf(t))$ est intégrable sur $]0, x]$ (par combinaison linéaire), et on a

$$\int_0^x \ln(f(t))dt = \int_0^x \ln(tf(t))dt - \int_0^x \ln(t)dt = \int_0^x \ln(tf(t))dt - x\ln(x) + x.$$

En divisant par x et en appliquant exp :

$$\exp\left(\frac{1}{x}\int_0^x \ln(f(t))dt\right) = \exp\left(\frac{1}{x}\int_0^x \ln(tf(t))dt\right) e^{1-\ln(x)} = \frac{e}{x}\exp\left(\frac{1}{x}\int_0^x \ln(tf(t))dt\right).$$

Reste à majorer la dernière intégrale en utilisant l'inégalité de Jensen intégrale de Q1. : on se place d'abord sur un segment $[\varepsilon, x]$ avec $0 < \varepsilon < x$ (pour avoir la continuité de $t \mapsto \ln(tf(t))$), et on obtient par convexité de exp :

$$\exp\left(\frac{1}{x-\varepsilon}\int_\varepsilon^x \ln(tf(t))dt\right) \leq \frac{1}{x-\varepsilon}\int_\varepsilon^x tf(t)dt,$$

puis on fait tendre $\varepsilon \to 0^+$ pour avoir, par continuité de exp et convergence des intégrales impropres en 0 :

$$\exp\left(\frac{1}{x}\int_0^x \ln(tf(t))dt\right) \leq \frac{1}{x}\int_0^x tf(t)dt.$$

Finalement :

$$\exp\left(\frac{1}{x}\int_0^x \ln(f(t))dt\right) \leq \frac{e}{x} \times \frac{1}{x}\int_0^x tf(t)dt = \frac{e}{x^2}\int_0^x tf(t)dt.$$

Q 6. L'inégalité précédente se réécrit :

$$\forall x > 0, \qquad 0 < \exp\left(\frac{1}{x}\int_0^x \ln(f(t))dt\right) \leq eh(x).$$

Puisque h est intégrable sur $]0, +\infty[$ (fonction positive telle que $\int_0^{+\infty} h$ converge d'après Q4.), on en déduit par comparaison que $x \mapsto \exp\left(\frac{1}{x}\int_0^x \ln(f(t))dt\right)$ est intégrable sur $]0, +\infty[$ et par croissance de l'intégrale, on obtient :

$$\int_0^{+\infty} \exp\left(\frac{1}{x}\int_0^x \ln(f(t))dt\right)dx \leq e\int_0^{+\infty} h = e\int_0^{+\infty} f$$

(en utilisant l'égalité de Q4.).

* * *

Exercice 2 : Permutations conjuguées

Q 1. La relation $\mathcal{R}$ est réflexive car pour tout $x \in [\![1,n]\!]$, on a $x = Id(x) = \sigma^0(x)$.
Elle est symétrique car si $x\mathcal{R}y$, alors $y = \sigma^k(x)$ avec $k \in \mathbb{Z}$, donc (puisque σ est bijective) : $x = \sigma^{-k}(y)$ ce qui montre $y\mathcal{R}x$.
Enfin, elle est transitive car si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $y = \sigma^k(x)$ et $z = \sigma^{k'}(y)$ avec $(k,k') \in \mathbb{Z}^2$, donc par composition $z = \sigma^{k+k'}(x)$ avec $k+k' \in \mathbb{Z}$, donc $x\mathcal{R}z$.
Ainsi, $\mathcal{R}$ est une relation d'équivalence sur $[\![1,n]\!]$.

Q 2.

- Pour $i \in [\![1,n]\!]$ fixé, l'ensemble $\{k \in \mathbb{N}^*,\ \sigma^k(i) = i\}$ est une partie non vide de $\mathbb{N}$: en effet, la suite infinie $(\sigma^k(i))_{k\geq 1}$ est à valeurs dans l'ensemble fini $[\![1,n]\!]$, donc nécessairement il existe $1 \leq k_1 < k_2$ tels que $\sigma^{k_1}(i) = \sigma^{k_2}(i)$, d'où (par bijectivité de σ) : $\sigma^{k_2-k_1}(i) = i$ avec $k_2 - k_1 \in \mathbb{N}^*$. Cet ensemble possède donc un minimum, noté :

$$\ell = \min\{k \in \mathbb{N}^*,\ \sigma^k(i) = i\}.$$

Remarque
On peut aussi utiliser le fait que dans le groupe symétrique $\mathfrak{S}_n$, fini de cardinal $n!$, l'élément σ est d'ordre fini, donc il existe $p \in \mathbb{N}^*$ tel que $\sigma^p = Id$, ce qui a fortiori donne $\sigma^p(i) = i$. Mais attention, on a seulement $\ell \leq ord(\sigma)$, pas nécessairement l'égalité : en effet, toute puissance qui fixe tous les points de $[\![1,n]\!]$ fixe i, mais pas l'inverse !

- Par définition de la relation $\mathcal{R}$, la classe de i est $X_i = \{\sigma^k(i),\ k \in \mathbb{Z}\}$. Mais par division euclidienne, tout $k \in \mathbb{Z}$ s'écrit $k = q\ell + r$ avec $0 \leq r < \ell$, donc

$$\sigma^k(i) = \sigma^r\left(\sigma^{q\ell}(i)\right) = \sigma^r\left(\sigma^\ell \circ \cdots \circ \sigma^\ell(i)\right) = \sigma^r(i),$$

ce qui montre que $X_i = \{\sigma^r(i),\ 0 \leq r \leq \ell - 1\}$ comme souhaité.

- Enfin, vérifions que les éléments $(\sigma^r(i))_{0\leq r\leq \ell-1}$ sont bien deux à deux distincts : s'il existe $0 \leq r_1 < r_2 \leq \ell - 1$ tels que $\sigma^{r_1}(i) = \sigma^{r_2}(i)$, alors $\sigma^{r_2-r_1}(i) = i$ avec $0 < r_2 - r_1 < \ell$, ce qui est impossible par minimalité de ℓ. Donc X_i est bien de cardinal ℓ.

Q 3. Etant donnée une permutation $\sigma \in \mathfrak{S}_n$, on peut d'après les questions précédentes partitionner $[\![1,n]\!]$ suivant les classes d'équivalences de la relation $\mathcal{R}$ associée :

$$[\![1,n]\!] = X_{i_1} \cup \cdots \cup X_{i_m}$$

(réunion disjointe), en notant $m \in [\![1,n]\!]$ le nombre de classes, et $\{i_1, \cdots, i_m\}$ un système de représentants de chaque classe.
Vu que $\sigma \neq Id$, au moins une des classes est de cardinal ≥ 2. Quitte à permuter les classes dans la réunion, on peut supposer que $X_{i_1}, \cdots, X_{i_r}$ sont de cardinal ≥ 2 (avec $1 \leq r \leq m$), et $X_{i_{r+1}}, \cdots, X_{i_m}$ sont des singletons (qu'on ne fera donc pas apparaître dans la décomposition en cycles). A chaque classe non singleton, notée :

$$\forall k \in [\![1,r]\!], \qquad X_{i_k} = \{i_k, \sigma(i_k), \cdots, \sigma^{\ell_k-1}(i_k)\},$$

on associe le cycle $\gamma_k = (i_k \quad \sigma(i_k) \quad \cdots \quad \sigma^{\ell_k-1}(i_k)) \in \mathfrak{S}_n$, de longueur $\ell_k = |X_{i_k}| \geq 2$.
Il est alors facile de vérifier que

$$\sigma = \gamma_1 \circ \cdots \circ \gamma_r$$

(en testant chaque élément de chaque classe, qui n'est déplacé que par le cycle associé à sa classe, ou non déplacé s'il s'agit d'un élément d'une classe singleton), et ce produit est commutatif puisque les supports des cycles sont deux à deux disjoints (en tant que classes d'une relation d'équivalence).

Q 4. On va calculer $\rho\gamma_1\rho^{-1}(x)$ pour chaque $x \in [\![1,7]\!]$, en distinguant deux cas :

- Si $x \notin \rho(Supp(\gamma_1)) = \{\rho(1), \rho(3), \rho(7)\} = \{2,6,4\}$, alors par bijectivité de ρ, $\rho^{-1}(x) \notin \{1,3,7\}$ (même si on ne connaît pas ρ en entier), donc $\gamma_1(\rho^{-1}(x)) = \rho^{-1}(x)$, et il s'ensuit :

$$\rho\gamma_1\rho^{-1}(x) = \rho(\rho^{-1}(x)) = x.$$

- Sinon :

$$\rho\gamma_1\rho^{-1}(2) = \rho(\gamma_1(1)) = \rho(3) = 6,$$
$$\rho\gamma_1\rho^{-1}(6) = \rho(\gamma_1(3)) = \rho(7) = 4,$$
$$\rho\gamma_1\rho^{-1}(4) = \rho(\gamma_1(7)) = \rho(1) = 2.$$

En résumé, on constate que $\rho\gamma_1\rho^{-1} = (2 \quad 6 \quad 4) = \gamma_2$.

Q 5. Notons dans $\mathfrak{S}_n$ deux cycles de même longueur $\ell \in [\![2, n]\!]$:

$$\gamma_1 = (a_1 \quad \cdots \quad a_\ell), \qquad \gamma_2 = (b_1 \quad \cdots \quad b_\ell).$$

On reprend alors l'idée de l'exemple précédent, en choisissant une permutation $\rho \in \mathfrak{S}_n$ telle que

$$\forall 1 \leq i \leq \ell, \qquad \rho(a_i) = b_i$$

(ce qui est possible car les (a_k) sont deux à deux distincts, ainsi que les (b_k), mais attention, les supports $\{a_1, \cdots, a_\ell\}$ et $\{b_1, \cdots, b_\ell\}$ sont en général non disjoints !).
Il suffit alors de vérifier que $\rho\gamma_1\rho^{-1} = \gamma_2$, exactement comme précédemment : pour $x \in [\![1, n]\!]$,

- si $x \notin \{b_1, \cdots, b_\ell\}$, alors $\rho^{-1}(x) \notin \{a_1, \cdots, a_\ell\}$ donc $\gamma_1(\rho^{-1}(x)) = \rho^{-1}(x)$, d'où $\rho\gamma_1\rho^{-1}(x) = x$
- si $x = b_i$ avec $1 \leq i \leq \ell$, alors $\rho\gamma_1\rho^{-1}(b_i) = \rho(\gamma_1(a_i)) = \rho(a_{i+1}) = b_{i+1}$.

Donc $\rho\gamma_1\rho^{-1} = (b_1 \quad \cdots \quad b_\ell) = \gamma_2$, ce qui montre bien que γ_1 et γ_2 sont conjugués.

Q 6. Considérons deux permutations σ et τ dans $\mathfrak{S}_n$.
Evacuons le cas trivial où l'une des deux permutations est l'identité : dans ce cas puisque $\forall \rho \in \mathfrak{S}_n,\ \rho Id\rho^{-1} = Id$, les deux permutations sont conjuguées ssi elles sont égales à Id (ce qui revient à dire que $c_1(\sigma) = c_1(\tau) = n$ et pour $\ell \geq 2$, $c_\ell(\sigma) = c_\ell(\tau) = 0$).
Supposons donc $\sigma \neq Id$ et $\tau \neq Id$, chacune décomposée en produit de cycles de longueur ≥ 2 et de supports disjoints :

$$\sigma = \gamma_1 \cdots \gamma_r, \qquad \tau = \gamma'_1 \ldots \gamma'_s,$$

avec $r, s \geq 1$. Pour toute permutation $\rho \in \mathfrak{S}_n$, on remarque que :

$$\rho\sigma\rho^{-1} = (\rho\gamma_1\rho^{-1}) \cdots (\rho\gamma_r\rho^{-1}),$$

et d'après les calculs faits en Q5., chaque permutation conjuguée $\rho\gamma_i\rho^{-1}$ est elle-même un cycle $\tilde{\gamma}_i$ de même longueur que γ_i et de support tel que $Supp(\tilde{\gamma}_i) = \rho(Supp(\gamma_i))$.

$\boxed{\Rightarrow}$ Si σ et τ sont conjuguées, alors il existe $\rho \in \mathfrak{S}_n$ telle que $\tau = \rho\sigma\rho^{-1}$, donc avec les notations précédentes :

$$\gamma'_1 \ldots \gamma'_s = (\rho\gamma_1\rho^{-1}) \cdots (\rho\gamma_r\rho^{-1}) = \tilde{\gamma}_1 \cdots \tilde{\gamma}_r.$$

Puisque les cycles $\tilde{\gamma}_i$ sont de longueurs ≥ 2 et de supports disjoints (vu que par injectivité de ρ, $\rho(Supp(\gamma_i)) \cap \rho(Supp(\gamma_j)) = \rho(Supp(\gamma_i) \cap Supp(\gamma_j)) = \emptyset$ si $i \neq j$), on peut utiliser l'unicité de la décomposition en cycles à l'ordre des facteurs près (admise par l'énoncé), ce qui donne $s = r$ et $\{\gamma'_1, \cdots, \gamma'_r\} = \{\tilde{\gamma}_1, \cdots, \tilde{\gamma}_r\}$, donc $c_\ell(\sigma) = c_\ell(\tau)$ pour tout $2 \leq \ell \leq n$ (puisque chaque cycle $\tilde{\gamma}_i$ a même longueur que γ_i). Enfin, n'oublions pas les points fixes :

$$c_1(\sigma) = n - \sum_{\ell=2}^{n} \ell c_\ell(\sigma) = n - \sum_{\ell=2}^{n} \ell c_\ell(\tau) = c_1(\tau).$$

$\boxed{\Leftarrow}$ Réciproquement, supposons que $c_\ell(\sigma) = c_\ell(\tau)$ pour tout $1 \leq \ell \leq n$. Cela entraîne notamment

$$r = \sum_{\ell=2}^{n} c_\ell(\sigma) = \sum_{\ell=2}^{n} c_\ell(\tau) = s.$$

De plus, quitte à permuter les cycles dans les décompositions de σ et τ, on peut supposer que pour tout $1 \leq i \leq r$, le cycle $\gamma'_i = (b_{i,1} \quad \cdots \quad b_{i,\ell_i})$ est de même longueur que le cycle $\gamma_i = (a_{i,1} \quad \cdots \quad a_{i,\ell_i})$. En reprenant le principe de Q5., on va construire une permutation qui conjugue σ et τ. Pour cela, on choisit $\rho \in \mathfrak{S}_n$ telle que

$$\forall i \in [\![1, r]\!],\ \forall k \in [\![1, \ell_i]\!], \qquad \rho(a_{i,k}) = b_{i,k}$$

(ce qui est possible car les $(a_{i,k})$ sont deux à deux distincts, ainsi que les $(b_{i,k})$). On a alors d'après les calculs fait en Q5. :

$$\rho\sigma\rho^{-1} = (\rho\gamma_1\rho^{-1})\cdots(\rho\gamma_r\rho^{-1}) = \gamma'_1\cdots\gamma'_r = \tau,$$

et donc σ et τ sont bien conjuguées.

* * *

Exercice 3 : Fonctions arithmétiques multiplicatives et applications

A. Propriétés générales de la loi $*$

Q 1. Pour $f \in \mathbb{A}$, on a

$$\forall n \in \mathbb{N}^*, \qquad (f*\delta)(n) = \sum_{d|n} f(d)\delta(n/d) = f(n)\delta(1) = f(n),$$

puisque le seul terme $\delta(n/d)$ non nul de la somme correspond à $d = n$.
Donc $f * \delta = f$, et de même, on montre que $\delta * f = f$.
On en déduit que δ est élément neutre de $*$.

Q 2. Soit $(f, g) \in \mathbb{A}^2$. Posons $\omega(a, b) = f(a)g(b)$ pour tout $(a, b) \in (\mathbb{N}^*)^2$.
L'application $\varphi : \left\{ \begin{array}{ccc} \mathcal{D}_n & \longrightarrow & \mathcal{C}_n \\ d & \longmapsto & (d, n/d) \end{array} \right.$ est une bijection, d'inverse $\psi : \left\{ \begin{array}{ccc} \mathcal{C}_n & \longrightarrow & \mathcal{D}_n \\ (d_1, d_2) & \longmapsto & d_1 \end{array} \right.$.
On en déduit que pour tout $n \in (\mathbb{N}^*)^2$:

$$(f*g)(n) = \sum_{d\in\mathcal{D}_n} \omega(d, n/d) = \sum_{d\in\mathcal{D}_n} \omega(\varphi(d)) = \sum_{(d_1,d_2)\in\mathcal{C}_n} \omega(d_1, d_2) = \sum_{(d_1,d_2)\in\mathcal{C}_n} f(d_1)g(d_2).$$

Q 3. L'expression précédente étant clairement symétrique en f et g (puisque $(d_1, d_2) \mapsto (d_2, d_1)$ est une bijection de $\mathcal{C}_n$ dans lui-même), on en déduit $f * g = g * f$, et donc la loi $*$ est commutative.

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

$$((f*g)*h)(n) = \sum_{d|n}(f*g)(d)h(n/d) = \sum_{d|n}\sum_{i|d} f(i)g(d/i)h(n/d) = \sum_{d|n}\sum_{i|d} \omega(i, d/i, n/d)$$

en posant $\omega(a, b, c) = f(a)g(b)h(c)$ pour tout $(a, b, c) \in (\mathbb{N}^*)^3$.
Or, l'application

$$\varphi : \left\{ \begin{array}{ccc} \{(i,d) \in (\mathbb{N}^*)^2,\ d|n \text{ et } i|d\} & \longrightarrow & \mathcal{C}'_n \\ (i,d) & \longmapsto & (i, d/i, n/d) \end{array} \right.$$

est une bijection, d'inverse

$$\psi : \left\{ \begin{array}{ccc} \mathcal{C}'_n & \longrightarrow & \{(i,d) \in (\mathbb{N}^*)^2,\ d|n \text{ et } i|d\} \\ (d_1, d_2, d_3) & \longmapsto & (d_1, d_1d_2) \end{array} \right. ,$$

donc

$$((f*g)*h)(n) = \sum_{d|n}\sum_{i|d} \omega(\varphi(i,d)) = \sum_{(d_1,d_2,d_3)\in\mathcal{C}'_n} \omega(d_1, d_2, d_3) = \sum_{(d_1,d_2,d_3)\in\mathcal{C}'_n} f(d_1)g(d_2)h(d_3).$$

En outre, par commutativité de $*$, on a de même (en permutant les rôles) :

$$(f*(g*h))(n) = ((g*h)*f)(n) = \sum_{(d_1,d_2,d_3)\in\mathcal{C}'_n} g(d_1)h(d_2)f(d_3),$$

et en utilisant que $(d_1, d_2, d_3) \mapsto (d_3, d_1, d_2)$ est une bijection de $\mathcal{C}'_n$ dans lui-même, on obtient

$$(f*(g*h))(n) = \sum_{(d_3,d_1,d_2)\in\mathcal{C}'_n} g(d_1)h(d_2)f(d_3) = \sum_{(a,b,c)\in\mathcal{C}'_n} f(a)g(b)h(c) = ((f*g)*h)(n),$$

donc finalement, $(f * g) * h = f * (g * h)$, ce qui montre l'associativité de $*$.

Q 5. En tant qu'ensemble de fonctions à valeurs dans le groupe commutatif $(\mathbb{C}, +)$, l'ensemble $(\mathbb{A}, +)$ est naturellement un groupe commutatif. La deuxième loi $*$ est commutative, associative, possède un élément neutre (δ) et elle est distributive sur $+$, puisque $\forall (f, g, h) \in \mathbb{A}^3$:

$$\forall n \in \mathbb{N}^*, \qquad (f * (g + h))(n) = \sum_{d|n} f(d)(g + h)(n/d) = \sum_{d|n} f(d)(g(n/d) + h(n/d))$$

$$= \sum_{d|n} f(d)g(n/d) + \sum_{d|n} f(d)h(n/d) = ((f * g) + (f * h))(n),$$

donc $f * (g + h) = f * g + f * h$.
Finalement, $(\mathbb{A}, +, *)$ est un anneau commutatif.

B. Groupe des fonctions multiplicatives

Q 6. Soit f, g deux fonctions multiplicatives qui vérifient :

$$\forall p \in \mathcal{P},\ \forall k \in \mathbb{N}^*, \qquad f(p^k) = g(p^k).$$

Montrons que $f = g$.

- Soit $n \geq 2$ entier, qu'on décompose en facteurs premiers : $n = p_1^{k_1} \cdots p_m^{k_m}$, avec les $m \geq 1$, les p_i premiers distincts et les $k_i \in \mathbb{N}^*$. Puisque les $p_i^{k_i}$ sont premiers entre eux deux à deux et que f et g sont multiplicatives, on a par récurrence immédiate

$$f(n) = f\left(\prod_{i=1}^{m} p_i^{k_i}\right) = \prod_{i=1}^{m} f(p_i^{k_i}) = \prod_{i=1}^{m} g(p_i^{k_i}) = g\left(\prod_{i=1}^{m} p_i^{k_i}\right) = g(n).$$

- Ne pas oublier le cas $n = 1$! Vu que $1 \wedge 1 = 1$, on a $f(1) = f(1 \times 1) = f(1)^2$, donc puisque $f(1) \neq 0$, on en déduit $f(1) = 1$. De même, $g(1) = 1$ donc $f(1) = g(1)$.

On en conclut que $f(n) = g(n)$ pour tout $n \in \mathbb{N}^*$, donc $f = g$.

Remarque
Au passage, on a montré qu'une fonction arithmétique multiplicative vérifie automatiquement $f(1) = 1$.

Q 7. L'application $\pi : \begin{cases} \mathcal{D}_n \times \mathcal{D}_m & \longrightarrow & \mathcal{D}_{mn} \\ (d_1, d_2) & \longmapsto & d_1 d_2 \end{cases}$ est bien définie car si d_1 divise n et d_2 divise m, alors le produit $d_1 d_2$ divise mn.

Première méthode pour montrer la bijectivité de π :
Soit $d \in \mathcal{D}_{mn}$. Montrons qu'il existe un unique couple $(d_1, d_2) \in \mathcal{D}_n \times \mathcal{D}_m$ tel que $d = d_1 d_2$.
Si un tel couple existe, alors on a d_1 qui divise d et n, donc d_1 divise $pgcd(d, n)$.
Mais il existe $k \in \mathbb{Z}$ tel que $n = d_1 k$, donc

$$pgcd(d, n) = pgcd(d_1 d_2, d_1 k) = d_1 \times pgcd(d_2, k) = d_1$$

(en effet $d_2 | m$, $k | n$ et $pgcd(n, m) = 1$, donc $pgcd(d_2, k) = 1$).
De même, on montre que $d_2 = pgcd(d, m)$, d'où l'unicité du couple (d_1, d_2) sous réserve d'existence.
Montrons maintenant que $(d_1, d_2) = (pgcd(d, n), pgcd(d, m))$ convient. On a bien $d_1 | n, d_2 | m$, reste à voir que $d_1 d_2 = d$.
Déjà $pgcd(d_1, d_2) = 1$ car ce sont des diviseurs de n et m premiers entre eux. Vu que ce sont aussi des diviseurs de d, on en déduit que $d_1 d_2 | d$.
Enfin, il existe des coefficients $(u_1, v_1, u_2, v_2) \in \mathbb{Z}^4$ tels que

$$du_1 + nv_1 = d_1, \qquad du_2 + mv_2 = d_2,$$

donc

$$d_1 d_2 = (du_1 + nv_1)(du_2 + mv_2) \in d\mathbb{Z} + mn\mathbb{Z},$$

mais $d|mn$ donc $d|d_1d_2$. Par double divisibilité dans $\mathbb{N}$, on en conclut que $d = d_1d_2 = \pi(d_1, d_2)$, ce qui montre l'existence voulue.

Seconde méthode pour montrer la bijectivité de π :

Soit $d \in \mathcal{D}_{mn}$. Notons $d = \prod_{i=1}^{D} p_i^{\alpha_i}$ la décomposition en facteurs premiers de d, avec les p_i premiers distincts et les $\alpha_i \in \mathbb{N}^*$ (éventuellement $D = 0$ si $d = 1$).
Chacun des p_i divise mn, donc par le lemme d'Euclide, p_i divise m ou n, et pas les deux à la fois (puisque $pgcd(m, n) = 1$). Posons alors $d_1 = \prod_{i,\ p_i|n} p_i^{\alpha_i}$ et $d_2 = \prod_{i,\ p_i|m} p_i^{\alpha_i}$ (ces produits sont éventuellement vides). On a $d_1d_2 = d$ par construction, $d_1|mn$ (puisque $d_1|d$ et $d|mn$), et d_1 est premier avec m (aucun des facteurs premiers de d_1 ne divise m), donc par le lemme de Gauss d_1 divise n. De même façon, d_2 divise m. On a donc construit un couple $(d_1, d_2) \in \mathcal{D}_n \times \mathcal{D}_m$ tel que $d = d_1d_2$, ce qui montre la surjectivité de π.
Enfin, π est injective car si $d_1d_2 = d_1'd_2'$ avec d_1, d_1' dans $\mathcal{D}_n$ et d_2, d_2' dans $\mathcal{D}_m$, alors $d_1'|d_1d_2$ et d_1' est premier avec d_2 (puisque m et n sont premiers entre eux), donc $d_1'|d_1$ par le lemme de Gauss, et par symétrie des rôles, $d_1|d_1'$, donc $d_1 = d_1'$. Il s'ensuit $d_2 = d_2'$, d'où l'injectivité.

Q 8. Soit f, g dans $\mathbb{M}$. Montrons que $f * g \in \mathbb{M}$.
Déjà, on a $(f * g)(1) = f(1)g(1) \neq 0$ car $f(1)$ et $g(1)$ sont non nuls.
Ensuite, si m, n sont deux entiers naturels non nuls premiers entre eux, alors en utilisant Q2. la bijection π de Q7., on peut réécrire :

$$(f * g)(mn) = \sum_{d \in \mathcal{D}_{mn}} f(d)g(mn/d) = \sum_{(d_1,d_2) \in \mathcal{D}_n \times \mathcal{D}_m} f(d_1d_2)g(mn/d_1d_2).$$

En outre, pour chaque couple $(d_1, d_2) \in \mathcal{D}_n \times \mathcal{D}_m$, $d_1 \wedge d_2 = 1$, ainsi que $(n/d_1) \wedge (m/d_2) = 1$ (en effet, m et n étant premiers entre eux, les diviseurs de l'un sont premiers avec les diviseurs de l'autre). Par multiplicativité de f et g, on a donc

$$(f * g)(mn) = \sum_{(d_1,d_2) \in \mathcal{D}_n \times \mathcal{D}_m} f(d_1)f(d_2)g(n/d_1)g(m/d_2)$$

$$= \sum_{d_1 \in \mathcal{D}_n} f(d_1)g(n/d_1) \times \sum_{d_2 \in \mathcal{D}_m} f(d_2)g(m/d_2) = (f * g)(n) \times (f * g)(m),$$

ce qui montre que $f * g \in \mathbb{M}$.

Q 9. Soit $f \in \mathbb{M}$. On considère, pour tout $p \in \mathcal{P}$, la suite récurrente $(a_{p,k})_{k \in \mathbb{N}}$ définie par les relations :

$$a_{p,0} = 1, \qquad \forall k \in \mathbb{N}^*,\ a_{p,k} = -\sum_{i=1}^{k} f(p^i)a_{p,k-i}.$$

En reprenant le principe de Q6., il existe une unique fonction multiplicative g telle que $\forall (p, k) \in \mathcal{P} \times \mathbb{N}^*,\ g(p^k) = a_{p,k}$. En effet, cette fonction est définie par $g(1) = 1$ et pour $n = p_1^{k_1} \cdots p_m^{k_m} \geq 2$ (avec $m \geq 1$, les p_i premiers distincts et les $k_i \in \mathbb{N}^*$) :

$$g(n) = a_{p_1,k_1} \cdots a_{p_m,k_m}.$$

On a donc l'existence (et l'unicité) d'une fonction $g \in \mathbb{M}$ qui vérifie la propriété demandée.
Montrons maintenant que $f * g = \delta$. Puisque f et g sont dans $\mathbb{M}$, on a $f * g \in \mathbb{M}$ (d'après Q8.), et $\delta \in \mathbb{M}$ (admis en début d'énoncé mais trivial à vérifier), donc par la question Q6., il suffit de montrer que $f * g$ et δ coïncident sur les p^k (avec p premier et $k \in \mathbb{N}^*$) :

$$(f * g)(p^k) = \sum_{d|p^k} f(d)g(p^k/d) = \sum_{i=0}^{k} f(p^i)g(p^{k-i}) = g(p^k) + \sum_{i=1}^{k} f(p^i)g(p^{k-i}) = 0 = \delta(p^k)$$

(puisque $p^k \geq p > 1$). On a donc bien $f * g = \delta$.

Q 10. Q8. montre que $*$ est une loi de composition interne sur $\mathbb{M}$, et cette loi est associative, commutative, possède un élément neutre (δ). De plus, Q9. montre que tout élément $f \in \mathbb{M}$ possède un symétrique g (i.e. $f * g = g * f = \delta$), donc $(\mathbb{M}, *)$ est un groupe commutatif.

C. La fonction de Möbius

Q 11. On a déjà $\mu(1) = 1 \neq 0$.

Ensuite, soit $m, n \geq 1$ deux entiers premiers entre eux. Ils n'ont aucun nombre premier en commun dans leur décomposition en facteurs premiers (éventuellement vide), donc l'ensemble des facteurs premiers intervenant dans le produit mn est la réunion disjointe des ensembles des facteurs premiers intervenant dans m et n. Deux cas se présentent alors :

- Si $\mu(mn) = 0$, alors il existe $p \in \mathcal{P}$ tel que p^2 divise mn. Par le lemme d'Euclide, p divise m ou n. Mais par disjonction des décompositions primaires de m et n, on a donc p^2 divise m ou bien p^2 divise n, donc $\mu(m) = 0$ ou bien $\mu(n) = 0$. D'où $\mu(m)\mu(n) = 0 = \mu(mn)$.
- Si $\mu(mn) \neq 0$, alors m et n sont des produits de nombres premiers distincts (sinon, il existerait $p \in \mathcal{P}$ tel que p^2 divise m ou n, donc p^2 diviserait mn, ce qui est contradictoire). Notons $\mu(m) = (-1)^r$ et $\mu(n) = (-1)^s$ (avec éventuellement r ou s nul). Par définition de μ et disjonction des décompositions primaires, on a $\mu(mn) = (-1)^{r+s} = \mu(m)\mu(n)$.

Ceci montre que $\mu \in \mathbb{M}$.

Q 12. Puisque μ et $\mathbf{1}$ sont multiplicatives, $\mu * \mathbf{1}$ l'est aussi. Puisque δ est également multiplicative, il suffit de calculer les images des p^k (d'après Q6.) :

$$\forall p \in \mathcal{P},\ \forall k \in \mathbb{N}^*, \quad (\mu * \mathbf{1})(p^k) = \sum_{d|p^k} \mu(d) = \mu(1) + \mu(p) + \sum_{i=2}^{k} \mu(p^i) = 1 - 1 + 0 = 0 = \delta(p^k),$$

(puisque $p^k \geq p > 1$), ce qui permet de conclure que $\mu * \mathbf{1} = \delta$.

Q 13. L'hypothèse se traduit par $F = f * \mathbf{1}$, donc d'après Q12. :

$$f = \delta * f = (\mu * \mathbf{1}) * f = \mu * (\mathbf{1} * f) = \mu * (f * \mathbf{1}) = \mu * F.$$

(puisque $*$ est associative et commutative). Ainsi :

$$\forall n \in \mathbb{N}^*, \quad f(n) = (\mu * F)(n) = \sum_{d|n} \mu(d) F(n/d).$$

Q 14. D'après le cours, la fonction indicatrice d'Euler φ vérifie $\varphi(1) = 1$ et pour tout m, n non nuls premiers entre eux, $\varphi(mn) = \varphi(m)\varphi(n)$. Donc φ est multiplicative. Puisque μ et $\mathbf{I} : n \mapsto n$ le sont aussi, on en déduit que $\mu * \mathbf{I}$ est multiplicative. En outre, toujours d'après le cours :

$$\forall p \in \mathcal{P},\ \forall k \in \mathbb{N}^*, \quad \varphi(p^k) = p^k - p^{k-1},$$

et d'autre part :

$$\forall p \in \mathcal{P},\ \forall k \in \mathbb{N}^*, \quad (\mu * \mathbf{I})(p^k) = \sum_{d|p^k} \mu(d)(p^k/d) = \sum_{i=0}^{k} \mu(p^i)(p^{k-i}) = \mu(1)p^k + \mu(p)p^{k-1} + 0 = p^k - p^{k-1},$$

donc $\varphi(p^k) = (\mu * \mathbf{I})(p^k)$, ce qui montre d'après Q6. que $\varphi = \mu * \mathbf{I}$.

D. Déterminant de Smith

Q 15. Il suffit de calculer les coefficients de ces matrices : pour tout $(i, j) \in [\![1, n]\!]$:

$$(M' D^T)[i, j] = \sum_{k=1}^{n} m'_{i,k} d_{j,k} = \sum_{k|i,\ k|j} m'_{i,k} d_{j,k} = \sum_{k|i,\ k|j} g(k).$$

Or, diviser deux entiers i et j revient à diviser leur pgcd, donc

$$(M' D^T)[i, j] = \sum_{k|i \wedge j} g(k) = (g * \mathbf{1})(i \wedge j).$$

Mais $g * \mathbf{1} = (f * \mu) * \mathbf{1} = f * (\mu * \mathbf{1}) = f * \delta = f$, donc $(M' D^T)[i, j] = f(i \wedge j) = m_{i,j}$, ce qui montre bien que $M = M' D^T$.

Q 16. Par multiplicativité et invariance par transposition du déterminant on obtient par la question précédente :

$$\det(M) = \det(M')\det(D).$$

Or, les matrices D et M' sont triangulaires inférieures (car si $j > i$, j ne divise pas i et donc le coefficient (i,j) correspondant est nul), donc

$$\det(M) = \left(\prod_{i=1}^{n} \underbrace{m'_{i,i}}_{=g(i)}\right) \times \left(\prod_{i=1}^{n} \underbrace{d_{i,i}}_{=1}\right) = \prod_{i=1}^{n} g(i).$$

E. Séries de Dirichlet

Q 17. Attention, $A_c(f)$ est une borne inférieure, pas nécessairement un minimum. On ne peut donc pas affirmer que $\sum_{k\geq 1} \frac{|f(k)|}{k^{A_c(f)}}$ converge !

L'idée est d'intercaler un réel t entre $A_c(f)$ et s, et de procéder par comparaison : si $s > A_c(f)$, alors par définition d'un inf, s ne minore pas l'ensemble $\{t \in \mathbb{R},\ \sum_{k\geq 1} \frac{|f(k)|}{k^t} < +\infty\}$, donc il existe $t < s$ tel que $\sum_{k\geq 1} \frac{|f(k)|}{k^t} < +\infty$. Par comparaison de SATP, on en déduit :

$$\sum_{k=1}^{+\infty} \frac{|f(k)|}{k^s} \leq \sum_{k=1}^{+\infty} \frac{|f(k)|}{k^t} < +\infty,$$

donc $\sum_{k\geq 1} \frac{f(k)}{k^s}$ converge absolument.

Q 18. Question difficile !

Notons $\alpha = \max(A_c(f), A_c(g)) \in \mathbb{R}$. Par hypothèse, on a

$$\forall s > \alpha, \qquad L_f(s) = L_g(s),$$

c'est-à-dire, en posant $a_k = f(k) - g(k)$:

$$\forall s > \alpha, \qquad \sum_{k=1}^{+\infty} \frac{a_k}{k^s} = 0 \qquad (*).$$

On va montrer que tous les a_k sont nuls, en s'inspirant de la preuve de l'unicité d'un développement limité (cf. cours MP2I). Supposons par l'absurde qu'il existe $k \neq 1$ tel que $a_k \neq 0$. Considérons alors le plus petit entier $k_0 \geq 1$ tel que $a_{k_0} \neq 0$. L'hypothèse $(*)$ se réécrit alors :

$$\forall s > \alpha, \qquad \frac{a_{k_0}}{k_0^s} + \sum_{k=k_0+1}^{+\infty} \frac{a_k}{k^s} = 0.$$

En multipliant par k_0^s, il vient

$$\forall s > \alpha, \qquad a_{k_0} + \sum_{k=k_0+1}^{+\infty} a_k \left(\frac{k_0}{k}\right)^s = 0 \qquad (**).$$

On fait alors tendre $s \to +\infty$. Le reste $R(s) = \sum_{k=k_0+1}^{+\infty} a_k \left(\frac{k_0}{k}\right)^s$ semble tendre vers 0 (somme infinie de termes qui tendent vers 0), prouvons-le rigoureusement.

Déjà, pour tout $k \geq k_0 + 1$, on a $0 < \frac{k_0}{k} \leq \frac{k_0}{k_0+1} < 1$, donc une première majoration naïve de ce reste est

$$\forall s > \alpha, \qquad |R(s)| \leq \left(\frac{k_0}{k_0+1}\right)^s \sum_{k=k_0+1}^{+\infty} |a_k|,$$

mais il est possible que $\sum_{k=k_0+1}^{+\infty} |a_k| = +\infty$.
Intercalons-donc plutôt une abscisse s telle que $\sum_{k\geq 1} \frac{|a_k|}{k^s} < +\infty$, par exemple $s = \alpha + 1$ (d'après Q17., on a bien convergence absolue de $L_f(s)$ et $L_g(s)$, donc de $\sum a_k/k^s$ dès que $s > \alpha$) :

$$\forall s > \alpha+1, \qquad |R(s)| = \left| \sum_{k=k_0+1}^{+\infty} a_k \left(\frac{k_0}{k}\right)^{s-\alpha-1} \left(\frac{k_0}{k}\right)^{\alpha+1} \right| \leq k_0^{\alpha+1} \left(\frac{k_0}{k_0+1}\right)^{s-\alpha-1} \sum_{k=k_0+1}^{+\infty} \frac{|a_k|}{k^{\alpha+1}}.$$

En posant $C_{k_0} = k_0^{\alpha+1} \sum_{k=k_0+1}^{+\infty} \frac{|a_k|}{k^{\alpha+1}} < +\infty$, on a donc

$$\forall s > \alpha+1, \qquad |R(s)| \leq C_{k_0} \left(\frac{k_0}{k_0+1}\right)^{s-\alpha-1} \underset{s\to+\infty}{\to} 0,$$

ce qui prouve la convergence voulue, et donc en faisant $s \to +\infty$ dans $(**)$, il vient $a_{k_0} = 0$, ce qui est contradictoire avec la définition de l'entier k_0. Ainsi, tous les a_k sont nuls et donc $f = g$.

Q 19. En notant $\alpha = \max(A_c(f), A_c(g)) \in \mathbb{R}$, on a convergence absolue (par Q17.) des séries $L_f(s)$ et $L_g(s)$, donc la famille double $(a_{k,m}) = \left(\frac{f(k)g(m)}{k^s m^s}\right)_{(k,m)\in(\mathbb{N}^*)^2}$ est sommable, puisque d'après le théorème de Fubini positif :

$$\sum_{(k,m)\in(\mathbb{N}^*)^2} |a_{k,m}| = \sum_{k=1}^{+\infty}\sum_{m=1}^{+\infty} \frac{|f(k)|}{k^s}\frac{|g(m)|}{m^s} = \sum_{k=1}^{+\infty} \frac{|f(k)|}{k^s} \sum_{m=1}^{+\infty} \frac{|g(m)|}{m^s} < +\infty.$$

L'idée est maintenant de sommer les $(a_{k,m})$ suivant des paquets bien choisis.

- On partitionne $(\mathbb{N}^*)^2$ suivant la valeur du produit des coordonnées (afin de faire apparaître des diviseurs)
$$(\mathbb{N}^*)^2 = \bigcup_{n=1}^{+\infty} \mathcal{C}_n,$$
où $\mathcal{C}_n = \{(k,m) \in (\mathbb{N}^*)^2,\ km = n\}$ (comme en Q1.). Cette réunion est disjointe et la famille $(a_{k,m})$ est sommable, donc par le théorème de sommation par paquets, on obtient
$$\sum_{(k,m)\in(\mathbb{N}^*)^2} a_{k,m} = \sum_{n=1}^{+\infty} \left(\sum_{(k,m)\in\mathcal{C}_n} a_{k,m} \right) = \sum_{n=1}^{+\infty} \left(\sum_{(k,m)\in\mathcal{C}_n} \frac{f(k)g(m)}{n^s} \right) = \sum_{n=1}^{+\infty} \frac{(f*g)(n)}{n^s}.$$
Ainsi, $L_{f*g}(s)$ converge et $L_{f*g}(s) = \sum_{(k,m)\in(\mathbb{N}^*)^2} a_{k,m}$.
- Enfin, on peut aussi sommer "en rectangle" :
$$\sum_{(k,m)\in(\mathbb{N}^*)^2} a_{k,m} = \sum_{k=1}^{+\infty}\sum_{m=1}^{+\infty} \frac{f(k)}{k^s}\frac{g(m)}{m^s} = \sum_{k=1}^{+\infty} \frac{f(k)}{k^s} \sum_{m=1}^{+\infty} \frac{g(m)}{m^s} = L_f(s)L_g(s),$$
donc finalement $L_f(s)L_g(s) = L_{f*g}(s)$.

* * *