

I. Quelques résultats utiles

I.A. Propriétés générales de la loi *

1. Soit $f \in \mathbb{A}$. Soit $n \in \mathbb{N}$. On a :

$$(f * \delta)(n) = f(n)\delta\left(\frac{n}{n}\right) + \sum_{d|n, d \neq n} f(d)\delta\left(\frac{n}{d}\right) = 1f(n) + 0 = f(n)$$

$$\text{Ainsi } f * \delta = f \text{ et } f = \delta * f \text{ car } (\delta * f)(n) = \delta(1)f\left(\frac{n}{1}\right) + \sum_{d|n, d \neq 1} \delta(d)f\left(\frac{n}{d}\right) = f(n)$$

d'où δ est un élément neutre pour la loi * sur $\mathbb{A}$

2. Soit $n \in \mathbb{N}^*$. L'application $\begin{matrix} \mathcal{C}_n & \longrightarrow & \{d \in \mathbb{N} \mid d \mid n\} \\ (d_1, d_2) & \longmapsto & d_1 \end{matrix}$ est bien définie

$$\text{de bijection réciproque : } \begin{matrix} \{d \in \mathbb{N} \mid d \mid n\} & \longrightarrow & \mathcal{C}_n \\ d & \longmapsto & \left(d, \frac{n}{d}\right) \end{matrix}$$

$$\text{ainsi on a bien } (f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{(d_1, d_2) \in \mathcal{C}_n} f(d_1)g(d_2)$$

3. Soit $f, g \in \mathbb{A}$. Soit $n \in \mathbb{N}^*$.

L'application $\begin{matrix} \mathcal{C}_n & \longrightarrow & \mathcal{C}_n \\ (d_1, d_2) & \longmapsto & (d_2, d_1) \end{matrix}$ est bijective de bijection réciproque elle-même. Ainsi

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

d'où $f * g = g * f$ et * est commutative

4. Soit $f, g, h \in \mathbb{A}$. Soit $n \in \mathbb{N}^*$. On a, en utilisant la bijection : $(d_1, d_2, d_3) \in \mathcal{C}'_n \mapsto (d_1, d_1 d_2) \in \{(e, d) \mid d \mid n \text{ et } e \mid d\}$

$$[(f * g) * h](n) = \sum_{d|n} \left(\sum_{e|d} f(e)g\left(\frac{d}{e}\right) \right) h\left(\frac{n}{d}\right) = \sum_{d|n, e|d} f(e)g\left(\frac{d}{e}\right) h\left(\frac{n}{d}\right) = \sum_{(d_1, d_2, d_3) \in \mathcal{C}'_n} f(d_1)g(d_2)h(d_3)$$

$$\text{Puis de manière analogue, on obtient : } \sum_{(d_1, d_2, d_3) \in \mathcal{C}'_n} f(d_1)g(d_2)h(d_3) = [f * (g * h)](n)$$

d'où $(f * g) * h = f * (g * h)$ et ainsi * est associative

5. On sait que $(\mathbb{A}, +)$ est un groupe commutatif car pour tout ensemble $X \neq \emptyset$, $(\mathbb{C}^X, +, \cdot)$ est un $\mathbb{C}$ espace vectoriel. De plus, * est commutative (3), associative (4) et admet un élément neutre (1).

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

$$[(f + g) * h](n) = \sum_{d|n} (f(d) + g(d)) h\left(\frac{n}{d}\right) = \sum_{d|n} f(d)h\left(\frac{n}{d}\right) + \sum_{d|n} g(d)h\left(\frac{n}{d}\right) = [(f * h) + (g * h)](n)$$

Donc $(f + g) * h = (f * h) + (g * h)$ et $h * (f + g) = (h * f) + (h * g)$ car * commutative.

On peut dire que $(\mathbb{A}, +, *)$ est un anneau commutatif

I.B. Groupe des fonctions multiplicatives

6. On suppose que $\forall p \in \mathcal{P}, \forall k \in \mathbb{N}^*, f(p^k) = g(p^k)$. Soit $n \in \mathbb{N}^*$.

Si $n = 1$, on a $1 \wedge 1 = 1$ donc $f(1) = f(1^2) = f(1)^2$ or $f(1) \neq 0$ donc $f(1) = 1 = g(1)$ (analogue)

Si $n > 2$, on écrit la décomposition en facteurs premiers :

$$n = \prod_{i=1}^r p_i^{\alpha_i} \text{ avec } r \in \mathbb{N}^*, \text{ les } p_i \in \mathcal{P} \text{ (distincts deux à deux) et les } \alpha_i \in \mathbb{N}^*$$

Par récurrence immédiate, on a $\forall k \in \llbracket 1, r \rrbracket, f\left(\prod_{i=1}^k p_i^{\alpha_i}\right) = \prod_{i=1}^k f(p_i^{\alpha_i})$

Puis en utilisant l'hypothèse $f(n) = \prod_{i=1}^r f(p_i^{\alpha_i}) = \prod_{i=1}^r g(p_i^{\alpha_i}) = g(n)$ de façon analogue

En conclusion $\boxed{f = g}$

7. **bien définie :** Soit $(d_1, d_2) \in \mathcal{D}_n \times \mathcal{D}_m$.

On peut écrire $n = d_1 q_1$ et $m = d_2 q_2$ avec $q_1, q_2 \in \mathbb{N}^*$

donc $nm = (d_1 d_2)(q_1 q_2)$

d'où $d_1 d_2 \mid nm$ et ainsi $d_1 d_2 \in \mathcal{D}_{mn}$

donc π est bien définie.

injective : Soit (d_1, d_2) et $(e_1, e_2) \in \mathcal{D}_n \times \mathcal{D}_m$ tels que $\pi(d_1, d_2) = \pi(e_1, e_2)$

On a $d_1 d_2 = e_1 e_2$ ainsi $e_1 \mid d_1 d_2$

Comme $n \wedge m = 1$, donc n et m n'ont aucun facteurs premiers en commun

comme $e_1 \mid n$ et $d_2 \mid m$, alors e_1 et d_2 n'ont aucun facteurs premiers en commun

donc $e_1 \wedge d_2 = 1$. Ainsi avec le théorème de Gauss, $e_1 \mid d_1$

et de façon analogue $d_1 \mid e_1$

comme $d_1 \in \mathbb{N}$ et $e_1 \in \mathbb{N}$, on a $e_1 = d_1$

puis on obtient $(d_1, d_2) = (e_1, e_2)$

Ce qui prouve l'injectivité de π

surjective : Soit $d \in \mathcal{D}_{mn}$.

On écrit les décompositions en facteurs premiers de n et m : $n = \prod_{i=1}^r p_i^{\alpha_i}$ et $m = \prod_{i=1}^s q_i^{\beta_i}$

Comme $n \wedge m = 1$, les p_i sont distincts des q_i et on peut écrire

$$d = \left(\prod_{i=1}^r p_i^{\alpha'_i} \right) \left(\prod_{i=1}^s q_i^{\beta'_i} \right) \text{ avec } 0 \leq \alpha'_i \leq \alpha_i \text{ et } 0 \leq \beta'_i \leq \beta_i$$

On pose $d_1 = \prod_{i=1}^r p_i^{\alpha'_i}$ et $d_2 = \prod_{i=1}^s q_i^{\beta'_i}$ de sorte que $d = d_1 d_2$, $d_1 \mid n$ et $d_2 \mid m$

d'où $(d_1, d_2) \in \mathcal{D}_n \times \mathcal{D}_m$ et $\pi(d_1, d_2) = d$

Ce qui prouve la surjectivité de π

En conclusion $\boxed{\pi \text{ est bien définie et réalise une bijection entre } \mathcal{D}_n \times \mathcal{D}_m \text{ et } \mathcal{D}_{mn}}$

8. On suppose que f et g sont deux fonctions multiplicatives. Alors $f(1) = 1 = g(1)$ d'après 6 d'où

$$(f * g)(1) = \sum_{d \mid 1} f(d) g\left(\frac{1}{d}\right) = f(1) g(1) = 1 \neq 0$$

Soit $n, m \in \mathbb{N}^*$ tel que $n \wedge m = 1$. En utilisant la bijectivité de π de 7 :

$$(f * g)(nm) = \sum_{d \in \mathcal{D}_{nm}} f(d)g\left(\frac{nm}{d}\right) = \sum_{(d_1, d_2) \in \mathcal{D}_n \times \mathcal{D}_m} f(d_1 d_2)g\left(\frac{nm}{d_1 d_2}\right)$$

En regardant les facteurs premiers on voit que pour $(d_1, d_2) \in \mathcal{D}_n \times \mathcal{D}_m$, on a $d_1 \wedge d_2 = 1 = \frac{n}{d_1} \wedge \frac{m}{d_2}$ donc

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

donc $(f * g)(nm) = (f * g)(n)(f * g)(m)$ et ainsi $f * g$ est encore multiplicative

9. On veut juste l'existence de g mais pour rechercher g , On traite cela par analyse synthèse.

Analyse : Soit $g \in \mathbb{M}$ convenant.

Ainsi selon 6, on a $g(1) = 1$.

Puis pour $p \in \mathcal{P}$ par récurrence sur $k \in \mathbb{N}^*$, les $g(p^k)$ sont définis par

$$g(p^0) = 1 \text{ et la relation } \forall k \in \mathbb{N}^*, g(p^k) = - \sum_{i=1}^k f(p^i)g(p^{k-i})$$

Ainsi g est définie sur $P_P = \{p^k \mid k \in \mathbb{N} \text{ et } p \in \mathcal{P}\}$

Enfin pour $n \in \mathbb{N}^* \setminus P_P$, on écrit sa décomposition en facteurs premiers $n = \prod_{i=1}^r p_i^{\alpha_i}$ et nécessairement

$$g(n) = \prod_{i=1}^r g(p_i^{\alpha_i}) \quad (*)$$

car les $p_i^{\alpha_i}$ sont premiers entre eux deux à deux.

Synthèse : Soit g défini par $g(1) = 1$ puis sur P_P par les relations de récurrence (pour chaque $p \in \mathcal{P}$) et enfin par la relation (*).

Par unicité de la décomposition en facteurs premiers, l'application g est ainsi bien définie et la formule (*) est valable pour $n \in P_P$. (Pour $n = 1$, on a $r = 0$ et pour $n \in P_P \setminus \{1\}$, on a $r = 1$).

Soit alors $n, m \in \mathbb{N}^*$ tels que $n \wedge m = 1$.

On écrit les décompositions en facteurs premiers de $n = \prod_{i=1}^r p_i^{\alpha_i}$ et $m = \prod_{i=1}^s q_i^{\beta_i}$. Comme $n \wedge m = 1$, la

décomposition (à l'ordre près) de nm en produit de facteurs premiers est $nm = \left(\prod_{i=1}^r p_i^{\alpha_i}\right) \left(\prod_{i=1}^s q_i^{\beta_i}\right)$.

On a alors :

$$g(nm) = g\left[\left(\prod_{i=1}^r p_i^{\alpha_i}\right) \left(\prod_{i=1}^s q_i^{\beta_i}\right)\right] = \prod_{i=1}^r g(p_i^{\alpha_i}) \cdot \prod_{i=1}^s g(q_i^{\beta_i}) = g(n)g(m)$$

Conclusion : On a bien une fonction g multiplicative vérifiant $\forall k \in \mathbb{N}^*, \forall p \in \mathcal{P}, g(p^k) = - \sum_{i=1}^k f(p^i)g(p^{k-i})$

On remarque que l'unicité a été établie.

D'après l'énoncé et 8, les fonctions δ et $f * g$ sont multiplicatives.

Soit $p \in \mathcal{P}$ et $k \in \mathbb{N}^*$. Pour montrer que $\delta = f * g$, il suffit d'établir que $\delta(p^k) = (f * g)(p^k)$, en utilisant 6.

Comme on a $\mathcal{D}_{p^k} = \{p^i \mid i \in \llbracket 0, k \rrbracket\}$, on a

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

Par définition (*) de g et comme $k \in \mathbb{N}^*$, on a

$$(f * g)(p^k) = g(p^k) - g(p^k) = 0 = \delta(p^k)$$

Ce qui permet de conclure que : $\boxed{f * g = \delta}$

On remarque pour la suite qu'une fonction de $\mathbb{M}$ est caractérisée par les valeurs prises sur $\{p^k \mid p \in \mathcal{P}, k \in \mathbb{N}^*\}$.

10. D'après 8, $*$ induit une loi de composition interne sur $\mathbb{M}$.

Avec 3, 4, 1, on voit que $*$ est commutative, associative et admet pour neutre $\delta \in \mathbb{M}$.

De plus, on vient de voir que $\forall f \in \mathbb{M}, \exists g \in \mathbb{M}, f * g = \delta = g * f$ ce qui prouve tout élément de $\mathbb{M}$ admet un symétrique pour $*$ dans $\mathbb{M}$.

On peut conclure que $\boxed{(\mathbb{M}, *) \text{ est un groupe abélien}}$

I.C. La fonction de Möbius

11. On a $\mu(1) = 1 \neq 0$.

Soit $n, m \in \mathbb{N}^*$ tels que $n \wedge m = 1$. Montrons $\mu(nm) = \mu(n)\mu(m)$.

Si $n = 1$, alors on a bien $\mu(nm) = \mu(m) = \mu(n)\mu(m)$. Si $m = 1$, c'est analogue.

Si n ou m n'est pas produit de nombres premiers distincts, alors il en est de même pour nm et on a $\mu(nm) = \mu(n)\mu(m)$.

Si n et m sont produits respectivement de r et s nombres premiers distincts.

Alors comme $n \wedge m = 1$ alors nm est le produit de $r + s$ nombres premiers distincts

et on a $\mu(nm) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(n)\mu(m)$

On a bien montré que $\boxed{\mu \text{ est multiplicative}}$

12. Pour établir que $\mu * \mathbf{1} = \delta$ il suffit d'établir que μ est le symétrique de $\mathbf{1}$ dans le groupe $(\mathbb{M}, *)$.

La relation établi en 9 détermine $g \in \mathbb{M}$ comme étant le symétrique de f .

Soit $p \in \mathcal{P}$ et $k \in \mathbb{N}^*$. Il suffit alors d'établir que $\mathbf{1}(p^k) = -\sum_{i=1}^k \mu(p^i) \mathbf{1}(p^{k-i})$ c'est à dire $1 + \sum_{i=1}^k \mu(p^i) = 0$

Comme $\mu(p) = -1$ et $\forall j \geq 2, \mu(j) = 0$, l'égalité est établie.

On a montré que $\boxed{\mu * \mathbf{1} = \delta}$

13. On a $\forall n \in \mathbb{N}^*, F(n) = \sum_{d|n} f(d) \mathbf{1}\left(\frac{n}{d}\right) = (f * \mathbf{1})(n)$.

Ainsi $F = f * \mathbf{1}$.

Comme $*$ est commutative et que μ et $\mathbf{1}$ sont symétriques dans le groupe $(\mathbb{M}, *)$ d'après 12. On a

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

donc $\boxed{\text{pour tout } n \in \mathbb{N}^*, f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)}$

14. On sait d'après le cours que $\varphi \in \mathbb{M}$ (admis aujourd'hui).

Soit $p \in \mathcal{P}$ et $k \in \mathbb{N}^*$. Il suffit de montrer que $\varphi(p^k) = \mu * \mathbf{I}(p^k)$.

Soit $k \in \mathbb{N}^*$, comme p est premier, on a $N \wedge p^k = 1$ si et seulement si $N \wedge p = 1$, on compte alors les multiples de p entre 1 et p^k , d'où :

$$\varphi(p^k) = p^k - p^{k-1}$$

et

$$(\mu * \mathbf{I})(p^k) = \sum_{i=0}^k \mu(p^i) \mathbf{I}(p^{k-i}) = \mu(1) \mathbf{I}(p^k) + \mu(p) \mathbf{I}(p^{k-1}) + 0 = p^k - p^{k-1}$$

ainsi on a bien $\varphi(p^k) = \mu * \mathbf{I}(p^k)$ ce qui permet de conclure que $\boxed{\varphi = \mu * \mathbf{I}}$

I.D. Déterminant de Smith

15. On note d'_{ij} respectivement n'_{ij} le terme général de $D^\top$ respectivement $M'D^\top$. On a

$$n'_{ij} = \sum_{k=1}^n m'_{ik} d'_{kj} = \sum_{k=1}^n m'_{ik} d_{jk} = \sum_{k|j, k|i} g(k) = \sum_{k|(i \wedge j)} g(k) = (g * \mathbf{1})(i \wedge j)$$

or $g * \mathbf{1} = f * \mu * \mathbf{1} = f$ d'après 12 donc $n'_{ij} = f(i \wedge j) = m_{ij}$

d'où $\boxed{M = M'D^\top}$

16. Pour $i, j \in \llbracket 1, n \rrbracket$, si $j \mid i$ alors $j \leq i$ donc si $j > i$, on a $d_{ij} = m'_{ij} = 0$.

Ainsi les matrices D et M' sont triangulaires inférieures donc avec 15,

$$\det(M) = \det(D^\top) \det(M') = \left(\prod_{i=1}^n d_{ii} \right) \left(\prod_{i=1}^n m'_{ii} \right) = \left(\prod_{i=1}^n 1 \right) \left(\prod_{i=1}^n g(i) \right)$$

Ainsi $\boxed{\text{le déterminant de } M \text{ vaut bien } \det(M) = \prod_{k=1}^n g(k)}$

I.E. Séries de Dirichlet

17. On suppose que $s > A_c(f) = \inf\{u \in \mathbb{R}, \text{ la série } \sum \frac{f(k)}{k^u} \text{ converge absolument}\}$.

La caractérisation de la borne inférieure, nous fournit $t < s$ et $t \in \{u \in \mathbb{R}, \text{ la série } \sum \frac{f(k)}{k^u} \text{ converge absolument}\}$

Ainsi $\frac{f(k)}{k^s} \underset{k \rightarrow +\infty}{=} o\left(\frac{f(k)}{k^t}\right)$.

Par comparaison de séries à termes positifs, la série $\sum_{k \geq 1} \frac{f(k)}{k^s}$ converge absolument.

Ainsi $\boxed{\text{si } s > A_c(f), \text{ alors la série } \sum \frac{f(k)}{k^s} \text{ converge absolument}}$

18. On suppose que pour tout $s > \max(A_c(f), A_c(g))$, $L_f(s) = L_g(s)$. On va procéder en plusieurs étapes.

étape 1 : On se ramène à la nullité d'une fonction arithmétique bornée.

On pose $d = f - g$ et $R = 1 + \max(A_c(f), A_c(g))$

de sorte que $R > \max(A_c(f), A_c(g))$ et pour tout $s \geq R$, la série $\sum \frac{d(s)}{k^s}$ converge de somme nulle.

On remarque que $\forall t \geq 0, \sum_{k=1}^{+\infty} \frac{d(k)/k^R}{k^t} = 0$.

On pose $h : k \mapsto \frac{d(k)}{k^R} = \frac{f(k) - g(k)}{k^R}$ et il suffit d'établir que

$$\forall k \in \mathbb{N}^*, h(k) = 0$$

On va le faire par récurrence dans l'étape 3.

On remarque que la série $\sum h(k)$ converge absolument donc h tend vers 0 en $+\infty$ d'où h est bornée.

Ceci nous fournit $M > 0$ tel que $\forall k \in \mathbb{N}, |h(k)| \leq M$ et on rappelle que $\forall s \geq 0, L_h(s) = \sum_{k=1}^{+\infty} \frac{h(k)}{k^s} = 0$.

étape 2 : *Un résultat asymptotique.*

Pour $p \geq 1$, on pose $R_p : s \mapsto \sum_{k=p}^{+\infty} \frac{h(k)}{k^s}$

Pour $s > 1$ et $p \geq 2$, à l'aide d'une comparaison série/intégrale, on a existences des membres et l'inégalité :

$$|R_p(s)| \leq \sum_{k=p}^{+\infty} \frac{M}{k^s} \leq \int_{p-1}^{+\infty} \frac{M}{t^s} dt$$

car $t \mapsto \frac{M}{t^s}$ est continue, positive, décroissante et intégrable sur $[1, +\infty[$

donc $|R_p(s)| \leq \frac{M(p-1)^{1-s}}{s-1}$ et ainsi $R_p(s) \underset{s \rightarrow +\infty}{=} o((p-1)^{-s})$.

On conclut que pour tout $p \in \mathbb{N}^*$, on a $R_{p+1}(s) \underset{s \rightarrow +\infty}{=} o\left(\frac{1}{p^s}\right)$ et donc

$$p^s R_{p+1}(s) \xrightarrow{s \rightarrow +\infty} 0$$

étape 3 : On va procéder par récurrence forte.

Initialisation : On a $\forall s > 1, 0 = L_h(s) = \frac{h(1)}{1^s} + R_2(s) = h(1) + 1^s R_2(s)$

À l'aide de la relation asymptotique, on a

$$0 = L_h(s) \xrightarrow{s \rightarrow +\infty} h(1)$$

d'où $h(1) = 0$.

Hérédité : Soit $p \in \mathbb{N}^*$ tel que $\forall k \in \llbracket 1, p \rrbracket, h(k) = 0$. Montrons $h(p+1) = 0$.

On a $\forall s > 1, 0 = L_h(s) = \frac{h(p+1)}{(p+1)^s} + R_{p+2}(s)$

À l'aide de la relation asymptotique, on trouve

$$0 = (p+1)^s L_h(s) = h(p+1) + R_{p+2}(s) \xrightarrow{s \rightarrow +\infty} h(p+1)$$

d'où $h(p+1) = 0$.

Conclusion : On a bien établi par récurrence que $\forall k \in \mathbb{N}^*, \frac{f(k) - g(k)}{k^R} = 0$.

On peut alors conclure que $\boxed{f = g}$

19. Soit $s > \max(A_c(f), A_c(g))$.

Les séries $\sum_{p \geq 1} \frac{f(p)}{p^s}$ et $\sum_{k \geq 1} \frac{g(k)}{k^s}$ convergent absolument.

Soit $p \geq 1$. La série $\sum_{k \geq 1} \frac{|f(p)g(k)|}{k^s p^s}$ converge par linéarité, de somme : $\left(\sum_{k=1}^{+\infty} \frac{|g(k)|}{k^s} \right) \frac{|f(p)|}{p^s}$ (i)

Par linéarité la série $\sum_{p \geq 1} \left(\sum_{k=1}^{+\infty} \frac{|g(k)|}{k^s} \right) \frac{|f(p)|}{p^s}$ converge (ii)

Avec (i) et (ii), la famille $\left(\frac{f(p)g(k)}{(pk)^s} \right)_{(p,k) \in (\mathbb{N}^*)^2}$ est sommable

en menant un calcul analogue avec la famille sommable on trouve : $\sum_{(p,k) \in (\mathbb{N}^*)^2} \frac{f(p)g(k)}{(pk)^s} = L_f(s)L_g(s)$

De plus, avec les $\mathcal{C}_n$ introduits avant $2, (\mathbb{N}^*)^2 = \bigcup_{n=1}^{+\infty} \mathcal{C}_n$ (union disjointe dénombrable)

Ainsi en effectuant une sommation par paquets on a (avec convergence absolue)

$$L_f(s)L_g(s) = \sum_{n=1}^{+\infty} \left(\sum_{(p,k) \in \mathcal{C}_n^2} \frac{f(p)g(k)}{(pk)^s} \right)$$

Soit $n \in \mathbb{N}$. On a :

$$\sum_{(p,k) \in \mathcal{C}_n^2} \frac{f(p)g(k)}{(pk)^s} = \sum_{d|n} \frac{f(d)g(n/d)}{n^s} = \frac{(f * g)(n)}{n^s}$$

donc $L_f(s)L_g(s) = \sum_{n=1}^{+\infty} \frac{(f * g)(n)}{n^s}$ avec convergence absolue

ainsi $\boxed{\text{pour tout } s > \max(A_c(f), A_c(g)), \text{ on a } L_f(s)L_g(s) = L_{f*g}(s)}$ et aussi $s > A_c(f * g)$

On ne s'est pas servi du fait que f ou g étaient multiplicatives.

II. Matrices et endomorphismes de permutation

II.A. Similitude de deux matrices de permutation

20. On note $P_\rho P_{\rho'} = (q_{ij})$, $P_\rho = (p_{ij})$ et $P_{\rho'} = (p'_{ij})$ Comme $p'_{kj} = 0 \Leftrightarrow k \neq \sigma'(j)$, alors on a

$$q_{ij} = \sum_{k=1}^n p_{ik} p'_{kj} = p_{i\sigma'(j)} p'_{\sigma'(j)j} = p_{i\sigma'(j)}$$

donc

$$q_{ij} = 0 \Leftrightarrow i \neq \sigma(\sigma'(j)) \Leftrightarrow i \neq \sigma\sigma'(j) \text{ et } q_{(\sigma\sigma'(j))j} = 1$$

Ainsi $\boxed{P_{\rho\rho'} = P_\rho P_{\rho'}}$

En remarquant que $P_{\text{Id}_n} = I_n$, on a donc $P_\rho P_{\rho^{-1}} = P_{\text{Id}_n} = I_n$. Ainsi $P_\rho \in \text{GL}_n(\mathbb{K})$ et $(P_\rho)^{-1} = P_{\rho^{-1}}$.

On remarque que $\rho \in \mathfrak{S}_n \mapsto P_\rho \in \text{GL}_n(\mathbb{C})$ est un morphisme de groupes.

On suppose que σ et τ sont des permutations conjuguées dans $\mathfrak{S}_n$. Ceci nous fournit $\rho \in \mathfrak{S}_n$ tel que $\tau = \rho\sigma\rho^{-1}$.

Ainsi $P_\tau = P_\rho P_\sigma P_{\rho^{-1}} = P_\rho P_\sigma P_\rho^{-1}$ et $\boxed{P_\sigma \text{ et } P_\tau \text{ sont semblables}}$

21. Soit $k \in \llbracket 1, 7 \rrbracket$. On va établir que $\rho\gamma_1(k) = \gamma_2\rho(k)$.

Premier cas : on a $k \notin \{1, 3, 7\}$. Alors $\rho\gamma_1(k) = \rho(k)$

Comme $\rho(k) \notin \{2, 6, 4\}$ car ρ est injective, on a $\gamma_2\rho(k) = \rho(k)$

Deuxième cas : on a $k = 1$. Alors $\rho\gamma_1(k) = \rho(3) = 6$

et $\gamma_2\rho(1) = \gamma_2(2) = 6$.

Troisième cas : on a $k \in \{3, 7\}$. Alors de manière analogue au cas précédent $\rho\gamma_1(k) = \gamma_2\rho(k)$.

Ainsi on a montré $\rho\gamma_1 = \gamma_2\rho$ et ainsi $\boxed{\rho\gamma_1\rho^{-1} = \gamma_2}$

22. On considère $\gamma = (a_1 \ a_2 \ \cdots \ a_\ell)$ et $\gamma' = (b_1 \ b_2 \ \cdots \ b_\ell)$ deux cycles de $\mathfrak{S}_n$ de même longueur $\ell \geq 2$.

Il existe une bijection $\psi : \llbracket 1, n \rrbracket \setminus \{a_1, \dots, a_\ell\} \longrightarrow \llbracket 1, n \rrbracket \setminus \{b_1, \dots, b_\ell\}$ car ces ensembles ont pour même cardinal $n - \ell$. On définit alors ρ sur $\llbracket 1, n \rrbracket$ par

$$\forall x \in \llbracket 1, n \rrbracket \setminus \{a_1, \dots, a_\ell\}, \rho(x) = x \text{ et } \forall i \in \llbracket 1, \ell \rrbracket, \rho(a_i) = b_i$$

On montre facilement que $\rho \in \mathfrak{S}_n$. Et de façon analogue à 21, on montre $\rho\gamma_1\rho^{-1} = \gamma_2$

Ainsi $\boxed{\text{dans } \mathfrak{S}_n, \text{ deux cycles de même longueur sont conjugués}}$

23. On peut remarquer deux cycles à supports disjoints commutent. Ainsi dans la décomposition d'une permutation en produit de cycle à supports disjoints, on peut regrouper les cycles par cycles de même longueurs.

Soit $\sigma \in \mathfrak{S}_n$ et $\tau \in \mathfrak{S}_n$. On peut alors écrire (en gardant la notation multiplicative) :

$$\sigma = \prod_{\ell=2}^n \left(\prod_{i=1}^{c_\ell(\sigma)} \gamma_i^{(\ell)} \right) \text{ et } \tau = \prod_{\ell=2}^n \left(\prod_{i=1}^{c_\ell(\tau)} \beta_i^{(\ell)} \right)$$

où $\gamma_i^{(\ell)}$ et $\beta_i^{(\ell)}$ sont des cycles de longueur ℓ et avec la convention qu'un produit vide est Id_n .

$\Rightarrow$: On suppose que σ et τ sont conjugués dans $\mathfrak{S}_n$. Ceci nous fournit $\rho \in \mathfrak{S}_n$ tel que $\rho\sigma\rho^{-1} = \tau$.

Pour un cycle $\gamma = (a_1 \ a_2 \ \cdots \ a_\ell)$, on a $\rho\gamma\rho^{-1} = (\rho(a_1) \ \rho(a_2) \ \cdots \ \rho(a_\ell))$.

Par ailleurs, l'application $\theta \mapsto \rho\theta\rho^{-1}$ est un automorphisme du groupe $(\mathfrak{S}, \circ)$. donc

$$\tau = \prod_{\ell=2}^n \left(\prod_{i=1}^{c_\ell(\sigma)} \rho\gamma_i^{(\ell)}\rho^{-1} \right)$$

où les $\rho\gamma_i^{(\ell)}\rho^{-1}$ sont des cycles de longueurs ℓ à supports disjoints car ρ est bijective. Ainsi

$$\forall \ell \in \llbracket 2, n \rrbracket, c_\ell(\tau) = c_\ell(\sigma)$$

et

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

$\Leftarrow$: On suppose que $\forall \ell \in \llbracket 1, n \rrbracket, c_\ell(\sigma) = c_\ell(\tau)$.

On construit l'application $\rho : \llbracket 1, n \rrbracket \longrightarrow \llbracket 1, n \rrbracket$ qui envoie bijectivement le support de $\gamma_i^{(\ell)}$ sur le support de $\beta_i^{(\ell)}$ (pour $\ell \in \llbracket 2, n \rrbracket$ et $i \in \llbracket 1, c_\ell(\sigma) \rrbracket$) et $\{i \in \llbracket 1, n \rrbracket \mid \sigma(i) = i\}$ sur $\{i \in \llbracket 1, n \rrbracket \mid \tau(i) = i\}$.

Ceci est possible car on a deux recouvrements disjoints de $\llbracket 1, n \rrbracket$ et chaque ensemble mis en correspondance sont équipotents (de même cardinal).

Ainsi construit, on a $\rho \in \mathfrak{S}_n$ et l'application $\theta \mapsto \rho\theta\rho^{-1}$ est encore un automorphisme. De sorte que

$$\rho\gamma\rho^{-1} = \prod_{\ell=2}^n \left(\prod_{i=1}^{c_\ell(\sigma)} (\rho\gamma_i^{(\ell)}\rho^{-1}) \right) = \prod_{\ell=2}^n \left(\prod_{i=1}^{c_\ell(\tau)} \beta_i^{(\ell)} \right) = \tau$$

ainsi $\boxed{\sigma \in \mathfrak{S}_n \text{ et } \tau \in \mathfrak{S}_n \text{ sont conjugués si et seulement si pour tout } \ell \in \llbracket 1, n \rrbracket, c_\ell(\sigma) = c_\ell(\tau)}$

24. D'après la question 22, les cycles γ et $c = (1 \ 2 \ \dots \ \ell)$ sont conjugués car de même longueur.

D'après la question 20, les matrices P_γ et $P_c = \Gamma_\ell$ sont semblables.

Ainsi le polynôme caractéristique étant un invariant de similitude, on a $\chi_\gamma = \chi_{\Gamma_\ell} = \det(XI_n - \Gamma_\ell)$.

D'où en effectuant $L_1 \leftarrow L_1 + X^{i-1}L_i$ pour i allant de 2 à ℓ :

$$\chi_\gamma = \begin{vmatrix} X & 0 & \dots & \dots & 0 & -1 \\ -1 & X & 0 & \dots & 0 & 0 \\ 0 & -1 & \ddots & & \vdots & 0 \\ \vdots & \ddots & \ddots & \ddots & 0 & \vdots \\ \vdots & & \ddots & -1 & X & 0 \\ 0 & \dots & \dots & 0 & -1 & X \end{vmatrix} = \begin{vmatrix} 0 & 0 & \dots & \dots & 0 & X^\ell - 1 \\ -1 & X & 0 & \dots & 0 & 0 \\ 0 & -1 & \ddots & & \vdots & 0 \\ \vdots & \ddots & \ddots & \ddots & 0 & \vdots \\ \vdots & & \ddots & -1 & X & 0 \\ 0 & \dots & \dots & 0 & -1 & X \end{vmatrix}$$

puis en développant par rapport la première ligne

$$\chi_\gamma = (-1)^{\ell-1}(X^\ell - 1) \begin{vmatrix} -1 & X & 0 & \dots & 0 \\ 0 & -1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & -1 & X \\ 0 & \dots & \dots & 0 & -1 \end{vmatrix}_{[\ell-1]}$$

et en reconnaissant une matrice triangulaire $\boxed{\chi_\gamma(X) = X^\ell - 1}$

25. Soit $\sigma \in \mathfrak{S}_n$. On peut le décomposer en support de cycles à support disjoint $\sigma = \gamma_1 \cdots \gamma_p$

On note l_i la longueur de γ_i .

On définit pour i allant à 1 à p , le cycle de longueur l_i : $\gamma'_i = ((p_i + 1) \ (p_i + 2) \ \dots \ (p_i + l_i))$ où $p_i = \sum_{j=1}^{i-1} l_j$

puis le produit de cycles à supports disjoints $\tau = \gamma'_1 \cdots \gamma'_p \in \mathfrak{S}_n$.

Par construction, on a $\forall \ell \in \llbracket 1, p \rrbracket, c_\ell(\tau) = c_\ell(\sigma)$.

D'après 23 et 20, P_τ et P_σ sont semblables donc ont même polynôme caractéristique.

Or par construction $P_\tau = \text{diag}(\Gamma_{l_1}, \dots, \Gamma_{l_p}, I_{c_1(\tau)})$ (matrice diagonale par blocs) et donc

$$\chi_\sigma = \chi_\tau = \left(\prod_{i=1}^p (X^{l_i} - 1) \right) (X - 1)^{c_1(\tau)} = \prod_{\ell=1}^n (X^\ell - 1)^{c_\ell(\tau)}$$

On a bien montré que $\boxed{\chi_\sigma(X) = \prod_{\ell=1}^n (X^\ell - 1)^{c_\ell(\sigma)}}$

26. On suppose que P_σ et P_τ sont semblables ainsi $\prod_{\ell=1}^n (X^\ell - 1)^{c_\ell(\sigma)} = \chi_\sigma(X) = \chi_\tau(X) = \prod_{\ell=1}^n (X^\ell - 1)^{c_\ell(\tau)}$

Soit $q \in \llbracket 1, n \rrbracket$. Soit $\omega = \exp\left(\frac{2\pi i}{q}\right) \in \mathbb{U}_q$.

Soit $\ell \in \llbracket 1, n \rrbracket$.

Le théorème de la division euclidienne nous fournit $(b, r) \in \mathbb{N}$ tels que $\ell = bq + r$ et $0 \leq r \leq q - 1$.

On a ainsi $\omega^\ell = \omega^r = \exp\left(\frac{r2\pi i}{q}\right)$ donc $\omega^\ell - 1 = 0 \iff r = 0 \iff q \mid \ell$

De plus les racines de $X^\ell - 1$ sont au nombres de ℓ (les éléments de $\mathbb{U}_\ell$), elles sont donc toutes simples. donc ω est racine de $X^\ell - 1$ si et seulement si $q \mid \ell$ et dans ce cas la multiplicité est 1

Ainsi la multiplicité de ω dans $\prod_{\ell=1}^n (X^\ell - 1)^{c_\ell(\sigma)}$ est $\sum_{\substack{\ell=1 \\ q \mid \ell}}^n c_\ell(\sigma)$

et il en est de même pour τ d'où $\sum_{\substack{\ell=1 \\ q \mid \ell}}^n c_\ell(\sigma) = \sum_{\substack{\ell=1 \\ q \mid \ell}}^n c_\ell(\tau)$

27. Pour établir la propriété (S), on traite la réciproque de la question 20.

On suppose que P_σ et P_τ sont semblables. Ainsi selon la question précédente, on a

$$\forall q \in \llbracket 1, n \rrbracket, \sum_{\substack{\ell=1 \\ q \mid \ell}}^n c_\ell(\sigma) = \sum_{\substack{\ell=1 \\ q \mid \ell}}^n c_\ell(\tau)$$

On note $T_\sigma D = (x_1 \ x_2 \ \cdots \ x_n)$. Pour $q \in \llbracket 1, n \rrbracket$, on a

$$x_q = \sum_{j=1}^n c_j(\sigma) d_{jq} = \sum_{\substack{\ell=1 \\ q \mid \ell}}^n c_\ell(\sigma)$$

Par conséquent $T_\sigma D = T_\tau D$

Or la matrice D est inversible car $\det(D) = 1$ selon 16.

donc $T_\sigma = T_\tau$ et ainsi σ et τ sont conjugués d'après la remarque qui suit 22.

On a bien établi la propriété (S)

II.B. Endomorphismes de permutation

28. Soit $u \in \mathcal{L}(E)$. On remarque que pour une base $\mathcal{B} = (e_1, \dots, e_n)$ de E et une permutation $\sigma \in \mathfrak{S}_n$, on a

$$\mathcal{M}_{\mathcal{B}}(u) = P_\sigma \iff \forall j \in \llbracket 1, n \rrbracket, u(e_j) = e_{\sigma(j)}$$

ainsi un endomorphisme est de permutation si et seulement il est représenté par une matrice de permutation

29. Il existe une base dans laquelle u est représentée par P_σ avec $\sigma \in \mathfrak{S}_n$. D'après 25, P_σ est semblable à une matrice diagonale par blocs dont les blocs sont des matrices de la forme Γ_ℓ ($\ell \geq 1$), où Γ_ℓ est définie ci-dessus si $\ell \geq 2$ et où $\Gamma_\ell = (1)$ si $\ell = 1$.

Ceci nous fournit une base $\mathcal{B}$, tel que $\mathcal{M}_{\mathcal{B}}(u) = \text{diag}(\Gamma_{\ell_1}, \dots, \Gamma_{\ell_p})$ avec $\ell_1, \dots, \ell_p \in \mathbb{N}^*$.

De plus on a vu en II que pour tout $\ell \in \mathbb{N}^*$, la matrice Γ_ℓ a pour polynôme caractéristique $X^\ell - 1$ qui est scindé à racines simples dans $\mathbb{C}[X]$.

Ceci nous fournit $Q_1, \dots, Q_p$ matrices inversibles tel que pour $i \in \llbracket 1, p \rrbracket$, $Q_i^{-1} \Gamma_{\ell_i} Q_i$ est diagonale.

En posant $Q = \text{diag}(Q_1, \dots, Q_p) \in \mathcal{M}_n(\mathbb{C})$ et $Q' = \text{diag}(Q_1^{-1}, \dots, Q_p^{-1})$,

par calculs par blocs, on a : $QQ' = I_n$ et $Q' \mathcal{M}_{\mathcal{B}}(u) Q$ diagonale.

Donc $\mathcal{M}_{\mathcal{B}}(u)$ est diagonalisable et il en est de même pour u .

Pour $i \in \llbracket 1, p \rrbracket$, on a $\text{Tr}(\Gamma_{\ell_i}) = 0$ si $\ell_i \geq 2$ et $\text{Tr}(\Gamma_{\ell_i}) = 1$ si $\ell_i = 1$

Comme $\text{Tr}(u) = \text{Tr}(\text{diag}(\Gamma_{\ell_1}, \dots, \Gamma_{\ell_p})) = \sum_{i=1}^p \text{Tr}(\Gamma_{\ell_i}) \in \llbracket 0, n \rrbracket$

On conclut que u est diagonalisable et que sa $\text{Tr}(u) = c_1(\sigma) \in \llbracket 0, n \rrbracket$

30. Si A et B sont semblables alors, elles ont le même polynôme caractéristique, d'après le cours.

Réciproquement on suppose que les matrices A et B diagonalisables ont même polynôme caractéristique.

A (respectivement B) est semblable à une matrice diagonale $D = \text{diag}(\lambda_1, \dots, \lambda_n)$ (respectivement $D' = \text{diag}(\mu_1, \dots, \mu_n)$) avec $\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_n \in \mathbb{C}$. Ainsi

$$\prod_{i=1}^n (X - \lambda_i) = \chi_D = \chi_A = \chi_B = \chi_{D'} = \prod_{i=1}^n (X - \mu_i)$$

Par unicité des racines et de leurs multiplicités dans un polynôme, il existe $\sigma \in \mathfrak{S}_n$ tel que $\forall i \in \llbracket 1, n \rrbracket, \lambda_{\sigma(i)} = \mu_i$. On considère d , l'endomorphisme canoniquement associé à D et $\mathcal{B} = (e_1, \dots, e_n)$ la base canonique de $\mathbb{C}^n$ de sorte que $\mathcal{M}_{\mathcal{B}}(d) = D$. On note $\mathcal{B}' = (e_{\sigma(1)}, \dots, e_{\sigma(n)})$ qui est une nouvelle base de $\mathcal{B}$.

On a $\mathcal{M}_{\mathcal{B}'}(d) = \text{diag}(\lambda_{\sigma(1)}, \dots, \lambda_{\sigma(n)}) = D'$

donc D est semblable à D'

comme la similitude est une relation d'équivalence A est semblable à B

On a montré que A et B sont semblables si et seulement si elles ont même polynôme caractéristique

31. On a vu en 29 qu'un endomorphisme de permutation avait sa trace dans $\llbracket 0, n \rrbracket \subset \mathbb{N}$.

Réciproquement, on suppose que $\text{Tr}(u) \in \mathbb{N}$.

Comme $u^2 = \text{Id}_E$, u est une symétrie et alors $E = E_1(u) \oplus E_{-1}(u)$.

On note $n_1 = \dim(E_1(u))$ et $n_2 = \dim(E_{-1}(u))$.

En écrivant la matrice de u dans une base adaptée à $E_1(u) \oplus E_{-1}(u)$,

on voit que $\text{Tr}(u) = n_1 - n_2$ ainsi $n_1 \geq n_2$.

En réorganisant les vecteurs de cette base, on peut construire une nouvelle base $\mathcal{B}$ telle que

$\mathcal{M}_{\mathcal{B}}(u) = \text{diag}(A, \dots, A, I_{n_1-n_2})$ matrice diagonale par blocs dans laquelle il y a n_1 occurrences de la matrice diagonale $A = \text{diag}(1, -1)$.

Or la matrice A est semblable $R = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (matrice de réflexion)

Ceci nous fournit une nouvelle base $\mathcal{B}'$ telle que $\mathcal{M}_{\mathcal{B}'}(u) = \text{diag}(R, \dots, R, I_{n_1-n_2})$

donc $\mathcal{M}_{\mathcal{B}'}(u) = P_{\sigma}$ où $\sigma = \gamma_1 \dots \gamma_{n_1}$ où $\gamma_i = ((2j-1) \ 2j)$.

d'où u est un endomorphisme de permutation.

On a montré que u est un endomorphisme de permutation si et seulement si $\text{Tr}(u)$ est un entier naturel

32. $\Rightarrow$: Le sens direct de la question précédente persiste selon la question 29.

$\Leftarrow$ et $k = 3$: On suppose que $\text{Tr}(u) \in \mathbb{N}$ et $u^3 = \text{Id}_E$.

On traite ce cas de façon analogue au cas $k = 2$.

Le polynôme $X^3 - 1$ est annulateur de u donc u est diagonalisable et $\text{Sp}(u) \subset \{1, j, \bar{j}\}$.

On note $n_1 = \dim(E_1(u))$ et $n_2 = \dim(E_j(u))$ et $n_3 = \dim(E_{\bar{j}}(u))$.

On a alors $n_1 + n_2 j + n_3 \bar{j} \in \mathbb{N}$.

En regardant la partie imaginaire puis la partie réelle, on a $n_2 = n_3$ puis $n_1 \geq n_2$.

Ainsi la matrice de u dans une certaine base est diagonale par blocs avec des blocs de la forme $\text{diag}(1, j, \bar{j})$ ou $I_{n_1-n_2}$

Pour conclure comme ci-dessus, il suffit de montrer que $\text{diag}(1, j, \bar{j})$ est semblable à une matrice de permutation.

On considère $\sigma = (1 \ 2 \ 3) \in \mathfrak{S}_3$ cycle de longueur 3.

On a $\chi_{\sigma} = X^3 - 1$ scindé à racines simples : $1, j, \bar{j}$

donc P_{σ} est diagonalisable donc semblable à $\text{diag}(1, j, \bar{j})$

ce qui permet de conclure comme ci-dessus que u est une matrice de permutation.

$\Leftarrow$ et $k = 4$: On suppose que $\text{Tr}(u) \in \mathbb{N}$ et $u^4 = \text{Id}_E$.

Si $n = 1$, alors la matrice d'une homothétie de rapport $\lambda \in \mathbb{N}$ tel que $\lambda^4 = 1$ donc en $\lambda = 1$ et toute matrice de u est (1) matrice de $\text{Id}_{\{1\}} \in \mathfrak{S}_1$.

On se place dans le cas où $n \geq 2$.

On considère u dont la matrice dans une base de E est la matrice diagonale $\text{diag}(i, -i, 1, \dots, 1)$.

On a $u^4 = \text{Id}_E$ et $\text{Tr}(u) = n - 2 \in \mathbb{N}$

Par l'absurde si u était un endomorphisme de permutation notée σ .

Alors avec 25, on a

$$(X - i)(X + i)(X - 1)^{n-2} = \chi_u(X) = \chi_\sigma(X) = \prod_{\ell=1}^n (X^\ell - 1)^{c_\ell(\sigma)}$$

Si $c_\ell(\sigma) \neq 0$, alors comme -1 n'est pas de $X^\ell - 1$, d ℓ est impair et donc i n'est pas racine de $X^\ell - 1$.

Il y a là une contradiction. Ainsi u n'est pas un endomorphisme de permutation.

Conclusions :

Si $u^3 = \text{Id}_E$ alors, u est un endomorphisme de permutation si et seulement si $\text{Tr}(u)$ est un entier naturel

Si $n = 1$ et $u^4 = \text{Id}_E$ alors u est un endomorphisme de permutation si et seulement si $\text{Tr}(u)$ est un entier naturel

mais si $n \geq 2$ il existe un endomorphisme u qui n'est pas de permutation tel que $u^4 = \text{Id}_E$ et $\text{Tr}(u) \in \mathbb{N}$

Remarque : en temps limité, pour le cas $k = 4$, On se serait contenté du contre-exemple avec $n = 2$ ce qui est largement suffisant.

33. On suppose que u est un endomorphisme de permutation.

Alors u est représenté dans une certaine base par la matrice $\mathcal{P}_\sigma$ avec $\sigma \in \mathfrak{S}_n$ et donc

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

Ainsi u vérifie la condition (a)

La groupe $(\mathfrak{S}_n, \circ)$ est fini d'ordre $n!$ donc σ est d'ordre fini N (on sait que $N \mid n!$)

donc $(\mathcal{P}_\sigma)^N = \mathcal{P}_{\sigma^N} = \text{Id}_n$ puis $u^N = \text{Id}_E$

d'où u vérifie la condition (b)

Réciproquement on suppose que u vérifie les conditions (a) et (b)

Comme $X^N - 1$ est scindé à racines simples, u est diagonalisable.

On écrit $\chi_u = \prod_{\ell=1}^n (X^\ell - 1)^{c_\ell}$ avec $c_1, \dots, c_n \in \mathbb{N}$.

On peut alors trouver une base de vecteurs propres de u dans laquelle les matrices est diagonale par blocs de matrices diagonales tailles ℓ ($1 \leq \ell \leq n$) dont le polynôme caractéristique est $X^\ell - 1$.

Pour conclure, il suffit de montrer que pour $\ell \in \mathbb{N}^*$, la matrice $\text{diag}((\omega)_{\omega \in \mathbb{U}_\ell})$ est semblable à une matrice de permutation (comme dans les questions précédentes)

On peut remarquer comme précédemment que tout cycle γ de longueur ℓ de $\mathfrak{S}_\ell$ convient.

En effet $\mathcal{P}_\gamma \in \mathcal{M}_\ell(\mathbb{C})$ et $\chi_\gamma(X) = X^\ell - 1$.

ainsi u est un endomorphisme de permutation si et seulement s'il vérifie (a) et (b)

où (a) et (b) sont les deux conditions suivantes :

(a) il existe des entiers naturels $c_1, \dots, c_n$ tels que $\chi_u = \prod_{\ell=1}^n (X^\ell - 1)^{c_\ell}$.

(b) il existe N tel que $u^N = \text{Id}_E$.

34. Comme χ_u et χ_v sont dans $\mathbb{C}[X]$, ces polynômes sont scindés d'après d'Alembert-Gauss.

Ainsi u et v sont trigonalisables.

On note $\text{Sp}(u) \cup \text{Sp}(v) = \{\lambda_1, \lambda_2, \dots, \lambda_p\}$

On note $m_1, \dots, m_p$ les multiplicités associées dans χ_u respectivement à $\lambda_1, \dots, \lambda_p$.

On remarque que $\sum_{i=1}^p m_i = n$ et $\chi_u(X) = \prod_{i=1}^p (X - \lambda_i)^{m_i}$ et les $m_i \in \mathbb{N}$.

Alors u est représentable par une matrice triangulaire dans une base $\mathcal{B}$ avec m_i occurrences de λ_i pour $i \in \llbracket 1, p \rrbracket$.

Ainsi pour $k \in \mathbb{N}$, u^k est représentable par une matrice triangulaire dans une base $\mathcal{B}$ avec m_i occurrences de

λ_i^k pour $i \in \llbracket 1, p \rrbracket$ donc $\forall k \in \mathbb{N}$, $\text{Tr}(u^k) = \sum_{i=1}^p m_i \lambda_i^k$.

Soit $j \in \llbracket 1, p \rrbracket$. On note $L_j = \prod_{\substack{i=1 \\ i \neq j}}^p \frac{X - \lambda_j}{\lambda_i - \lambda_j} = \sum_{k=0}^{p-1} a_k X^k$ où les $a_k \in \mathbb{C}$.

On a $\forall i \in \llbracket 1, p \rrbracket$, $L_j(\lambda_i) = \delta_{i,j}$ (symbole de Kronecker). Ainsi

$$\sum_{k=0}^{p-1} a_k \text{Tr}(u^k) = \sum_{k=0}^{p-1} \left(\sum_{i=1}^p m_i \lambda_i^k \right) a_k = \sum_{i=1}^p m_i \sum_{k=0}^{p-1} a_k \lambda_i^k = \sum_{i=1}^p m_i L_j(\lambda_i) = m_j$$

En notant pour $i \in \llbracket 1, p \rrbracket$, n_i la multiplicité de λ_i dans χ_v , on a de manière analogue

$$n_j = \sum_{k=0}^{p-1} a_k \text{Tr}(v^k) = \sum_{k=0}^{p-1} a_k \text{Tr}(u^k) = m_j$$

$$\text{donc } \chi_u(X) = \prod_{i=1}^p (X - \lambda_i)^{m_i} = \prod_{i=1}^p (X - \lambda_i)^{n_i} = \chi_v(X)$$

d'où u et v ont même polynôme caractéristique

Autre méthode : On peut aussi le faire avec la matrice de Vandermonde de $\lambda_1, \dots, \lambda_p$ et remarquer que $(m_1 - n_1, \dots, m_p - n_p)$ est dans le noyau d'icelle.

C'est sans doute plus court.

35. $\Rightarrow$ On suppose que u est un endomorphisme de permutation.

Alors u peut être représenté par une matrice diagonale par blocs dont les blocs diagonaux sont de la forme Γ_ℓ avec $\ell \in \llbracket 1, n \rrbracket$ selon 28 et 25.

Pour $\ell \in \llbracket 1, n \rrbracket$, On note c_ℓ le nombre d'occurrences du bloc $\Gamma_\ell = P_\gamma$ où $\gamma_\ell \in \mathfrak{S}_\ell$ est un cycle de longueur ℓ

$$\text{Ainsi } \text{Tr}(u^k) = \sum_{\ell=1}^n c_\ell \text{Tr}(\Gamma_\ell^k)$$

Si $\ell \mid k$, alors comme $\Gamma_\ell^k = I_\ell$ et dans ce cas $\text{Tr}(\Gamma_\ell^k) = \ell$.

Si $\ell \nmid k$, alors Γ_ℓ a pour polynôme caractéristique $X^\ell - 1$ ainsi Γ_ℓ est semblable à $\text{diag}(1, \omega, \dots, \omega^{\ell-1})$ où

$$\omega = \exp\left(\frac{2\pi i}{\ell}\right). \text{ Comme } \omega^k \neq 1, \text{ on a } \text{Tr}(\Gamma_\ell^k) = \frac{1 - (\omega^k)^\ell}{1 - \omega^k} = 0$$

$$\text{donc } \text{Tr}(u^k) = \sum_{\substack{\ell=1 \\ \ell \mid k}}^n \ell c_\ell \text{ où les } c_\ell \in \mathbb{N}.$$

$\Leftarrow$ On suppose l'existence des entiers naturels $c_1, \dots, c_n$ tels que, pour tout $k \in \mathbb{N}$, $\text{Tr}(u^k) = \sum_{\substack{\ell=1 \\ \ell|k}}^n \ell c_\ell$.

Pour $k = 0$, on trouve $n = \text{Tr}(\text{Id}_E) = \sum_{\substack{\ell=1 \\ \ell|0}}^n \ell c_\ell = \sum_{\ell=1}^n \ell c_\ell$

On peut alors considérer alors la matrice de permutation $A \in \mathcal{M}_n(\mathbb{C})$ diagonale par blocs dont les blocs diagonaux sont les Γ_ℓ (avec $\ell \in \llbracket 1, n \rrbracket$) avec une occurrence de c_ℓ .

On note B la matrice représentant u dans une base militaire.

Avec le travail fait dans le sens direct, on a

$$\forall k \in \mathbb{N}, \text{Tr}(A^k) = \sum_{\substack{\ell=1 \\ \ell|k}}^n \ell c_\ell = \text{Tr}(u^k) = \text{Tr}(B^k)$$

En utilisant 34 avec les endomorphismes canoniquement associés, A et B ont même polynôme caractéristique.

or A est diagonalisable car A est une matrice de permutation et B l'est car u l'est.

donc selon 30, A et B sont semblables

donc A représente u dans une nouvelle base.

ainsi u est une matrice de permutation.

En conclusion :

u est un endomorphisme de permutation si et seulement si $\exists c_1, \dots, c_n \in \mathbb{N}$, $\forall k \in \mathbb{N}$, $\text{Tr}(u^k) = \sum_{\substack{\ell=1 \\ \ell|k}}^n \ell c_\ell$

III. Valeurs propres de la matrice de Redheffer

36. On note $C_n = (c_{ij})_{1 \leq i, j \leq n}$

Si $i = j = 1$: alors $c_{1,1} = \sum_{k=1}^n a_{1k} h_{k1} = \sum_{k=1}^n \mu(k) = M(n)$

Si $i > 1$ et $j = 1$: alors $c_{i,1} = \sum_{k=1}^n a_{ik} h_{k1} = 1h_{i1} + 0 = 1$

Si $i > 1$ et $j > 1$: alors $c_{i,j} = \sum_{k=1}^n a_{ik} h_{kj} = 1h_{ij} + 0 = h_{ij}$

donc $c_{i,j} = 1$ si et seulement si $i|j$ et sinon $c_{i,j} = 0$

On remarque dans ce cas si $i > j$, $c_{i,j} = 0$ et que si $i = j$, alors $c_{i,j} = 1$.

Si $i = 1$ et $j > 1$: alors en utilisant la partie I et en particulier la question 12 :

$$c_{1,j} = \sum_{k=1}^n a_{1k} h_{kj} = \sum_{k=1}^n \mu(k) h_{kj} = \sum_{k|j} \mu(k) \mathbf{1}(j/k) = \delta(j) = 0$$

La première ligne de la matrice C_n est $(M(n) \ 0 \ \dots \ 0)$.

En développant le déterminant la matrice H_n selon cette ligne, on a $\det(H_n) = M(n) \det(T)$ où $T = (c_{ij})_{2 \leq i, j \leq n} \in \mathcal{M}_{n-1}(\mathbb{C})$

À l'aide des calculs des coefficients de C_n , la matrice T est triangulaire supérieure avec 1 comme seuls coefficients diagonaux

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

37. On note $B_n(\lambda)(\lambda I_n - H_n) = (r_{ij})_{1 \leq i, j \leq n}$ de sorte que : $r_{i,j} = \sum_{k=1}^n b_{ik}(\delta_{k,j}\lambda - h_{kj}) = \lambda b_{ij} - \sum_{k=1}^n b_{ik}h_{kj}$.

Si $i = j = 1$: alors $r_{1,1} = \lambda b_{1,1} - \sum_{k=1}^n b_{1k}h_{k1} = \lambda \mathbf{b}(1) - \sum_{k=1}^n \mathbf{b}(k)h_{k1} = \lambda - \sum_{k=1}^n \mathbf{b}(k)$

Si $i > 1$ et $j = 1$: alors $r_{i,1} = \lambda b_{i1} - \sum_{k=1}^n b_{ik}h_{k1} = 0 - h_{i1} - 0 = -1$

Si $i > 1$ et $j > 1$ et $i \neq j$: alors $r_{i,j} = \lambda b_{ij} - \sum_{k=1}^n b_{ik}h_{kj} = \lambda \delta_{ij} - h_{ij} - 0 = \lambda \delta_{ij} - h_{ij} = -h_{ij}$

donc $r_{i,j} = -1$ si et seulement si $i|j$ et sinon $r_{i,j} = 0$

On remarque dans ce cas si $i > j$, $r_{i,j} = 0$.

Si $i = j > 1$: $r_{i,i} = \lambda - h_{ii} = \lambda - 1$

Si $i = 1$ et $j > 1$: $r_{1,j} = \lambda \mathbf{b}(j) - \sum_{k=1}^n \mathbf{b}(k)h_{kj} = \frac{\lambda}{\lambda - 1} \sum_{d|j, d \neq j} \mathbf{b}(d) - \sum_{k|j, k \neq j} \mathbf{b}(k) - \mathbf{b}(j) = 0$

Ainsi en calculant le déterminant de la matrice $B_n(\lambda)(\lambda I_n - H_n)$, on a un calcul analogue à la question précédente, les coefficients diagonaux de la matrice triangulaire de taille $n - 1$ devenant $\lambda - 1$. Ainsi

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

La matrice $B_n(\lambda)$ étant triangulaire, on a $\det(B_n(\lambda)) = \mathbf{b}(1) \times 1^{n-1} = 1$ car $\mathbf{b}(1) = 1$

Ainsi : $\boxed{\chi_n(\lambda) = 1 \det(\lambda I_n - H_n) = (\lambda - 1)^n - (\lambda - 1)^{n-1} \sum_{j=2}^n \mathbf{b}(j)}$

38. Soit $n \in \mathbb{N}^*$. On a :

$$(\mathbf{f} * \mathbf{b})(n) = \sum_{d|n} \mathbf{f}(d) \mathbf{b}(n/d) = (1 + w) \sum_{d|n} \delta(d) \mathbf{b}(n/d) - w \sum_{d|n} \mathbf{1}(d) \mathbf{b}(n/d) = (1 + w) \mathbf{b}(n) - w \sum_{d|n} \mathbf{b}(n/d)$$

Comme $d \in \mathcal{D}_n \mapsto \frac{n}{d} \in \mathcal{D}_n$ est une bijection de bijection réciproque elle-même, on

$$(\mathbf{f} * \mathbf{b})(n) = (1 + w) \mathbf{b}(n) - w \sum_{d|n} \mathbf{b}(d) = \mathbf{b}(n) - w \sum_{d|n, d \neq n} \mathbf{b}(d)$$

Si $n = 1$, alors on a $(\mathbf{f} * \mathbf{b})(1) = \mathbf{b}(1) - 0 = 1 = \delta(1)$.

Si $n \neq 1$, alors $n \geq 2$ et on a $(\mathbf{f} * \mathbf{b})(n) = \left(\frac{1}{\lambda - 1} - w \right) \sum_{d|n, d \neq n} \mathbf{b}(d) = 0$

On a bien établi que $\boxed{\mathbf{f} * \mathbf{b} = \delta}$

39. On a $\mathbf{f}(1) = (1+w)\delta(1) - w\mathbf{1}(1) = 1 = 1 + w - w$ et pour $n \geq 2$, on a $\mathbf{f}(n) = (1+w)\delta(n) - w\mathbf{1}(n) = -w$.

Soit $s \in \mathbb{R}$. Comme $\mathbf{f}$ est stationnaire de limite non nulle, on a

$$\sum_k \frac{\mathbf{f}(k)}{k^s} \text{ converge absolument si et seulement si } \sum_k \frac{1}{k^s} \text{ converge c'est à dire } s > 1$$

On trouve alors $\boxed{\forall s > 1, L_{\mathbf{f}}(s) = 1 + w - wL_{\mathbf{1}}(s)}$

40. Soit $s > 1$. On a $L_{\mathbf{f}}(s) = 1 - \sum_{k=2}^{+\infty} \frac{w}{k^s} = 1 - A(s)$ en ayant noté $A = L_{w(\mathbf{1}-\delta)}$.

En reprenant le résultat asymptotique de Q18 (étape 2), on a $\lim_{s \rightarrow +\infty} A(s) = 0$.

Ce qui nous fournit $R > 0$ tel que $\forall s \geq R, |A(s)| < 1$.

Soit $s \geq R$. On a alors

$$\frac{1}{L_{\mathbf{f}}(s)} = \frac{1}{1 - A(s)} = \sum_{m=0}^{+\infty} A(s)^m \quad (**)$$

On suppose dans un premier temps que $\lambda > 1$ et donc que $w > 0$.

Montrons par récurrence sur $m \in \mathbb{N}^*$ que $\sum_{k \geq 2} w^m D_m(k) k^{-s}$ converge et que $A(s)^m = \sum_{k=2}^{+\infty} w^m D_m(k) k^{-s}$.

Initialisation : On remarque que $\forall k \geq 2, D_1(k) = 1$ et que

$$A(s)^1 = \sum_{k=2}^{+\infty} \frac{w}{k^s} = \sum_{k=2}^{+\infty} w^1 D_1(k) k^{-s}$$

et on a bien la convergence de $\sum_{k \geq 2} w^1 D_1(k) k^{-s}$.

Hérédité : Soit $m \in \mathbb{N}^*$ tel que la propriété soit vraie.

Alors les séries $\sum_{p \geq 2} w^1 D_1(p) p^{-s}$ et $\sum_{q \geq 2} w^m D_m(q) q^{-s}$ convergent de sommes respectives $A(s)$ et $A(s)^m$.

Pour $p \geq 2$, la série $\sum_{q \geq 2} w^{m+1} D_1(p) D_m(q) (pq)^{-s}$ converge de somme $A(s)^m w^1 D_1(p) p^{-s}$ par linéarité

Et par linéarité, la série $\sum_{p \geq 2} A(s)^m w^1 D_1(p) p^{-s}$ converge de somme $A(s)^{m+1}$.

Comme la famille $(w^{m+1} D_1(p) D_m(q) (pq)^{-s})_{p, q \geq 2}$ est à terme positifs, cette famille est sommable de somme

$$\sum_{\substack{p \geq 2 \\ q \geq 2}} w^{m+1} D_1(p) D_m(q) (pq)^{-s} = A(s)^{m+1}$$

Pour $k \geq 2$, On note $I_k = \{(p, q) \in \mathbb{N}^2 \mid p, q \geq 2 \text{ et } pq = k\}$

de sorte que $\{(p, q) \in \mathbb{N}^2 \mid p, q \geq 2\} = \bigcup_{k=2}^{+\infty} I_k$ (union disjointe dénombrable)

Ainsi par théorème de sommation par paquets : on a

$$A(s)^{m+1} = \sum_{k=2}^{+\infty} \sum_{(p, q) \in I_k} w^{m+1} D_1(p) D_m(q) (pq)^{-s} = \sum_{k=2}^{+\infty} \sum_{(p, q) \in I_k} w^{m+1} D_1(p) D_m(q) k^{-s}$$

Pour décomposer un entier $k \geq 2$ en $m+1$ facteurs ≥ 2 , on commence par choisir un diviseur $p \geq 2$ et tel que $k/p \geq 2$. Puis on décompose k/p en m facteurs ≥ 2 . On obtient alors

$$D_{m+1}(k) = \sum_{\substack{p|k \\ 2 \leq p \leq k/2}} D_m(k/p) = \sum_{\substack{p|k \\ 2 \leq p \leq k/2}} D_1(p) D_m(k/p) = \sum_{(p,q) \in I_k} D_1(p) D_m(q)$$

$$\text{donc } A(s)^{m+1} = \sum_{k=2}^{+\infty} w^{m+1} D_{m+1}(k) k^{-s} \text{ et on a bien la convergence de } \sum_{k \geq 2} w^{m+1} D_{m+1}(k) k^{-s}$$

$$\textbf{Conclusion :} \text{ On a bien } \forall m \in \mathbb{N}^*, A(s)^m = \sum_{k=2}^{+\infty} w^m D_m(k) k^{-s}$$

Ainsi selon (**), pour tout $s \geq R$, on a

$$\frac{1}{L_f(s)} = 1 + \sum_{m=1}^{+\infty} \sum_{k=2}^{+\infty} k^{-s} w^m D_m(k) = 1 + \sum_{k=1}^{+\infty} \sum_{m=2}^{+\infty} m^{-s} w^k D_k(m) < +\infty$$

Comme $\forall k \geq 1, \forall m \geq 2, m^{-s} w^k D_k(m) \geq 0$, la famille est sommable et on peut donc appliquer Fubini :

$$\frac{1}{L_f(s)} = 1 + \sum_{m=2}^{+\infty} \sum_{k=1}^{+\infty} m^{-s} w^k D_k(m) = 1 + \sum_{m=2}^{+\infty} m^{-s} \sum_{k=1}^{+\infty} w^k D_k(m)$$

Pour $m \geq 2$ et $k \in \mathbb{N}^*$, On remarque que si $m < 2^k$ alors $D_k(m) = 0$ or

$$2^k \leq m \iff k \leq \frac{\ln(m)}{\ln(2)} \iff k \leq \lfloor \log_2 m \rfloor$$

$$\text{donc } \frac{1}{L_f(s)} = 1 + \sum_{m=2}^{+\infty} m^{-s} \sum_{k=1}^{\lfloor \log_2 m \rfloor} w^k D_k(m)$$

Dans le cas où $\lambda < 1$ et $w < 0$, on travaille avec $\lambda' = 2 - \lambda$ et $w' = \frac{1}{\lambda' - 1} = |w|$ pour établir les sommabilité des différentes familles doubles. Ensuite la sommabilité étant acquise, les calculs (sommation par paquets et Fubini) restent valables et on a bien, dans tous les cas :

pour s réel suffisamment grand, $\frac{1}{L_f(s)} = 1 + \sum_{m=2}^{+\infty} m^{-s} \sum_{k=1}^{\lfloor \log_2 m \rfloor} w^k D_k(m)$

(en fait le cas $\lambda > 1$ suffisait pour les questions suivantes).

$$41. \text{ On définit } \mathbf{c} \in \mathbb{A} \text{ par } \mathbf{c}(1) = 1 \text{ et pour } m \geq 2, \mathbf{c}(m) = \sum_{k=1}^{\lfloor \log_2 m \rfloor} w^k D_k(m)$$

De sorte que d'après la question précédente, pour s réel suffisamment grand, on a $\frac{1}{L_f(s)} = L_{\mathbf{c}}(s)$.

En reprenant les notations du I.E et à l'aide de 19 (valable pour toute fonction arithmétique), on a $A_c(L_{\mathbf{c}}) < +\infty$ et pour s assez grand

$$L_{\delta}(s) = 1 = L_f(s) L_{\mathbf{c}}(s) = L_{f * \mathbf{c}}(s)$$

Dans la question 18, on remarque que l'égalité ci-dessus pour s assez grand, suffit à obtenir l'égalité : $\delta = \mathbf{f} * \mathbf{c}$ donc comme l'anneau $(\mathbb{A}, +, *)$ est commutatif, $\mathbf{f}$ est inversible d'inverse $\mathbf{c}$.

Or d'après 38, $\mathbf{f}$ est inversible d'inverse $\mathbf{b}$.

Par unicité de l'inverse, on a donc

$$\forall m \geq 2, \mathbf{b}(m) = \sum_{k=1}^{\lfloor \log_2 m \rfloor} w^k D_k(m)$$

D'après 37, on a alors

$$\chi_n(\lambda) = (\lambda - 1)^n - (\lambda - 1)^{n-1} \sum_{m=2}^n \sum_{k=1}^{\lfloor \log_2 m \rfloor} w^k D_k(m) = (\lambda - 1)^n - (\lambda - 1)^{n-1} \sum_{m=2}^n \sum_{k=1}^{\lfloor \log_2 n \rfloor} w^k D_k(m)$$

dans le troisième membre, on a rajouté des 0. Or

$$\sum_{m=2}^n \sum_{k=1}^{\lfloor \log_2 n \rfloor} w^k D_k(m) = \sum_{k=1}^{\lfloor \log_2 n \rfloor} w^k \sum_{m=2}^n D_k(m) = \sum_{k=1}^{\lfloor \log_2 n \rfloor} (\lambda - 1)^{-k} \sum_{m=2}^n D_k(m)$$

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

42. Comme deux polynômes qui coïncident sur une infinités de valeurs sont égaux, on a alors

$$\chi_n = (X-1)^n - \sum_{k=1}^{\lfloor \log_2 n \rfloor} (X-1)^{n-k-1} S_k(n) = (X-1)^{n-\lfloor \log_2 n \rfloor-1} \left[(X-1)^{\lfloor \log_2 n \rfloor+1} - \sum_{k=1}^{\lfloor \log_2 n \rfloor} (X-1)^{\lfloor \log_2 n \rfloor-k} S_k(n) \right]$$

On note $Q(X) = (X-1)^{\lfloor \log_2 n \rfloor+1} - \sum_{k=1}^{\lfloor \log_2 n \rfloor} (X-1)^{\lfloor \log_2 n \rfloor-k} S_k(n)$

De sorte que $\chi_n(X) = (X-1)^{n-\lfloor \log_2 n \rfloor-1} Q(X)$

et on a $Q(1) = 0 - \sum_{k=1}^{\lfloor \log_2 n \rfloor-1} 0 - S_{\lfloor \log_2 n \rfloor}(n) = -S_{\lfloor \log_2 n \rfloor}(n)$

Enfin $S_{\lfloor \log_2 n \rfloor}(n) = \sum_{m=2}^n D_{\lfloor \log_2 n \rfloor}(m)$ or $n \geq 2$ donc $2 \leq 2^{\lfloor \log_2 n \rfloor} \leq n$. Ainsi

$$S_{\lfloor \log_2 n \rfloor}(n) \geq 0 + D_{\lfloor \log_2 n \rfloor}(2^{\lfloor \log_2 n \rfloor}) = 1$$

donc $Q(1) \neq 0$ car $Q(1) \leq -1$

ainsi H_n possède 1 comme valeur propre de multiplicité est exactement $n - \lfloor \log_2 n \rfloor - 1$