I Quelques résultats utiles

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

Q 1. On a $f*\delta(n)=\sum_{d|n} f(d)\delta(n/d)$. Le seul terme non nul est lorsque $n/d=1$ soit lorsque $d=n$. Il vient $f*\delta(n)=f(n)$ pour tout $n\in\mathbb{N}^*$ donc $f*\delta=f$. De même $\delta*f=f$.

Q 2. l'application $\theta : d\mapsto (d,n/d)$ est une bijection entre $\mathcal{D}_n$ et $\mathcal{C}_n$: elle est bien définie, elle est directement injective et si $(d_1,d_2)\in\mathcal{C}_n$ alors $d_1d_2=n$ donc $d_1\in\mathcal{D}_n$ et $\theta(d_1)=(d_1,d_2)$. On a alors, pour $n\in{}^*_N$,

$$(f*g)(n)=\sum_{d\in\mathcal{D}_n} f(d)g\left(\frac{n}{d}\right)=\sum_{(d1,d_2)\in\mathcal{C}_n} f(d_1)g\left(\frac{n}{d_1}\right)=\sum_{(d1,d_2)\in\mathcal{C}_n} f(d_1)g(d_2)$$

Q 3. L'application $(d_1,d_2)\in\mathcal{C}_n\mapsto(d_2,d_1)\in\mathcal{C}_n$ est une bijection de $\mathcal{C}_n$. On a donc

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

Q 4. pour $n\in\mathbb{N}^*$,

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

le triplet $(d,\frac{d}{k},\frac{n}{d})$ est dans $\mathcal{C}'_n$. Réciproquement si $(d_1,d_2,d_3)\in\mathcal{C}'_n$, alors en posant $k=d_1d_2$ et $d=d_1$, on a $(d_1,d_2,d_3)=(d,\frac{k}{d},\frac{n}{k})$ avec $\frac{k}{d}$ et $\frac{n}{d}$ qui sont entiers donc $d|n$ et $k|d$. On en déduit que

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

On montre de la même manière que $(f*(g*h))(n)=\sum_{(d_1,d_2,d_3)\in\mathcal{C}'_n} f(d_1)g(d_2)h(d_3)$, ce qui donne l'associativité de la loi $*$.

Q 5. On vérifie que $(\mathbb{A},+,*)$ est un anneau commutatif :

- $(\mathbb{A},+)$ est un groupe car $\mathbb{C}$ est un groupe donc $\mathcal{F}(\mathbb{N},\mathbb{C}),+)$ aussi
- on vérifie la distributivité de la loi + sur la loi $*$ (il faut l'écrire) - à droite ou à gauche car $*$ est commutative
- on a prouvé l'associativité de $*$, sa commutativité et l'existence d'un élément neutre pour $*$

I.B - Groupe des fonctions multiplicatives

Q 6. si $n\in\mathbb{N}^*$ avec $n\geqslant 2$ et $n=p_1^{\alpha_1}\dots p_q^{\alpha_q}$ une décomposition en facteurs premiers distincts (on a besoin de $n\geqslant 2$), alors par récurrence

$$f(n)=\prod_{k=1}^{q} f(p_k^{\alpha_k})$$

On a la même formule pour g et finalement $g(n)=f(n)$ si $n\geqslant 2$. Il reste à montrer que $f(1)=g(1)$.
On a $f(1)=f(1^2)=f(1)f(1)$ car $1\wedge 1=1$. Puisque $f(1)\neq 0$, on a $f(1)=1$. De même pour g.
On a bien montré que $f=g$.

Q 7.

- tout d'abord π est bien définie : si $d_1|n$ et $d_2|m$, alors il existe des entiers naturels non nuls k_1 etk_2 tel que $n=k_1d_1$ et $m=k_2d_2$ d'où $mn=(k_1k_2)(d_1d_2)$ donc $d_1d_2\in\mathcal{D}_{mn}$.
- l'application est injective : si $\pi((d_1,d_2))=\pi((d'_1d'_2))$ alors $d_1d_2=d'_1d'_2$. On a donc $d_1|(d'_1d'_2)$. De plus d_1 est un diviseur de n, d'_2 est un diviseur de m donc si q est un diviseur commun à d_1 et d'_2 alors q divise m et n. Puisqu'ils sont premiers entre eux, alors d_1 et d'_2 sont premiers entre eux. On a donc $d_1|d'_1$. Par symétrie $d'_1|d_1$ et finalement $d_1=d'_1$. Il reste alors $d_2=d'_2$. L'application est injective.
- L'application est surjective : on utilise les décompositions en facteurs premiers de m et n :

$$m=\prod_{k=1}^{r} p_i^{\alpha_i} \text{ et } n=\prod_{j=1}^{s} q_j^{\beta_j}$$

où $p_1,\dots,p_r,q_1,\dots,q_s$ sont des nombres premiers deux à deux distincts (car m et n n'ont aucun facteur premier en commun) et les α_i et β_j sont dans $\mathbb{N}^*$. On a

$$mn=\prod_{k=1}^{r} p_i^{\alpha_i}.\prod_{j=1}^{s} q_j^{\beta_j}$$

et un diviseur de mn s'écrit

$$d = \prod_{k=1}^{r} p_i^{\alpha'_i} . \prod_{j=1}^{s} q_j^{\beta'_j}$$

avec $\alpha'_i \leqslant \alpha_i$ et $\beta'_j \leqslant \beta_j$ (des entiers naturels). En posant

$$d_1 = \prod_{k=1}^{r} p_i^{\alpha'_i} \text{ et } d_2 = \prod_{j=1}^{s} q_j^{\beta'_j}$$

alors $(d_1, d_2) \in \mathcal{D}_n \times \mathcal{D}_m$ et $\pi((d_1, d_2)) = d$. On a la surjectivité

Q 8. Soient m et n deux entiers non nuls premiers entre eux,

$$(f*g)(mn) = \sum_{d|mn} f(d)g(mn/d) = \sum_{(d_1,d_2)\in\mathcal{D}_n\times\mathcal{D}_m} f(d_1d_2)g\left(\frac{mn}{d_1d_2}\right) = \sum_{(d_1,d_2)\in\mathcal{D}_n\times\mathcal{D}_m} f(d_1d_2)g\left(\frac{n}{d_1}\frac{m}{d_2}\right)$$

D'après la question précédente, d_1 et d_2 sont premiers entre eux, ainsi que n/d_1 et m/d_2 (diviseurs de n et m). On a donc

$$(f*g)(mn) = \sum_{d_1|n}\sum_{d_2|m} f(d_1)f(d_2)g\left(\frac{n}{d_1}\right)g\left(\frac{m}{d_2}\right) = \left(\sum_{d_1|n} f(d_1)g\left(\frac{n}{d_1}\right)\right)\left(\sum_{d_2|m} f(d_2)g\left(\frac{m}{d_2}\right)\right) = (f*g)(n).(f*g)(m)$$

On a également $(f*g)(1) = f(1)g(1) neq 0$. La fonction $f*g$ est encore multiplicative.

Q 9. On commence par montrer qu'une fonction multiplicative est définie de façon unique à partir de ses valeurs en les p^k avec p premier et $k \in \mathbb{N}^*$:

- on a $g(1) = 1$.
- soit $n \geqslant 2$ un entier. Si $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ avec $p_1, \ldots, p_k$ premiers deux à deux distincts et $\alpha_i \in \mathbb{N}^*$, alors $g(n) = \prod_{i=1}^{k} g\left(p_i^{\alpha_i}\right)$.
- réciproquement une telle fonction est bien multiplicative : si

$$m = \prod_{k=1}^{r} p_i^{\alpha_i} \text{ et } n = \prod_{j=1}^{s} q_j^{\beta_j}$$

avec des facteurs premiers tous distincts ($m \wedge n = 1$) et des exposants non nuls, on a alors

$$g(mn) = \prod_{k=1}^{r} g\left(p_i^{\alpha_i}\right) . \prod_{j=1}^{s} g\left(q_j^{\beta_j}\right)$$

et on constate que c'est exactement $g(m)g(n)$. L'unicité est alors garantie par la question **Q6**.

Les relations $g(p^k) = -\sum_{i=1}^{k} f(p^i)g(p^{k-i})$ permettent de définir g sur les nombres p^k avec p premiers et $k \in \mathbb{N}^*$ et cela permet donc de définir entièrement une application multiplicative g.
On a alors, pour p premier et $k \in \mathbb{N}^*$,

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

On a également $(f*g) = 1$. L'application $f*g$ est nulle sur tous les p^k donc coïncide avec δ sur ces entiers et donc partout par unicité de la question **Q6**. On a bien une application multiplicative g telle que $f*g = \delta$.

Q 10. L'ensemble est non vide, la loi $*$ est une loi de composition interne, associative et commutative. On a un éléments neutre δ ainsi qu'un symétrique pour toute application. L'ensemble $(\mathbb{M}, *)$ est un groupe commutatif.

I.C - La fonction de Möbius

Q 11. soit m et n premiers entre eux. Si l'un d'eux est divisible par le carré d'un nombre premier alors leur produit aussi et $\mu(mn) = 0 = \mu(m)\mu(n)$. Si n est le produit de k entiers premiers distincts et m de l entiers premiers distincts, alors mn est produit de $k+l$ entiers premiers distincts et $\mu(mn) = (-1)^{k+l} = (-1)^k(-1)^l = \mu(m)\mu(n)$. La fonction est multiplicative.

Q 12. On a $\mu * \mathbb{1}(1) = 1$ et la fonction est multiplicative. Soit $p \in \mathcal{P}$ et $k \in \mathbb{N}^*$, alors

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

puisque tous les $\mu(p^i)$ sont nuls si $i \geqslant 2$. La fonction multiplicative coïncide avec δ sur les entiers p^k donc $\mu * \mathbb{1} = \delta$.

Q 13. On remarque de $F = f * \mathbb{1} = \mathbb{1} * f$. On a alors $\mu * F = \mu * \mathbb{1} * f = f$ ce qui correspond à la relation demandée.

Q 14. De nouveau, on a deux fonctions multiplicatives et on montre qu'elles sont égales sur les p^k.

- on a $\varphi(p^k) = p^k - p^{k-1}$: ce sont tous les entiers entre 1 et p^k qui ne sont as multiples de p : il y a p^{k-1} multiples de p, les $p.q$ avec $q \in [\![1; p^{k-1}]\!]$.
- $(\mu * \mathbb{I})(p^k) = \mu(1)\mathbb{I}(p^k) + \mu(p)\mathbb{I}(p^{k-1}) + 0 = p^k - p^{k-1}$

On a donc l'égalité $\varphi = \mu * \mathbb{I}$.

Remarque : on trouve alors $\mathbb{I} = \varphi * \mathbb{1}$, ce qui donne, pour tout $n \in \mathbb{N}^*$,

$$n = \sum_{d|n} \varphi(d)$$

I.D - Déterminant de Smith

Q 15. On calcule le terme en position (i, j) de $M'D^T$: il vaut

$$a_{ij} = \sum_{k=1}^{n} m'_{ik} d_{jk} = \sum_{k|j} m'_{ik} = \sum_{k|i,k|j} g(k) = \sum_{k|i\wedge j} g(k).1 = (g * \mathbb{1})(i \wedge j)(f * \mu * \mathbb{1})(i \wedge j) = (f * \delta)(i \wedge j) = f(i \wedge j)$$

Cela donne $M = M'D^T$.

Q 16. Ainsi $\det M = \det M' . \det D$. Les matrices D et M' sont triangulaires. Les éléments diagonaux de D valent 1. On a donc

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

I.E - Séries de Dirichlet

Q 17. Si $s \geqslant s'$, alors pour tout $k \in \mathbb{N}^*$, $\left|\frac{f(k)}{k^s}\right| \leqslant \left|\frac{f(k)}{k^{s'}}\right|$. On note $B_f = \{s \in \mathbb{R}, \sum \frac{f(k)}{k^s}$ converge absolument$\}$. Si B_f est non vide et si $s \in B_f$ alors $[s, \infty[\subset B_f$. On en déduit que $B_f =]A_c(f), +\infty[$ ou $[A_c(f), +\infty[$ s'il est non vide. Cela donne la convergence absolue de la série pour tout $s > A_c(f)$.

Q 18. on note $M = \max(A_c(f), A_c(g))$. Par différence, on a, pour tout $s > M$, $\sum_{k=1}^{+\infty} \frac{a_k}{k^s} = 0$ où $a_k = f(k) - g(k)$. La série $\sum \frac{a_k}{k^s}$ converge absolument pour tout $s > M$. On suppose que les a_k ne sont pas tous nuls et on note i l'indice minimal pour lequel $a_i \neq 0$. On a donc, pour tout $s > M$,

$$\frac{a_i}{i^s} + \sum_{k=i+1}^{+\infty} \frac{a_k}{k^s} = 0$$

ou encore

$$a_i + \sum_{k=i+1}^{+\infty} a_k \frac{i^s}{k^s} = 0$$

Puisque $0 < \frac{i}{k} < 1$, on a $\lim_{s\to+\infty} \frac{i^s}{k^s} = 0$. On va justifier qu'on peut permuter somme et limite en $+\infty$. On note $f_k(s) = a_k \frac{i^s}{k^s}$. Pour tout $s \geqslant M+1$, on a $\left|f_k(s)\right| \leqslant |f_k(M+1)| = i^{M+1} \frac{|a_k|}{k^{M+1}}$ terme général d'une série convergente. On a donc convergence normale de $\sum f_k$ sur $[M+1, +\infty[$. On peut appliquer le théorème de permutation des limites et obtenir $a_i + 0 = 0$ donc une contradiction. On a bien, pour tout $k \in \mathbb{N}^*$, $a_k = 0$ et donc $f = g$.

Q 19. On note de nouveau M le maximum des abscisses de convergence. On a pour $s > M$,

$$L_f(s)L_g(s) = \sum_{(k,l)\in(\mathbb{N}^*)^2} \frac{f(k)g(l)}{(kl)^s}$$

et la famille $\left(\frac{f(k)g(l)}{(kl)^s}\right)_{(k,l)\in(\mathbb{N}^*)^2}$ est sommable car chaque série converge absolument. On effectue alors une sommation par paquet en regroupant tous les produits kl qui valent un certain entier n :

$$(N^*)^2 = \bigcup_{n\in\mathbb{N}^*} \mathcal{C}_n$$

où $\mathcal{C}_n = \{(k,l) \in (\mathbb{N}^*)^2, kl = n\}$. On a donc

$$L_f(s)L_g(s) = \sum_{n=1}^{+\infty} \left(\sum_{(k,l)\in\mathcal{C}_n} \frac{f(k)g(l)}{(kl)^s} \right) = \sum_{n=1}^{+\infty} \left(\sum_{(k,l)\in\mathcal{C}_n} \frac{f(k)g(l)}{n^s} \right) = \sum_{n=1}^{+\infty} \left(\sum_{k|n} \frac{f(k)g(n/k)}{n^s} \right) = \sum_{n=1}^{+\infty} \frac{(f*g)(n)}{n^s} = L_{f*g}(s)$$

II Matrices et endomorphismes de permutation

II.A - Similitude de deux matrices de permutation

Q 20. On peut le faire par calcul direct mais également plus simplement. On note $\mathscr{B} = (e_1, \dots, e_n)$ la base canonique de $E = \mathbb{R}^n$. On note f_σ l'endomorphisme de E tel que $f_\sigma(e_j) = e_{\sigma(j)}$. La matrice P_σ est la matrice de f_σ dans la base $\mathscr{B}$. On a $(f_\sigma f_{\sigma'})(e_j) = f_\sigma(e_{\sigma'(j)} = f_{\sigma\sigma'}(e_j)$ pour tout $j \in [\![1;n]\!]$, ce qui donne $f_\sigma f_{\sigma'} = f_{\sigma\sigma'}$ et matriciellement $P_\sigma.P_{\sigma'} = P_{\sigma\sigma'}$.
Si σ et τ sont conjuguées, il existe une permutation ρ telle que $\tau = \rho\sigma\rho^{-1}$. On a alors $P_\tau = P_\rho P_\sigma P_{\rho^{-1}}$. Or $P_\rho.P_{\rho^{-1}} = P_{\mathrm{Id}} = I_n$ donc $P_{\rho^{-1}} = (P_\rho)^{-1}$. Cela donne bien la similitude de P_σ et P_τ.

Q 21. on essaie plutôt de vérifier que $\rho\gamma_1 = \gamma_2\rho$:

- si $k = 1 : \gamma_2\rho(1) = \gamma_2(2) = 6$ et $\rho\gamma_1(1) = \rho(3) = 6$,
- si $k = 3$, on a vérifie que $\gamma_2\rho(3) = \rho\gamma_1(3) = 6$ et de même avec $k = 7$ et la valeur 4.
- $k \notin \{1,3,7\} : \rho\gamma_1(k) = \rho(k)$ et $\gamma_2\rho(k) = \rho(k)$ car $\rho(k) \notin \{2,4,6\} = \mathrm{Supp}(\gamma_2)$.

Q 22. si $\gamma_1 = (a_1 a_2 \dots a_\ell)$ et $\gamma_2 = (b_1 b_2 \dots b_\ell)$ sont deux cycles de même longueur, on prend ρ une permutation telle que $\rho(a_i) = b_i$. On vérifie comme précédemment que $\rho\gamma_1 = \gamma_2\rho$ (avec par exemple $\rho\gamma_1(a_i) = b_{i+1}$ si $i \in [\![1;\ell-1]\!]$ et b_1 si $i = \ell$et de même pour $\gamma_2\rho$).

Q 23. si σ est un cycle $(a_1 a_2 \dots a_k)$ de longueur k et ρ une permutation alors les calculs précédents montrent que $\rho\sigma\rho^{-1}$ est le cycle de longueur k également, $(\rho(a_1)\rho(a_2)\dots\rho(a_k))$. De plus si ue permutation s est produit de cycles à support disjoints $s = c_1 \dots c_p$, alors

$$\rho s\rho^{-1} = \left(\rho c_1\rho^{-1}\right)\left(\rho c_2\rho^{-1}\right)\dots\left(\rho c_p\rho^{-1}\right)$$

est encore un produit de cycles à supports disjoints, chaque cycle $\rho c_i\rho^{-1}$ étant de même longueur que c_i.

- si σ et τ sont conjugués alors il existe ρ tel que $\tau = \rho\sigma\rho^{-1}$. On décompose σ en produit de cycles à supports disjoints. On vient de voir que $\rho\sigma\rho^{-1}$ s'écrit encore sous la forme de produit de cycles à supports disjoints avec exactement les mêmes longueurs pour les cycles qui apparaissent. On a donc $c_\ell(\sigma) = c_\ell(\tau)$ pour tout les entiers $\ell \in [\![2;n]\!]$. Pour $\ell = 1 : k$ est un point fixe de σ si et seulement si $\rho(k)$ en est un pour τ :

  $$\sigma(k) = k \Leftrightarrow \rho\sigma(k) = \rho(k) \Leftrightarrow (\rho\sigma\rho^{-1})(\rho(k)) = \rho(k) \Leftrightarrow \tau(\rho(k)) = \rho(k)$$

  Les deux permutations ont le même nombre de points fixes. Finalement si τ et σ sont conjuguées alors elles ont le même type cyclique.
- Réciproquement si σ et τ ont le même type cyclique. On décompose σ et τ en produit de cycles à supports disjoints $\sigma = c_1 c_2 \dots c_p$ et $\tau = d_1 d_2 \dots d_p$ avec c_i et d_i de même longueur (ou on regroupe les cycles à support disjoints de même longueur). On crée alors une permutation qui conjugue chaque c_i à chaque d_i (possible car les supports des c_i et des d_i sont disjoints) et qui envoie les points fixes de σ sur ceux de τ (il n'y a pas unicité : on peut déjà permuter tous les points fixes, ainsi que choisir l'ordre des cycles de même taille et même sur un cycle, l'ordre des éléments peut être décalé).

Remarque : jusqu'à quel point faut-il rédiger cette question ? si on veut vraiment tout formaliser, c'est faisable mais ça prend du temps...

Q 24. Le cycle γ est conjugué au cycle $\gamma' = (12\dots\ell)$. Les matrices P_γ et $P_{\gamma'}$ sont semblables et ont du même polynôme caractéristique. La matrice $P_{\gamma'}$ est Γ_ℓ. On calcule son polynôme caractéristique :

$$d_n = \begin{vmatrix} X & 0 & 0 & -1 \\ -1 & \ddots & \ddots & \ddots \\ & \ddots & X & 0 \\ 0 & & -1 & X \end{vmatrix}$$

On développe par rapport à la première ligne pour obtenir deux déterminants de matrices triangulaires : inférieures pour la première avec des X sur la diagonale et supérieure avec des -1 sur la diagonale pour l'autre. Cela donne

$$d_n = X.X^{\ell-1} + (-1)(-1)^{\ell+1}.(-1)^{\ell-1} = X^\ell - 1$$

Q 25. On décompose σ en produit de cycles à supports disjoints : $\sigma = c_1 c_2 \dots c_k$ avec ℓ_i la longueur du cycle c_i. On crée une permutation conjugué $\tau = c'_1 c'_2 \dots c'_k$ avec c'_1 cycle $(12\dots\ell_1)$, $c'_2 = (\ell_1\ell_1+1\dots\ell_1+\ell_2)$... c'_i étant le cycle $(s_i s_i+1\dots s_i+\ell_i)$ où s_i est la somme des longueurs précédentes $s_i = \sum_{j=1}^{i-1} \ell_j$. Les derniers entiers restants étant laissés invariants. Les deux cycles sont conjugués et les matrices associées ont même polynôme caractéristique. La matrice P_τ est diagonale par blocs avec des blocs $\Gamma_{\ell_1}, \Gamma_{\ell_2}, \dots, \Gamma_{\ell_k}$ et un derniers blocs identité $I_{c_1(\sigma)}$. Le polynôme caractéristique est alors

$$\chi_\sigma(X) = (X-1)^{c_1(\sigma)} \prod_{i=1}^{k} (X^{\ell_i} - 1)$$

En regroupant les cycles de même longueur, on obtient le résultat

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

Q 26. Si P_σ et P_τ sont semblables, alors elles ont le même polynôme caractéristique. Les racines de ces polynômes caractéristiques sont des racines de l'unité d'ordre au plus n. On fixe $q \in [\![1;n]\!]$ et on regarde les multiplicités pour la racine $\omega = e^{2i\pi/q}$. On a ω racine de $X^\ell - 1$ si et seulement si $\omega^\ell = 1$ donc si et seulement si ℓ est un multiple de q (ou q un diviseur de ℓ). Dans ce cas, on a ω qui est racine simple de $X^\ell - 1$ et de multiplicité $c_\ell(\sigma)$ dans $(X^\ell - 1)^{c_\ell(\sigma)}$. Finalement ω est de multiplicité $\sum_{q|\ell} c_\ell(\sigma)$. Il en est de même pour τ. On a donc les égalités pour chaque entier $q \in [\![1;n]\!]$.

Q 27. On calcule $T_\sigma D$. T_σ est une matrice ligne $(c_1 c_2 \dots c_n)$. Le produit est aussi une matrice ligne $(a_1 a_2 \dots a_n)$ avec $a_j = \sum_{k=1}^{n} c_k d_{kj}$ Or d_{kj} ne vaut 1 que si $j|k$ et 0 sinon. Cela donne $a_j = \sum_{j|k} c_k(\sigma)$, exactement les quantités précédentes. Ainsi on obtient $T_\sigma D = T_\tau D$. Puisque D est de déterminant 1, elle est inversible et ainsi $T_\sigma = T_\tau$. Les deux permutations ont bien le même type cyclique et sont donc conjuguées.

II.B - Endomorphismes de permutation

Q 28. Si u est un endomorphisme de permutation et $\mathscr{B} = (a_1, \dots, e_n)$ une base comme dans la définition, alors la matrice de u dans la base $\mathscr{B}$ est P_σ : en colonne j, on a un coefficient 1 si $i = \sigma(j)$ et 0 sinon. Réciproquement si la matrice de u dans une base $\mathscr{B} = (e_1, \dots, e_n)$ est P_σ alors $u(e_j) = e_{\sigma(j)}$ pour tout $j \in [\![1;n]\!]$.

Q 29. Soit u l'endomorphisme associé à la permutation σ. Soit k l'ordre de la permutation σ. On a $(P_\sigma)^k = P_{\sigma^k} = P_{\mathrm{Id}} = I_n$. Le polynôme $X^k - 1$ est un polynôme annulateur scindé à racines simples pour P_σ et aussi u - donc la matrice P_σ et l'endomorphisme u sont diagonalisable. Puisque P_σ a des éléments diagonaux qui valent 0 ou 1, sa trace est un entier entre 0 et n. Il en est de même pour $\mathrm{tr}\, u$.

Q 30. Si les matrices sont semblables alors elles ont le même polynôme caractéristique. Réciproquement si A est diagonalisable avec $\chi_A = \prod_{k=1}^{m} (X - \lambda_k)^{n_k}$ avec $\lambda_1, \dots, \lambda_m$ les valeurs propres distinctes de A, alors A est semblable la matrice diagonale avec les valeurs propres qui apparaissent autant de fois que leur multiplicité (dans le même ordre). Si A et B sont diagonalisables avec le même polynôme caractéristique alors elles sont semblables à une même matrice diagonale donc semblables par transitivité.

Q 31. la réciproque a déjà été vue. On suppose que $u^2 = \mathrm{Id}_E$ et que $\mathrm{tr}(u) \in \mathbb{N}$. L'endomorphisme u est diagonalisable avec deux valeurs propres possibles ± 1. Si on note α la multiplicité de 1 et β celle de -1, on a $\alpha + \beta = n$ et $\mathrm{tr}\, u = \alpha - \beta$. On a donc $\alpha \geqslant \beta$. On a donc un polynôme caractéristique $\chi_u = (X-1)^\alpha (X+1)^\beta = (X^2-1)^\beta (X-1)^{\alpha-\beta}$. On note A la matrice de u dans une base de E. La matrice B diagonale par blocs avec β blocs $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $\alpha - \beta$ termes valant 1 ensuite possède le même polynôme caractéristique, elle est diagonalisable car chaque bloc $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ est semblable à $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et c'est la matrice de la permutation $(12)(34)\dots(2\beta-1\ 2\beta)$. Les matrices A et B sont semblables. Il existe donc une base dans laquelle la matrice de u est la matrice d'une permutation.

Q 32. Le sens réciproque est toujours vrai (pour tout k).

- $k = 3$: le polynôme $X^3 - 1 = (X-1)(X-j)(X-\overline{j})$ est annulateur de u donc A est diagonalisable avec $\mathrm{Sp}\, A \subset \{1, j, \overline{j}\}$. On note α, β, γ les multiplicités respectives des trois valeurs propres éventuelles (la multiplicité peut être nulle). On a $\alpha + \beta + \gamma = n$ et $\alpha + \beta j + \gamma \overline{j} \in \mathbb{N}$. La partie imaginaire est nulle donc $\beta = \gamma$. Puisque $j + \overline{j} = j + j^2 = -1$, on a $\mathrm{tr}\, u = \alpha - \beta$ donc $\beta = \gamma \leqslant \alpha$ et
$$\chi_u = ((X-1)(X-j)(X-j^2))^\beta (X-1)^{n-3\beta} = (X^3-1)^\beta (X-1)^{n-3\beta}.$$
La matrice Γ_3 admet (X^3-1) comme polynôme caractéristique et est diagonalisable (polynôme caractéristique scindé à racines simples). On note B la matrice par blocs avec β blocs de la forme Γ_3 et le reste de la diagonale à 1. Cette matrice est diagonalisable et a le même polynôme caractéristique que A donc A et B sont semblables. De nouveau B est la matrice d'une permutation (produit de cycles de longueurs 3 : (1 2 3), (4 5 6) ...). On en déduit qu'il existe une base dans laquelle la matrice de A est la matrice d'une permutation.
- $k = 4$: ça ne fonctionne plus... la matrice $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ a un polynôme caractéristique $X^2 + 1$ qui n'est pas du type qu'on doit obtenir (question 25) et vérifie $u^4 = I_2$. Pour généraliser, on prend une matrice avec ce bloc et $n-2$ termes diagonaux qui valent 1 (et 0 ailleurs).
Remarque : si on essaie de faire comme avant, on a des multiplicités α pour 1, β pour -1 et $\gamma = \delta$ pour i et $-i$. La trace donne seulement $\alpha - \beta \in \mathbb{N}$ mais aucune contrainte sur γ qui permettrait de regrouper 4 par 4 afin d'avoir des blocs Γ_4.

Q 33. Pour le sens direct : la question 25 donne la première propriété. Pour la seconde, si on note N l'ordre de la permutation (on est dans un groupe fini), on a $u^N = \mathrm{Id}_E$. On s'intéresse à la réciproque.

- le (b) nous dit que u est diagonalisable car il admet un polynôme annulateur scindé à racines simples.
- Le (a) nous dit que u possède la même polynôme caractéristique qu'une permutation σ de $\mathfrak{S}_n$ qui aurait $c_\ell(\sigma) = c_\ell$ pour tout entier $\ell \in [\![1;n]\!]$ (on en a construit une en question 25). La matrice de l'endomorphisme u dans une certaine base est donc semblable à la matrice de la permutation σ (question 30). Ainsi u est un endomorphisme de permutation.

Q 34. deux versions... aucune vraiment immédiate :

- on utilise les fonctions symétriques des racines (ça déborde un peu du programme). L'endomorphisme u est trigonalisable et il existe une base dans laquelle sa matrice est triangulaire avec une diagonale $\lambda_1, \lambda_2, \dots, \lambda_n$. On a alors $\mathrm{tr}\, u^k = \sum_{i=1}^{n} \lambda_i^k$. On développe le polynôme $\chi_u = \prod_{i=1}^{n} (X - \lambda_i)$ et chaque coefficient s'exprime à l'aide des sommes $\sum_{i=1}^{n} \lambda_i^k$, donc des $\mathrm{tr}\,(u^k)$. On en déduit que u et v ont le même polynôme caractéristique.
- on le démontre en résolvant un système faisant apparaître les valeurs propres. On pourrait noter $\lambda_1, \dots, \lambda_p$ les valeurs propres distinctes de u et $\mu_1, \dots, \mu_q$ celle de v mais c'est compliqué à rédiger. Le plus simple est de regrouper ces valeurs propres en un seul ensemble : on note $\lambda_1, \dots, \lambda_r$ les différentes valeurs propres de u et v et on note $n_1, \dots, n_r$ leurs multiplicités dans χ_u et $m_1, \dots, m_r$ celles dans χ_v (certaines peuvent être nulles). Cela donne alors, pour tout $k \in \mathbb{N}$, $\mathrm{tr}\,(u^k) = \sum_{i=1}^{r} n_i \lambda_i^k = \sum_{i=1}^{r} m_i \lambda_i^k = \mathrm{tr}\,(v^k)$ et ainsi $\sum_{i=1}^{r} (n_i - m_i)\lambda_i^k = 0$ pour tout $k \in \mathbb{N}$. En écrivant les r premières équations (pour k allant de 0 à $r-1$), on obtient un système d'équations dont le déterminant est un déterminant de Vandermonde inversible - les inconnues étant les $n_i - m_i$. Chaque $m_i - n_i$ est donc nul et pour tout $i \in [\![1;r]\!]$, on a $m_i = n_i$. Les deux matrices ont donc les mêmes valeurs propres avec les mêmes multiplicités et donc le même polynôme caractéristique.

Q 35. On cherche à démontrer les deux points de la question 33. Une fois qu'on aura montré que ch_u^i est sous la forme de (a), on en déduira que les valeurs propres de u sont des racines de l'unité. En prenant N le ppcm des ordres des racines de χ_u, puisque u est diagonalisable, il admettra une matrice diagonale dans une certaine base et la matrice de u^N dans cette base sera I_n. On aura donc le point (b). Il reste donc à voir (a). Pour cela on ma montrer que u et v vérifie la propriété de 34 lorsque v est l'endomorphisme de permutation créé à la question 25 : pour chaque entier $\ell \in [\![1;n]\!]$, on a c_ℓ blocs Γ_ℓ. Il reste donc à calculer $\mathrm{tr}\,(v^k)$ pour un tel endomorphisme. On a tout d'abord $\mathrm{tr}\,(v^k) = \sum_{\ell=1}^{n} c_\ell \mathrm{tr}\,(\Gamma_\ell^k)$ (on prend la trace de chaque bloc). Il reste à étudier les traces de Γ_ℓ^k.

On note γ le cycle $(1\ 2 \cdots \ell)$ et $A = P_\gamma$. On prend $(e_1, \dots, e_\ell)$ la base canonique de $\mathbb{R}^\ell$ ou $\mathbb{C}^\ell$ et u l'endomorphisme canoniquement associé à γ : on a $u(e_k) = e_{k+1}$ si $k \in [\![1;\ell-1]\!]$ et $u(e_\ell) = e_1$. Puisque $\gamma^e ll$ est l'identité, on a $\Gamma_\ell^\ell = I_\ell$. Si $p \in [\![1;\ell-1]\!]$ alors, pour $k \in [\![1;\ell]\!]$, $u^p(e_k) = e_{k+p}$ si $k+p \leqslant \ell$ et $u^p(e_k) = e_{k+p-\ell}$ si $k+p \geqslant \ell+1$. On a donc des termes nuls sur la diagonale. On en déduit que $\mathrm{tr}\,(\Gamma_\ell^k) = 0$ si $k \in [\![1;\ell-1]\!]$. Puisque $\Gamma_\ell^\ell = I_n$, on a $\mathrm{tr}\,(\Gamma_\ell^k) = 0$ si k n'est pas un multiplie de ℓ et $\mathrm{tr}\,(\Gamma_\ell^k) = \ell$ sinon.

On a donc obtenu que $\mathrm{tr}\,(v^k) = \sum_{\ell=1}^{n} c_\ell \mathrm{tr}\,(\Gamma_\ell^k) = \sum_{l=1,\ell|k}^{n} \ell c_\ell$. Cela termine la démonstration.

Remarque : un autre moyen pour calculer $\mathrm{tr}\,(\Gamma_\ell^k)$ est de la diagonaliser : son polynôme caractéristique est $X^\ell - 1$. Elle est donc semblable à la matrice diagonale $(1, \omega_\ell, \omega_\ell^2, \dots, \omega_\ell^{\ell-1})$ où $\omega_\ell = \exp(2i\pi/\ell)$. On a alors $\mathrm{tr}\,(\Gamma_\ell^k) = \sum_{p=0}^{\ell-1} (\omega_\ell^k)^p$. Suivant que ω_ℓ^k vaut 1 ou non, on trouve 0 ou ℓ.

III Valeurs propres de la matrice de Redheffer

Q 36. On calcule les différents termes : on note c_{ij} les coefficients de C_n

- $c_{11} = \sum_{k=1}^{n} \mu(k) = M_n$,
- si $j \in [\![2;n]\!]$, $c_{1j} = \sum_{k=1}^{n} a_{1k} h_{kj} = \sum_{k=1}^{n} \mu(k) h_{kj} = \sum_{k|j} \mu(k) = (\mu * \mathbb{1})(j) = \delta(j) = 0$ puisque $j \geqslant 2$,
- si $i \geqslant 2$, $c_{ij} = \sum_{k=1}^{n} a_{ik} h_{kj} = h_{ij}$

La première ligne de la matrice C_n est donc $M(n)$ suivi par $n-1$ termes nuls. On développe $\det C_n$ par rapport à cette ligne. On a donc $\det C_n = M(n).\det B$ où B est la matrice extraite de H_n en retirant la première et la dernière ligne. On représente la matrice H_n : hormis sur la première colonne (avec des 1), les termes non nuls sont tous au dessus de la diagonale, avec des 1 sur la diagonale. La matrice B est donc triangulaire supérieure avec des 1 sur la diagonale. On a $\det B = 1$ et $\det C_n = M(n)$. Puisque $\det A_n = 1$, on a obtenu $\det H_n = M(n)$.

Q 37. On note $F_n = B_n(\lambda)H_n$. On effectue les mêmes calculs que dans la question précédente. On commence par remarquer que la définition de $b(j)$ équivaut à $\lambda b(j) = \sum_{d|j} b(d)$.

- $f_{11} = \sum_{k=1}^{n} d(k)$
- si $j \in [\![2;n]\!]$, $f_{1j} = \sum_{k=1}^{n} b_{1k}h_{kj} = \sum_{k=1}^{n} b(k)h_{kj} = \sum_{k|j} b(k) = \lambda b(j)$,
- si $i \geqslant 2$, $c_{ij} = \sum_{k=1}^{n} a_{ik}h_{kj} = h_{ij}$

La matrice $\lambda B_n(\lambda) - B_n(\lambda)H_n$ est donc sous la forme :

$$\begin{pmatrix} \lambda - \sum_{j=1}^{n} b(j) & \lambda b(2) - \lambda b(2) & \dots & \dots & \lambda b(n) - \lambda b(n) \\ -1 & \lambda - 1 & x & x & x \\ \vdots & 0 & \lambda - 1 & x & x \\ \vdots & \vdots & \ddots & \ddots & x \\ -1 & 0 & \cdots & 0 & \lambda - 1 \end{pmatrix} = \begin{pmatrix} \lambda - \sum_{j=1}^{n} b(j) & 0 & \dots & \dots & 0 \\ -1 & \lambda - 1 & (x) & (x) & (x) \\ \vdots & 0 & \lambda - 1 & (x) & (x) \\ \vdots & \vdots & \ddots & \ddots & (x) \\ -1 & 0 & \cdots & 0 & \lambda - 1 \end{pmatrix}$$

On développe par rapport à la première ligne (ou un calcule un déterminant par blocs). On obtient

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

Puisque $\det B_n(\lambda) = 1$, on obtient $\chi_n(\lambda) = (\lambda - 1)^n - (\lambda - 1)^{n-1} \sum_{j=2}^{n} b(j)$.

Q 38. Soit $n \in \mathbb{N}^*$, on calcule $f * b(n) = (1 + w)\delta * b(n) - w\mathbb{1} * d(n) = (1 + w)\delta * b(n) - wd * \mathbb{1}(n)$:

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

ce qui donne $(f * b)(n) = b(n) - w \sum_{d|n, d\neq n} b(d)$. Pour $n \geqslant 2$, on obtient 0 par définition de b. Pour $n = 1$, on obtient $b(1) = 1$. Finalement $f * b = \delta$.

Q 39. Lorsque les séries convergent, on peut écrire $L_f(s) = (1+w)L_\delta(s) - wL_{\mathbb{1}}(s) = (1+w) - wL_{\mathbb{1}}(s)$. Puisque $f(n) = -w$ dès que $n \geqslant 2$, la convergence a lieu si et seulement si $s > 1$.

Q 40. On a, pour tout $s > 1$, $L_f(s) = 1 - w \sum_{k=2}^{+\infty} \frac{1}{k^s}$. La série de fonctions $f_k : s \mapsto \frac{1}{k^s}$ converge normalement sur $[2, +\infty[$ (majorée par $1/k^2$) et chaque fonction tend vers 0 lorsque s tend vers $+\infty$. Il existe donc s_0 tel que pour tout $s > s_0$, $\left| w \sum_{k=2}^{+\infty} \frac{1}{k^s} \right| < 1$ (on peut même mettre $< 1/2$ si on veut se laisser de la marge). On suppose que $s > s_0$ dans la suite. On regarde comment se passent les calculs :

$$\begin{aligned} \frac{1}{L_f(s)} &= \frac{1}{1 - w \sum_{k=2}^{+\infty} \frac{1}{k^s}} = 1 + \sum_{k=1}^{+\infty} \left(w \sum_{n=2}^{+\infty} \frac{1}{k^s} \right)^n \\ &= 1 + \sum_{k=1}^{+\infty} w^n \left(\sum_{k=2}^{+\infty} \frac{1}{k^s} \right)^n = 1 + \sum_{k=1}^{+\infty} w^n \left(\sum_{k_1, k_2, \dots, k_n \geqslant 2} \frac{1}{k_1^s} \frac{1}{k_2^s} \cdots \frac{1}{k_n^s} \right) \end{aligned}$$

Pour l'instant les calculs sont valables : on a utiliser une somme d'une série géométrique de raison entre 0 et 1. Pour la relation : $\left(\sum_{k_1, k_2, \dots, k_n \geqslant 2} \frac{1}{k_1^s} \frac{1}{k_2^s} \cdots \frac{1}{k_n^s} \right) = \left(\sum_{n=2}^{+\infty} \frac{1}{k^s} \right)^n$ cela vient d'une sommation par paquets sur une famille à termes positifs. On s'intéresse à cette quantité : on note $I_n = [\![2, +\infty[\![^n$. On regroupe les n-uplets $(k_1, \dots, k_n)$ en paquet à produit constant - on note $J_m = \{(k_1, k_2, \dots, k_n) \in I_n, k_1 k_2 \dots k_n = m\}$. On a alors $I_n = \biguplus_{m \geqslant 2^n} J_m$. Les termes étant tous positifs, on a donc

$$\sum_{k_1, k_2, \dots, k_n \geqslant 2} \frac{1}{k_1^s} \frac{1}{k_2^s} \cdots \frac{1}{k_n^s} = \sum_{m \geqslant 2^n} \sum_{(k_1, \dots, k_n) \in J_m} \frac{1}{(k_1 \dots k_n)^s} = \sum_{m \geqslant 2^n} \frac{D_n(m)}{m^s}.$$

La convergence de la dernière série étant assurée par la sommabilité. On a donc, pour s assez grand,

$$\frac{1}{L_f(s)} = 1 + \sum_{k=1}^{+\infty} \sum_{m=2^n}^{+\infty} w^n \frac{D_n(m)}{m^s}.$$

Les calculs sont identiques si on remplace w par $|w|$ ce qui garantit que la famille $\left(w^n \frac{D_n(m)}{m^s}\right)_{k\geqslant 1, m\geqslant 2^n}$ est sommable. Cela permet de permuter l'ordre des sommes et obtenir : ($m \geqslant 2^n$ équivaut à $\log_2(m) \geqslant n$, soit $n \leqslant \lfloor \log_2(m) \rfloor$)

$$\frac{1}{L_f(s)} = 1 + \sum_{m=2}^{+\infty} \sum_{n=1}^{\lfloor \log_2 m \rfloor} w^n \frac{D_n(m)}{m^s} = 1 + \sum_{m=2}^{+\infty} m^{-s} \sum_{n=1}^{\lfloor \log_2 m \rfloor} w^n D_n(m).$$

Q 41. On a montré que $f * b = \delta$. On a envie d'écrire $L_{f*b}(s) = L_\delta(s) = 1 = L_f(s)L_b(s)$ et ainsi $L_b(s) = \frac{1}{L_f(s)}$ mais on ne sait pas encore si l'abscisse de convergence de b est finie. On note alors $c_m = \sum_{n=1}^{\lfloor \log_2 m \rfloor} w^n D_n(m)$ de sorte que $\frac{1}{L_f(s)} = L_c(s)$ pour $s > s_0$ (de la partie précédente) et notamment $A_c(c)$ est fini. Pour s assez grand, on a $L_f(s)L_c(s) = 1 = L_\delta(s)$. D'après la question 19, on a pour s assez grand $L_f(s)L_c(s) = L_{f*c}(s)$ et avec la question 19, $f * c = \delta$. Puisque $f * b = \delta$ et par unicité de l'inverse, on a $b = c$ et b est d'abscisse de convergence finie et par unicité, $b_m = \sum_{k=1}^{\lfloor \log_2 m \rfloor} w^k D_k(m)$ si $m \geqslant 2$. On rappelle que $w = \frac{1}{\lambda - 1}$. On a donc

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

Si $k \geqslant \lfloor \log_2 m \rfloor + 1$ donc si $k > \log_2 m$, alors $2^k > m$ et $D_k(m) = 0$ (on ne peut pas décomposer m en produits de k facteurs supérieurs à 2. Cela permet d'écrire que

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

et de permuter les deux sommes pour obtenir :

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

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

Q 42. On peut factoriser χ_n par $(\lambda-1)^{n-1-\lfloor \log_2 n \rfloor}$, ce qui donne

$$\chi_n(\lambda) = (\lambda-1)^{n-1-\lfloor \log_2 n \rfloor} Q(\lambda)$$

où $Q(\lambda) = (\lambda-1)^{\lfloor \log_2 n \rfloor + 1} - \left(\sum_{k=1}^{\lfloor \log_2 n \rfloor - 1} (\lambda-1)^{\lfloor \log_2 n \rfloor - k} S_k(n) \right) - S_{\lfloor \log_2 n \rfloor}(n)$ et notamment $Q(1) = -S_{\lfloor \log_2 n \rfloor}(n)$. Il reste à prouver que cette valeur est non nulle pour obtenir le résultat quant à la multiplicité de la racine. On a

$$S_{\lfloor \log_2 n \rfloor}(n) = \sum_{m=2}^{n} D_{\lfloor \log_2 n \rfloor}(m)$$

Si on note $p = \lfloor \log_2 n \rfloor$ alors $2^p \leqslant n$ et $S_{\lfloor \log_2 n \rfloor}(n) \geqslant D_p(2^p) = 1$: tous les termes sont positifs ou nuls et l'entier 2^p se décompose bien en produit de p facteurs égaux à 2. On a donc un coefficient non nul comme souhaité et la multiplicité de la racine 1 dans χ_n est bien $n - 1 - \lfloor \log_2 n \rfloor$.

Remarque : la matrice de Redheffer a donc un déterminant égal à la fonction de Mertens. Cette matrice a un intérêt concernant la conjecture de Riemann. En effet cette dernière conjecture est équivalent à montrer que $M(x) = \mathrm{O}(x^{1/2+\varepsilon})$ pour tout $\varepsilon > 0$ assez petit. La conjecture de Mertens est que $|M(n)/\sqrt{n}| < 1$ - elle impliquerait donc l'hypothèse de Riemann... sauf qu'en 1985, il a été montré que cette conjecture était fausse.