Convolution arithmétique

On note $\mathcal{F}$ l'ensemble des fonctions de $\mathbb{N}^*$ vers $\mathbb{R}$. On munit $\mathcal{F}$ d'une loi additive définie par :

$$\forall u,v\in\mathcal{F},\forall n\in\mathbb{N}^*,(u+v)(n)=u(n)+v(n)\,.$$

Pour tout $n\in\mathbb{N}^*$, on note :

- D_n l'ensemble des $d\in\mathbb{N}^*$ tels que $d\mid n$.
- C_n l'ensemble des $(d_1,d_2)\in(\mathbb{N}^*)^2$ tels que $d_1d_2=n$.

On définit une seconde loi $\star$ sur $\mathcal{F}$ par :

$$\forall u,v\in\mathcal{F},\forall n\in\mathbb{N}^*,(u\star v)(n)=\sum_{d\in D_n}u(d)v(n/d)\,.$$

Par abus, on pourra aussi noter :

$$(u\star v)(n)=\sum_{d\mid n}u(d)v(n/d)\,.$$

Partie I : Etude de structure

1. Justifier que pour tout $u,v\in\mathcal{F}$ on a :

$$\forall n\in\mathbb{N}^*,(u\star v)(n)=\sum_{(d_1,d_2)\in C_n}u(d_1)v(d_2)\,.$$

   Quelle propriété de la loi $\star$ découle de manière immédiate de cette relation.
2. Montrer que la loi $\star$ est associative.
3. Montrer que la loi $\star$ admet un élément neutre ε que l'on précisera.
4. La structure $(\mathcal{F},+,\star)$ est-elle un anneau ?

Partie II : Fonctions multiplicatives

Une fonction u de $\mathcal{F}$ est dite multiplicative si et seulement si :

$$\forall m,n\in\mathbb{N}^*,m\wedge n=1\Rightarrow u(mn)=u(m)u(n)\,.$$

Par exemple les fonctions θ et ψ de $\mathbb{N}^*$ vers $\mathbb{R}$ définies par : $\theta(n)=1$ et $\psi(n)=n$ sont clairement multiplicatives.

1. Pour tout $n\in\mathbb{N}^*$, on note $\omega(n)$ le nombre de nombres premiers distincts intervenant dans la décomposition primaire de n. Montrer que l'application $n\mapsto(-1)^{\omega(n)}$ est multiplicative.
2. Soit $u\in\mathcal{F}$ une fonction multiplicative et $n\in\mathbb{N}^*$ connu par sa décomposition primaire $n=\prod_{i=1}^{N}p_i^{\alpha_i}$ (avec $p_1,\ldots,p_N$ nombres premiers deux à deux distincts).
   Exprimer $u(n)$ en fonction des $u(p_i^{\alpha_i})$.
3. Soit $m,n\in\mathbb{N}^*$ tels que $m\wedge n=1$ et $\pi:D_m\times D_n\to D_{mn}$ l'application définie par $\pi(d_1,d_2)=d_1d_2$.

3.a Montrer que l'application π est bijective.

3.b En déduire que si $u,v\in\mathcal{F}$ sont multiplicatives alors $u\star v$ l'est aussi.

4. On pose $\delta=\theta\star\theta$ et $\sigma=\psi\star\theta$.

4.a Que représentent les quantités $\delta(n)$ et $\sigma(n)$?

4.b Soit $n\in\mathbb{N}^*$ connu par sa décomposition primaire $n=\prod_{i=1}^{N}p_i^{\alpha_i}$ (avec $p_1,\ldots,p_N$ nombres premiers deux à deux distincts). Exprimer $\delta(n)$ et $\sigma(n)$

Partie III : Formule d'inversion de Möbius

On définit une fonction μ de $\mathcal{F}$ en posant pour tout $n \in \mathbb{N}^*$:

$\mu(n) = 0$ si n est divisible par le carré d'un nombre premier et

$\mu(n) = (-1)^k$ si n s'écrit comme le produit de k nombres premiers deux à deux distincts.

1. Montrer que cette fonction μ est multiplicative.

2. Soit p un nombre premier.
Calculer $(\mu \star \theta)(p)$ et $(\mu \star \theta)(p^\alpha)$ pour $\alpha \in \mathbb{N}^*$.
En déduire que μ est l'inverse de θ pour la loi $\star$.

3. Soit $u, v \in \mathcal{F}$. Etablir l'équivalence :
$$\forall n \in \mathbb{N}^*, v(n) = \sum_{d|n} u(d) \Leftrightarrow \forall n \in \mathbb{N}^*, u(n) = \sum_{d|n} \mu(n/d) v(d).$$

4. En déduire que pour tout $u \in \mathcal{F}$ et tout $n \in \mathbb{N}^*$ la relation :
$$u(n) = \sum_{d|n} \sum_{c|d} \mu(d/c) u(c)$$

Partie IV : Fonction indicatrice d'Euler

Pour tout $x \in \mathbb{Z}$ et $n \in \mathbb{N}^*$, on note $(x)_n$ la classe de x dans $\mathbb{Z}/n\mathbb{Z}$.

1. Dans toute la suite du problème, on pose pour tout $n \in \mathbb{N}^*$,
$$\varphi(n) = \text{Card}\left\{k \in [\![1, n]\!] / k \wedge n = 1\right\}.$$

1.a Rappeler quels sont les éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.
Combien y en a-t-il ?

1.b Soit p un nombre premier. Calculer $\varphi(p)$ et $\varphi(p^\alpha)$ pour $\alpha \in \mathbb{N}^*$.

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

2.a Quels sont les éléments inversibles de l'anneau $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$.
Combien y en a-t-il ?

2.b Etablir que l'application $f : \mathbb{Z}/mn\mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ définie par $f((x)_{mn}) = ((x)_m, (x)_n)$ est un isomorphisme d'anneaux.

2.c En déduire que $\varphi(mn) = \varphi(m)\varphi(n)$.

3. Soit $n \in \mathbb{N}^*$ et d diviseurs positifs de n.

3.a Calculer le cardinal de l'ensemble $\left\{k \in [\![1, n]\!] / \text{pgcd}(k, n) = d\right\}$.

3.b En déduire la relation
$$\sum_{d|n} \varphi(d) = n.$$

Partie V : Calcul de quelques déterminants non triviaux

Soit $n \in \mathbb{N}*$. On souhaite calculer le déterminant de la matrice $A = (a_{i,j}) \in M_n(\mathbb{R})$ définie par $a_{i,j} = \text{pgcd}(i, j)$.

1. On pose $L = (\ell_{i,d}) \in M_n(\mathbb{R})$ la matrice définie par $\ell_{i,d} = \begin{cases} 1 \text{ si } d \mid i \\ 0 \text{ sinon} \end{cases}$

et $U = (u_{d,j}) \in M_n(\mathbb{R})$ celle définie par $u_{d,j} = \begin{cases} \varphi(d) \text{ si } d \mid j \\ 0 \quad \text{sinon} \end{cases}$

1.a Calculer $\det L$ et $\det U$.

1.b Etablir que $A = LU$ et donner une expression de $\det A$.

On souhaite maintenant calculer le déterminant de la matrice $B=(u(a_{i,j}))\in M_n(\mathbb{R})$ où u désigne un élément de $\mathcal{F}$ et $a_{i,j}$ le pgcd de i et j comme ci-dessus.

2. On pose $V=(v_{d,j})\in M_n(\mathbb{R})$ la matrice définie par $v_{d,j}=\begin{cases}\sum_{c|d}\mu(d/c)u(c) & \text{si } d\mid j\\ 0 & \text{sinon}\end{cases}$

2.a Calculer LV.

2.b En déduire une expression de $\det B$.

3. On note $C=(c_{i,j})\in M_n(\mathbb{R})$ la matrice définie par $c_{i,j}=\text{ppcm}(i,j)$
Donner une expression de $\det C$.

Correction

Partie I

1. L'application de D_n vers C_n qui envoie d sur le coupe $(d,n/d)$ est bijective donc
$\sum_{d\in D_n}u(d)v(n/d)=\sum_{(d_1,d_2)\in C_n}u(d_1)v(d_2)$.
On en déduit que la loi $\star$ est commutative car la dernière expression est visiblement symétrique en u et v.

2. Soit $u,v,w\in\mathcal{F}$.
$\big((u\star v)\star w\big)(n)=\sum_{d|n}(u\star v)(d)w(n/d)=\sum_{d|n}\sum_{c|d}u(c)v(d/c)w(n/d)$
Dans la sommation, l'entier d peut se percevoir sous la forme bc avec b divisant n/c
donc $\big((u\star v)\star w\big)(n)=\sum_{c|n}\sum_{b|(n/c)}u(c)v(b)w((n/c)/b)$ soit
$\big((u\star v)\star w\big)(n)=\sum_{c|n}u(c)(v\star w)(n/c)=\big(u\star(v\star w)\big)(n)$.
Ainsi la loi $\star$ est associative.

3. Posons $\varepsilon(n)=1$ si $n=1$ et 0 sinon.
$(u\star\varepsilon)(n)=\sum_{d|n}u(d)\varepsilon(n/d)=u(n)\varepsilon(1)+0=u(n)$.
Ainsi $u\star\varepsilon=u=\varepsilon\star u$ et ε est élément neutre.

4. $(\mathcal{F},+)$ est un groupe abélien (structure connue).
$(\mathcal{F},\star)$ est un magma associatif possédant un neutre.
La distributivité de $\star$ sur $+$ est immédiate.
Oui, $(\mathcal{F},+,\star)$ est un anneau.

Partie II

1. Si n et m sont premiers entre eux alors ils n'ont pas de facteurs premiers en commun. Par suite l'ensemble des facteurs premiers intervenant dans le produit mn est la réunion disjointes des ensembles des facteurs premiers intervenant dans m et n. Par suite $\omega(mn)=\omega(m)+\omega(n)$ puis
$(-1)^{\omega(mn)}=(-1)^{\omega(m)}\times(-1)^{\omega(n)}$.

2. Les nombres $p_i^{\alpha_i}$ étant deux à deux premiers entre eux, la multiplicativité de u entraîne
$u(n)=\prod_{i=1}^{n}u(p_i^{\alpha_i})$.

3.a L'application π est bien définie car $d_1\mid m$ et $d_2\mid n$ entraîne $d_1d_2\mid mn$.
Soit $d\in D_{mn}$.
Analyse : Si $d=d_1d_2$ avec $d_1\mid m$ et $d_2\mid n$ alors $\text{pgcd}(m,d)=\text{pgcd}(m,d_1d_2)=d_1\,\text{pgcd}(m/d_1,d_2)$ avec m/d_1 et d_2 premiers entre eux cas diviseurs respectifs de m et n nombres premiers entre eux. Ainsi

$d_1 = \text{pgcd}(m,d)$ et de même $d_2 = \text{pgcd}(n,d)$.

Synthèse : Posons $d_1 = \text{pgcd}(m,d)$ et $d_2 = \text{pgcd}(n,d)$. On a clairement $d_1 \mid m$ et $d_2 \mid n$. Or m et n sont premiers entre eux donc d_1 et d_2 le sont aussi. Puisque $d_1 \mid d$, $d_2 \mid d$ et $d_1 \wedge d_2 = 1$, on a $d_1 d_2 \mid d$. Par égalité de Bézout, on peut écrire $d_1 = u_1 m + v_1 d$ et $d_2 = u_2 n + v_2 d$ (avec $u_i, v_i \in \mathbb{Z}$) donc $d_1 d_2 = umn + vd$ (avec $u, v \in \mathbb{Z}$). Or $d \mid mn$ donc $d \mid d_1 d_2$. Enfin par double divisibilité $d = d_1 d_2$.

Au terme de cette étude, on peut affirmer :

$\forall d \in D_{mn}, \exists !(d_1,d_2) \in D_m \times D_n, d = d_1 d_2$

ce qui se comprend comme étant la bijectivité de π.

3.b Supposons m et n sont premiers entre eux.

$(u \star v)(mn) = \sum_{d \mid mn} u(d) v(mn/d) = \sum_{d_1 \mid m} \sum_{d_2 \mid n} u(d_1 d_2) v(mn/(d_1 d_2))$.

Par multiplicativité de u et v :

$(u \star v)(mn) = \sum_{d_1 \mid m} \sum_{d_2 \mid n} u(d_1) v(m/d_1) u(d_2) v(n/d_2)$

puis

$(u \star v)(mn) = \sum_{d_1 \mid m} u(d_1) v(m/d_1) \sum_{d_2 \mid n} u(d_2) v(n/d_2) = (u \star v)(m)(u \star v)(n)$.

4.a $\delta(n) = \sum_{d \mid n} 1$ est le nombre de diviseurs positifs de n.

$\sigma(n) = \sum_{d \mid n} d$ est la somme des diviseurs positifs de n.

4.b Pour p nombre premier et $\alpha \in \mathbb{N}^*$

$D_{p^\alpha} = \{1, p, \ldots, p^\alpha\}$ donc $\delta(p^\alpha) = \alpha + 1$ et $\sigma(p^\alpha) = \dfrac{p^{\alpha+1} - 1}{p - 1}$.

Par suite $\delta(n) = \prod_{i=1}^{N} (\alpha_i + 1)$ et $\sigma(n) = \prod_{i=1}^{N} \dfrac{p_i^{\alpha_i + 1} - 1}{p_i - 1}$.

Partie III

1. Supposons m et n premiers entre eux.

Si l'un des deux est divisible par le carré d'un nombre premier, le produit mn l'est encore donc $\mu(mn) = 0 = \mu(m)\mu(n)$.

Sinon mn n'est pas divisible par le carré d'un nombre premier car m et n n'ont pas de facteurs premiers en commun. Par suite $\mu(mn) = (-1)^{\omega(m)\omega(n)} = (-1)^{\omega(m)}(-1)^{\omega(n)} = \mu(m)\mu(n)$.

2. $(\mu \star \theta)(p) = \sum_{d \mid p} \mu(d) = \mu(1) + \mu(p) = 1 - 1 = 0$.

$(\mu \star \theta)(p^\alpha) = \sum_{d \mid p^\alpha} \mu(d) = \mu(1) + \mu(p) + \cdots + \mu(p^\alpha) = 1 - 1 + 0 + \cdots + 0 = 0$.

Si $n = \prod_{i=1}^{N} p_i^{\alpha_i}$ alors $(\mu \star \theta)(n) = \prod_{i=1}^{N} 0 = \begin{cases} 1 \text{ si } N = 0 \\ 0 \text{ sinon} \end{cases}$.

Ainsi $\mu \star \theta = \varepsilon = \theta \star \mu$.

3. Remarquons $\forall n \in \mathbb{N}^*, v(n) = \sum_{d \mid n} u(d) \Leftrightarrow v = u \star \theta$ et

$\forall n \in \mathbb{N}^*, u(n) = \sum_{d \mid n} \mu(n/d) v(d) \Leftrightarrow u = v \star \mu$.

L'équivalence proposée correspond donc $v = u \star \theta \Leftrightarrow u = v \star \mu$.

Cette dernière est vraie puisque θ et μ sont inverses l'une de l'autre pour la loi $\star$.

4. Pour $u = \theta \star (\mu \star u)$ donne $u(n) = \sum_{d \mid n} \sum_{c \mid d} \mu(d/c) u(c)$.

Partie IV

1.a Les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les $(k)_n$ avec $k \wedge n = 1$. Il y en a exactement $\varphi(n)$.

1.b $\varphi(p) = p-1$ car $1, 2, \ldots, p-1$ sont premier avec le nombre premier p.
Dans $[\![1, p^\alpha]\!]$ les nombres qui ne sont pas premier avec p^α sont ceux qui sont divisibles par p, il y en a exactement $p^{\alpha-1}$. Par suite $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

2.a Les inversibles de $(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})$ sont les couples formé d'un inversible de $\mathbb{Z}/m\mathbb{Z}$ et d'un inversible de $\mathbb{Z}/n\mathbb{Z}$. Il y en a $\varphi(m)\varphi(n)$.

2.b L'application considérée est bien définie car $\forall x, y \in \mathbb{Z}$, $x = y \quad [mn] \Rightarrow (x)_m = (y)_m$ et $(x)_n = (y)_n$.
Aisément on vérifie $f(1_{\mathbb{Z}/mn\mathbb{Z}}) = 1_{\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}}$, $f((x)_{mn} + (y)_{mn}) = f((x)_{mn}) + f((y)_{mn})$ et $f((x)_{mn}(y)_{mn}) = f((x)_{mn})f((y)_{mn})$.
De plus $f((x)_{mn}) = ((0)_m, (0)_n) \Rightarrow m \mid x$ et $n \mid x$ donc $mn \mid x$ car $m \wedge n = 1$. Ainsi $\ker f = \{(0)_{mn}\}$ et donc f est injective.
De plus $\text{Card}(\mathbb{Z}/mn\mathbb{Z}) = mn = \text{Card}(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})$ donc f est bijective et c'est donc un isomorphisme.

2.c L'isomorphisme d'anneaux f fait correspondre les inversibles de $\mathbb{Z}/mn\mathbb{Z}$ et ceux de $(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})$.
On en déduit $\varphi(mn) = \varphi(m)\varphi(n)$. La fonction φ est donc multiplicative.

3.a Pour $k \in [\![1, n]\!]$, $\text{pgcd}(k, n) = d \Leftrightarrow k = d\ell$ avec $\ell \in [\![1, n/d]\!]$ et $\text{pgcd}(\ell, n/d) = 1$. Par suite $\text{Card}\{k \in [\![1, n]\!] / \text{pgcd}(k, n) = d\} = \varphi(n/d)$.

3.b $[\![1, n]\!]$ est la réunion disjointe des ensembles $\{k \in [\![1, n]\!] / \text{pgcd}(k, n) = d\}$ pour d divisant n. Par cardinalité : $n = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d)$.
Cette relation peut aussi se percevoir : $\varphi \star \theta = \psi$ mais cela est sans importance pour la suite.

Partie V

1.a Si $d > i$ alors $d \nmid i$ donc $\ell_{i,d} = 0$. Ainsi la matrice L est triangulaire inférieure et son déterminant est le produit des coefficients diagonaux, tous égaux à 1. Ainsi $\det L = 1$.
De même, la matrice U est triangulaire supérieure et $\det U = \prod_{d=1}^{n} \varphi(d)$.

1.b Le coefficient d'indice (i, j) de la matrice LU est :
$(LU)_{i,j} = \sum_{d=1}^{n} \ell_{i,d} u_{d,j} = \sum_{d|i, d|j} \varphi(d)$.
Or les diviseurs communs à i et j sont les diviseurs de $\text{pgcd}(i, j)$ donc
$(LU)_{i,j} = \sum_{d|\text{pgcd}(i,j)} \varphi(d) = \text{pgcd}(i, j)$ en vertu de la relation du IV.4.b
Ainsi $A = LU$ puis $\det A = \det L \det U = \prod_{d=1}^{n} \varphi(d)$.

2.a $(LV)_{i,j} = \sum_{d=1}^{n} \ell_{i,d} v_{d,j} = \sum_{d|i, d|j} \sum_{c|d} \mu(d/c) u(c)$ puis $(LV)_{i,j} = \sum_{d|\text{pgcd}(i,j)} \sum_{c|d} \mu(d/c) u(c) = u(\text{pgcd}(i, j))$ en vertu de la relation du III.4.
Ainsi $LV = B$.

2.b $\det B = \det L \det V = \prod_{d=1}^{n} \sum_{c|d} \mu(d/c) u(c)$

3. $c_{i,j} = \dfrac{ij}{\text{pgcd}(i,j)}$. En factorisant chaque ligne par i et chaque colonne par j :

$\det C = (n!)^2 \det B$ avec $B = \left(\dfrac{1}{\text{pgcd}(i,j)}\right) \in M_n(\mathbb{R})$ où $u : k \mapsto 1/k$.

Par suite $\det C = (n!)^2 \prod_{d=1}^{n} \sum_{c|d} \dfrac{\mu(d/c)}{c} = \prod_{d=1}^{n} \sum_{c|d} \dfrac{d^2 \mu(d/c)}{c} = \prod_{d=1}^{n} \sum_{c|d} dc\mu(c)$.