Énoncé

Pour tout naturel non nul n, on désigne par $D(n)$ l'ensemble des diviseurs de n dans $\mathbb{N}$ et par $C(n)$ l'ensemble des couples de diviseurs :

$$C(n) = \left\{(d_1, d_2) \in \mathbb{N}^2 \text{ tq } d_1 d_2 = n\right\}$$

Une *fonction arithmétique* est une fonction définie dans $\mathbb{N}^*$ et à valeurs complexes. On note $\mathcal{F}$ l'ensemble des fonctions arithmétiques et on définit deux opérations notées $+$ et $*$ ($*$ est appelée la *convolution de Dirichlet*) sur $\mathcal{F}$.

$$\forall (f,g) \in \mathcal{F}^2, \forall n \in \mathbb{N}^* : \begin{cases} (f+g)(n) = f(n) + g(n) \\ (f*g)(n) = \displaystyle\sum_{(d_1,d_2)\in C(n)} f(d_1)g(d_2) = \sum_{d \in D(n)} f(d) g(\frac{n}{d}) \end{cases}$$

Une fonction arithmétique f est dite *multiplicative* lorsque :

$$\forall (p,q) \in \mathbb{N}^{*2},\ p \wedge q = 1 \Rightarrow f(pq) = f(p)f(q)$$

On définit des fonctions arithmétiques particulières par l'image d'un naturel non nul n quelconque.

- $I(n) = n$
- $e_0(n) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ si } n > 1 \end{cases}$
- $e(n) = 1$.
- $d(n)$ est le nombre de diviseurs de n dans $\mathbb{N}$.
- $\sigma(n)$ est la somme des diviseurs de n dans $\mathbb{N}$.
- fonction indicatrice d'Euler : $\phi(n)$ est le nombre de $k \in [\![1, n]\!]$ premiers avec n. On pose aussi $\phi(1) = 1$.
- fonction de Pillai (somme de pgcd)

$$\beta(n) = \sum_{k=1}^{n} k \wedge n$$

- fonction de Möbius

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \text{ est divisible par un carré d'entier autre que 1} \\ (-1)^s & \text{si } n \text{ est le produit de } s \text{ nombres premiers distincts} \end{cases}$$

On rappelle que 1 n'est pas un nombre premier. Ces notations sont valables dans tout le problème.

Partie I. Structure d'anneau

1. Exemples
   a. Calculer $\beta(6)$. Calculer $(\sigma * \mu)(12)$.
   b. Montrer que $e*e$ et $I*e$ sont des fonctions définies dans l'introduction (à préciser).
   c. Soit p un nombre premier. Former une relation entre $\phi(p)$, $\sigma(p)$, p et $d(p)$. Que vaut $(\mu * e)(p^m)$ pour m naturel non nul ?
2. a. Montrer que l'opération $*$ est commutative.
   b. Montrer que e_0 est l'élément neutre de l'opération $*$.
   c. Pour tout $n \in \mathbb{N}^*$, on note

$$T(n) = \left\{(d_1, d_2, d_3) \in \mathbb{N}^3 \text{ tq } n = d_1 d_2 d_3\right\}$$

   Démontrer, en utilisant $T(n)$ que l'opération $*$ est associative.

   Les autres propriétés se vérifiant facilement, on pourra utiliser dans la suite du problème que $(\mathcal{F}, +, *)$ est un anneau commutatif d'élément unité e_0.
3. Fonctions multiplicatives
   a. Soit m et n deux nombres naturels non nuls et premiers entre eux. Montrer que l'application

$$P : \begin{cases} D(m) \times D(n) \to D(mn) \\ (a,b) \mapsto ab \end{cases}$$

   est bijective.
   b. Soit f et g deux fonctions multiplicatives, montrer que $f * g$ est multiplicative.
   c. Montrer que les fonctions I, e_0, e, d, σ, μ sont multiplicatives.
4. Norme d'une fonction. Pour toute fonction arithmétique f non nulle, on définit sa *norme* $N(f)$ par

$$N(f) = \min\left\{k \in \mathbb{N}^* \text{ tq } f(k) \neq 0\right\}$$

   Soit f et g des fonctions arithmétiques non nulles, montrer que $f * g$ est non nulle et que $N(f*g) = N(f)N(g)$.

Partie II. Inversion de Möbius et applications.

1. a. Montrer que $\mu * e = e_0$.
   b. Soit f et g deux fonctions arithmétiques, montrer que

$$f = g * e \Leftrightarrow g = f * \mu$$

2. a. Soit n un naturel non nul, d et δ des diviseurs de n tels que $n = d\delta$. On introduit deux ensembles

$$F = \{k \in [\![1, d]\!] \text{ tq } k \wedge d = 1\} \qquad \Delta = \{s \in [\![1, n]\!] \text{ tq } s \wedge n = \delta\}$$

Montrer que $k \mapsto \delta k$ définit une bijection de F vers Δ. Comment s'exprime le nombre d'éléments de F ?

b. Discuter, suivant le paramètre $a \in [\![1, n]\!]$ du nombre de solutions de l'équation $n \wedge x = a$ d'inconnue $x \in [\![1, n]\!]$.

c. Montrer que $I = e * \phi$ puis que $\phi = I * \mu$.

d. Montrer que $\beta * e = I * I$.

3. Théorème de Makowski

a. Montrer que $\sigma * \phi = I * I$

b. Montrer que, si n est un naturel non nul vérifiant $\phi(n) + \sigma(n) = nd(n)$, alors n est un nombre premier.

Corrigé

Partie I. Structure d'anneau

1. Exemples

a. On trouve $\beta(6) = 15$ car

$$\beta(6) = 1 \wedge 6 + 2 \wedge 6 + 3 \wedge 6 + 4 \wedge 6 + 5 \wedge 6 + 6 \wedge 6 = 1 + 2 + 3 + 2 + 1 + 6 = 15.$$

On trouve $(\sigma * \mu)(12) = 12$ en utilisant $\mu(4 \times 2) = 0$, $\mu(2 \times 3) = (-1)^2 = 1, \cdots$ et

$$\begin{aligned}(\sigma*\mu)(12) &= \sigma(1)\mu(12)+\sigma(2)\mu(6)+\sigma(3)\mu(4)+\sigma(4)\mu(3)+\sigma(6)\mu(2)+\sigma(12)\mu(1)\\ &= 1\times 0+(1+2)\times 1+(1+3)\times 0+(1+2+4)\times(-1)+(1+2+3+6)\times(-1)\\ &\quad +(1+2+3+4+6+12)\times 1 = 3-7-12+28 = 12.\end{aligned}$$

b. On trouve $e * e = d$ car, pour tout naturel non nul n,

$$(e * e)(n) = \sum_{d \in D(n)} \underbrace{e(d)}_{=1} \underbrace{e(\frac{n}{d})}_{=1} = \sharp D(n) = d(n).$$

On trouve $I * e = \sigma$ car

$$(I * e)(n) = \sum_{d \in D(n)} \underbrace{I(d)}_{=d} \underbrace{e(\frac{n}{d})}_{=1} = \sigma(n).$$

c. Soit p un nombre premier. Alors $\phi(p) = p - 1$, $\sigma(p) = 1 + p$, $d(p) = 2$. On en déduit

$$\phi(p) + \sigma(p) = pd(p).$$

Les diviseurs de p^m sont les p^k avec k entre 0 et n. Ils sont divisibles par un carré sauf les deux premiers, on en tire

$$(\mu * e)(p^m) = \mu(1) + \mu(p) + \underbrace{\mu(p^2) + \cdots}_{=0} = 1 - 1 = 0.$$

2. a. Pour montrer la commutativité, on change la variable locale de sommation en posant $\delta = \frac{n}{d}$ puis on permute les fonctions (multiplication dans $\mathbb{C}$) en revenant au nom initial

$$(f * g)(n) = \sum_{\delta \in D(n)} f(\frac{n}{\delta}) g(\delta) = \sum_{\delta \in D(n)} g(\delta) f(\frac{n}{\delta}) = \sum_{d \in D(n)} g(d) f(\frac{n}{d}) = (g * f)(n).$$

b. Soit f une fonction arithmétique quelconque. Comme $e_0(n)$ est nul sauf si $n = 1$, le seul diviseur qui contribue vraiment à $e_0 * f = f * e_0$ est 1. On en tire

$$\forall n \in \mathbb{N}^*,\ (e_0 * f)(n) = (f * e_0)(n) = e_0(1)f(n) \Rightarrow e_0 * f = f * e_0 = f.$$

c. Soient f, g, h trois fonctions arithmétiques et n quelconque dans $\mathbb{N}^*$. Remarquons que

$$(d_1, d_2, d_3) \in T(n) \Leftrightarrow (d_1, d_2d_3) \in C(n) \Leftrightarrow d_1 \in D(n) \text{ et } (d_2, d_3) \in C(\frac{n}{d_1})$$
$$\Leftrightarrow d_1d_2 \in D(\frac{n}{d_3}) \text{ et } d_3 \in C(n).$$

Cela se traduit au niveau des sommes par :

$$(f * (g * h))(n) = \sum_{d_1 \in D(n)} f(d_1)(g * h)(\frac{n}{d_1})$$
$$= \sum_{d_1 \in D(n)} f(d_1) \left(\sum_{(d_2,d_3) \in C(\frac{n}{d_1})} g(d_2)h(d_3) \right)$$
$$= \sum_{(d_1,d_2,d_3) \in T(n)} f(d_1)g(d_2)h(d_3) = \sum_{d_3 \in D(n)} \left(\sum_{(d_1,d_2) \in C(\frac{n}{d_3})} f(d_1)g(d_2) \right) h(d_3)$$
$$= \sum_{d_3 \in D(n)} (f * g)(\frac{n}{d_3})h(d_3) = ((f * g) * h)(n).$$

Ceci prouve l'associativité de $*$. On ne vérifie pas en détail les autres propriétés. Les opérations définissent une structure d'anneau sur l'ensemble des fonctions multiplicatives.

3. Fonctions multiplicatives.

a. Rien dans le cours ne permet d'affirmer que $D(m) \times D(n)$ et $D(mn)$ ont le même nombre d'éléments. Le démontrer est même une des justifications de la question. On doit donc prouver l'injectivité et la surjectivité de la fonction P. Cela revient à un raisonnement par analyse-synthèse.
Considérons un diviseur d quelconque de mn.
Analyse.
Si $P((a, b)) = d$ alors $ab = d$ avec $a \in D(m)$ et $b \in D(n)$ donc a est un diviseur commun à d et m donc a divise le pgcd $m \wedge d$. De même, b divise $n \wedge d$.

D'autre part, $m \wedge d$ divise d donc divise mn. Comme $m \wedge d$ divise m qui est premier avec n, on tire que $m \wedge d$ est premier avec n. Il est donc aussi premier avec b qui divise n. On peut alors utiliser le théorème de Gauss :

$$\left.\begin{array}{l} m \wedge d \text{ divise } d = ab \\ m \wedge d \text{ premier avec } b \end{array}\right\} \Rightarrow m \wedge d \text{ divise } a \Rightarrow m \wedge d = a.$$

On démontre de même que $n \wedge d = b$. Ceci achève l'analyse qui prouve l'injectivité : le seul couple éventuellement antécédent de d par P est $(m \wedge d, n \wedge d)$.
Synthèse.
Utilisons la décomposition en facteurs premiers : $m \wedge d$ est le produit de tous les diviseurs premiers de d qui divisent m alors que $n \wedge d$ est formé par ceux qui divisent n. Ces deux ensembles de diviseurs premiers sont disjoints donc

$$(m \wedge d)(n \wedge d) = d \Rightarrow P((m \wedge d, n \wedge d)) = d.$$

Ceci prouve la surjectivité.

b. Soient f et g deux fonctions multiplicatives et m, n des entiers premiers entre eux. D'après la question précédente :

$$(f * g)(mn) = \sum_{d \in D(mn)} f(d)g(\frac{mn}{d}) = \sum_{(d_m,d_n) \in D(m) \times D(n)} f(d_m d_n)g(\frac{m}{d_m}\frac{n}{d_n})$$
$$= \sum_{(d_m,d_n) \in D(m) \times D(n)} f(d_m)f(d_n)g(\frac{m}{d_m})g(\frac{n}{d_n}) \text{ car } d_m \wedge d_n = 1,\ \frac{m}{d_m} \wedge \frac{n}{d_n} = 1$$
$$= \left(\sum_{d_m \in D(m)} f(d_m)g(\frac{m}{d_m}) \right) \left(\sum_{d_n \in D(n)} f(d_n)g(\frac{n}{d_n}) \right) = (f * g)(m)(f * g)(n).$$

c. – La fonction I est multiplicative car $I(mn) = mn = I(m)I(n)$ même si m et n ne sont pas premiers entre eux.
– La fonction e_0 est multiplicative car $e_0(mn) = 0 = I(m)I(n)$ si m ou n est différent de 1.
– La fonction e est multiplicative car $e(mn) = 1 = e(m)e(n)$ même si m et n ne sont pas premiers entre eux.
– La fonction d (nombre de diviseurs) est multiplicative car la fonction P est bijective. (montré en a.)
– On a vu en I.1.b que $\sigma = I * e$. La fonction est multiplicative d'après la question b car I et e le sont.

– La fonction de Möbius est multiplicative car si m ou n est divisible par un carré, le produit l'est aussi. Si aucun n'est divisible par un carré et qu'ils sont premiers entre eux les nombres de diviseurs premiers distincts s'ajoutent.

4. Norme d'une fonction arithmétique. On se donne deux fonctions multiplicatives non nulles f et g. On note n_f et n_g leurs normes. On a donc :

$$f(n_f) \neq 0,\ g(n_g) \neq 0,\ \forall k < n_f : f(k) = 0,\ \forall k < n_g : (k) = 0.$$

Soit k un diviseur de $n_f n_g$. Si $k > n_f$ alors $\frac{n_f n_g}{k} < n_g$ donc $g(\frac{n_f n_g}{k}) = 0$. On raisonne symétriquement si $k > n_g$. Le seul couple de diviseurs qui contribue réellement à la somme dans $(f * g)(n_f n_g)$ est (n_f, n_g) donc

$$(f * g)(n_f n_g) = f(n_f) g(n_g) \neq 0.$$

La fonction $f * g$ est donc non nulle et sa norme est inférieure ou égale à $n_f n_g$.
Considérons un $m < n_f n_g$ et k un diviseur de m.
Si $k \geq n_f$ alors $\frac{m}{k} < n_g$ donc $g(\frac{m}{k}) = 0$. Si $k < n_f$ alors $f(k) = 0$. Cette fois personne ne contribue à la somme : $(f * g)(k) = 0$. On a donc bien prouvé

$$N(f * g) = N(f) N(g).$$

Partie II. Inversion de Möbius

1. a. Comme toutes les fonctions en jeu sont multiplicatives (questions II.3. b. et c.), on va seulement vérifier la relation pour des entiers n de la forme p^m où p est premier et m naturel non nul.
Les diviseurs de n sont les p^k avec $k \leq m$. On en tire

$$(\mu * e)(n) = \sum_{k=0}^{m} \mu(p^k) e(p^{m-k}) \qquad \text{(seuls 0 et 1 contribuent)} = 1 + (-1) = 0.$$

Comme par définition $(\mu * e)(1) = \mu(1) e(1) = 1$, on a bien démontré par multiplicativité la relation fondamentale

$$\mu * e = e_0.$$

b. Il s'agit s'implement de multiplier (étoiler) d'un côté ou de l'autre en exploitant commutativité et associativité.

$$f = g * e \Rightarrow f * \mu = (g * e) * \mu = g * (e * \mu) = g * (\mu * e) = g * e_0 = g$$
$$g = f * \mu \Rightarrow g * e = (f * \mu) * e = f * (\mu * e) = f * e_0 = f$$

2. a. Vérifions d'abord que la fonction est bien définie c'est à dire que $k \in F$ entraîne $\delta k \in \Delta$. Cela résulte de la linéarité du pgcd :

$$(k\delta) \wedge n = (k\delta) \wedge (d\delta) = \delta(k \wedge d) = \delta.$$

L'injectivité de $k \to \delta k$ est évidente par simplification.
Considérons un élément s quelconque dans Δ. Par définition $\delta = s \wedge n$ donc δ divise s, il existe k tel que $s = \delta k$. De plus,

$$\left.\begin{array}{l} n = \delta d \\ s = \delta k \\ \delta = s \wedge n \end{array}\right\} \Rightarrow d \wedge k = 1 \Rightarrow k \in F.$$

Ceci prouve la surjectivité.
On en déduit que le F et Δ ont le même nombre d'éléments. Ce nombre est aussi $\phi(d)$ où ϕ est la fonction *indicatrice d'Euler* introduite au début de l'énoncé.

b. On considère ici l'équation $n \wedge x = a$ d'inconnue x entier entre 1 et n.
– Si a n'est pas un diviseur de n, cette équation est évidemment sans solution.
– Si a est un diviseur de n. L'ensemble des solutions est alors le Δ de la question précédente (avec $\delta = a$ et $d = \frac{n}{a}$). Le nombre de solutions est donc $\phi(d) = \phi(\frac{n}{a})$.

c. Classons les entiers x entre 1 et n selon la valeur de $n \wedge x$. On obtient autant de classes que de diviseurs d. Pour chaque d, il existe $\phi(\frac{n}{d})$ éléments tels que $n \wedge x = d$. On en déduit

$$\text{(nb entiers entre 1 et } n) = n = \sum_{d \in D(n)} \phi(\frac{n}{d}) = (e * \phi)(n) = (\phi * e)(n).$$

Cela s'écrit $I = \phi * e$. On peut ensuite étoiler

$$I = \phi * e \Rightarrow I * \mu = (\phi * e) * \mu = \phi * (e * \mu) = \phi * e_0 = \phi$$

d. On reprend l'idée du classement des entiers entre 1 et n selon la valeur du pgcd $n \wedge x$ (attaché à la discussion de l'équation de la question b.) On l'applique à la somme des pgcd. Quand on regroupe les pgcd égaux (à un diviseur arbitraire d), l'indicatrice d'Euler apparait d'après la question 2.b..

$$\beta(n) = \sum_{k=1}^{n} k \wedge n = \sum_{d \in D(n)} \underbrace{\phi(\frac{n}{d})}_{\text{nb de } k \text{ tq } k \wedge n = d} \qquad d. = (I * \phi)(n)$$

Ensuite on étoile

$$\beta = I * \phi \Rightarrow \beta * e = I * (\phi * e) = I * I.$$

3. Théorème de Makowski.

   a. On a vu en I.1.b. que $\sigma = I * e$. Or $I = e * \phi$ d'après 2.c. donc

$$\sigma * \phi = (I * e) * \phi) = I * (e * \phi) = I * I.$$

   b. Précisons ce $I * I$ qui est mis en avant dans cette fin de problème :

$$(I * I)(n) = \sum_{d \in D(n)} I(d) I(\frac{n}{d}) = \sum_{d \in D(n)} d\,\frac{n}{d} = \sum_{d \in D(n)} n = d(n)n.$$

   car $d(n)$ est le nombre de diviseurs. D'après a., la condition de l'énoncé s'écrit

$$\phi + \sigma = \phi * \sigma.$$

   Or

$$(\phi * \sigma)(n) = \underbrace{\phi(1)}_{=1}\sigma(n) + \cdots + \phi(n)\underbrace{\sigma(1)}_{=1}$$

   où $\cdots$ désigne la somme étendue aux autres diviseurs de n. La condition de l'énoncé impose que cette somme soit nulle ce qui ne peut se produire que s'il n'existe aucun diviseur de n autres que 1 et n car les fonctions ϕ et σ sont à valeurs strictement positives.
   On avait trouvé en I.1.c que, si p est premier,

$$\phi(p) + \sigma(p) = 2p = pd(p).$$

   La condition $\phi(p) + \sigma(p) = 2p = pd(p)$ caractérise donc les nombres premiers.