# DS 3 de mathématiques – Corrigé

## 1 Structure des groupes abéliens finis

### 1.1 Ordres et exposant

1. On note de même $\tau_{a^{-1}} : G \to G, x \mapsto a^{-1}x$. Si $x \in G$, on a $\tau_{a^{-1}} \circ \tau_a(x) = a^{-1}ax = x$, donc $\tau_{a^{-1}} \circ \tau_a = \mathrm{id}_G$ et de même $\tau_a \circ \tau_{a^{-1}} = \mathrm{id}_G$.
   On en déduit que $\tau_a$ est une bijection (de bijection réciproque $\tau_{a^{-1}}$).

2. Comme $\tau_a$ est une bijection, $P$ s'écrit aussi $\prod_{y\in G}(ay)$ (*on fait le changement de variable* $x = ay$). Ainsi,
   $$P = a^n \prod_{y\in G} y = a^n P.$$
   Comme dans un groupe, tout élément est simplifiable, on en déduit que $a^n = 1$. Et donc que $\omega(a) \mid n$.

3. (a) Pour simplifier les notations, on note $k = \omega(a)$ et $\ell = \omega(b)$. Soit $r \in \mathbb{Z}$ tel que $(ab)^r = 1$. Comme les éléments commutent, on en déduit $a^r = b^{-r}$. En élevant à la puissance $\ell$ :
   $$a^{r\ell} = (a^r)^\ell = (b^{-r})^\ell = (b^\ell)^{-r} = 1.$$
   Par caractérisation de l'ordre de $a$, $\omega(a) = k \mid r\ell$. Comme $k \wedge \ell = 1$, $\omega(a) \mid r$, par le lemme de Gauss.
   De même, $\omega(b) \mid r$. Comme $\omega(a) \wedge \omega(b) = 1$, on en déduit que $\omega(a)\omega(b)$ divise $r$.
   De plus, on a $(ab)^{k\ell} = (a^k)^\ell (b^\ell)^k = 1 \times 1 = 1$. Ceci montre que $\omega(ab) = k\ell$.

   (b) Soit $n \in \mathbb{Z}$. On a les équivalences :
   $$(x^r)^n = 1 \iff x^{nr} = 1 \iff p^\alpha r \mid nr \iff np^\alpha \mid n.$$
   Ainsi, $\omega(x^r) = p^\alpha$.
   Le même argument montre que $\omega(y^{p^\beta}) = s$. Comme $p^\alpha$ et $s$ sont premiers entre eux, on peut appliquer la question précédente aux éléments $x^r$ et $y^{p^\beta}$ et on obtient que $\omega(x^r y^{p^\beta}) = p^\alpha s$.

   (c) Comme on a choisi $y$ d'ordre maximal, l'ordre de $x^r p^{y^\beta}$ doit être inférieur à $e$. On a donc $p^\alpha s \leq p^\beta s$ et donc $\alpha \leq \beta$.
   Ainsi, pour tout premier $p$, $\nu_p(\omega(x)) \leq \nu_p(e)$. On en déduit que $\omega(x) \mid e$.

4. **Un exemple.** D'après la question 2, l'exposant de $G$ qui est l'ordre d'un certain élément doit être un diviseur de $p^3$. De plus, 1 est exclu car un tel exposant signifierait que tout élément est d'ordre 1 ; mais seul l'élément neutre est d'ordre 1.
Les possibilités restantes sont $p$, $p^2$ et $p^3$.

   - Pour $p^3$, le groupe cyclique $\mathbb{Z}/p^3\mathbb{Z}$ convient. Un générateur (par exemple la classe de 1) est d'ordre $p^3$ et l'exposant ne peut pas être plus grand.
   - Pour $p^2$, on considère $Z/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. L'élément $(\mathrm{cl}_{p^2}(1), \mathrm{cl}_p(0))$ est d'ordre $p^2$ et, si $a, b \in \mathbb{Z}$, $p^2(\mathrm{cl}_{p^2}(a), \mathrm{cl}_p(b)) = (\mathrm{cl}_{p^2}(p^2a), \mathrm{cl}_p(pb)) = (\mathrm{cl}_{p^2}(0), \mathrm{cl}_p(0))$, ce qui montre que tout élément a un ordre divisant $p^2$.
   - Pour $p$, on considère $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ et on montre de façon analogue qu'il est d'exposant $p$.

## 1.2 Prolongement de caractères

5. On considère l'application $f : \mathbb{Z} \to G, k \mapsto a^k$. On sait que c'est un morphisme de groupes. L'ensemble $A = \{k \in \mathbb{Z} \mid a^k \in H\}$ vaut $f^{-1}(H)$, c'est donc un sous-groupe de $\mathbb{Z}$. Ce sous-groupe n'est pas réduit à $\{0\}$ : en effet, il contient le noyau de $f$ et celui-ci n'est pas réduit à $\{0\}$ car $f$ n'est pas injective (application d'un ensemble infini vers un ensemble fini).
Donc, $A$ est de la forme $d\mathbb{Z}$, pour un certain $d \in \mathbb{N}^*$, d'après la structure des sous-groupes additifs de $\mathbb{Z}$. L'entier $d$ est bien le minimum de $\{k \in \mathbb{N}^* \mid a^k \in H\}$ et il vérifie $a^k \in H \iff d \mid k$ par construction.

6. (a) *On peut utiliser directement la description par le bas du sous-groupe engendré par une partie. Pour simplifier les notations, il est peut-être plus simple d'adapter la preuve à ce cas.*
   Notons $L = \{ha^k, h \in H \text{ et } k \in \mathbb{Z}\}$. C'est un sous-groupe de $G$ ; en effet :
   - $1 \in H$ et $1 = 1 \times a^0$ ;
   - si $ha^k$ et $h'a^{k'}$ sont dans $L$ (avec des notations transparentes), leur produit vaut $(hh')a^{k+k'}$ (car $G$ est abélien) et $hh' \in H$ (car $H$ sous-groupe), donc leur produit est dans $L$ ;
   - l'inverse de $ha^k$ est $h^{-1}a^{-k}$ (toujours par commutativité), et $h^{-1} \in H$ (car $H$ sous-groupe).

   De plus, $L$ contient manifestement $H$ et $a$. Enfin, tout groupe contenant $H \cup \{a\}$ doit contenir $H$ et les itérés de $a$, donc les produits d'éléments de $H$ et des itérés de $a$, donc $L$.
   Ceci montre que $K = L$.

   (b) Comme $\chi(h_0)$ est un élément de $\mathbb{U}$, il admet une racine $d$-ème, comme tout nombre complexe.

(c) Le problème de définition de $\chi'$ vient de la non-unicité de l'écriture précédente d'un élément de $k$. Soient $h, h' \in H$ et $k, k' \in \mathbb{Z}$ tels que $ha^k = h'a^{k'}$. On a donc $h'^{-1}h = a^{k'-k}$. Le membre de gauche est dans $H$, donc celui de droite aussi. Par la question 5, $d \mid k' - k$. On peut donc écrire $k' - k = du$, pour un $u \in \mathbb{Z}$ et $h'^{-1}h = (a^d)^u = h_0^u$.
Comme $\chi$ est un morphisme de $H$ dans $\mathbb{U}$, on a alors $\chi(h'^{-1}h) = \chi(h_0)^u$ et donc $\chi(h) = \chi(h')\chi(h_0)^u = \omega^{du} = \omega^{k'-k}$. On a donc $\chi(h)\omega^k = \chi(h')\omega(k')$ et cette relation montre que la définition de $\chi'$ sur l'élément $ha^k = h'a^{k'}$ est indépendante du choix de l'écriture.

Soient maintenant $u, u' \in K$. On les écrit $u = ha^k$ et $u' = h'a^{k'}$, avec $h, h' \in H$ et $k, k' \in \mathbb{Z}$. Alors,

$$\chi'(uu') = \chi'((hh')a^{k+k'}) = \chi(hh')\omega^{k+k'} = \chi(h)\omega^k\chi(h')\omega^{k'} = \chi'(u)\chi'(u'),$$

ce qui montre que $\chi'$ est un caractère de $K$.
Enfin, comme un élément $h \in H$ peut s'écrire $h = h \times a^0$, on a $\chi'(h) = \chi(h)\omega^0 = \chi(h)$, ce qui montre que $\chi'$ prolonge $\chi$.

(d) On construit une suite finie de sous-groupes de $G$ ainsi :

- $H_0 = H$ ;
- On suppose $H_k$ défini pour un $k \in \mathbb{N}$. Si $H_k = G$, on arrête la suite ; sinon, on choisit un élément $a_k \in G \setminus H_k$ et on note $H_{k+1}$ le sous-groupe de $G$ engendré par $H_k$ et $a_k$.

Cette construction s'arrête après un nombre fini d'étapes car les cardinaux des $H_k$ forment une suite strictement croissante, majorée par le cardinal de $G$ (fini).
Par la question précédente, on peut définir récursivement pour tout $k$ un caractère de $H_k$ ainsi : $\chi_0 = \chi$ ; si $\chi_k$ est défini, on construit un caractère $\chi_{k+1}$ de $H_{k+1}$ dont la restriction à $H_k$ est $\chi_k$.
On a ainsi prolongé de proche en proche le caractère $\chi$ de $H$ ; comme le dernier groupe dans notre suite croissante est $G$, on obtient à la dernière étape un caractère $\hat{\chi}$ de $G$ prolongeant $\chi$.

## 1.3 Théorème de structure

7. Le sous-groupe $\langle x \rangle$ de $G$ est monogène par définition et fini car c'est un sous-groupe de $G$. En tant que groupe cyclique, il est donc isomorphe à un groupe $\mathbb{Z}/r\mathbb{Z}$ par le cours ; comme $x$ est d'ordre $e$, on sait que $\langle x \rangle$ est de cardinal $e$, donc $r = e$.

8. Le groupe $\mathbb{U}_e$ est aussi un groupe cyclique ; comme il est de cardinal $e$, il est aussi isomorphe à $\mathbb{Z}/e\mathbb{Z}$. Donc, en composant les isomorphismes, on en déduit un isomorphisme de $\langle x \rangle$ dans $\mathbb{U}_e$. On peut noter $\chi$ cet isomorphisme et le considérer comme un caractère de $\langle x \rangle$, en augmentant son espace d'arrivée à $\mathbb{U}$.

9. On sait que $\chi(\langle x\rangle) = \mathbb{U}_e$ donc on a l'inclusion $\mathbb{U}_e \subset \hat{\chi}(G)$, car $\hat{\chi}$ prolonge $\chi$.
Réciproquement, si $g \in G$, on sait que $g^e = 1$ d'après la question 3. Comme $\hat{\chi}$ est un morphisme de groupes, on a $(\hat{\chi})(g)^e = \hat{\chi}(1) = 1$. Ainsi, $(\hat{\chi})(g)$ est une racine $e$-ème de l'unité. D'où l'inclusion réciproque et l'égalité $\hat{\chi}(G) = \mathbb{U}_e$.

   Soit $g \in G$. On sait donc que $\hat{\chi}(g) \in \mathbb{U}_e$ ; notons $\omega$ cet élément. Comme $\chi : \langle x\rangle \to \mathbb{U}_e$ est un isomorphisme, il existe un (unique) entier $k \in [\![0, e-1]\!]$ tel que $\chi(x^k) = \omega$. Alors, $\hat{\chi}(gx^{-k}) = \omega \times \omega^{-1} = 1$, de sorte que $gx^{-k}$ est dans $H = \operatorname{Ker}\hat{\chi}$ ; ceci montre l'existence d'une telle décomposition.
   Pour l'unicité, on remarque que si $g = x^k h$, alors en prenant l'image par $\hat{\chi}$, on doit avoir $\omega = \hat{\chi}(g) = \chi(x^k)$ ; avec $k \in [\![0, e-1]\!]$, ceci fixe la valeur de $k$ (puisque $\chi$ est injective sur $\langle x\rangle$) ; une fois $k$ fixé, $h \in \operatorname{Ker}\hat{\chi}$ l'est aussi.

10. On considère l'application $\psi : \langle x\rangle \times H \to G, (u, h) \mapsto uh$. C'est un morphisme de groupes car $G$ est abélien (et donc $uhu'h' = (uu')(hh')$). La question précédente a montré que tout élément de $G$ s'écrit de façon unique comme $\psi(u, h)$ avec $u \in \langle x\rangle$ et $h \in H$. D'où l'on déduit la bijectivité de $\psi$.
    Notons finalement $f : \mathbb{Z}/e\mathbb{Z} \to \langle x\rangle$ un isomorphisme de groupes ; alors l'application $\mathbb{Z}/e\mathbb{Z} \times H \to G, (\overline{k}, h) \mapsto \psi(f(\overline{k}), h)$ est un isomorphisme (par composition d'isomorphismes).

11. On raisonne par récurrence forte sur le cardinal $n$ de $G$.

    - Si $n = 2$, l'élément qui n'est pas l'élément neutre a nécessairement pour ordre 2, et donc $G$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ dans ce cas.
    - Supposons le résultat démontré pour tout groupe de cardinal $< n$, avec $n \geq 3$. On considère dans $G$ un élément d'ordre $e$ l'exposant de $G$. D'après les question précédentes, $G$ est alors isomorphe à $\mathbb{Z}/e\mathbb{Z} \times H$, avec $H$ un sous-groupe de $G$.
      - Si $H$ est trivial, $G$ est isomorphe à $\mathbb{Z}/e\mathbb{Z}$ et le résultat est démontré.
      - Sinon, il existe par hypothèse de récurrence (après réindexation) une suite finie $(d_2, \ldots, d_r)$ telle que $d_{k+1} \mid d_k$ si $k \in [\![2, r-1]\!]$ et $H$ est isomorphe à $\mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$. En composant les isomorphismes, $G$ est alors isomorphe à $\mathbb{Z}/e\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$.
        De plus, l'exposant de $\mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$ est égal à $d_2$ (adapter la question 4), donc c'est aussi celui de $H$ ; comme $H$ est un sous-groupe de $G$, on en déduit que $d_2 \mid e$. En renotant $e = d_1$, on a le résultat souhaité.

# 2 Convolution de Dirichlet et fonction de Möbius

## 2.1 Anneau des fonctions arithmétiques

1. C'est un exemple de cours.

   - La fonction nulle est élément neutre.

- Si $f$ est une fonction de $\mathbb{N}^*$ dans $\mathbb{C}$, $-f : n \mapsto -f(n)$ est son opposé.
- Si $f, g, h$ sont trois fonctions, alors $(f+g)+h : n \mapsto (f(n)+g(n))+h(n) = f(n)+(g(n)+h(n))$ donc $(f+g)+h = f+(g+h)$ et $f+g : n \mapsto f(n)+g(n) = g(n)+f(n)$ donc $f+g = g+f$. Ainsi, $+$ est associative et commutative.

Donc, $\mathcal{A}$ est un groupe abélien.

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

$$(f*g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}) = \sum_{d'|n} f(\frac{n}{d'})g(d') = (g*f)(n).$$

Pour la deuxième égalité, on utilise que l'application $d \mapsto \dfrac{n}{d}$ est une permutation (en fait une involution) de l'ensemble des diviseurs strictement positifs de $n$. Donc, $*$ est commutative.
Pour l'associativité, il est plus agréable d'utiliser la première formule du produit de convolution.

$$(f*g)*h(n) = \sum_{\substack{u,c\in\mathbb{N}^* \\ uc=n}} (f*g)(u)h(c) = \sum_{\substack{u,c\in\mathbb{N}^* \\ uc=n}} \Big( \sum_{\substack{a,b\in\mathbb{N}^* \\ ab=u}} f(a)g(b)\Big)h(c) = \sum_{\substack{a,b,c\in\mathbb{N}^* \\ abc=n}} f(a)g(b)h(c).$$

Un calcul analogue montre que c'est aussi la valeur de $f*(g*h)(n)$. Donc, $*$ est associative.

3. Soit $f \in \mathcal{A}$, soit $n \in \mathbb{N}$. On a

$$f*\delta_1(n) = \sum_{d|n} f(d)\delta_1(\frac{n}{d}) = f(n),$$

car $\delta_1(\dfrac{n}{d})$ est nul sauf quand $d = n$ et alors il vaut 1. Donc, $f*\delta_1 = f$. Comme $*$ est commutative, il n'y a pas besoin de vérifier que $\delta_1 * f = f$ ; $\delta_1$ est élément neutre pour $*$.

4. On a vu que

- $(\mathcal{A}, +)$ est un groupe abélien.
- $*$ est associative, commutative et a un élément neutre.
- Il reste seulement à montrer que $*$ est distributive sur $+$. Or, si $f, g, h \in \mathcal{A}$ :

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

Comme $*$ est commutative, cette égalité suffit à assurer la distributivité.

On note $(\mathcal{A}^\times, *)$ le groupe des inversibles de $\mathcal{A}$. Montrer que $f \in \mathcal{A}^\times \iff f(1) \neq 0$.

5. Supposons $f \in \mathcal{A}^\times$ ; notons $g$ son inverse. On a donc $f * g = \delta_1$. Donc,

$$1 = \delta_1(1) = \sum_{d|1} f(1)g(\frac{1}{d}) = f(1)g(1).$$

Ceci montre que $f(1) \neq 0$.

Pour la réciproque, on suppose que $f \in \mathcal{A}$ est telle que $f(1) \neq 0$. Soit $n \in \mathbb{N}^*$. On a

$$\begin{aligned} f * g(n) = \delta_1(n) &\iff \sum_{d|n} f(d)g(\frac{n}{d}) = 0 \\ &\iff f(1)g(n) + \sum_{\substack{d|n \\ d\neq n}} f(d)g(\frac{n}{d}) = 0 \\ &\iff g(n) = -f(1)^{-1} \sum_{\substack{d|n \\ d\neq n}} f(d)g(\frac{n}{d}). \end{aligned}$$

Le membre de droite ne dépend que des valeurs de $g$ sur les entiers strictement inférieurs à $n$. On peut ainsi définir $g$ par récurrence par :

- $g(1) = f(1)^{-1}$ ;
- $\forall n \geq 2, g(n) = -f(1)^{-1} \sum_{\substack{d|n \\ d\neq n}} f(d)g(\frac{n}{d})$.

Le calcul précédent montre alors que $g$ est l'inverse de $f$ pour $*$.

## 2.2 Fonctions multiplicatives

6. Notons $P_m$ et $P_n$ l'ensemble des diviseurs premiers de $m$ et $n$. Comme $m \wedge n = 1$, ces ensembles sont disjoints. On a

$$mn = \prod_{p\in P_m} p^{\nu_p(m)} \times \prod_{p\in P_n} p^{\nu_p(n)}.$$

D'une part, un diviseur strictement positif $d$ de $mn$ s'écrit $\prod_{p\in P_m} p^{\nu_p(d)} \times \prod_{p\in P_n} p^{\nu_p(d)}$, où pour $p \in P_m$, $\nu_p(d) \leq \nu_p(m)$ et pour $p \in P_n$, $\nu_p(d) \leq \nu_p(n)$. D'autre part, si $d_1 \in \mathrm{Div}(m)$ et $d_2 \in \mathrm{Div}(n)$, $d_1 = \prod_{p\in P_m} p^{\nu_p(d_1)}$ et $d_2 = \prod_{p\in P_n} p^{\nu_p(d_2)}$ avec $\nu_p(d_1) \leq \nu_p(m)$ si $p \in P_m$ et $\nu_p(d_2) \leq \nu_p(n)$ si $p \in P_n$. Il existe alors un unique couple $(d_1, d_2) \in \mathrm{Div}(m) \times \mathrm{Div}(n)$ tel que $d_1 d_2 = d$ (par unicité dans la décomposition en facteurs premiers) : c'est de prendre $d_1$ et $d_2$ tels que $\nu_p(d_1) = \nu_p(d)$ pour $p \in P_m$ et $\nu_p(d_2) = \nu_p(d)$ pour $p \in P_n$.

7. Soient $f, g \in \mathcal{M}$, soient $n, m \in \mathbb{N}^*$ tels que $n \wedge m = 1$. On a

$$\begin{aligned}(f*g)(nm) &= \sum_{d \in \mathrm{Div}(nm)} f(d)g(\frac{nm}{d}) \\ &= \sum_{\substack{d_1 \in \mathrm{Div}(n) \\ d_2 \in \mathrm{Div}(m)}} f(d_1 d_2)g(\frac{nm}{d_1 d_2}) \text{ par la question précédente} \\ &= \sum_{\substack{d_1 \in \mathrm{Div}(n) \\ d_2 \in \mathrm{Div}(m)}} f(d_1)f(d_2)g(\frac{n}{d_1})g(\frac{m}{d_2}) \text{ car } f, g \in \mathcal{M} \text{ et que } d_1 \wedge d_2 = \frac{n}{d_1} \wedge \frac{m}{d_2} = 1 \\ &= \sum_{d_1 \in \mathrm{Div}(n)} f(d_1)g(\frac{n}{d_1}) \times \sum_{d_2 \in \mathrm{Div}(m)} f(d_2)g(\frac{m}{d_2}) \\ &= (f*g)(n) \times (f*g)(m).\end{aligned}$$

Donc, $fg \in \mathcal{M}$.

8. Soit $f \in \mathcal{M}\{0\}$. Comme $f$ est non nulle, on peut trouver $n \in \mathbb{N}^*$ telle que $f(n) \neq 0$. Alors, comme $1 \wedge n = 1$, on a $f(n) = f(1 \times n) = f(1) \times f(n)$. Donc, $f(1) = 1$. Par la question 5, on en déduit que $f \in \mathcal{A}^\times$.

9. (a) Soit $g$ une fonction convenant. Soit $n \in \mathbb{N}^*$. On écrit $n = \prod_{p \in P_n} p^{\nu_p(n)}$, où $p_n$ est l'ensemble des diviseurs premiers de $n$. Par une récurrence immédiate sur le nombre de facteurs et la multiplicativité de $g$, on doit avoir :

$$g(n) = \prod_{p \in P_n} g(p^{\nu_p(n)}) = \prod_{p \in P_n} f^{-1}(p^{\nu_p(n)}).$$

Ceci montre l'unicité d'un tel $g$.
Réciproquement, on définit $g$ par la formule ci-dessus. Si $n$ et $m$ sont premiers entre eux, $nm = \prod_{p \in P_n} p^{\nu_p(n)} \times \prod_{p \in P_m} p^{\nu_p(m)}$ avec $P_n$ et $P_m$ disjoints. Donc,

$$g(nm) = \prod_{p \in P_n} g(p^{\nu_p(n)}) \times \prod_{p \in P_m} g(p^{\nu_p(m)}) = g(n)g(m)$$

et $g \in \mathcal{M}$. Et par construction, $g(p^k) = f^{-1}(p^k)$ si $p \in \mathbb{P}$ et $k \in \mathbb{N}^*$.

(b) Soient $p \in \mathbb{P}, k \in \mathbb{N}^*$. On calcule :

$$\begin{aligned}(g*f)(p^k) &= \sum_{d|p^k} g(d)f(\frac{p^k}{d}) \\ &= \sum_{i=0}^{k} g(p^i)f(p^{k-i}) \\ &= \sum_{i=0}^{k} f^{-1}(p^i)f(p^{k-i}) \\ &= \sum_{d|p^k} f^{-1}(d)f(\frac{p^k}{d}) \\ &= (f^{-1}*f)(p^k) \\ &= \delta_1(p^k) = 0 \text{ car } k \geq 1.\end{aligned}$$

(c) La fonction $g*f$ est multiplicative car $g$ et $f$ le sont et que $\mathcal{M}$ est stable par produit. Comme elle est nulle sur tous les $p^k$, avec $p$ premier, elle est nulle sur tout entier $n \geq 2$. De plus, $(g*f)(1) = g(1)f(1) = 1 \times 1 = 1$. En effet, $g(1)$ vaut 1 (car défini par un produit vide) et $f(1) = 1$ a été montré plus haut. Ceci montre que $g*f = \delta_1$, donc que $g$ est l'inverse de $f$.
Ainsi, l'inverse $f^{-1}$ de $f$ est dans $\mathcal{M}$.

## 2.3 Fonction de Möbius

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

- Si $\mu(n) = 0$, alors $n$ est divisible par le carré d'un nombre premier. Donc $nm$ aussi et $\mu(nm) = 0$. Dans ce cas, $\mu(nm) = \mu(n)\mu(m)$.
- De même, si $\mu(m) = 0$.
- Si $\mu(n)$ et $\mu(m)$ sont non nuls, $n$ est le produit de $r$ nombres premiers distincts, $m$ le produit de $s$ nombres premiers distincts. Alors, $nm$ est le produit de $r+s$ nombres premiers distincts car $n \wedge m = 1$ (et donc $n$ et $m$ n'ont pas de diviseur premier commun). Ainsi, $\mu(nm) = (-1)^{r+s} = (-1)^r \times (-1)^s = \mu(n)\mu(m)$. Donc, $\mu \in \mathcal{M}$.

11. (a) Les diviseurs de $p^k$ sont les $p^i$ avec $i \in [\![0, k]\!]$. Donc,

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

Dans cette somme, les termes pour $i \geq 2$ sont nuls car $p^i$ est divisible par $p^2$.

Comme $\mu(1) = 1$ et $\mu(p) = -1$, on a bien $\displaystyle\sum_{i=0}^{k} \mu(p^i) = 0$.

(b) La fonction $\mu * \mathbb{1}$ est multiplicative car $\mu$ et $\mathbb{1}$ le sont. D'après la question précédente, elle est nulle sur les puissances de nombres premiers ; donc elle est nulle sur tout entier $n \geq 2$. Et elle vaut $\mu(1)\mathbb{1}(1) = 1 \times 1 = 1$ en 1. Donc, $\mu * \mathbb{1} = \delta_1$ : $\mu$ est l'inverse de $\mathbb{1}$.
La relation de l'énoncé est une traduction immédiate de

$$\forall n \in \mathbb{N}^*, (\mu * \mathbb{1})(n) = \delta_1(n).$$

12. On peut traduire la définition de $g$ par un produit de convolution : $g = f * \mathbb{1}$. On multiplie par $\mu$ et on utilise l'associativité et la commutativité de $*$ :

$$f = f * (\mathbb{1} * \mu) = (f * \mathbb{1}) * \mu = g * \mu = \mu * g,$$

ce qui se traduit en $\forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d})$.

## 2.4 Produits eulériens

13. Un entier $k$ est dans $\mathbb{N}_{S,N}$ ssi il s'écrit $k = \prod_{p \in S} p^{\alpha_p}$, où pour tout $p \in S$, $\alpha_p \leq N$. Ainsi,

$$\begin{aligned}
\sum_{k \in \mathbb{N}_{S,N}} f(k) &= \sum_{\substack{\alpha_p \in [\![0,N]\!] \\ p \in S}} f\left(\prod_{p \in S} p^{\alpha_p}\right) \\
&= \sum_{\substack{\alpha_p \in [\![0,N]\!] \\ p \in S}} \prod_{p \in S} f(p^{\alpha_p}) \text{ car } f \in \mathcal{M} \\
&= \prod_{p \in S} \Big( \sum_{k=0}^{N} f(p^k) \Big) \text{ par super-distributivité}
\end{aligned}$$

14. La fonction $f : n \mapsto \dfrac{1}{n^s}$ est multiplicative. Si $p_j$ est un nombre premier et $N \in \mathbb{N}$, on a $\sum_{k=0}^{N} f(p_j^k) = \sum_{k=0}^{N} \left(\dfrac{1}{p_j^s}\right)^k = \dfrac{1 - p_j^{-s(N+1)}}{1 - p_j^{-s}}$, donc cette somme a pour limite $\dfrac{1}{1 - p_j^{-s}}$ quand $N \to +\infty$ (car $p_j^{-s} \in ]0,1[$). Par le passage à la limite admis, on a :

$$\zeta(s) = \lim_{n \to +\infty} \sum_{k=1}^{n} \frac{1}{n^s} = \lim_{r \to +\infty} \prod_{j=1}^{r} \frac{1}{1 - p_j^{-s}}.$$

15. La fonction $g : n \mapsto \dfrac{\mu(n)}{n^s}$ est multiplicative. Si $p_j$ est un nombre premier et $N \geq 1$, on a $\sum_{k=0}^{N} g(p_j^k) = \sum_{k=0}^{1} \mu(1) + \dfrac{\mu(p_j)}{p_j^s} = 1 - p_j^{-s}$ ; en effet les termes avec $k \geq 2$ sont nuls

car $\mu$ est nulle sur $p_j^k$ si $k \geq 2$. Ainsi,

$$\lim_{n\to+\infty} \sum_{k=1}^{n} \frac{\mu(k)}{k^s} = \lim_{r\to+\infty} \prod_{j=1}^{r} \left(1 - p_j^{-s}\right).$$

Le membre de droite est l'inverse du membre de droite de la question précédente, donc il vaut $\dfrac{1}{\zeta(s)}$, par cette question, ce qui conclut.

## 2.5 Probabilité que deux entiers soient premiers entre eux

16. Les ensembles $H_k^n$ avec $1 \leq k \leq n$ et $d \mid k$ sont deux à deux disjoints. Donc, la somme $\displaystyle\sum_{\substack{1\leq k\leq n\\ d|k}} |H_k^n|$ est le cardinal de $\displaystyle\bigcup_{\substack{1\leq k\leq n\\ d|k}} H_d^n$. Or, cet ensemble est celui des couples $(u,v) \in [\![1,n]\!]^2$ tels que $d \mid u \wedge v$, c'est-à-dire des couples $(u,v)$ tels que $d \mid u$ et $d \mid v$. Il y a $\lfloor \dfrac{n}{d} \rfloor$ multiples de $d$ dans $[\![1,n]\!]$, donc $\lfloor \dfrac{n}{d} \rfloor^2$ tels couples ; d'où l'égalité.

17. On fixe $n \in \mathbb{N}^*$ et on calcule la somme de droite :

$$\begin{aligned}
\sum_{k=1}^{n} \mu(k) \lfloor \frac{n}{k} \rfloor^2 &= \sum_{k=1}^{n} \mu(k) \Big( \sum_{\substack{1\leq k'\leq n\\ k|k'}} |H_{k'}^n| \Big) \\
&= \sum_{k'=1}^{n} |H_{k'}^n| \Big( \sum_{\substack{1\leq k\leq n\\ k|k'}} \mu(k) \Big) \\
&= |H_1^n|
\end{aligned}$$

car d'après la question 11.b), la somme intérieure vaut 1 si $k' = 1$ et 0 sinon.
*Le piège était de chercher à utiliser directement la formule d'inversion de Möbius, alors que la somme porte sur les multiples plutôt que sur les diviseurs. Il y a en fait deux formules d'inversion et on utilise la deuxième.*

18. D'après la question précédente, on a :

$$|H_1^n| - n^2 \sum_{k=1}^{n} \frac{\mu(k)}{k^2} = \sum_{k=1}^{n} \mu(k) \left( \lfloor \frac{n}{k} \rfloor^2 - \frac{n^2}{k^2} \right) = \sum_{k=1}^{n} \mu(k) \left( \lfloor \frac{n}{k} \rfloor - \frac{n}{k} \right) \left( \lfloor \frac{n}{k} \rfloor + \frac{n}{k} \right),$$

par identité remarquable. Par inégalité triangulaire, on a donc :

$$\left| |H_1^n| - n^2 \sum_{k=1}^{n} \frac{\mu(k)}{k^2} \right| \leq \sum_{k=1}^{n} |\mu(k)| \times \left| \left( \lfloor \frac{n}{k} \rfloor - \frac{n}{k} \right) \right| \times \left| \left( \lfloor \frac{n}{k} \rfloor + \frac{n}{k} \right) \right|.$$

On peut majorer $|\mu(k)|$ par 1, $\left|\left(\lfloor\frac{n}{k}\rfloor - \frac{n}{k}\right)\right|$ par 1 et $\left|\times\left|\left(\lfloor\frac{n}{k}\rfloor + \frac{n}{k}\right)\right|\right.$ par $\frac{2n}{k}$, d'où la majoration :

$$\left||H_1^n| - n^2\sum_{k=1}^{n}\frac{\mu(k)}{k^2}\right| \leq 2n\sum_{k=1}^{n}\frac{1}{k}.$$

De plus, si $k \geq 2$, on a $\frac{1}{k} \leq \int_{k-1}^{k}\frac{1}{t}dt$.

D'où $\sum_{k=1}^{n} \leq 1 + \sum_{k=2}^{n}\int_{k-1}^{n}\frac{dt}{t} = 1 + \ln(n-1) \leq 1 + \ln n$. D'où la deuxième inégalité.

19. D'après la question précédente, $\frac{|H_1^n|}{n^2} - \sum_{k=1}^{n}\frac{\mu(k)}{k^2}$ a sa valeur absolue majorée par $\frac{2(\ln n + 1)}{n}$, qui tend vers 0 par croissance comparée.

De plus, $\sum_{k=1}^{n}\frac{\mu(k)}{k^2}$ tend vers $\frac{1}{\zeta(2)}$ par la question 15. Par théorème d'encadrement, la probabilité recherchée vaut $\frac{1}{\zeta(2)}$.