

# DM 17 : un corrigé

## Questions préliminaires

1°)

◇ L'addition n'est pas une loi interne sur  $\mathbb{C}^*$ , car par exemple, 1 et  $-1$  sont dans  $\mathbb{C}^*$ , mais  $1 + (-1) = 0$  n'est pas dans  $\mathbb{C}^*$ . A fortiori,  $(\mathbb{C}^*, +)$  n'est pas un groupe.

◇ D'après le cours,  $(\mathbb{C}, +, \times)$  est un corps, donc  $\mathbb{C}^*$  est l'ensemble des inversibles de l'anneau  $(\mathbb{C}, +, \times)$  et, toujours d'après le cours, c'est donc un groupe pour la multiplication.

2°) ◇ Soit  $x \in G$ .

Soit  $n \in \mathbb{N}$ . Notons  $R(n)$  l'assertion :  $g(x^n) = g(x)^n$ .

Pour  $n = 0$ , on sait d'après le cours sur les morphismes de groupes que

$g(x^0) = g(1) = 1 = g(x)^0$ , d'où  $R(0)$ .

Pour  $n \in \mathbb{N}$ , supposons  $R(n)$  et montrons  $R(n + 1)$ .

$g(x^{n+1}) = g(x^n \cdot x) = g(x^n) \cdot g(x)$  car  $g$  est un morphisme, donc d'après  $R(n)$ ,  $g(x^{n+1}) = g(x)^n g(x) = g(x)^{n+1}$ , ce qui prouve  $R(n + 1)$ .

D'après le principe de récurrence, pour tout  $n \in \mathbb{N}$ ,  $g(x^n) = g(x)^n$ .

Soit maintenant  $n \in \mathbb{Z} \setminus \mathbb{N}$ . Alors, par définition de  $x^n$ ,  $g(x^n) = g((x^{-n})^{-1})$ , donc d'après le cours sur les morphismes de groupes,  $g(x^n) = (g(x^{-n}))^{-1}$ , or  $-n \in \mathbb{N}$ , donc ce qui précède permet d'écrire que  $g(x^n) = (g(x)^{-n})^{-1} = g(x)^n$ , ce qu'il fallait démontrer.

◇ En notation additive, si  $g$  est un caractère d'un groupe  $(G, +)$ , on a donc : pour tout  $x \in G$  et  $a \in \mathbb{Z}$ ,  $g(ax) = g(x)^a$ .

## Partie 1 : Caractères de $\mathbb{Z}$ et de $\mathbb{R}$

3°) Soit  $g$  un caractère de  $\mathbb{Z}$ .

D'après la question précédente, pour tout  $a \in \mathbb{Z}$ ,  $g(a) = g(a \times 1) = g(1)^a$ , donc si  $g$  est un caractère, il existe  $r \in \mathbb{C}^*$  tel que, pour tout  $a \in \mathbb{Z}$ ,  $g(a) = r^a$ .

Réciproquement, si  $g$  est de la forme  $a \mapsto r^a$ , où  $r \in \mathbb{C}^*$ , on vérifie aisément que, pour tout  $a, b \in \mathbb{Z}$ ,  $g(a + b) = g(a)g(b)$ , donc  $g$  est bien un caractère de  $\mathbb{Z}$ . En conclusion, les

caractères de  $\mathbb{Z}$  sont exactement les applications de la forme 
$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{C}^* \\ a & \longmapsto & r^a \end{array}, \text{ où } r \in \mathbb{C}^*.$$

4°)

◇ Pour tout  $r, s \in \mathbb{R}$ , on a  $g(r+s) = g(r)g(s)$ , et  $g$  est dérivable, donc en dérivant selon  $r$  à  $s$  fixé, on obtient, pour tout  $r, s \in \mathbb{R}$ ,  $g'(r+s) = g'(r)g(s)$ . De plus  $g(0) = 1$ , car  $g$  est un morphisme de groupes, donc, en remplaçant le couple  $(r, s)$  par  $(0, t)$ , on obtient que, pour tout  $t \in \mathbb{R}$ ,  $g'(t) = g'(0)g(t)$ , ce qu'il fallait démontrer en posant  $c = g'(0)$ .

◇ Posons  $h(t) = g(t)e^{-ct}$ , pour tout  $t \in \mathbb{R}$ .  $h$  est dérivable et  $h'(t) = e^{-ct}(g'(t) - cg(t))$ , donc  $h'(t) = 0$ , ce qui prouve que  $h$  est une application constante. Or  $h(0) = g(0) = 1$ , donc  $h$  est l'application constante égale à 1. Ainsi, on a montré que si  $g$  est un caractère dérivable sur  $\mathbb{R}$ , alors il existe  $c \in \mathbb{C}$  tel que  $g = (t \mapsto e^{ct})$ .

Réciproquement, si  $g$  est de cette forme, on vérifie aisément que  $g(r+s) = g(r)g(s)$  pour tout  $r, s \in \mathbb{R}$ .

En conclusion, l'ensemble des caractères dérivables de  $\mathbb{R}$  est  $\{t \mapsto e^{ct} / c \in \mathbb{C}\}$ .

5°) Soit  $g$  un caractère continu de  $\mathbb{R}$ .

Si, pour tout  $\varepsilon \in \mathbb{R}$ ,  $\int_0^\varepsilon g(t) dt = 0$ , alors en dérivant par rapport à  $\varepsilon$ , on obtient que  $g(\varepsilon) = 0$  pour tout  $\varepsilon \in \mathbb{R}$ , ce qui est faux car  $g$  est à valeurs dans  $\mathbb{C}^*$ . Ainsi, il existe  $\varepsilon \in \mathbb{R}$  tel que  $\int_0^\varepsilon g(t) dt \neq 0$ .

Pour tout  $r \in \mathbb{R}$ ,  $\int_0^\varepsilon g(r+t) dt = g(r) \int_0^\varepsilon g(t) dt$ , puis par changement de variables,  $g(r) \int_0^\varepsilon g(t) dt = \int_r^{r+\varepsilon} g(t) dt$ , donc en notant  $G$  une primitive de  $g$ , on peut écrire que, pour tout  $r \in \mathbb{R}$ ,  $g(r) = \frac{G(r+\varepsilon) - G(r)}{\int_0^\varepsilon g(t) dt}$ , or  $G$  est de classe  $C^1$ , donc,  $\varepsilon$  étant fixé,  $g$  est aussi de classe  $C^1$ .

Ainsi, l'ensemble des caractères continus de  $\mathbb{R}$  est inclus dans l'ensemble des caractères dérivables de  $\mathbb{R}$ . L'inclusion réciproque étant évidente, d'après la question précédente, l'ensemble des caractères continus de  $\mathbb{R}$  est  $\{t \mapsto e^{ct} / c \in \mathbb{C}\}$ .

## Partie 2 : Liberté de l'ensemble des caractères

### Cas d'un groupe commutatif

6°) Soit  $x, y \in G$ . On a  $g(x+y) = g(x)g(y)$ ,

or  $g(x+y) = \sum_{i=1}^n \lambda_i g_i(x+y) = \sum_{i=1}^n \lambda_i g_i(x)g_i(y)$  et  $g(x)g(y) = \sum_{i=1}^n \lambda_i g_i(x)g(y)$ ,

donc  $\sum_{i=1}^n \lambda_i g_i(x)(g_i(y) - g(y)) = 0$ .

Fixons  $y$  dans  $G$  et posons, pour tout  $i \in \mathbb{N}_n$ ,  $\mu_i = \lambda_i(g_i(y) - g(y))$ . Alors on peut

écrire que  $\sum_{i=1}^n \mu_i g_i = 0$ , or  $(g_1, \dots, g_n)$  est supposé libre, donc pour tout  $i \in \mathbb{N}_n$ ,

$$0 = \mu_i = \lambda_i (g_i(y) - g(y)).$$

$g$  est non nul, car  $g$  est à valeurs dans  $\mathbb{C}^*$ , donc il existe  $i_0 \in \mathbb{N}_n$  tel que  $\lambda_{i_0} \neq 0$ . Alors on peut affirmer que  $g = g_{i_0}$ , ce qu'il fallait démontrer.

7°) D'après le cours, il suffit de montrer que toute partie finie de  $\mathcal{G}$  est libre, ce que l'on va démontrer par récurrence sur le cardinal de la partie finie.

Soit  $n \in \mathbb{N}$ . On note  $R(n)$  l'assertion suivante : toute famille de  $n$  caractères distincts de  $G$  est libre.

Pour  $n = 0$ , une famille vide est toujours libre, d'où  $R(0)$ .

Pour  $n = 1$ , si  $g \in \mathcal{G}$ , alors  $g \neq 0$ , donc la famille  $(g)$  est libre, d'où  $R(1)$ .

Pour  $n \in \mathbb{N}^*$ , supposons  $R(n)$  et montrons  $R(n+1)$ .

Soit  $g_1, \dots, g_{n+1}$   $n+1$  caractères de  $G$  que l'on suppose distincts deux à deux.

Soit  $\alpha_1, \dots, \alpha_{n+1} \in \mathbb{C}$  tels que  $\sum_{i=1}^{n+1} \alpha_i g_i = 0$ .

Supposons qu'il existe  $i_0 \in \mathbb{N}_{n+1}$  tel que  $\alpha_{i_0} \neq 0$ . Quitte à réordonner les vecteurs  $g_1, \dots, g_{n+1}$ , on peut supposer que  $i_0 = n+1$ .

Alors  $g_{n+1} = -\sum_{i=1}^n \frac{\alpha_i}{\alpha_{n+1}} g_i$ , en posant  $\lambda_i = -\frac{\alpha_i}{\alpha_{n+1}}$ .

D'après  $R(n)$ ,  $(g_1, \dots, g_n)$  est libre, donc d'après la question précédente, il existe  $i \in \mathbb{N}_n$  tel que  $g_{n+1} = g_i$ , ce qui est faux par hypothèse. Ainsi, pour tout  $i \in \mathbb{N}_{n+1}$ ,  $\alpha_i = 0$ , ce qui prouve que la famille  $(g_1, \dots, g_{n+1})$  est libre. On a montré  $R(n+1)$ .

Le principe de récurrence permet de conclure.

## Cas d'un groupe fini

8°) Soit  $g$  un caractère de  $G$ . Soit  $x \in G$ . D'après le cours,  $x^n = 1$ , donc d'après la question 2,  $1 = g(1) = g(x^n) = g(x)^n$ , ce qui prouve que  $g(x) \in \mathbb{U}_n$ .

9°)  $\diamond$  Supposons d'abord que  $g = h$ . Alors  $\langle g|h \rangle = \langle g|g \rangle = \frac{1}{n} \sum_{x \in G} |g(x)|^2 = 1$ , car

d'après la question précédente, pour tout  $x \in G$ ,  $g(x) \in \mathbb{U}$ .

$\diamond$  On suppose maintenant que  $g \neq h$ . Ainsi, il existe  $x_0 \in G$  tel que  $g(x_0) \neq h(x_0)$ .

Lorsque  $z \in \mathbb{U}$ ,  $z\bar{z} = |z|^2 = 1$ , donc  $\bar{z} = \frac{1}{z}$ . Ainsi, d'après la première question,

$\langle g|h \rangle = \frac{1}{n} \sum_{x \in G} \frac{g(x)}{h(x)}$ . L'application  $G \rightarrow G$  est une bijection, dont la bijection

réciproque est  $G \rightarrow G$ , donc par changement de variable,

$\langle g|h \rangle = \frac{1}{n} \sum_{x \in G} \frac{g(x_0 x)}{h(x_0 x)} = \frac{g(x_0)}{h(x_0)} \frac{1}{n} \sum_{x \in G} \frac{g(x)}{h(x)}$  car  $g$  et  $h$  sont des morphismes.

Ainsi  $\langle g|h \rangle = \frac{g(x_0)}{h(x_0)} \langle g|h \rangle$ , or  $\frac{g(x_0)}{h(x_0)} \neq 1$ , donc le complexe  $\langle g|h \rangle$  est bien nul.

**10°)**  $G$  est fini, donc l'ensemble des applications de  $G$  dans  $\mathbb{U}_n$  étant fini,  $\mathcal{G}$  est aussi fini. Soit  $(\alpha_g)_{g \in \mathcal{G}} \in \mathbb{C}^{\mathcal{G}}$  une famille de complexes telle que  $\sum_{g \in \mathcal{G}} \alpha_g g = 0$ .

Ainsi, pour tout  $x \in G$ ,  $\sum_{g \in \mathcal{G}} \alpha_g g(x) = 0$

Soit  $h \in \mathcal{G}$ . Alors  $0 = \frac{1}{n} \sum_{x \in G} \left( \sum_{g \in \mathcal{G}} \alpha_g g(x) \right) \overline{h(x)} = \sum_{g \in \mathcal{G}} \alpha_g \frac{1}{n} \sum_{x \in G} g(x) \overline{h(x)}$ ,

donc  $0 = \sum_{g \in \mathcal{G}} \alpha_g \langle g|h \rangle$ . Alors, d'après la question précédente,  $0 = \alpha_h \langle h|h \rangle = \alpha_h$ .

Ceci prouve que  $\mathcal{G}$  est libre.

## Partie 3 : Le groupe dual

**11°)**  $\diamond$  Soit  $f, g \in \text{Hom}(G, H)$ . Montrons que  $fg$  est encore un élément de  $\text{Hom}(G, H)$  : Soit  $x, y \in G$  :  $(fg)(xy) = f(xy)g(xy)$  par définition de  $fg$ , or  $f$  et  $g$  sont des morphismes, donc  $(fg)(xy) = f(x)f(y)g(x)g(y)$ . De plus  $H$  est commutatif, donc  $(fg)(xy) = f(x)g(x)f(y)g(y) = (fg)(x).(fg)(y)$ .

Ainsi, la définition de  $fg$  lorsque  $f, g \in \text{Hom}(G, H)$  est une loi interne sur  $\text{Hom}(G, H)$ .

$\diamond$  Pour tout  $f, g \in \text{Hom}(G, H)$ , pour tout  $x \in G$ ,

$(fg)(x) = f(x)g(x) = g(x)f(x) = (gf)(x)$ , car  $H$  est abélien, donc  $fg = gf$ . Cette loi interne est donc commutative.

$\diamond$  Notons  $\mathbf{1}$  l'application de  $G$  dans  $H$  constante, égale à  $1_H$ . On vérifie que, pour tout  $x, y \in G$ ,  $\mathbf{1}(xy) = \mathbf{1}(x)\mathbf{1}(y)$ , donc  $\mathbf{1} \in \text{Hom}(G, H)$ .

On vérifie facilement que, pour tout  $f \in \text{Hom}(G, H)$ ,  $\mathbf{1}f = f$ , donc  $\mathbf{1}$  est un élément neutre.

$\diamond$  Pour tout  $f, g, h \in \text{Hom}(G, H)$ , pour tout  $x \in G$ ,

$(f(gh))(x) = f(x)[(gh)(x)] = f(x)[g(x)h(x)]$ , or la multiplication dans  $H$  est associative, donc  $(f(gh))(x) = [f(x)g(x)]h(x) = ((fg)h)(x)$ . Ainsi,  $f(gh) = (fg)h$ , ce qui prouve l'associativité.

$\diamond$  Soit  $f \in \text{Hom}(G, H)$ . Pour tout  $x \in G$ , posons  $g(x) = f(x)^{-1}$ .

Soit  $x, y \in G$  :  $g(xy) = f(xy)^{-1} = (f(x)f(y))^{-1} = f(y)^{-1}f(x)^{-1}$ , or  $H$  est commutatif, donc  $g(xy) = f(x)^{-1}f(y)^{-1} = g(x)g(y)$ . Ceci prouve que  $g \in \text{Hom}(G, H)$ .

De plus, pour tout  $x \in G$ ,  $(fg)(x) = f(x)f(x)^{-1} = 1_H$ , donc  $fg = \mathbf{1}$ . Ceci montre que tout élément de  $\text{Hom}(G, H)$  possède un inverse dans  $\text{Hom}(G, H)$ .

$\diamond$  En conclusion,  $\text{Hom}(G, H)$  est un groupe abélien, dont l'élément neutre est  $\mathbf{1}$  et tel que, pour tout  $f \in \text{Hom}(G, H)$ , pour tout  $x \in G$ ,  $(f^{-1})(x) = f(x)^{-1}$ .

$\diamond$  Lorsque  $(H, \cdot) = (\mathbb{C}^*, \cdot)$ , qui est bien commutatif,  $\text{Hom}(G, H) = \mathcal{G}$ , donc  $\mathcal{G}$  possède une structure de groupe abélien.

12°)

◇ Soit  $\tau = (a\ b)$  une transposition de  $\mathcal{S}_m$ . Il existe  $\sigma \in \mathcal{S}_m$  telle que  $\sigma(a) = 1$  et  $\sigma(b) = 2$  (en fait il en existe exactement  $(m-2)!$  et  $(m-2)! \geq 1$  car  $m \geq 2$ ). Alors on vérifie que  $\tau = \sigma^{-1}(1\ 2)\sigma$  : en effet,  $\sigma^{-1}(1\ 2)\sigma(a) = \sigma^{-1}(1\ 2)(1) = \sigma^{-1}(2) = b = \tau(a)$ ,  $\sigma^{-1}(1\ 2)\sigma(b) = \sigma^{-1}(1\ 2)(2) = \sigma^{-1}(1) = a = \tau(b)$  et lorsque  $x \in \mathbb{N}_m \setminus \{a, b\}$ ,  $\sigma(x) \notin \{1, 2\}$  (car  $\sigma$  est injective), donc  $(1\ 2)(\sigma(x)) = \sigma(x)$ , puis  $\sigma^{-1}(1\ 2)\sigma(x) = \sigma^{-1}\sigma(x) = x = \tau(x)$ .

◇ Soit  $g \in \mathcal{G}$ . Alors, avec les notations précédentes,

$g((a\ b)) = g(\sigma)^{-1}g((1\ 2))g(\sigma) = g((1\ 2))$ , car la multiplication dans  $\mathbb{C}$  est commutative. De plus  $g((1\ 2))^2 = g((1\ 2)^2) = g(\text{Id}_{\mathbb{N}_m}) = 1$ , donc  $g((1\ 2)) \in \{1, -1\}$ .

Supposons d'abord que  $g((1\ 2)) = 1$ . Ainsi, pour toute transposition  $\tau$  de  $\mathcal{S}_m$ ,  $g(\tau) = 1$ . D'après le cours, si  $\sigma \in \mathcal{S}_m$ ,  $\sigma$  se décompose comme un produit de transpositions. Or  $g$  est un morphisme, donc  $g(\sigma) = 1$ . Ainsi,  $g$  est l'application constante égale à 1.

Supposons maintenant que  $g((1\ 2)) = -1$ , alors en reprenant le raisonnement précédent, pour tout  $\sigma \in \mathcal{S}_m$ ,  $g(\sigma) = (-1)^n$  où  $n$  est le nombre de transpositions qui interviennent dans la décomposition de  $\sigma$ . Ainsi,  $g$  est la signature, notée  $\varepsilon$ .

Réciproquement, on sait que ces deux applications sont bien des morphismes.

En conclusion, le groupe dual de  $\mathcal{S}_m$  est égal  $\{1, \varepsilon\}$ .

13°) Notons encore  $\mathcal{G}$  le groupe dual de  $\mathbb{Z}/n\mathbb{Z}$ .

◇ D'après la question 8, pour tout  $g \in \mathcal{G}$ ,  $\varphi(g) = g(\bar{1}) \in \mathbb{U}_n$ .

◇ Soit  $g, h \in \mathcal{G}$ .  $\varphi(gh) = (gh)(\bar{1}) = g(\bar{1})h(\bar{1}) = \varphi(g)\varphi(h)$ , donc  $\varphi$  est un morphisme de  $\mathcal{G}$  dans  $\mathbb{U}_n$ .

◇ Soit  $g \in \text{Ker}(\varphi)$ . On a  $g(\bar{1}) = 1$ , donc pour tout  $k \in \mathbb{Z}$ , d'après la question 2,  $g(\bar{k}) = g(k\bar{1}) = g(\bar{1})^k = 1$ . Ainsi  $\text{Ker}(\varphi) = \{\mathbf{1}\}$ , ce qui prouve que  $\varphi$  est injective.

◇ Soit  $\alpha \in \mathbb{U}_n$ . Notons  $g: \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{C}^*$   
 $\bar{k} \longmapsto \alpha^k$ .  $g$  est correctement défini, car si  $h, k \in \mathbb{Z}$

avec  $\bar{h} = \bar{k}$ , alors  $k - h$  est un multiple de  $n$ , or  $\alpha^n = 1$ , donc  $\alpha^{k-h} = 1$  puis  $\alpha^k = \alpha^h$ . Pour tout  $h, k \in \mathbb{Z}$ ,  $g(\bar{h} + \bar{k}) = \alpha^k \alpha^h = g(\bar{h})g(\bar{k})$ , donc  $g \in \mathcal{G}$ . De plus  $\varphi(g) = g(\bar{1}) = \alpha$ , donc  $\varphi$  est une surjection de  $\mathcal{G}$  dans  $\mathbb{U}_n$ .

En conclusion,  $\varphi$  est un isomorphisme de  $\mathcal{G}$  dans  $\mathbb{U}_n$ .

14°) ◇ Lorsque  $f \in \text{Hom}(G_1 \times \cdots \times G_m, H)$ , on note, pour tout  $i \in \mathbb{N}_m$ ,

$$\varphi_i(f): G_i \longrightarrow H$$

$$x \longmapsto f(1_{G_1}, \dots, 1_{G_{i-1}}, x, 1_{G_{i+1}}, \dots, 1_{G_m})$$

Soit  $i \in \mathbb{N}_m$  et  $f \in \text{Hom}(G_1 \times \cdots \times G_m, H)$ . Montrons que  $\varphi_i(f) \in \text{Hom}(G_i, H)$ . En effet, pour tout  $x, y \in G_i$ ,

$$\begin{aligned} \varphi_i(f)(xy) &= f(1_{G_1}, \dots, 1_{G_{i-1}}, xy, 1_{G_{i+1}}, \dots, 1_{G_m}) \\ &= f((1_{G_1}, \dots, 1_{G_{i-1}}, x, 1_{G_{i+1}}, \dots, 1_{G_m}) \cdot (1_{G_1}, \dots, 1_{G_{i-1}}, y, 1_{G_{i+1}}, \dots, 1_{G_m})), \end{aligned}$$

or  $f$  est un morphisme, donc

$$\begin{aligned} \varphi_i(f)(xy) &= f((1_{G_1}, \dots, 1_{G_{i-1}}, x, 1_{G_{i+1}}, \dots, 1_{G_m})) \cdot f((1_{G_1}, \dots, 1_{G_{i-1}}, y, 1_{G_{i+1}}, \dots, 1_{G_m})) \\ &= \varphi_i(f)(x)\varphi_i(f)(y). \end{aligned}$$

Ainsi, en posant, pour tout  $f \in \text{Hom}(G_1 \times \cdots \times G_m, H)$ ,  $\varphi(f) = (\varphi_i(f))_{1 \leq i \leq m}$ , l'application  $\varphi$  ainsi définie va de  $\text{Hom}(G_1 \times \cdots \times G_m, H)$  dans  $\text{Hom}(G_1, H) \times \cdots \times \text{Hom}(G_m, H)$ .

Il reste à montrer que  $\varphi$  est un isomorphisme.

◇ Soit  $f, g \in \text{Hom}(G_1 \times \cdots \times G_m, H)$ . Soit  $i \in \mathbb{N}_m$ . Pour tout  $x \in G_i$ ,

$$\begin{aligned}\varphi_i(fg)(x) &= (fg)(1_{G_1}, \dots, 1_{G_{i-1}}, x, 1_{G_{i+1}}, \dots, 1_{G_m}) \\ &= f(1_{G_1}, \dots, 1_{G_{i-1}}, x, 1_{G_{i+1}}, \dots, 1_{G_m})g(1_{G_1}, \dots, 1_{G_{i-1}}, x, 1_{G_{i+1}}, \dots, 1_{G_m}) \\ &= \varphi_i(f)(x)\varphi_i(g)(x) \\ &= (\varphi_i(f)\varphi_i(g))(x),\end{aligned}$$

donc  $\varphi_i(fg) = \varphi_i(f)\varphi_i(g)$ . On en déduit que

$\varphi(fg) = (\varphi_i(fg))_{1 \leq i \leq m} = (\varphi_i(f)\varphi_i(g))_{1 \leq i \leq m} = \varphi(f) \cdot \varphi(g)$  d'après la loi d'un groupe produit. Ainsi  $\varphi$  est un morphisme de groupes.

◇ Soit  $f \in \text{Ker}(\varphi)$ . Alors  $(\varphi_i(f))_{1 \leq i \leq m} = \varphi(f) = (1_{\text{Hom}(G_1, H)}, \dots, 1_{\text{Hom}(G_m, H)})$ , donc pour tout  $i \in \mathbb{N}_m$ , pour tout  $x_i \in G_i$ ,  $f(1_{G_1}, \dots, 1_{G_{i-1}}, x_i, 1_{G_{i+1}}, \dots, 1_{G_m}) = 1$ .

Soit  $x = (x_1, \dots, x_m) \in G_1 \times \cdots \times G_m$ . On a

$$x = \prod_{i=1}^m (1_{G_1}, \dots, 1_{G_{i-1}}, x_i, 1_{G_{i+1}}, \dots, 1_{G_m}), \text{ or } f \text{ est un morphisme,}$$

$$\text{donc } f(x) = \prod_{i=1}^m f(1_{G_1}, \dots, 1_{G_{i-1}}, x_i, 1_{G_{i+1}}, \dots, 1_{G_m}) = 1.$$

Ainsi,  $f = \mathbf{1}$ . Donc  $\text{Ker}(\varphi) = \{\mathbf{1}\}$ , ce qui prouve que  $\varphi$  est injective.

◇ Soit  $(f_1, \dots, f_m) \in \prod_{i=1}^m \text{Hom}(G_i, H)$ .

Pour tout  $x = (x_1, \dots, x_m) \in G_1 \times \cdots \times G_m$ , posons  $f(x) = \prod_{i=1}^m f_i(x_i)$ .

Montrons que  $f \in \text{Hom}(G_1 \times \cdots \times G_m, H)$  et que  $\varphi(f) = (f_1, \dots, f_m)$ .

Soit  $x = (x_1, \dots, x_m) \in G_1 \times \cdots \times G_m$  et  $y = (y_1, \dots, y_m) \in G_1 \times \cdots \times G_m$ .

Alors  $f(xy) = f((x_1y_1, \dots, x_my_m)) = \prod_{i=1}^m f_i(x_iy_i) = \left( \prod_{i=1}^m f_i(x_i) \right) \left( \prod_{i=1}^m f_i(y_i) \right)$ , car  $H$  est

abélien. Ainsi,  $f(xy) = f(x)f(y)$ , ce qui prouve que  $f \in \text{Hom}(G_1 \times \cdots \times G_m, H)$ .

Soit  $i \in \mathbb{N}_m$ , soit  $x_i \in G_i$ . Alors

$\varphi_i(f)(x_i) = f(1_{G_1}, \dots, 1_{G_{i-1}}, x_i, 1_{G_{i+1}}, \dots, 1_{G_m}) = f_i(x_i)$ , car pour tout  $j \in \mathbb{N}_m \setminus \{i\}$ ,  $f_j(1_{G_j}) = 1_H$ . Ainsi, pour tout  $i \in \mathbb{N}_m$ ,  $\varphi_i(f) = f_i$ , puis  $\varphi(f) = (f_1, \dots, f_m)$ .

Ceci prouve que  $\varphi$  est surjectif.

En conclusion,  $\varphi$  est un isomorphisme.

### 15°)

◇ D'après l'énoncé, il existe un isomorphisme  $f$  de  $G$  dans  $G' = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_q\mathbb{Z}$ .

Si  $g \in \text{Hom}(G', \mathbb{C}^*)$  est un caractère de  $G'$ , posons  $\Psi(g) = g \circ f$ .

Pour tout  $g \in \text{Hom}(G', \mathbb{C}^*)$ ,  $\Psi(g)$  est un morphisme en tant que composé de morphismes, donc  $\Psi(g) \in \text{Hom}(G, \mathbb{C}^*)$ . Ceci montre que  $\Psi$  est une application de  $\text{Hom}(G', \mathbb{C}^*)$  dans  $\text{Hom}(G, \mathbb{C}^*)$ . Montrons que c'est un isomorphisme.

◇ Il est clair que  $\Psi$  est bijective et que son application réciproque

$$\text{est } \begin{array}{ccc} \text{Hom}(G, \mathbb{C}^*) & \longrightarrow & \text{Hom}(G', \mathbb{C}^*) \\ g & \longmapsto & g \circ f^{-1} \end{array}.$$

◇ Soit  $g, h \in \text{Hom}(G', \mathbb{C}^*)$ . Pour tout  $x \in G$ ,  $\Psi(gh)(x) = (gh)(f(x)) = g(f(x)).h(f(x))$ , par définition du produit dans  $\text{Hom}(G', \mathbb{C}^*)$ ,

donc  $\Psi(gh)(x) = \Psi(g)(x).\Psi(h)(x) = [\Psi(g).\Psi(h)](x)$ . Ainsi,  $\Psi(gh) = \Psi(g).\Psi(h)$ , ce qui montre que  $\Psi$  est un morphisme.

◇ Ainsi,  $\text{Hom}(G, \mathbb{C}^*)$ , le groupe dual de  $G$ , est isomorphe à  $\text{Hom}(\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_q\mathbb{Z}, \mathbb{C}^*)$ , lequel est d'après la question précédente isomorphe à  $\prod_{i=1}^m \text{Hom}(\mathbb{Z}/n_i\mathbb{Z}, \mathbb{C}^*)$ .

◇ Soit  $i \in \mathbb{N}_m$ . D'après la question 13,  $\text{Hom}(\mathbb{Z}/n_i\mathbb{Z}, \mathbb{C}^*)$  est isomorphe à  $\mathbb{U}_{n_i}$ . Ce dernier est un groupe cyclique d'ordre  $n_i$ , donc d'après le cours, il est isomorphe  $\mathbb{Z}/n_i\mathbb{Z}$ . Il existe donc un isomorphisme  $f_i$  de  $\text{Hom}(\mathbb{Z}/n_i\mathbb{Z}, \mathbb{C}^*)$  dans  $\mathbb{Z}/n_i\mathbb{Z}$ .

Pour tout  $g = (g_1, \dots, g_m) \in \prod_{i=1}^m \text{Hom}(\mathbb{Z}/n_i\mathbb{Z}, \mathbb{C}^*)$ , posons  $f(g) = (f_i(g_i))_{1 \leq i \leq m}$ . On

vérifie alors que  $f$  est un isomorphisme de  $\prod_{i=1}^m \text{Hom}(\mathbb{Z}/n_i\mathbb{Z}, \mathbb{C}^*)$  dans  $\prod_{i=1}^m \mathbb{Z}/n_i\mathbb{Z}$ , selon les mêmes techniques que précédemment. Ainsi, par composition d'isomorphismes, on a montré que  $\mathcal{G}$  est isomorphe à  $G$  :  $\mathcal{G}$  est isomorphe à  $\text{Hom}(\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_q\mathbb{Z}, \mathbb{C}^*)$ , lequel est isomorphe à  $\prod_{i=1}^m \text{Hom}(\mathbb{Z}/n_i\mathbb{Z}, \mathbb{C}^*)$  qui est isomorphe à  $\prod_{i=1}^m \mathbb{Z}/n_i\mathbb{Z}$  lequel est isomorphe à  $G$  d'après l'énoncé.

**16°)**

◇ Si  $G$  n'est pas abélien,  $\mathcal{G}$  est abélien donc  $\mathcal{G}$  et  $G$  ne sont pas isomorphes.

◇ On a vu en question 3 que lorsque  $G = \mathbb{Z}$ , alors  $\mathcal{G} = \{g_r \mid r \in \mathbb{C}^*\}$ , où  $g_r : \mathbb{Z} \rightarrow \mathbb{C}^*$  est définie par  $a \mapsto r^a$ . L'application  $\mathbb{C}^* \rightarrow \mathcal{G}$  est une bijection dont la bijection

reciproque est  $\mathcal{G} \rightarrow \mathbb{C}^*$  définie par  $g \mapsto g(1)$ , donc d'après le cours  $G = \mathbb{Z}$  est dénombrable alors que  $\mathcal{G}$  n'est pas dénombrable. Il n'existe donc pas de bijection de  $G$  dans son groupe dual et donc a fortiori ils ne sont pas isomorphes.

**17°)**

◇ Soit  $x \in G$  et  $g \in \mathcal{G} = \text{Hom}(G, \mathbb{C}^*)$ . Alors  $\Psi(x)(g) = g(x) \in \mathbb{C}^*$ , donc  $\Psi(x)$  est bien une application de  $\mathcal{G}$  dans  $\mathbb{C}^*$ .

◇ Soit  $g, h \in \mathcal{G}$ . Soit  $x \in G$ .  $\Psi(x)(gh) = (gh)(x) = g(x)h(x)$ , par définition du produit dans  $\mathcal{G}$ , donc  $\Psi(x)(gh) = \Psi(x)(g).\Psi(x)(h)$ , ce qui prouve que  $\Psi(x)$  est un morphisme de  $\mathcal{G}$  dans  $\mathbb{C}^*$ . Ainsi,  $\Psi(x)$  est un élément du dual de  $\mathcal{G}$ , c'est-à-dire du bidual de  $G$ , que l'on notera  $\widehat{G}$ .

Ceci prouve que  $\Psi$  est une application de  $G$  dans  $\widehat{G}$ .

◇ Soit  $x, y \in G$ . Soit  $g \in \mathcal{G}$ .

$\Psi(xy)(g) = g(xy) = g(x)g(y) = \Psi(x)(g).\Psi(y)(g) = (\Psi(x).\Psi(y))(g)$ , par définition du produit dans  $\widehat{G} = \text{Hom}(\mathcal{G}, \mathbb{C}^*)$ , donc  $\Psi(xy) = \Psi(x).\Psi(y)$ , ce qui prouve que  $\Psi$  est un morphisme de groupes.

◇ Soit  $x \in \text{Ker}(\Psi)$ .  $\Psi(x) = 1_{\widehat{G}}$ , donc pour tout  $g \in \mathcal{G}$ ,  $1 = \Psi(x)(g) = g(x)$ .

Admettons temporairement que  $x \neq 1 \implies [\exists g \in \mathcal{G}, g(x) \neq 1]$ . Alors par contraposée, on a  $x = 1$ , donc  $\text{Ker}(\Psi) = \{1\}$  ce qui prouve que  $\Psi$  est injective.

De plus, d'après la question 15 appliquée aux groupes abéliens finis  $G$  et  $\mathcal{G}$ ,  $|G| = |\mathcal{G}| = |\widehat{G}|$ , donc  $\Psi$  est un isomorphisme de  $G$  dans son bidual.

Il reste cependant à démontrer la propriété admise temporairement.

◇ Premier cas : supposons que  $G$  est le groupe  $\mathbb{Z}/n\mathbb{Z}$ , où  $n \in \mathbb{N}^*$ . On a vu en question 13 que l'application 
$$g : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{C}^* \\ \bar{k} & \longmapsto & e^{\frac{2i\pi k}{n}} \end{array}$$
 est un élément de  $\mathcal{G}$ . De plus, si  $g(\bar{k}) = 1$ ,

alors  $\frac{2\pi k}{n} \equiv 0 [2\pi]$ , donc  $k \equiv 0 [n]$ , puis  $\bar{k} = 0$ . Ainsi, par contraposée, si  $x \in \mathbb{Z}/n\mathbb{Z}$  avec  $x \neq 0$ , alors  $g(x) \neq 1$ , donc la propriété est démontrée lorsque  $G$  est le groupe  $\mathbb{Z}/n\mathbb{Z}$ .

◇ Second cas : Supposons qu'il existe  $q \in \mathbb{N}^*$  et  $n_1, \dots, n_q \in \mathbb{N}^*$  tels que  $G = \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_q\mathbb{Z}$ .

Soit  $x = (\bar{k}_1, \dots, \bar{k}_q) \in G$  tel que  $x \neq 0$ . Il existe  $j \in \mathbb{N}_q$  tel que  $\bar{k}_j \neq 0$ .

Notons alors 
$$g : \begin{array}{ccc} G & \longrightarrow & \mathbb{C}^* \\ (\bar{h}_1, \dots, \bar{h}_q) & \longmapsto & e^{\frac{2i\pi h_j}{n_j}} \end{array}$$
. Il s'agit de la composée du morphisme

utilisé au premier cas avec la  $j$ -ème projection  $\begin{array}{ccc} G & \longrightarrow & G_j \\ (\bar{h}_1, \dots, \bar{h}_q) & \longmapsto & \bar{h}_j \end{array}$ , donc  $g \in \mathcal{G}$ , en tant que composé de morphismes de groupes. De plus, pour les mêmes raisons qu'au premier cas,  $g(x) \neq 1$ .

◇ Dernier cas : cas général.  $(G, \cdot)$  étant un groupe abélien, d'après l'énoncé, il existe un isomorphisme  $f$  de  $G$  dans un groupe de la forme  $G' = \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_q\mathbb{Z}$ .

Soit  $x \in G$  avec  $x \neq 1$ .  $f$  étant injective,  $f(x) \neq 0$ , donc d'après le second cas, il existe  $g \in \text{Hom}(G', \mathbb{C}^*)$  tel que  $g(f(x)) \neq 1$ . Alors  $g \circ f$  est un élément du dual de  $G$  tel que  $(g \circ f)(x) \neq 1$ .