DM 23 : Un corrigé

Partie I : Groupes quotients

1°)

— Soit $a \in G$. $a - a = 0 \in H$ car H est un sous-groupe, donc $a \ R_H \ a$. Ainsi, R_H est réflexive.

— Soit $x, y \in G$ tels que $x \ R_H \ y$. Ainsi $y - x \in H$, mais H étant un sous-groupe il est stable par passage à l'opposé, donc $x - y \in H$ et $y \ R_H \ x$. Ainsi R_H est symétrique.

— Soit $x, y, z \in G$ tels que $x \ R_H \ y$ et $y \ R_H \ z$. Ainsi, $y - x \in H$ et $z - y \in H$, or H est stable pour l'addition, donc $z - x = (y - x) + (z - y) \in H$ puis $x \ R_H \ z$. Ainsi R_H est transitive.

En conclusion, R_H est bien une relation d'équivalence.

Soit $a \in G$. Pour tout $x \in G$, $x \in \overline{a} \iff a \ R_H \ x \iff \exists h \in H, \ \ x - a = h$, donc $x \in \overline{a} \iff \exists h \in H, \ \ x = a + h$. Ainsi, $\overline{a} = \{a + h \ / \ h \in H\} = a + H$.

2°)

— Commençons par montrer que la relation $\overline{a} + \overline{b} = \overline{a + b}$ définit convenablement une addition sur G/H, c'est-à-dire que $\overline{a + b}$ ne dépend que de $\overline{a}$ et $\overline{b}$ et non de (a, b).
En effet, si $a, b, a', b' \in G$ vérifient $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$, alors $a' - a, b' - b \in H$ donc $(a + b) - (a' + b') = (a - a') + (b - b') \in H$ puis $\overline{a + b} = \overline{a' + b'}$.

— Montrons ensuite que cette addition confère à G/H une structure de groupe.
  — Pour tout $\overline{a}, \overline{b} \in G/H$, $\overline{a} + \overline{b} \in G/H$, donc il s'agit bien d'une loi interne.
  — Pour tout $\overline{a}, \overline{b}, \overline{c} \in G/H$, $(\overline{a} + \overline{b}) + \overline{c} = \overline{a + b} + \overline{c} = \overline{(a + b) + c}$, or l'addition dans G est associative, donc $(\overline{a} + \overline{b}) + \overline{c} = \overline{a + (b + c)} = \overline{a} + (\overline{b} + \overline{c})$. Ceci prouve l'associativité.
  — Pour tout $\overline{a}, \overline{b} \in G/H$, $\overline{a} + \overline{b} = \overline{a + b} = \overline{b + a} = \overline{b} + \overline{a}$, ce qui prouve la commutativité.
  — Pour tout $a \in G$, $\overline{a} + \overline{0} = \overline{a + 0} = \overline{a}$, donc $\overline{0}$ est l'élément neutre.
  — Pour tout $a \in G$, $\overline{a} + \overline{-a} = \overline{a + (-a)} = \overline{0}$, donc $\overline{a}$ possède un symétrique, et $-\overline{a} = \overline{-a}$.

  En conclusion, G/H est bien un groupe abélien.

— Notons φ l'application de G dans G/H définie par : pour tout $a \in G$, $\varphi(a) = \overline{a}$. La définition de l'addition sur G/H dit que φ est un morphisme de groupes, donc d'après le cours, pour tout $n \in \mathbb{Z}$ et $a \in G$, $\varphi(na) = n\varphi(a)$, c'est-à-dire que $\overline{na} = n\overline{a}$.

— D'après le cours, les sous-groupes de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$, où $n \in \mathbb{N}$, donc les groupes de la forme $\mathbb{Z}/H$ sont les groupes (connus) $\mathbb{Z}/n\mathbb{Z}$, avec $n \in \mathbb{N}$.

3°) D'après le cours, les classes d'équivalence de R_H constituent une partition de G, donc $G = \bigsqcup_{x \in G/H} x$ puis en passant au cardinal, $|G| = \sum_{x \in G/H} |x|$.

Soit $x \in G/H$: il existe $a \in G$ tel que $x = \overline{a} = a+H$, or l'application $f : x \longmapsto a+x$ est une bijection sur G (de bijection réciproque $x \longmapsto x-a$), donc $|H| = |f(H)| = |\overline{a}| = |x|$.

On en déduit que $|G| = \sum_{x \in G/H} |H| = |H| \times |G/H|$.

Partie II : Quelques définitions

4°)

— Par hypothèse, il existe $A \subset G$ et $B \subset H$ tels que A et B sont finis, $G = \mathrm{Gr}(A)$ et $H = \mathrm{Gr}(B)$. Alors d'après le cours, $G = \mathrm{Gr}(A) = \left\{ \sum_{a \in A} n_a a \;/\; (n_a)_{a \in A} \in \mathbb{Z}^A \right\}$

et $H = \mathrm{Gr}(B) = \left\{ \sum_{b \in B} n_b b \;/\; (n_b)_{b \in B} \in \mathbb{Z}^B \right\}$.

Soit $(g,h) \in G \times H$.

Il existe $(n_a)_{a \in A} \in \mathbb{Z}^A$ et $(n_b)_{b \in B} \in \mathbb{Z}^B$ telles que $g = \sum_{a \in A} n_a a$ et $h = \sum_{b \in B} n_b b$.

Alors $(g,h) = (g,0) + (0,h) = \sum_{a \in A} n_a(a,0) + \sum_{b \in B} n_b(0,b)$,

donc $(g,h) \in \mathrm{Gr}[(A \times \{0\}) \cup (\{0\} \times B)]$.

Ainsi, $G \times H \subset \mathrm{Gr}[(A \times \{0\}) \cup (\{0\} \times B)]$ et l'inclusion réciproque est évidente car $[(A \times \{0\}) \cup (\{0\} \times B)] \subset G \times H$.

Ceci prouve que $G \times H$ est engendré par $(A \times \{0\}) \cup (\{0\} \times B)$. C'est une partie finie, donc $G \times H$ est bien de type fini.

— Par récurrence, on en déduit que si $G_1, \dots, G_p$ sont p groupes abéliens de types finis, alors $G_1 \times \cdots \times G_p$ est encore de type fini. Or $\mathbb{Z} = \mathrm{Gr}(\{1\})$ et $\mathbb{Z}/n\mathbb{Z} = \mathrm{Gr}(\{\overline{1}\})$ sont monogènes donc de types finis, donc pour tout $k, \ell \in \mathbb{N}^*$, pour tout $(d_i)_{1 \le i \le \ell} \in \mathbb{N}^{*\ell}$, $\mathbb{Z}^k \times (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_\ell\mathbb{Z})$ est un groupe abélien de type fini.

5°)

— $\mathbb{Z}/n\mathbb{Z}$ est fini, donc pour tout $x \in \mathbb{Z}/n\mathbb{Z}$, $\mathrm{Gr}(x)$ est fini : $\mathbb{Z}/n\mathbb{Z}$ est de torsion. Il n'est pas sans torsion, sauf lorsque $n = 1$, auquel cas $\mathbb{Z}/1\mathbb{Z} = \{0\}$.

— Pour tout $n \in \mathbb{Z}^*$, pour tout $m \in \mathbb{N}^*$, $nm \neq 0$, donc n est d'ordre infini : $\mathbb{Z}$ est sans torsion.

— $n(0,\overline{1}) = (0,\overline{n}) = 0$, donc $\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$ n'est pas sans torsion, sauf lorsque $n = 1$. Pour tout $p \in \mathbb{N}^*$, $p(1,0) = (p,0) \neq 0$, donc $\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$ n'est pas de torsion.

- Dans le groupe $(\mathbb{C}^*, \times)$, $i^2 = 1$, donc ce groupe n'est pas sans torsion. Cependant, pour tout $p \in \mathbb{N}^*$, $2^p \neq 1$, donc il n'est pas de torsion.
- Soit $x \in \mathbb{Q}/\mathbb{Z}$. Il existe $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ tels que $x = \overline{(\frac{p}{q})}$. Alors $qx = \overline{p} = 0$ car $p \in \mathbb{Z}$, donc $\mathbb{Q}/\mathbb{Z}$ est de torsion.

6°) Si G est de cardinal fini, alors $G = \mathrm{Gr}(G)$, donc G est de type fini. De plus pour tout $x \in G$, $\mathrm{Gr}(x)$ est fini, donc G est de torsion.
Réciproquement, supposons que G est de type fini et de torsion.
Il existe donc une partie finie A de G telle que $G = \mathrm{Gr}(A)$. Alors, pour tout $g \in G$, il existe $(n_a)_{a \in A} \in \mathbb{Z}^A$ telle que $g = \displaystyle\sum_{a \in A} n_a a$, mais pour tout $a \in A$, a est d'ordre fini, donc en notant $o(a)$ son ordre, pour tout $n \in \mathbb{Z}$, $na = ra$, où r est le reste de la division euclidienne de n par $o(a)$. Ainsi, $G \subset \left\{ \displaystyle\sum_{a \in A} n_a a \;/\; \forall a \in A,\ n_a \in \{0, \ldots, o(a) - 1\} \right\}$.
A étant fini, ce dernier ensemble est fini (son cardinal est inférieur à $\displaystyle\prod_{a \in A} o(a)$), donc G est fini.

Partie III : Groupes abéliens finis

7°) $o(x)o(y)(x + y) = o(y)(o(x)x) + o(x)(o(y)y) = 0 + 0 = 0$,
donc $o(x + y)$ divise $o(x)o(y)$.
Soit $n \in \mathbb{N}^*$ tel que $n(x + y) = 0$. Alors $nx = -ny$, donc $no(y)x = -no(y)y = 0$, puis $o(x) \mid no(y)$, mais $o(x) \wedge o(y) = 1$, donc d'après le théorème de Gauss, $o(x) \mid n$. De même, $o(y) \mid n$, or $o(x)$ et $o(y)$ sont premiers entre eux, donc $o(x)o(y) \mid n$. En particulier, lorsque $n = o(x + y)$, on a montré que $o(x)o(y)$ divise $o(x + y)$ et que $o(x + y)$ divise $o(x)o(y)$, donc ils sont égaux.

8°) Écrivons les décompositions de $o(x)$ et $o(y)$ en produit de nombres premiers : $o(x) = \displaystyle\prod_{p \in \mathbb{P}} p^{v_{o(x)}(p)}$ et $o(y) = \displaystyle\prod_{p \in \mathbb{P}} p^{v_{o(y)}(p)}$.
Posons $h = \displaystyle\prod_{\substack{p \in \mathbb{P} \\ v_{o(x)}(p) > v_{o(y)}(p)}} p^{v_{o(x)}(p)}$ et $k = \displaystyle\prod_{\substack{p \in \mathbb{P} \\ v_{o(x)}(p) \leq v_{o(y)}(p)}} p^{v_{o(y)}(p)}$.
Ainsi, h et k sont premiers entre eux et $hk = \displaystyle\prod_{p \in \mathbb{P}} p^{\max(v_{o(x)}(p), v_{o(y)}(p))} = o(x) \vee o(y)$.
Il existe $a, b \in \mathbb{N}^*$ tels que $o(x) = ah$ et $o(y) = bk$.
Pour tout $n \in \mathbb{Z}$, $n(ax) = 0 \iff (na)x = 0 \iff o(x) \mid na \iff h \mid n$, donc $h = o(ax)$.
De même, $k = o(by)$, donc d'après la question précédente, $o(ax+by) = hk = o(x) \vee o(y)$, ce qu'il fallait démontrer.

9°) En utilisant l'associativité du PPCM, on montre par récurrence sur n, que pour tout $n \in \mathbb{N}^*$, pour tout $x_1, \ldots, x_n \in G$, il existe $z \in G$ tel que l'ordre de z est égal au PPCM des ordres de $x_1, \ldots, x_n$.

Or G est fini, donc il existe $x_0 \in G$ tel que l'ordre de x_0 est égal au PPCM des ordres des éléments de G.
Soit $x \in G$: alors $o(x_0), o(x) \in \mathbb{N}^*$ et $o(x) \mid o(x_0)$, donc $o(x_0) \geq o(x)$. Ainsi, x_0 est d'ordre maximal et, pour tout $x \in G$, l'ordre de x divise l'ordre de x_0.

10°) On démontre cette propriété par récurrence forte sur $|G|$: soit $n \in \mathbb{N}^*$. Notons $R(n)$ la propriété suivante : pour tout groupe abélien G de cardinal n, il existe $\ell \in \mathbb{N}^*$ et $d_1, \ldots, d_\ell \in \mathbb{N}^*$ tels que, pour tout $i \in \{1, \ldots, \ell - 1\}$, d_{i+1} divise d_i, et tels que G est isomorphe à $(\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_\ell\mathbb{Z})$.
Lorsque $n = 1$, si G est de cardinal 1, alors $G = \{0\}$, donc il est isomorphe à $\mathbb{Z}/\mathbb{Z}$, ce qui prouve $R(1)$, avec $\ell = d_1 = 1$.
Supposons que $n \geq 2$ et que $R(k)$ est vraie pour tout $k \in \{1, \ldots, n-1\}$. Montrons $R(n)$. Soit G un groupe abélien de cardinal n. D'après la question précédente, il existe $x \in G$ d'ordre maximal. Notons d_1 l'ordre de x et $H = \mathrm{Gr}(x)$. D'après le cours, il existe un isomorphisme f de H dans $\mathbb{Z}/d_1\mathbb{Z}$.
D'après la question 3, $|G/H| = \dfrac{|G|}{|H|} < |G|$ car $d_1 \geq 2$: sinon, $d_1 = 1$, donc tous les éléments de G sont d'ordre 1, c'est-à-dire sont nuls et $G = \{0\}$, ce qui est faux car $n \geq 2$.
On peut donc appliquer l'hypothèse de récurrence au groupe abélien G/H : il existe $\ell \geq 2$ et $d_2, \ldots, d_l \in \mathbb{N}^*$ tels que, pour tout $i \in \{2, \ldots, \ell - 1\}$, d_{i+1} divise d_i, et tels qu'il existe un isomorphisme g de G/H dans $(\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_\ell\mathbb{Z})$.
D'après l'énoncé, il existe un isomorphisme h de G dans $H \times (G/H)$.
Pour tout $(y, z) \in H \times (G/H)$, notons $\varphi(y, z) = (f(y), g(z))$.
On a bien $\varphi((y, z) + (y', z')) = \varphi(y, z) + \varphi(y', z')$ pour tout $(y, z) \in H \times (G/H)$ et $(y', z') \in H \times (G/H)$, donc φ est un morphisme de $H \times (G/H)$ dans
$(\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_\ell\mathbb{Z})$.
Si $\varphi(y, z) = 0$, alors $f(y) = 0$ et $g(z) = 0$, mais f et g sont injectifs, donc $(y, z) = 0$. Ainsi, φ est injectif.
Pour tout $y' \in \mathbb{Z}/d_1\mathbb{Z}$ et $z' \in (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_\ell\mathbb{Z})$, f et g étant surjectifs, il existe $(y, z) \in H \times (G/H)$ tel que $y' = f(y)$ et $z' = g(z)$, donc $(y', z') = \varphi(y, z)$. Ainsi, φ est un isomorphisme de $H \times (G/H)$ dans $(\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_\ell\mathbb{Z})$. Par composition, $\Psi = \varphi \circ h$ est un isomorphisme de G dans $(\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_\ell\mathbb{Z})$.
Il reste à montrer que d_2 divise d_1 : Notons d l'ordre de $y = \Psi^{-1}(0, \overline{1}, 0, \ldots, 0)$ dans G. D'après la question précédente, d divise d_1.
De plus, $dy = 0$, donc $0 = \Psi(dy) = d(0, \overline{1}, 0, \ldots, 0) = (0, \overline{d}, 0, \ldots, 0)$. Ainsi, dans $\mathbb{Z}/d_2\mathbb{Z}$, $\overline{d} = 0$, donc d_2 divise d. Ceci prouve que d_2 divise d_1, d'où $R(n)$.
La question est démontrée d'après le principe de récurrence forte.

11°)

- Soit $(K,f) \in A$. Alors $K \subset K$ et $f|_K = f$, donc $(K,f) \preceq (K,f)$, ce qui montre que $\preceq$ est réflexive.
- Soit $(K,f),(K',f') \in A$ tels que $(K,f) \preceq (K',f')$ et $(K',f') \preceq (K,f)$. Ainsi, $K \subset K'$ et $K' \subset K$, donc $K = K'$. De plus, pour tout $x \in K$, $f(x) = f|_K(x) = f'(x)$, donc $f = f'$. Ainsi, $\preceq$ est antisymétrique.
- Soit $(K,f),(K',f'),(K'',f'') \in A$ tels que $(K,f) \preceq (K',f')$ et $(K',f') \preceq (K'',f'')$. $K \subset K'$ et $K' \subset K''$, donc $K \subset K''$. De plus, pour tout $x \in K$, $f''(x) = f''|_{K'}(x) = f'(x) = f'|_K(x) = f(x)$, donc $f''|_K = f$. Ainsi, $(K,f) \preceq (K'',f'')$. Ainsi, $\preceq$ est transitive.
  En conclusion, $\preceq$ est bien une relation d'ordre.
- Notons $B = \{(K,f) \in A \ / \ H \subset K \text{ et } f|_H = Id_H\}$.
  G étant fini, il ne possède qu'un nombre fini de sous-groupes et, pour chacun des sous-groupes K de G, lui-même fini, il n'existe qu'un nombre fini d'applications de K dans H, donc B est fini. À ce titre, il possède nécessairement un élément maximal. En effet, dans le cas contraire, pour tout $(K,f) \in A$, il existerait $(K',f') \in A$ tel que $(K,f) \prec (K',f')$, ainsi partant d'un élément (K_0,f_0) de A (A est non vide car $(H, Id_H) \in A$), on pourrait construire une suite $((K_n,f_n))_{n\in\mathbb{N}}$ strictement croissante d'éléments de A : c'est en contradiction avec la finitude de A.

12°)

$\diamond$ Notons d l'ordre de x_0 et $\omega = e^{2i\frac{\pi}{d}}$.
Pour tout $kx_0 \in H = \mathrm{Gr}(x_0)$, où $k \in \mathbb{Z}$, posons $g(kx_0) = \omega^k$.
g est correctement défini car si $kx_0 = hx_0$ avec $k, h \in \mathbb{Z}$, alors $k - h$ est un multiple de d, donc $\omega^k = \omega^h$.
On a clairement $g(kx_0 + hx_0) = g(kx_0)g(hx_0)$, donc g est un morphisme de groupes.
Si $g(kx_0) = 1$, alors $\omega^k = 1$, donc k est un multiple de d et $kx_0 = 0$. Ainsi $\mathrm{Ker}(g) = \{0\}$, ce qui prouve que g est injectif.

$\diamond$ $g \circ f$ est un morphisme de K dans $\mathbb{U}$
et $K' = \mathrm{Gr}(K \cup \{y_0\}) = \{x + ny_0 / x \in K \text{ et } n \in \mathbb{Z}\}$ (en effet, on peut vérifier que ce dernier ensemble est non vide et stable par différence, donc c'est un sous-groupe qui contient $K \cup \{y_0\}$ et tout sous-groupe contenant $K \cup \{y_0\}$ contient $\{x + ny_0 / n \in \mathbb{Z}\}$).
Ainsi, pour prolonger $g \circ f$ en un morphisme Ψ défini sur K', il faut choisir correctement $\Psi(y_0)$ dans $\mathbb{U}$. Posons a priori $\Psi(y_0) = e^{i\alpha}$ où $\alpha \in \mathbb{R}$.
On souhaite poser, pour tout $x \in K$ et $n \in \mathbb{Z}$, $\Psi(x + ny_0) = g \circ f(x)e^{in\alpha}$, mais il faut s'assurer que cette dernière égalité définit correctement une fonction, c'est-à-dire que la quantité $g \circ f(x)e^{in\alpha}$ ne dépend que de $x + ny_0$, ou encore que
(C) : $\forall x, x' \in K, \ \forall n, n' \in \mathbb{Z}, \ [x + ny_0 = x' + n'y_0 \Longrightarrow g \circ f(x)e^{in\alpha} = g \circ f(x')e^{in'\alpha}]$.
$(C) \iff \forall x, x' \in K, \ \forall n, n' \in \mathbb{Z}, \ [(n - n')y_0 = x' - x \Longrightarrow g \circ f(x - x') = e^{i(n'-n)\alpha}]$
$\iff \forall x \in K, \ \forall n \in \mathbb{Z}, \ [ny_0 = x \Longrightarrow g \circ f(x) = e^{in\alpha}]$
Notons b l'ordre de $\overline{y_0}$ dans K'/K :
pour tout $n \in \mathbb{Z}$, $ny_0 \in K \iff n\overline{y_0} = 0 \iff b \mid n$.

Soit $x \in K$ et $n \in \mathbb{Z}$ tels que $ny_0 = x$. Ainsi $b \mid n$, donc il existe $c \in \mathbb{Z}$ tel que $n = bc$. Ainsi, $x = c(by_0)$. $by_0 \in K$, donc $f(by_0)$ est défini et appartient à H. Ainsi, il existe $\beta \in \{0, \dots, d-1\}$ tel que $f(by_0) = \beta x_0$. Alors $g \circ f(by_0) = \omega^\beta$ puis $g \circ f(x) = \omega^{\beta c}$. Ainsi,
$g \circ f(x) = e^{in\alpha} \Longleftrightarrow e^{2i\pi \frac{\beta c}{d}} = e^{in\alpha} = e^{ibc\alpha} \Longleftarrow 2\pi \frac{\beta}{d} = b\alpha$.
On pose donc $\alpha = 2\pi \frac{\beta}{db}$ (ainsi α ne dépend que de x_0, y_0 et f).
Pour tout $(x, n) \in K \times \mathbb{Z}$, on pose $\Psi(x + ny_0) = g \circ f(x) e^{in\alpha}$.
La condition (C) est alors vérifiée, donc Ψ est une application correctement définie de K' dans H.
On a clairement, pour tout $x, x' \in K$ et $n, n' \in \mathbb{Z}$,
$\Psi((x + ny_0) + (x' + n'y_0)) = g \circ f(x).g \circ f(x') e^{in\alpha} e^{in'\alpha} = \Psi(x + ny_0)\Psi(x' + n'y_0)$, donc Ψ est un morphisme de K' dans $\mathbb{U}$, qui prolonge $g \circ f$ sur K'.

$\diamond$ Soit $x \in K'$: par construction de x_0, l'ordre de x_0 est un multiple de l'ordre de x. Ainsi, $dx = 0$, puis $1 = \Psi(dx) = \Psi(x)^d$, donc $\Psi(x) \in \mathbb{U}_d = g(H)$. Ceci démontre que Ψ est à valeurs dans $U_d = g(H)$, or $g|^{g(H)}$ est une bijection, donc $(g|^{g(H)})^{-1} \circ \Psi$ réalise un morphisme de K' dans H. De plus, si $x \in H$, $\Psi(x) = g \circ f(x) = g(x)$, donc $(g|^{g(H)})^{-1} \circ \Psi(x) = x$. On en déduit que le couple $(K', (g|^{g(H)})^{-1} \circ \Psi)$ est un élément de B, strictement supérieur au couple (K, f). Ceci contredit la maximalité de (K, f) dans B. C'est absurde.

13°) Il existe donc un morphisme f de G dans H tel que $f|_H = Id_H$.
Pour tout $x \in G$, posons $\varphi(x) = (f(x), \overline{x}) \in H \times G/H$.
φ est un morphisme de G dans $H \times G/H$ car, pour tout $x, y \in G$,
$\varphi(x + y) = (f(x) + f(y), \overline{x} + \overline{y}) = \varphi(x) + \varphi(y)$.
Soit $x \in \mathrm{Ker}(\varphi)$: $(f(x), \overline{x}) = 0$, donc $\overline{x} = 0$ et $f(x) = 0$, ainsi $x \in H$ puis
$0 = f(x) = f|_H(x) = x$. Ceci démontre que $\mathrm{Ker}(\varphi) = \{0\}$, donc φ est injective.
De plus, $|G| = |H| \times |G/H|$, donc f est une bijection. Il s'agit bien d'un isomorphisme entre G et $H \times G/H$.

Partie IV : Sommes directes

14°) **a)** Soit $x \in H_1 + H_2$. Supposons qu'il existe $h_1, h_1' \in H_1$ et $h_2, h_2' \in H_2$ tels que $x = h_1 + h_2 = h_1' + h_2'$.
Il existe $n_1, n_1', n_2, n_2' \in \mathbb{Z}$ tels que $h_1 = n_1(2, 1)$, $h_1' = n_1'(2, 1)$, $h_2 = n_2(0, 2)$ et $h_2' = n_2'(0, 2)$.
Ainsi $x = (2n_1, n_1 + 2n_2) = (2n_1', n_1' + 2n_2')$, donc $n_1 = n_1'$ puis $n_2 = n_2'$. On en déduit que $h_1 = h_1'$ et $h_2 = h_2'$, donc la somme $H_1 + H_2$ est directe.

b) Supposons d'abord que $a \neq 0$ et $b \neq 0$.
On peut écrire $0 = 0.a + 0.b = b.a - a.b$, donc la décomposition de 0 dans la somme $a\mathbb{Z} + b\mathbb{Z}$ n'est pas unique. Ceci prouve que cette somme n'est pas directe.
Supposons maintenant que $a = 0$: Soit $x \in a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z}$. Si $x = h_1 + h_2 = h_1' + h_2'$ avec $h_1, h_1' \in a\mathbb{Z} = \{0\}$ et $h_2, h_2' \in b\mathbb{Z}$, alors $h_1 = h_1' = 0$ puis $h_2 = h_2'$, donc dans ce cas, la somme est directe. C'est encore vrai lorsque $b = 0$.

15°) **a)** $H_1 + H_2$ est un groupe, car il contient 0, donc il est non vide, et si $h_1 + h_2, h'_1 + h'_2 \in H_1 + H_2$, alors $(h_1 + h_2) - (h'_1 + h'_2) = (h_1 - h'_1) + (h_2 - h'_2) \in H_1 + H_2$.
De plus $H_1 + H_2$ contient $H_1 \cup H_2$ (car $0 \in H_1 \cap H_2$).
Enfin, si H est un sous-groupe de G qui contient $H_1 \cup H_2$, alors, H étant stable pour l'addition, il contient $H_1 + H_2$.
En conclusion, $H_1 + H_2$ est le plus petit sous-groupe de G contenant $H_1 \cup H_2$, ce qu'il fallait démontrer.

b) Pour tout $(h_1, h_2) \in H_1 \times H_2$, notons $\varphi(h_1, h_2) = h_1 + h_2$. Ainsi, φ est une application de $H_1 \times H_2$ dans $H_1 + H_2$. Cette dernière somme étant directe, tout élément de $H_1 + H_2$ possède un unique antécédent par φ, donc φ est une bijection. De plus, φ est un morphisme car on vérifie que $\varphi((h_1, h_2) + (h'_1, h'_2)) = \varphi((h_1, h_2)) + \varphi((h'_1, h'_2))$.

16°)
◇ Soit $x \in (H_1 + H_2) + H_3$: il existe $h \in H_1 + H_2$ et $h_3 \in H_3$ tel que $x = h + h_3$.
De plus il existe $h_1 \in H_1$ et $h_2 \in H_2$ tels que $h = h_1 + h_2$.
Ainsi, l'addition dans G étant associative,
$x = (h_1 + h_2) + h_3 = h_1 + (h_2 + h_3) \in H_1 + (H_2 + H_3)$.
Ceci démontre que $(H_1 + H_2) + H_3 \subset H_1 + (H_2 + H_3)$. L'inclusion réciproque se démontre de la même façon.
◇ On suppose que $H_1 \oplus H_2$ est directe, ainsi que $(H_1 \oplus H_2) \oplus H_3$.
- Soit $h_2 + h_3 = h'_2 + h'_3 \in H_2 + H_3$. Alors $(0 + h_2) + h_3 = (0 + h'_2) + h'_3$ avec $(0 + h_2), (0 + h'_2) \in H_1 + H_2$ et $h_3, h'_3 \in H_3$, or la somme entre $H_1 + H_2$ et H_3 est directe, donc $0 + h_2 = 0 + h'_2$ et $h_3 = h'_3$. Ceci démontre que la somme $H_2 + H_3$ est directe.
- Soit $h_1 + h = h'_1 + h' \in H_1 + (H_2 \oplus H_3)$. Il existe $h_2, h'_2 \in H_2$ et $h_3, h'_3 \in H_3$ tels que $h = h_2 + h_3$ et $h' = h'_2 + h'_3$.
  On peut écrire $(h_1 + h_2) + h_3 = (h'_1 + h'_2) + h'_3$, or la somme entre $H_1 + H_2$ et H_3 est directe, donc $h_1 + h_2 = h'_1 + h'_2$ et $h_3 = h'_3$. De plus la somme entre H_1 et H_2 est directe, donc $h_1 = h'_1$ et $h_2 = h'_2$. Ainsi $h_1 = h'_1$ et $h = h'$, ce qui montre que la somme entre H_1 et $H_2 \oplus H_3$ est directe.

Partie V : Groupes abéliens de rangs finis

17°) Supposons que $B = (x_i)_{i \in I}$ est une base de G.
Soit $x \in G \setminus \{0\}$. Soit $n \in \mathbb{N}^*$. Il existe $(n_i)_{i \in I} \in \mathbb{Z}^{(I)}$ telle que $x = \sum_{i \in I} n_i x_i$. Or $x \neq 0$, donc il existe $i_0 \in I$ tel que $n_{i_0} \neq 0$.
Alors $nx = \sum_{i \in I} n n_i x_i$ et $n n_{i_0} \neq 0$, donc $nx \neq 0$: sinon $\sum_{i \in I} n n_i x_i$ et $\sum_{i \in I} 0.x_i$ serait deux décompositions différentes de 0 selon la base B. On a ainsi montré que pour tout $x \in G \setminus \{0\}$ et $n \in \mathbb{N}^*$, $nx \neq 0$, donc G est sans torsion.

18°) **a)** Pour tout $j \in \{1,\dots,n\}$, il existe une partie finie $I_j \subset I$ et une famille $(n_{i,j})_{i\in I_j} \in \mathbb{Z}^{I_j}$ telle que $x_j = \sum_{i\in I_j} n_{i,j}e_i$.

Posons $K = \bigcup_{1\leq j\leq n} I_j$. Soit $i \in I$. Il existe $k_1,\dots,k_n \in \mathbb{Z}$ tels que $e_i = \sum_{j=1}^{n} k_j x_j$, donc $e_i = \sum_{j=1}^{n} k_j \sum_{i\in I_j} n_{i,j}e_i$. Ainsi, il existe $(m_k)_{k\in K} \in \mathbb{Z}^K$ tel que $e_i = \sum_{k\in K} m_k e_k$. Or $(e_i)_{i\in I}$ est une base, donc $i \in K$: sinon l'égalité précédente fournirait deux décompositions différentes de e_i dans la base $(e_j)_{j\in I}$. On a montré que $I \subset K$, or K est fini, donc I est fini.

b)

$\diamond$ $0 \in H$, donc H est non vide, et si $2x, 2y \in H$, alors $2x - 2y = 2(x-y) \in H$, donc H est bien un sous-groupe de G.

$\diamond$ Soit $x, y \in G$. Il existe $k_1,\dots,k_n,h_1,\dots,h_n \in \mathbb{Z}$ tels que $x = \sum_{i=1}^{n} k_i x_i$ et $y = \sum_{i=1}^{n} h_i x_i$. Alors, $x\ R_H\ y \Longleftrightarrow \sum_{i\in I}(h_i - k_i)x_i \in H \Longleftrightarrow \forall i \in I,\ \ h_i - k_i \in 2\mathbb{Z}$. En effet, "$\Longleftarrow$" est évidente et si $\sum_{i\in I}(h_i - k_i)x_i \in H$, il existe $y = \sum_{i\in I} m_i x_i$ tel que $\sum_{i\in I}(h_i - k_i)x_i = 2\sum_{i\in I} m_i x_i$, or $(x_i)_{1\leq i\leq n}$ est une base, donc pour tout $i \in I$, $h_i - k_i = 2m_i \in 2\mathbb{Z}$.

On en déduit que $G/H = \left\{\overline{\sum_{i=1}^{n} \varepsilon_i x_i}\ /\ \forall i \in I,\ \ \varepsilon_i \in \{0,1\}\right\}$ et que lorsque $(\varepsilon_i)_{1\leq i\leq n}, (\varepsilon'_i)_{1\leq i\leq n} \in \{0,1\}^n$ avec $(\varepsilon_i)_{1\leq i\leq n} \neq (\varepsilon'_i)_{1\leq i\leq n}$, alors $\overline{\sum_{i=1}^{n} \varepsilon_i x_i} \neq \overline{\sum_{i=1}^{n} \varepsilon'_i x_i}$.

Ceci démontre que $|G/H| = 2^n$.

$\diamond$ Si $(y_1,\dots,y_p)$ est une autre base de G (nécessairement finie), alors G/H est aussi de cardinal 2^p, donc $p = n$.

19°) **a)** Soit X une partie génératrice finie de G.

Posons $N = \left\{\sum_{x\in X} |n_x|\ /\ (n_x)_{x\in X} \in \mathbb{Z}^X \setminus \{0\} \text{ et } \sum_{x\in X} n_x x = 0\right\}$.

Par hypothèse, X n'est pas une base de G, donc il existe $g \in G$ tel que g possède deux décompositions différentes selon la famille X : $g = \sum_{x\in X} k_x x = \sum_{x\in X} h_x x$ avec $(k_x)_{x\in X} \neq (h_x)_{x\in X}$. Ainsi, en posant pour tout $x \in X$, $n_x = k_x - h_x$, on a $(n_x)_{x\in X} \in \mathbb{Z}^X \setminus \{0\}$ et $\sum_{x\in X} n_x x = 0$. Ceci montre que N est non vide, or c'est une partie de $\mathbb{N}$, donc d'après le cours, N possède bien un minimum.

b) Notons M l'ensemble des cardinaux des parties finies génératrices de G. G étant

de type fini, M est non vide. Or M est une partie de $\mathbb{N}$, donc M possède bien un minimum, que l'on note n.
On note ensuite $K = \{m_X / |X| = n \wedge (X \text{ est génératrice de } G)\}$. K est encore une partie non vide de $\mathbb{N}$, donc elle possède un minimum, noté m_0. Alors il existe une partie génératrice X_0 de G de cardinal n tel que $m_{X_0} = m_0$.

c) Supposons qu'il existe $x_0 \in X_0$ tel que $|n_{x_0}| = 1$. Alors $x_0 = \varepsilon \sum_{x \in X_0 \setminus \{x_0\}} n_x x$ où $\varepsilon \in \{-1, 1\}$, donc $X \setminus \{x_0\}$ est génératrice de G, ce qui est absurde car $|X \setminus \{x_0\}| = n - 1$, ce qui contredit la minimalité de n.

d) $\{|n_x| \ / \ x \in X_0\} \cap \mathbb{N}^*$ est une partie non vide, car $(n_x)_{x \in X_0}$ est non nulle, donc elle possède un minimum : il existe $x_0 \in X_0$ tel que $n_{x_0} \neq 0$ et tel que, pour tout $x \in X_0$, $n_x = 0$ ou bien $|n_x| \geq |n_{x_0}|$.
Supposons que pour tout $y \in X_0$, $|n_{x_0}| \mid |n_y|$. Alors on peut écrire
$n_{x_0}\Big(x_0 + \sum_{x \in X_0 \setminus \{x_0\}} \frac{n_x}{n_{x_0}} x\Big) = 0$, car $\frac{n_x}{n_{x_0}} \in \mathbb{Z}$, or G est sans torsion,
donc $x_0 + \sum_{x \in X_0 \setminus \{x_0\}} \frac{n_x}{n_{x_0}} x = 0$, ce qui prouve à nouveau que $X \setminus \{x_0\}$ est génératrice de G, ce qui est absurde. On en déduit qu'il existe $y \in X_0$ tel que $|n_{x_0}|$ ne divise pas $|n_y|$.
En particulier, $n_y \neq 0$ et $|n_y| \neq |n_{x_0}|$, donc $0 < |n_{x_0}| < |n_y|$.

e) La division euclidienne de $|n_y|$ par $|n_{x_0}|$ s'écrit $|n_y| = q|n_{x_0}| + r$ avec $0 \leq r < |n_{x_0}|$.
De plus $r \neq 0$ car $|n_{x_0}|$ ne divise pas $|n_y|$.
Il existe $\varepsilon, \varepsilon' \in \{-1, 1\}$ tels que $n_y = \varepsilon q n_{x_0} + \varepsilon' r$, donc

$$\begin{aligned} 0 &= \sum_{z \in X_0} n_z z = n_{x_0} x_0 + (\varepsilon q n_{x_0} + \varepsilon' r) y + \sum_{z \in X_0 \setminus \{x_0, y\}} n_z z \\ &= n_{x_0}(x_0 + \varepsilon q y) + \varepsilon' r y + \sum_{z \in X_0 \setminus \{x_0, y\}} n_z z \ : \ (1). \end{aligned}$$

Notons $Y = (X_0 \setminus \{x_0\}) \cup \{x_0 + \varepsilon q y\}$. Pour tout $g \in G$, il existe $(m_z)_{z \in X_0} \in \mathbb{Z}^{X_0}$ tel que $g = \sum_{z \in X_0} m_z z$, donc $g = \sum_{z \in X_0 \setminus \{x_0, y\}} m_z z + n_{x_0}(x_0 + \varepsilon q y) + (n_y - \varepsilon q n_{x_0}) y$. Ainsi, Y est une famille génératrice de G de cardinal n. Donc $m_Y \geq m_{X_0}$, mais d'après la relation (1) et le fait que $r \neq 0$, $m_Y \leq |n_{x_0}| + |r| + \sum_{z \in X_0 \setminus \{x_0, y\}} |n_z| < |n_{x_0}| + |n_y| + \sum_{z \in X_0 \setminus \{x_0, y\}} |n_z| = m_{X_0}$.
C'est impossible.

20°)

◇ Supposons que G est un groupe sans torsion de type fini. D'après la question précédente, il est de rang fini, donc il existe une base de G de la forme $(e_1, \ldots, e_n)$.
Pour tout $(k_1, \ldots, k_n) \in \mathbb{Z}^n$, notons $\varphi(k_1, \ldots, k_n) = \sum_{i=1}^{n} k_i e_i$. On vérifie que φ est un morphisme du groupe $(\mathbb{Z}^n, +)$ dans G. Il est bijectif car $(e_1, \ldots, e_n)$ est une base de G.
Ainsi, il existe $n \in \mathbb{N}$ tel que G est isomorphe à $\mathbb{Z}^n$.

◇ Réciproquement, supposons qu'il existe un isomorphisme φ de $\mathbb{Z}^n$ dans G.

Pour tout $i \in \{1, \dots, n\}$, posons $e_i = \varphi((\delta_{i,j})_{1 \leq j \leq n})$.

Soit $g \in G$ et $(k_1, \dots, k_n) \in \mathbb{Z}^n$. Alors $g = \sum_{i=1}^{n} k_i e_i$ si et seulement si

$\varphi^{-1}(g) = \sum_{i=1}^{n} k_i \varphi^{-1}(e_i) = \sum_{i=1}^{n} k_i (\delta_{i,j})_{1 \leq j \leq n} = (k_1, \dots, k_n)$, donc $(e_1, \dots, e_n)$ est une base de G. Ainsi G est de rang fini, donc il est sans torsion et de type fini.

◇ On a montré que si G est isomorphe à $\mathbb{Z}^n$, alors G est de rang fini égal à n, donc d'après la question 18.b, n est unique.

Partie VI : Théorème de structure des groupes de types finis

21°) $1.0 = 0$, donc $0 \in T(G)$.

Soit $x, y \in T(G)$. Notons $o(x)$ et $o(y)$ les ordres de x et y.

Alors $o(x)o(y)(x - y) = o(y)(o(x)x) - o(x)(o(y)y) = 0$, donc $x - y \in T(G)$.

Ainsi, $T(G)$ est un sous-groupe de G.

22°)

◇ Soit $\overline{x} \in G/T(G)$. Supposons que $\overline{x}$ est d'ordre fini. Ainsi, il existe $n \in \mathbb{N}^*$ tel que $0 = n\overline{x} = \overline{nx}$, donc $nx \in T(G)$: c'est un élément de G d'ordre fini, donc il existe $m \in \mathbb{N}^*$ tel que $m(nx) = 0$. Ainsi x est aussi d'ordre fini, donc $x \in T(G)$ puis $\overline{x} = 0$. Ceci prouve que $G/T(G)$ est sans torsion.

◇ G est de type fini, donc il existe $(x_1, \dots, x_n)$ tel que $G = \text{Gr}(\{x_1, \dots, x_n\})$.

Soit $\overline{x} \in G/T(G)$. $x \in G$, donc il existe $(k_1, \dots, k_n) \in \mathbb{Z}^n$ tel que $x = \sum_{i=1}^{n} k_i x_i$. Alors $\overline{x} = \sum_{i=1}^{n} k_i \overline{x_i}$. Ceci prouve que $\{\overline{x_1}, \dots, \overline{x_n}\}$ est une partie génératrice de $G/T(G)$, donc $G/T(G)$ est de type fini.

23°)

◇ D'après la question 19, $G/T(G)$ est de rang fini, donc il existe $k \in \mathbb{N}$ et une base $(\overline{x_1}, \dots, \overline{x_k})$ de $G/T(G)$.

Posons $H = \text{Gr}(\{x_1, \dots, x_k\})$: H est un sous-groupe de G.

◇ Montrons que $G = H \oplus T(G)$:

— Soit $g \in G$. $\overline{g} \in G/T(G)$, donc il existe $(h_1, \dots, h_k) \in \mathbb{Z}^k$ tel que $\overline{g} = \sum_{i=1}^{k} h_i \overline{x_i}$.

  Ainsi, si l'on pose $t = g - \sum_{i=1}^{k} h_i x_i$, $\overline{t} = 0$, donc $t \in T(G)$.

  Alors $g = t + \sum_{i=1}^{k} h_i x_i \in T(G) + H$. Ceci démontre que $G = H + T(G)$.

— Supposons que $t + h = t' + h'$, avec $t, t' \in T(G)$ et $h, h' \in H$.

Alors $t - t' \in H \cap T(G)$. Ainsi, il existe $n \in \mathbb{N}^*$ tel que $n(h - h') = 0$. On en déduit que $n\overline{(h - h')} = 0$, mais $G/T(G)$ est sans torsion, donc $\overline{h - h'} = 0$. Si l'on pose $h = \sum_{i=1}^{k} h_i x_i$ et $h' = \sum_{i=1}^{k} h'_i x_i$, alors $\sum_{i=1}^{k} h_i \overline{x_i} = \sum_{i=1}^{k} h'_i \overline{x_i}$, or $(\overline{x_1}, \ldots, \overline{x_k})$ est une base de $G/T(G)$, donc $h_i = h'_i$ pour tout $i \in \{1, \ldots, k\}$. On en déduit que $h = h'$, puis que $t = t'$. Ceci prouve que $H + T(G)$ est une somme directe.

$\diamond$ D'après la question 15.b, il existe un isomorphisme φ de G dans $H \times T(G)$.

$\diamond$ Pour tout $(h_1, \ldots, h_k) \in \mathbb{Z}^k$, notons $\Psi(h_1, \ldots, h_k) = \sum_{i=1}^{k} h_i x_i$. Ainsi Ψ est un morphisme de $\mathbb{Z}^k$ dans H, clairement surjectif. De plus, si $(h_1, \ldots, h_k) \in \mathrm{Ker}(\Psi)$, $0 = \sum_{i=1}^{k} h_i \overline{x_i}$, donc à nouveau, $h_i = 0$ pour tout $i \in \{1, \ldots, k\}$. Ainsi $\mathrm{Ker}(\Psi) = \{0\}$ et Ψ est un isomorphisme de $\mathbb{Z}^k$ dans H.

$\diamond$ Notons F l'application de G dans $T(G)$ définie par : $F(h + t) = t$, pour tout $h \in H$ et $t \in T(G)$: F est bien définie car $G = H \oplus T(G)$.

On vérifie que F est un morphisme de groupes.

G est de type fini, donc il existe $(y_1, \ldots, y_p) \in G^p$ tel que $\{y_1, \ldots, y_p\}$ est génératrice de G.

Soit $t \in T(G)$. Alors $t \in G$, donc il existe $(h_1, \ldots, h_p) \in \mathbb{Z}^p$ tel que $t = \sum_{i=1}^{p} h_i y_i$. On en déduit que $t = F(t) = \sum_{i=1}^{p} h_i F(y_i)$, donc $\{F(y_1), \ldots, F(y_p)\}$ est génératrice de $T(G)$.

Ainsi, $T(G)$ est un groupe de torsion et de type fini. D'après la question 6, $T(G)$ est un groupe fini et d'après la question 10, il existe $\ell \in \mathbb{N}^*$ et $d_1, \ldots, d_\ell \in \mathbb{N}^*$ tels que, pour tout $i \in \{1, \ldots, \ell - 1\}$, d_{i+1} divise d_i et $T(G)$ est isomorphe à $(\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_\ell\mathbb{Z})$.

$\diamond$ En conclusion, il existe un isomorphisme F_1 de H dans $\mathbb{Z}^k$ et un isomorphisme F_2 de $T(G)$ dans $(\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_\ell\mathbb{Z})$.

Alors, en posant pour tout $g \in G$, $\varphi(g) = (\varphi_1(g), \varphi_2(g)) \in H \times T(G)$,
l'application $g \longmapsto (F_1(\varphi_1(g)), F_2(\varphi_2(g)))$ est un isomorphisme de G
dans $\mathbb{Z}^k \times [(\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_\ell\mathbb{Z})]$, dont l'isomorphisme réciproque
est $(x_1, x_2) \longmapsto \varphi^{-1}(F_1^{-1}(x_1), F_2^{-1}(x_2))$.