Lycée Louis-Le-Grand, Paris
MPSI 4 – Mathématiques
A. Troesch

Pour le 22/02/2019

# DM n° 13 : Groupes

## Correction du problème 1 – Structure des groupes abéliens de type fini

### Partie I – Sommes directes

1. Les éléments de $H_1 + H_2$ sont les éléments de $\mathbb{Z}^2$ s'écrivant $(2n, n+2m)$. Autrement dit, ce sont les éléments $(k, \ell)$, où $k$ est pair et $\ell$ est de la parité de $\frac{k}{2}$.
   Supposons $x = n(2,1) + m(0,2) = n'(2,1) + m'(0,2)$. On a donc en particulier $2n = 2n'$, donc $n = n'$, puis $n + 2m = n + 2m'$, donc $m = m'$. Ainsi, la décomposition d'un élément $x$ de $H_1 + H_2$ est unique, donc $\boxed{H_1 + H_2 \text{ est directe}}$.
2. Soit $d = a \wedge b$ (pgcd de $a$ et $b$). Soit $n \in a\mathbb{Z} + b\mathbb{Z}$. Il existe donc $u$ et $v$ des entiers tels qie $n = au + bv$, et par conséquent, $d$ divise $n$ (puisque $d$ divise $a$ et $b$). Donc $n \in d\mathbb{Z}$. Réciproquement, supposons $n \in d\mathbb{Z}$, disons $n = dk$. D'après le théorème de Bézout, on peut trouver $u$ et $v$ tels que $au + bv = d$ (si vous ne connaissez pas cette version de théorème de Bézout, appliquez le théorème classique pour les deux entiers $\frac{a}{d}$ et $\frac{b}{d}$ premiers entre eux). Ainsi, $auk + bvk = n$. On en déduit que $d\mathbb{Z} \subset a\mathbb{Z} = b\mathbb{Z}$.
   Ainsi $\boxed{a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}}$, où $d = a \wedge b$.
   Si $(a,b) \neq (0,0)$, $\boxed{\text{la somme n'est pas directe}}$. En effet, $0 = 0a + 0b = au + bv$ avec $u = b$ et $= -a$. Ainsi, la décomposition de $O$ n'est pas unique
3. (a)
   - $G$ étant stable par $+$, on a bien $H_1 + H_2 \subset G$
   - Comme $0_G \in H_1$ et $0_G \in H_2$, on a $0_G = 0_G + 0_G \in H_1 + H_2$. Donc $H_1 + H_2$ n'est pas vide.
   - Soit $g, g' \in H_1 + H_2$ et $h_1, h_1' \in H_1$, $h_2, h_2' \in H_2$ tels que $g = h_1 + h_2$ et $g' = h_1' + h_2'$. On a alors
   $$g - g' = h_1 + h_2 - h_1' - h_2' = (h_1 - h_1') + (h_2 - h_2').$$
   Or, $H_1$ et $H_2$ étant des sous groupes de $G$, $h_1 - h_1' \in H_1$ et $h_2 - h_2' \in H_2$. Par conséquent, $g - g' \in H_1 + H_2$.
   On en déduit que $\boxed{H_1 + H_2 \text{ est un sous-groupe de } G}$.

   (b) Supposons que $H_1 + H_2$ est directe. On définit $\varphi : H_1 \times H_2 \longrightarrow H_1 + H_2$ par
   $$\varphi((h,k)) = h + k.$$
   - $\varphi$ est un homomorphisme de groupe. En effet, pour tout $(h,k)$, $(h',k') \in H_1 \times H_2$, on a
   $$\varphi((h,k) + (h',k')) = \varphi((h+h', k+k')) = h + h' + k + k' = \varphi((h,k)) + \varphi((h',k')),$$
   puisque $G$ est abélien.
   - $\varphi$ est surjective, par définition même de $H_1 + H_2$
   - $\varphi$ est injective : en effet, soit $(h,k) \in \mathrm{Ker}(\varphi)$, on a donc $h + k = 0$. Comme on a aussi $0 + 0 = 0$, par unicité de la décomposition, on a $h = k = 0$. Ainsi, $\mathrm{Ker}(\varphi) = \{(0,0) = 0_{H_1 \times H_2}\}$. Cela suffit à jusitifier l'injectivité, par caractérisation de l'injectivité par le noyau.

   Ainsi, $\boxed{\varphi \text{ est un isomorphisme de } H_1 \times H_2 \text{ sur } H_1 \oplus H_2.}$
4. - L'associativité de la somme des sous-groupes provient de l'associativité de la loi de $G$. En effet, soit $x \in (H_1 + H_2) + H_3$. Il existe donc $h_1 \in H_1$, $h_2 \in H_2$ et $h_3 \in H_3$ tels que $x = (h_1 + h_2) + h_3 = h_1 + (h_2 + h_3)$, égalité de laquelle on déduit que $x \in H_1 + (H_2 + H_3)$. L'autre sens se fait de la même façon.
     Ainsi : $\boxed{(H_1 + H_2) + H_3 = H_1 + (H_2 + H_3)}$
   - Supposons $H_1 \oplus H_2$ directe, ainsi que $(H_1 + H_2) \oplus H_3$. Alors pour tout $h \in H_2 + H_3$, il existe $h_2 \in H_2$ et $h_3 \in H_3$ tels que $h = h_2 + h_3$. Soit $h_2' \in H_2$ et $h_3' \in H_3$ vérifiant aussi $h = h_2' + h_3'$. Comme $H_2 \subset H_1 + H_2$, les décompositions $h = h_2 + h_3 = h_2' + h_3'$ sont aussi des décompositions de $h$ dans la somme directe $(H_1 + H_2) \oplus H_3$. Ainsi, par unicité de cette décomposition $h_2 = h_2'$ et $h_3 = h_3'$. Ainsi $\boxed{\text{la somme } H_2 \oplus H_3 \text{ est directe}}$.

- De même, soit $h = h_1 + h_{23} = h'_1 + h'_{23} \in H_1 + (H_2 + H_3)$, où $h_1, h'_1 \in H_1$ et $h_{23}, h'_{23} \in H_2 + H_3$. On a alors l'existence de $h_2, h'_2 \in H_2$ et $h_3, h'_3 \in H_3$ tels que $h_{23} = h_2 + h_3$ et $h'_{23} = h'_2 + h'_3$. Alors, par associativité,

$$h = (h_1 + h_2) + h_3 = (h'_1 + h'_2) + h'_3.$$

Comme la somme $(H_1 + H_2) \oplus H_3$ est supposée directe, par unicité de la décomposition, on obtient :

$$h_1 + h_2 = h'_1 + h'_2 \qquad \text{et} \qquad h_3 = h'_3.$$

La somme $H_1 \oplus H_2$ étant aussi supposée directe, la première égalité amène $h_1 = h'_1$ et $h_2 = h'_2$. On en déduit finalement $h_1 = h'_1$ et $h_{23} = h'_{23}$. Ainsi, $\boxed{\text{la somme } H_1 \oplus (H_2 + H_3) \text{ est directe}}$.

**Partie II – Groupes abéliens libres de type fini**

1. Pour tout $k \in [\![1, n]\!]$, $x_k \in \bigoplus_{i \in I} \langle y_i \rangle$. Ainsi, par définition d'une somme directe infinie, et du fait que tout élément de $\langle y \rangle$ s'écrit de la forme $ny$, il existe des entiers entiers $n_i$ presque tous nuls tels que

$$x_k = \sum_{i \in I} n_i y_i.$$

Notons $I_k \subset I$ l'ensemble des indices $i \in I$ tels que $n_i \neq 0$. On a alors :

$$x_k = \sum_{i \in I_k} n_i y_i,$$

et par définition, $I_k$ est un ensemble fini.

Notons $J = \bigcup_{k=1}^{n} I_k$. Cet ensemble est fini en tant qu'union finie d'ensembles finis. Par ailleurs, par construction des $I_k$, pour tout $k \in [\![1, n]\!]$

$$\boxed{x_k \in \bigoplus_{i \in J} \langle y_i \rangle}.$$

Du fait que cette somme directe est un sous-groupe de $G$ (par itération du cas de la somme de deux sous-groupes ; c'est même vrai pour une somme infinie, la vérification n'en est pas très dure), elle est stable par somme. Donc toute combinaison des $x_i$ à coefficients entiers est encore dans $\bigoplus_{i \in J} \langle y_i \rangle$. On en déduit que

$$\bigoplus_{k=1}^{n} \langle x_k \rangle \subset \bigoplus_{i \in J} \langle y_i \rangle .$$

Or, le premier terme est égal à $G$ (car $(x_1, \ldots, x_n)$ est une base de $G$) et le second terme est inclus dans $G$. Ainsi

$$G = \bigoplus_{i \in J} \langle y_i \rangle .$$

Par ailleurs, comme $J$ est fini et $I$ est infini, il existe $i_0 \in I \setminus J$. Soit un tel $i_0$. On a alors

$$y_{i_0} \in G = \bigoplus_{i \in J} \langle y_i \rangle .$$

Il existe donc des entiers $n_i$, $i \in J$ tels que

$$y_{i_0} = \sum_{i \in J} n_i y_i.$$

Cela donne aussi une décomposition de $y_{i_0}$ dans la somme directe $\bigoplus_{i \in I} \langle y_i \rangle$. Or, une autre décomposition de $y_{i_0}$ est :

$$y_{i_0} = 1 \times y_{i_0} + \sum_{i \in I \setminus \{i_0\}} 0 \times y_i.$$

Cela contredit l'unicité de la décomposition de $y_{i_0}$.

Ainsi, il ne peut pas exister de base infinie de $G$.

Conclusion : $\boxed{\text{si } G \text{ admet une base finie, toute base est finie}}$.

2. Soit $\varphi : G \mapsto G$ définie par $x \mapsto 2x$.

(a) On a, pour tout $(x, y) \in G$, par commutativité,

$$\varphi(x + y) = 2(x + y) = 2x + 2y = \varphi(x) + \varphi(y).$$

Ainsi, $\boxed{\varphi \text{ est un morphisme de groupes.}}$

Remarquez que sans commutativité, ce ne serait pas vrai : $2(x + y) = x + y + x + y$, et on reste ensuite coincé pour associer les deux termes $x$ et les deux termes $y$.

(b) • Tout d'abord, montrons que pour tout $i \in [\![1, n]\!]$, $\langle 2x_i \rangle \simeq \mathbb{Z}$. Soit :

$$\varphi_i : \langle x_i \rangle \longrightarrow \langle 2x_i \rangle ,$$

définie par $\varphi_i(a) = 2a$. L'application $\varphi_i$ est bien à valeurs dans $\langle 2x_i \rangle$, et c'est de façon évidente un homomorphisme de groupes (même justification que pour $\varphi$). Par ailleurs :

∗ $\varphi_i$ est surjective : en effet,pour tout $y \in \langle 2x_i \rangle$, il existe $k \in \mathbb{Z}$ tel que $y = k \times 2x_i = 2(kx_i) = \varphi(kx_i)$.

∗ $\varphi_i$ est injective : en effet, si $\varphi_i(y) = 0$, alors $2y = 0$. Écrivons $y = kx_i$. On a donc $2kx_i = 0$. Comme $\langle x_i \rangle \simeq \mathbb{Z}$, $x_i$ est d'ordre infini (sinon l'ordre de $\langle x_i \rangle$ serait fini, donc différent de celui de $\mathbb{Z}$). Ainsi, $2kx_i = 0$ n'est possible que si $2k = 0$, donc $k = 0$, donc $y = 0$. par conséquent, $\mathrm{Ker}(\varphi_i) = \{0\}$, puis $\varphi_i$ est injective.

En conclusion, $\varphi_i$ est un isomophisme, donc $\langle 2x_i \rangle \simeq \langle x_i \rangle$. Par ailleurs, $\langle x_i \rangle \simeq \mathbb{Z}$ par définition. La composée de deux isomorphismes étant un isomorphisme, on a bien $\boxed{\langle 2x_i \rangle \simeq \mathbb{Z}}$.

• Montrons maintenant que la somme $\sum_{i=1}^{n} \langle 2x_i \rangle$ est directe. Pour cela, il suffit de montrer que pour tout tout $y$ de cette somme se décompose de façon unique. Soit donc un élément $y$ de la somme et deux décompositions :

$$y = \sum_{i=1}^{n} n_i 2x_i = \sum_{i=1}^{n} n'_i 2x_i.$$

Par unicité de la décomposition dans la somme directe $\bigoplus_{i=1}^{n} \langle x_i \rangle$, on obtient donc pour tout $i \in [\![1, n]\!]$, $2n_i = 2n'_i$, donc $n_i = n'_i$. D'où l'unicité de la décomposition.

Ainsi, la somme $\bigoplus_{i=1}^{n} \langle 2x_i \rangle$ est directe.

• Puisque chaque $2x_i$ est dans $\varphi(G)$, on a, par stabilité par somme (puisque $\varphi(G)$ est un sous-groupe de $G$) :

$$\bigoplus_{i=1}^{n} \langle 2x_i \rangle \subset \varphi(G).$$

• Réciproquement, soit $y \in \varphi(G)$ et $x \in G$ tel que $y = \varphi(x)$. Écrivons

$$x = \sum_{i=1}^{n} n_i x_i.$$

On a alors,

$$y = \varphi(x) = \sum_{i=1}^{n} 2n_i x_i = \sum_{i=1}^{n} n_i (2x_i) \in \bigoplus_{i=1}^{n} \langle 2x_i \rangle .$$

Ainsi, $\varphi(G) = \bigoplus_{i=1}^{n} \langle 2x_i \rangle$, et pour tout $i \in [\![1, n]\!]$, $\langle 2x_i \rangle \simeq \mathbb{Z}$.

On en déduit que $\boxed{\varphi(G) \text{ est un groupe libre de base } (2x_1, \ldots, 2x_n)}$.

(c) Soit $x \equiv y \mod \varphi(G)$. Écrivons

$$x = \sum_{i=1}^{n} n_i x_i \qquad \text{et} \qquad y = \sum_{i=1}^{n} m_i x_i.$$

On a donc

$$y - x = \sum_{i=1}^{n} (n_i - m_i) x_i.$$

D'après la question précédente, et l'unicité des décompositions, $y - x$ est dans $\varphi(G)$ si et seulement si pour tout $i \in [\![1, n]\!]$, $n_i - m_i$ est un multiple de 2, donc si $n_i$ et $m_i$ sont de même parité.
Par conséquent, les classes d'équivalence modulo $H$ sont déterminées par la classe de parité des coefficients de la décomposition dans la somme $\bigoplus_{i=1}^{n} \langle x_i \rangle$. Pour chacun des $n$ coefficients, on a deux classes de parité possibles, donc $2^n$ classes d'équivalences modulo $H$ (le choix d'une parité pour chacun des coefficients).
Le nombre de classes d'équivalence modulo $\varphi(G)$ est appelé indice du sous-groupe $\varphi(G)$ dans le groupe $G$, et noté $[G : \varphi(G)]$. On a donc obtenu :

$$\boxed{[G : \varphi(G)] = 2^n}.$$

3. La description de $\varphi$ ne dépend pas du choix de la base, donc l'indice $[G : \varphi(G)]$ est aussi indépendant du choix de la base. Donc l'entier $n$ est aussi indépendant du choix de la base. Ainsi, $\boxed{\text{toute base de } G \text{ a même cardinal } n}$.

**Partie III – Groupes abéliens sans torsion**

1. - $\boxed{\mathbb{Q} \text{ est un groupe sans torsion}}$. En effet, tout $x \in \mathbb{Q}$ non nul est d'ordre infini ($nx \neq 0$, pour tout $n \in \mathbb{Z}^*$)
   - $\boxed{\mathbb{Q}/\mathbb{Z} \text{ est un groupe de torsion}}$. En effet, pour tout $x \in \mathbb{Q}$, disons $x = \frac{p}{q}$, il existe un entier non nul, en l'occurrence $q$, tel que $qx \in \mathbb{Z}$, donc $q\overline{x} = 0$ dans $\mathbb{Q}/\mathbb{Z}$.
   - $\boxed{\mathbb{C}^* \text{ n'est ni sans torsion ni de torsion}}$. Il s'agit ici évidemment du groupe multiplicatif (puisqu'il n'y a pas 0). Il existe des éléments d'ordre infini par exemple 2, et des éléments distincts de 1 et d'ordre fini, par exemple $-1$, ou toute racine $n$-ième de l'unité différente de 1.
2. Soit $G$ un groupe abélien libre, et $(x_i)_{i \in I}$ une famille de générateurs. Soit $x \in G$ non nul, se décomposant en

$$x = \sum_{i \in I} a_i x_i,$$

les $a_i$ étant entiers, et presque tous nuls. Puisque $x \neq 0$, il existe $i_0$ tel que $a_{i_0} \neq 0$. Pour tout $n \in \mathbb{N}$, on a alors la décomposition suivante de $nx$ dans la somme directe $\bigoplus_{i \in I} \langle x_i \rangle$ :

$$nx = \sum_{i \in I} n a_i x_i.$$

Comme $na_{i_0} \neq 0$, il ne s'agit pas de l'unique décomposition de 0, donc $nx \neq 0$. Ainsi, $x$ est d'ordre infini.
Par conséquent, $\boxed{\text{un groupe abélien libre est sans torsion}}$.
3. On veut montrer que réciproquement, un groupe sans torsion de type fini est libre. Soit $G$ un groupe abélien de type fini, sans torsion.
   (a) L'ensemble $C_X = \left\{ \sum_{x \in X} |n_x| \;\middle|\; n_x \in \mathbb{Z} \text{ non tous nuls et } \sum_{x \in X} n_x x = 0. \right\}$ est un sous-ensemble de $\mathbb{N}^*$. Il s'agit essentiellement de montrer qu'il est non vide, autrement dit qu'il existe une relation non triviale (c'est-à-dire telle que tous les coefficients ne soient pas nuls) :

$$\sum_{x \in X} n_x x = 0.$$

Supposons que ce ne soit pas le cas. On aurait en particulier, en considérant tous les coefficients nuls sauf un, pour tout $n \in \mathbb{Z}^*$, et tout $x \in X$, $nx \neq 0$. Ainsi, $\langle x \rangle$ est un groupe monogène infini, donc isomorphe à $\mathbb{Z}$ (un isomorphisme explicite étant donné par $n \mapsto nx$). Par ailleurs, pour tout $y \in \bigoplus_{x \in X} \langle x \rangle$, on aurait unicité de la décomposition de $x$ dans cette somme directe. En effet, si

$$y = \sum_{x \in X} a_x x = \sum_{x \in X} b_x x,$$

alors

$$0 = \sum_{x \in X} (a_x - b_x) x,$$

d'où $a_x = b_x$ pour tout $x$, puisqu'on a supposé qu'il n'existe pas de relation non triviale entre les $x$ de $X$. Ainsi, $G$ serait un groupe libre dont une base serait $X$. Cela contredit l'hypothèse.

Par conséquent, l'ensemble $C_X$ est un sous-ensemble non vide de $\mathbb{N}^*$, et admet donc un minimum $m_X$, d'après la propriété fondamentale de $\mathbb{N}$.

Par définition d'une famille de type fini, il existe une famille génératrice $X$ de cardinal fini, et toujours d'après la propriété fondamentale de $\mathbb{N}$, il existe donc une famille génératrice $X$ de cardinal minimal, que l'on note $n$.

L'ensemble $\{m_X,\ X \text{ génératrice de cardinal } n\}$ est donc un sous-ensemble non vide de $\mathbb{N}$ (et même de $\mathbb{N}^*$, les expressions $m_X$ étant entières strictement positives). Ainsi, la propriété fondamentale de $\mathbb{N}$ nous assure encore une fois l'existence d'une famille génératrice de cardinal $n$ telle que $m_X$ soit minimal parmi les familles génératrices de cardinal $n$.
Soit $X$ une telle famille, et $(n_x)_{x\in X}$ réalisant le minimum $m_X$, c'est-à-dire telle que

$$\sum_{x\in X} n_x x = 0 \qquad \text{et} \qquad \sum_{x\in X} |n_x| = m_x.$$

(b) Supposons qu'il existe $x \in X$ tel que $|n_x| = 1$. On pourrait alors écrire

$$x = n_x \sum_{y\in X\setminus\{x\}} n_y y,$$

donc $x \in \bigoplus_{y\in X\setminus\{x\}} \langle y\rangle$.
On en déduit sans peine que $X \setminus \{x\}$ est encore une famille génératrice, dont le cardinal est strictement inférieur à celui de $X$. Cela contredit la minimalité du cardinal de $X$.
Ainsi, pour tout $x \in X$, $n_x \neq 1$.

(c) Soit $x$ tel que $|n_x|$ soit non nul et minimal (encore la propriété fondamentale de $\mathbb{N}$ !). Si pour tout $y \in X$, $n_x | n_y$, alors, en posant pour tout $y \in X$, $n'_y = \frac{n_y}{n_x}$, on a toujours une relation

$$\sum_{y\in Y} n'_y y = 0,$$

et comme $|n_x| > 1$ d'après la question précédente, on obtient

$$\sum_{y\in Y} |n'_y| < \sum_{y\in Y} |n_y| = m_X,$$

ce qui contredit la minimalité de $m_X$.
Par conséquent, il existe $y \in X$ tel que $n_x$ ne divise pas $n_y$, donc en particulier $|n_x| \neq |n_y|$, et $|n_y| \neq 0$. Comme $|n_x|$ a été choisi minimal parmi les éléments non nuls, il en résulte que $|n_x| < |n_y|$.

(d) Soit $q$ et $r$ des entiers tels que $n_y = qn_x + r$, où $r \in [\![0, |n_x| - 1]\!]$. On a alors

$$n_x(x + qy) + ry + \sum_{z\in X\setminus x,y} n_z z.$$

Posons $x' = x + qy$ et $X' = \{x'\} \cup (X \setminus \{x\})$. Il s'agit encore d'une famille génératrice (car tout vecteur de $X$ est dans $X'$, à part $x$ qui s'obtient facilement comme combinaison d'éléments de $X'$, en l'occurrence $x = x' - qy$). Son cardinal est encore $n$, et de plus, en notant $n'_x = n_x$, $n'_y = r$ et pour tout $z \in X' \setminus \{x', y\}$, $n'_z = n_z$, on a :

$$\sum_{z\in X'} n'_z z = 0 \qquad \text{et} \qquad \sum_{z\in X'} |n'_z| = \sum_{z\in X} |n_z| + r - |n_y| < \sum_{z\in X} |n_z| = m_X,$$

puisque $r < |n_x| < |n_y|$. On obtient donc $m_{X'} \leqslant m_X$. Cela fboxcontredit le choix de $X$, assurant la minimalité de $m_X$ parmi les familles génératrices de cardinal $n$.

4. L'hypothèse initiale, à savoir la non existence d'une base finie, amène une contradiction. Par conséquent, $G$ admet une base finie, donc s'écrit sous la forme :

$$G = \bigoplus_{i=1}^{n} \langle x_i\rangle,$$

où pour tout $i \in [\![1,n]\!]$, $\langle x_i \rangle \simeq \mathbb{Z}$ (par un certain isomorphisme $\varphi_i$). La partie I-3(b) nous assure alors l'existence d'un isomorphisme entre $G = \bigoplus_{i=1}^{n} \langle x_i \rangle$ et $\prod_{i=1}^{n} \langle x_i \rangle$. Par ailleurs, on vérifie sans peine que l'application $\varphi$ :

$$\varphi(y_1, \ldots, y_n) = (\varphi_1(y_1), \varphi_2(y_2), \ldots, \varphi_n(y_n)),$$

est un isomorphisme de $\prod_{i=1}^{n} \langle x_i \rangle$ sur $\prod_{i=1}^{n} \mathbb{Z} = \mathbb{Z}^n$. Plus généralement, si $H \simeq H'$ et $K \simeq K'$, alors $H \times K \simeq H' \times K'$.

Par composition d'isomorphismes, $\boxed{G \text{ est isomorphe à } \mathbb{Z}^n}$.

Pour terminer, montrons que si $\Phi : G \longrightarrow \mathbb{Z}^m$ est un isomorphisme, alors, nécessairement, $m = n$ (rang de $G$, égal au cardinal commun de ses bases). En effet, soit pour tout $i \in [\![1,m]\!]$, $e_i = (0, \cdots, 1, \cdots, 0)$, l'unique 1 étant en position $i$. La famille $(e_i)_{i \in [\![1,m]\!]}$ est clairement une base de $\mathbb{Z}^m$. Soit pour tout $i \in [\![1,m]\!]$, $f_i = \Phi^{-1}(x_i)$. Alors :

- pour tout $n \in NN^*$, $\Phi(nf_i) = n\Phi(f_i) = ne_i \neq 0$, donc $nf_i \neq 0$, donc $f_i$ est d'ordre infini. Ainsi, $\langle f_i \rangle \simeq \mathbb{Z}$.
- Par ailleurs, pour tout $x \in G$, il existe des entiers $n_i$, $i \in [\![1,m]\!]$ tels que $\Phi(x) = \sum_{i=1}^{m} n_i e_i$, d'où, en appliquant $\Phi^{-1}$, qui est aussi un morphisme,
$$x = \sum_{i=1}^{m} n_i f_i.$$
Par conséquent $(f_1, \ldots, f_m)$ est une famille génératrice, c'est à dire $G = \sum_{i=1}^{m} \langle f_i \rangle$.
- Enfin, soit $x \in G$, et deux décompositions
$$x = \sum_{i=1}^{m} n_i f_i = \sum_{i=1}^{m} n'_i f_i.$$
En appliquant le morphisme $\Phi$, il vient :
$$\Phi(x) = \sum_{i=1}^{m} n_i e_i = \sum_{i=1}^{m} n'_i e_i.$$
Comme $(e_1, \ldots, e_m)$ est une base de $\mathbb{Z}^m$, on a unicité de la décomposition de $\Phi(x)$, donc $n_i = n'_i$ pour tout $i \in [\![1,n]\!]$. Ainsi, la décomposition de tout $x \in G$ est unique, d'où :
$$G = \bigoplus_{i=1}^{m} \langle x_i \rangle .$$
On en déduit que $(f_1, \ldots, f_m)$ est une base de $G$, et donc que $\boxed{m = n}$ (le rang de $G$) d'après II-3.
Ainsi, $\boxed{G \simeq \mathbb{Z}^n \text{ pour une unique valeur de } n}$.

**Partie IV – Groupes de torsion**

1. Soit $(x_1, \ldots, x_n)$ une famille génératrice de $G$. Ainsi,
$$G = \sum_{i=1}^{n} \langle x_i \rangle = \left\{ \sum_{i=1}^{n} \alpha_i x_i, \alpha_i \in [\![0, b_i - 1]\!] \right\},$$
où $b_i$ est l'ordre de $x_i$. Ainsi, il y a un nombre fini de $n$-uplets $(\alpha_1, \ldots, \alpha_n)$ possibles, donc un nombre fini d'éléments dans $G$. Ainsi $\boxed{G \text{ est fini}}$.
2. On démontre un lemme classique, utilisant un peu d'arithmétique :

   **Lemme :** Soit $x$ et $y$ deux éléments d'ordres $a$ et $b$ dans $G$. Alors il existe un élément $z$ d'ordre $a \vee b$.

   *Démonstration du lemme :*
   On se ramène d'abord au cas où $a$ et $b$ sont premiers entre eux : notons
$$a \vee b = \prod_{p \in \mathbb{P}} p^{\alpha_p}$$

la décomposition primaire de $a \vee b$, où $\alpha_p = \max(v_p(a), v_p(b))$. Soit $\mathcal{P}_1$ le sous-ensemble de $\mathbb{P}$ constitué des $p \in \mathbb{P}$ tels que $\alpha_p = v_p(a)$, et $\mathcal{P}_2$ les autres (donc tels que $\alpha_p = v_p(b)$). Soit

$$a' = \prod_{p \in \mathcal{P}_1} p^{\alpha_p} \qquad \text{et} \qquad b' = \prod_{p \in \mathcal{P}_2} p^{\alpha_p}.$$

Par construction, on a, pour tout $p \in \mathbb{P}$, $v_p(a') \leqslant v_p(a)$ et $v_p(b') \leqslant v_p(b)$, donc $a'|a$ et $b'|b$, et par ailleurs $a' \wedge b' = 1$ (les entiers premiers intervenant dans leurs dcompositions sont distincts). Enfin, $a' \vee b' = a'b' = \prod_{p \in \mathbb{P}} p^{\alpha_p} = a \vee b$.

Par ailleurs, comme $a'|a$, on peut trouver dans le groupe cyclique $\langle x \rangle$ un élément $x'$ d'ordre $a'$ (par exemple $x' = dx$, où $a'd = a$). De même, on peut trouver dans $\langle y \rangle$ un élément $y$ d'ordre $b'$.

On en déduit qu'il existe deux éléments $x'$ et $y'$, d'ordres $a'$ et $b'$ premiers entre eux, et tels que $a' \vee b' = a'b' = a \vee b$.

Considérons alors $z = x' + y'$. Soit $n \in \mathbb{Z}^*$ tel que $nz = 0$, soit $nx = -ny$. On a alors $b'nx = -nb'y = 0$, donc $b'n \in a'\mathbb{Z}$, et de même $a'n \in b'\mathbb{Z}$. On en déduit que $a'$ divise $b'n$ et $b'$ divise $a'n$. Comme $a'$ et $b'$ sont premiers entre eux, on en déduit d'abord, par le lemme de Gauss, que $a' \mid n$ et $b' \mid n$, puis que $a'b' \mid n$. Ainsi, $n \in a'b'\mathbb{Z}$. Par conséquent, l'ordre de $z$, s'il est fini, est un multiple de $a'b'$. Par ailleurs,

$$a'b'z = b'(a'x) + a'(b'x) = 0,$$

donc l'ordre de $z$ est fini et divise $a'b'$.

On déduit des deux points ci-dessus que $\boxed{z \text{ est d'ordre } a'b' = a \vee b}$.

*Réponse à la question posée*

Soit alors $x$ dans $G$ d'ordre maximal $d_1$ (possible car $G$ est fini et tout élément est d'ordre fini). Soit $y \in G$, d'ordre $b$. D'après le lemme, il existe un élément d'ordre $d_1 \vee b \geqslant d_1$. Comme $d_1$ est l'ordre maximal d'un élément de $G$, on a nécessairement $d_1 \vee b = d_1$, ce qui signifie très exactement que $b$ divise $a$.

Ainsi, $\boxed{\text{l'ordre de tout } y \text{ de } G \text{ divise l'ordre de } x}$.

En particulier, l'ordre de $x$ est le ppcm de l'ordre de tous les éléments de ce groupe (ce ppcm ne peut pas être plus petit, à cause de $x$ lui-même). On a donc montré que dans un groupe abélien fini, il existe un élément dont l'ordre est égal au ppcm de l'ordre de tous les éléments. Cet ordre maximal est appelé exposant du groupe abélien $G$.

3. $H = \langle x \rangle$ est un sous-groupe de $G$. Comme $G$ est abélien, $H$ est nécessairement distingué, donc la loi de $G$ passe au quotient, définissant une $\boxed{\text{structure de groupe sur } G/H}$.

4. Pour construire un isomorphisme $\varphi : G \longrightarrow H \times G/H$, il faut dans un premier temps construire un morphisme $G \longrightarrow H$, et c'est cela le plus dur.
   - Considérons $E = \{(K, \psi) \mid H < K < G, \quad \psi \in \mathrm{Hom}(K, H), \text{ et } \psi_{|H} = \mathrm{id}\}$, l'ensemble des couples formés d'un sous-groupe $K$ de $G$ contenant $H$, et d'un morphisme $\varphi_k$ prolongeant à $K$ l'identité de $H$. On va construire un argument du type Zorn, à part que comme on est en cardinal fini, on n'aura pas besoin de faire recourt au lemme de Zorn. Mais la démarche est la même : commençons par ordonner $E$, en définissant $(K, \psi) \leqslant (K', \psi')$ si et seulement si $K < K'$ et $\varphi'_{|K} = \psi$, donc si $\psi'$ prolonge $\psi$ à $K'$.
     De façon évidente, cela définit une relation d'ordre sur $E$. Comme $G$ est fini, il a un nombre fini de sous-ensembles, donc aussi de sous-groupes. Par ailleurs, pour chaque sous-groupe $K$, $\mathrm{Hom}(K, H)$ est inclu dans l'ensemble fini $H^K$, donc est lui-même fini. Ainsi, $E$ est fini. Il admet donc un élément maximal pour l'ordre défini ci-dessus (cette existence est ici automatique en cas d'ensemble ordonné fini, ce qui évite le recours à une zornette). Notons $(K, \psi)$ un tel élément maximal.
   - Si $K \neq G$, considérons un élément $y \in G \setminus K$, et montrons qu'on peut prolonger $\psi$ sur $K' = K + \langle y \rangle$, contredisant ainsi la maximalité de $K$.
     Soit $a$ l'ordre de $y$ dans $G$ et $b$ l'ordre de $\overline{y}$ dans $G/K$. Ainsi, $b$ est le plus petit entier tel que $by \in K$. Éventuellement, il peut arriver que $a = b$ (si $< y > \cap K = \{0\}$). Notons $x_0 = by$
     Pour commencer, on remarque qu'on peut plonger $H$ dans $\mathbb{U}$, $H$ étant isomorphe à un groupe (multiplicatif) $\mathbb{U}_{n_0}$, $n_0$ étant l'ordre de $x$, donc l'exposant du groupe $G$. On note $\psi' : K \to H \to \mathbb{U}$ la composée de $\psi$ et de cette injection. En particulier, l'image de $\psi'$ est incluse dans $\mathbb{U}_{n_0}$.
     Pour prolonger $\psi$, on va comencer par prolonger $\psi'$, ce qui est plus simple, car on sait « diviser » par un entier dans $\mathbb{U}$ (mutliplicativement, cela revient à prendre des racines). On définit $\tilde{\psi'}$ sur $K + < y >$ par :

     $$\tilde{\psi'}(k + \lambda y) = \psi'(k) + \lambda \tilde{\psi'}(y),$$

     où $\tilde{\psi'}(y)$ est posé de sorte que $\psi'(\tilde{by}) = \psi'(x_0)$, cette dernière quantité étant définie, puisque $x_0 \in K$. Ainsi, si $\psi'(x_0) = \mathrm{e}^{\mathrm{i}\,\theta}$, il suffit par exemple de poser $\tilde{\psi'}(y) = \mathrm{e}^{\mathrm{i}\,\theta/b}$.

- Justifions que $\tilde{\psi'}$ est bien définie. Pour cela, il faut vérifier que pour $k$, $k'$ dans $K$ et $\lambda$, $\lambda'$ dans $\mathbb{Z}$, si $k+\lambda y = k'+\lambda' y$, alors $\tilde{\psi'}(k+\lambda y) = \tilde{\psi'}(k'+\lambda' y)$.
  Or, $k+\lambda y = k'+\lambda' y$ implique $(\lambda-\lambda')y = k'-k \in K$, donc la classe de $(\lambda-\lambda')y$ modulo $K$ est nulle. Comme $b$ est l'ordre de $y$ modulo $K$, $b$ divise $\lambda-\lambda'$. On peut écrire $\lambda-\lambda' = \alpha b$, pour $\alpha \in \mathbb{Z}$. On a alors $k'-k = ax_0$, donc $\psi'(k')-\psi'(k) = a\psi'(x_0)$. De plus :

  $$(\lambda-\lambda')\tilde{\psi'}(y) = \alpha b\tilde{\psi'}(y) = \alpha\psi'(x_0).$$

  Cela fournit bient l'égalité :

  $$\psi'(k)+\lambda\tilde{\psi'}(y) = \psi'(k')+\lambda'\tilde{\psi'}(y) \qquad \text{donc:} \qquad \tilde{\psi'}(k+\lambda y) = \tilde{\psi'}(k'+\lambda' y).$$

- De façon évidente, $\tilde{\psi'}$ ainsi définie est un morphisme de groupe (additif, vers multiplicatif)
- L'ordre de $y$ étant $a$, on a $ay = 0$, donc $\psi'(ay) = 0$, donc $\tilde{\psi'}(y)^a = 0$. Ainsi, l'ordre de $\tilde{\psi'}(y)$ dans $\mathbb{U}$ divise $a$. Or, l'ordre $n_0$ de $x$ est par définition l'exposant du groupe $G$, donc est divisible par l'ordre de tout élément de $G$. Ainsi, $a$ divise $n_0$, donc l'ordre de $\tilde{\psi'}(y)$ divise $n_0$ dans $\mathbb{U}$, ce qui implique que $\tilde{\psi'}(y)^{n_0} = 1$, donc $\tilde{\psi'}(y) \in \mathbb{U}_{n_0}$. Or, il s'agit là de l'image du morphisme injectif de $H$ dans $\mathbb{U}$. En corestreignant cette injection sur son image, on obtient un isomorphisme. En composant $\tilde{\psi'}$ par sa réciproque, on obtient un morphisme $\psi' = K \to H$ prolongeant $\psi$, ce qui est contradictoire.
- Ainsi, on a nécessairement $K = G$, d'où l'$\boxed{\text{existence d'un morphisme } \psi : G \to H \text{ prolongeant l'identité de } H}$.
- On peut aussi définir $\psi'$ sans passer par $\mathbb{U}$, avec un peu d'arithmétique : il faut définir $\psi'(y)$ tel que $b\psi'(y) = \psi(by)$ ; donc envoyer $x$ sur un élément $z$ de $H$ tel que $bz = \psi(by)$. Autrement dit, il faut essayer de « diviser » $\psi(by)$ par $b$ dans $H$.
  Comme $by$ est d'ordre $c = \frac{b}{a}$, $c\psi(by) = \psi(cby) = \psi(0) = 0$. Puisque $\psi(by) \in H = \langle x\rangle$, il existe $k$ tel que $\psi(by) = kx$. On a donc $ckx = 0$, donc $d_1 \mid ck$. Par ailleurs, $c$ divise $a$ donc aussi $d_1$ (question 2), donc $\frac{d_1}{c} \mid k$. On en déduit qu'il existe $c'$ entier tel que

  $$\psi(by) = kx = \frac{d_1c'}{c}x = \frac{d_1bc'}{a}x.$$

  On pose alors $y' = \frac{d_1c'}{a}x$, ce qui a du sens puisque $a$ divise $d_1$, et on pose $\psi'(y) = y'$.
  On termine la contruction et la preuve comme ci-dessus.
- Le plus dur est fait. Définissons maintenant $\Phi : G \longrightarrow H \times G/H$ par :

  $$\Phi(g) = (\psi(g), \overline{g}).$$

  Il s'agit clairement d'un morphisme de groupes : si $g$ et $g'$ sont deux éléments de $g$,

  $$\Phi(g+g') = (\psi(g+g'), \overline{g+g'}) = (\psi(g)+\psi(g'), \overline{g}+\overline{g'}) = (\psi(g),\overline{g}) + (\psi(g'),\overline{g'}) = \Phi(g)+\Phi(g').$$

  Par ailleurs, $\Phi$ est injective. Pour le montrer, étudions son noyau. Soit $g \in \mathrm{Ker}(\Phi)$. On a donc $\Phi(g) = 0$, donc $\psi(g) = 0$, et $\overline{g} = 0$. La deuxième égalité amène $g \in H$, et $\psi$ étant l'identité sur $H$, on déduire de la première que $g = 0$. Ainsi, $\mathrm{Ker}(\Phi) = 0$.
  Par conséquent $\Psi$ est un morphisme injective, de $G$ sur $H \times G/H$. Par ailleurs, tous les cardinaux étant finis, on peut écrire :

  $$|H \times G/H| = |H| \times \frac{|G|}{|H|} = |G|.$$

  Ainsi, l'égalité des cardinaux finis prouve que la fonction injective $\Phi$ est en fait bijective.
  Ainsi, $\boxed{\Phi \text{ est un isomorphisme de } G \text{ sur } H \times G/H}$

5. On raisonne par récurrence forte sur $|G|$. Si $|G| = 1$, le résultat est trivial, avec $\ell = 1$ et $d_1 = 1$.
   Soit $n \in \mathbb{N}$ supérieur ou égal à 2 telle que la décomposition soit assurée pour tout groupe de cardinal strictement plus petit que $n$. Soit $G$ de cardinal $n$. Le sous-groupe $H$ construit précédemment n'est pas de cardinal 1, car le seul élément d'ordre 1 dans un groupe est l'élément neutre : s'il y a au moins deux éléments, l'élément d'ordre maximal sera donc d'ordre au moins 2. Par conséquent $|H| \geqslant 2$, et donc $G/H$ est de cardinal strictement inférieur à $n$. On peut donc appliquer l'hypothèse de récurrence à $G/H$, qui est donc isomorphe à un groupe

   $$G/H \simeq \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_\ell\mathbb{Z},$$

   pour un certain entier $\ell \geqslant 2$, et des entiers $d_2, \ldots, d_\ell$ tels que $d_\ell | d_{\ell-1} | \cdots | d_2$. En particulier, l'élément $(1, 0, \ldots, 0)$ de ce produit est d'ordre $d_2$. Il existe donc un élément $\overline{g}$ d'ordre $d_2$ dans $G/H$. On en déduit que l'ordre de $g$ est un multiple de $d_2$ (même raisonnement que plus haut), et comme cet ordre divise $d_1$ (question 2), on en

déduit que $d_2$ divise $d_1$. Ainsi, en utilisant la question 4, et le fait que $H$ soit isomorphe à $\mathbb{Z}/d_1\mathbb{Z}$, on a bien obtenu un isomorphisme :

$$\boxed{G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_\ell\mathbb{Z}},$$

où $d_\ell | \cdots | d_2 | d_1$.

## Partie V – Théorème de structure des groupes de type fini

1. • $*$ $1^1 = 1$, donc $1 \in T(G)$.
   $*$ Soit $x, y$ dans $T(G)$, d'ordres respectifs $a$ et $b$. On a alors

   $$ab(x-y) = b(ax) - a(by) = 0,$$

   donc $x - y \in T(G)$.
   $*$ Donc $\boxed{T(G) \text{ est un sous-groupe de } G}$.
   • Tout d'abord, $G$ étant de type fini, il existe une famille génératrice $(x_1, \ldots, x_n)$. Alors $(\overline{x_1}, \ldots, \overline{x_n})$ est génératrice dans le quotient $G/T(G)$. Ainsi, $\boxed{G/T(G) \text{ est de type fini}}$.
   • Par ailleurs, soit $X \in G/T(G)$, $X \neq \overline{0} = T(G)$, et soit $x$ un représentant de $X$ dans $G$ (donc nécessairement $x \notin T(G)$). S'il existe $n \in \mathbb{Z}^*$ tel que $nX = 0$, alors $nx \in T(G)$. Soit alors $a$ l'ordre (fini) de $nx$. On a donc $anx = 0$, avec $an \neq 0$, ce qui contredit le fait que $x \notin T(G)$. Ainsi, pour tout $n \in \mathbb{Z}^*$, $nX \neq 0$. On en déduit que $\boxed{G/T(G) \text{ est sans torsion}}$.
   • Étant de type fini et sans torsion, $\boxed{G \text{ est libre}}$ d'après la partie III.
2. Comme $G/T(G)$ est libre de type fini, on peut considérer $(\overline{x_1}, \ldots, \overline{x_n})$ une base de $G/T(G)$, de représentants $x_1, \ldots, x_n$ dans $G$. Montrons qu'on a alors

   $$G = T(G) \oplus \bigoplus_{i=1}^{n} \langle x_i \rangle,$$

   et que pour tout $i \in [\![1, n]\!]$, $\langle x_i \rangle \simeq \mathbb{Z}$.
   • Ce dernier point est immédiat : si ce n'était pas de cas, $\langle x_i \rangle$ serait cyclique, donc fini, donc $\langle \overline{x_i} \rangle$ serait aussi fini (donc cyclique) dans $G/T(G)$, ce qui est contradictoire. Ainsi, pour tout $i \in [\![1, n]\!]$, $\boxed{\langle x_i \rangle \simeq \mathbb{Z}}$.
   • La grosse somme de droite est directe, ce qui équivaut à dire que toute décomposition dans cette somme est unique : soit $x$ tel que

   $$x = \sum_{i=1}^{n} \alpha_i x_i = \sum_{i=1}^{n} \beta_i x_i.$$

   En passant au quotient,

   $$\sum_{i=1}^{n} \alpha_i \overline{x_i} = \sum_{i=1}^{n} \beta_i \overline{x_i}.$$

   Comme $(\overline{x_1}, \ldots, \overline{x_n})$ est une base, on a donc pour tout $i \in [\![1, n]\!]$, $\alpha_i = \beta_i$. Ainsi, la somme $\bigoplus_{i=1}^{n} \langle x_i \rangle$ est directe. Ceci combiné au premier point démontré peut se réexprimer en disant que la famille est libre.
   • Soit $g \in G$ tel que

   $$g = x + y = x' + y',$$

   où $x, x' \in T(G)$, et $y, y' \in \bigoplus_{i=1}^{n} \langle x_i \rangle$. On a alors

   $$x - x' = y' - y.$$

   Or, si $y' - y$ est non nul dans le groupe libre $\bigoplus_{i=1}^{n} \langle x_i \rangle$, il est d'ordre infini, ce qui contredit le fait que $x - x' \in T(G)$. Ainsi, $y' - y = 0$, puis $x = x'$, $y = y'$. Ainsi, on a unicité de la déomposition d'où la somme directe :

   $$T(G) \oplus \bigoplus_{i=1}^{n} \langle x_i \rangle.$$

- Il nous reste enfin à voir que cette somme vaut bien $G$ tout entier. C'est un sous-groupe de $G$. Il faut justifier l'inclusion réciproque. Soit $g \in G$. Puisque $(\overline{x_1}, \dots, \overline{x_n})$ est une base de $G/T(G)$, on peut écrire

$$\overline{g} = \sum_{i=1}^{n} \alpha_i \overline{x_i} = \overline{\sum_{i=1}^{n} \alpha_i x_i}, \qquad \text{soit:} \qquad \overline{g - \sum_{i=1}^{n} \alpha_i x_i} = \overline{0}.$$

  Ainsi, il existe $x_0 \in T(G)$ tel que

$$g - \sum_{i=1}^{n} \alpha_i x_i = x_0, \qquad \text{donc:} \qquad g = x_0 + \sum_{i=1}^{n} \alpha_i x_i.$$

  Ainsi, $g \in T(G) \oplus \bigoplus_{i=1}^{n} \langle x_i \rangle$.

- On a donc prouvé que $\boxed{G = T(G) \oplus \bigoplus_{i=1}^{n} \langle x_i \rangle}$.

- Par ailleurs, d'après la partie III, le groupe $\bigoplus_{i=1}^{n} \langle x_i \rangle$, libre de type fini et de rang $n$, est isomorphe à $\mathbb{Z}^n$, et le groupe de type fini $T(G)$ est isomorphe à un groupe $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_\ell\mathbb{Z}$ , avec $d_\ell | \cdots | d_2 | d_1$ (partie IV), donc

$$G \simeq \mathbb{Z}^n \oplus (\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_\ell\mathbb{Z}) .$$

- Mais au fait, pourquoi $T(G)$ est-il de type fini ? En notant $H$ la somme directe des $\langle x_i \rangle$ ci-dessus, on a $G = T(G) \oplus H$. On peut alors considérer un morphisme

$$f : G \mapsto H,$$

  défini pour tout $x \in G$ se décomposant en $x = x_T + x_H$, avec $x_T \in T(G)$ et $x_H \in H$ :

$$f(x) = x_T$$

  (projection sur $T(G)$ parallèlement à $H$. L'application $f$ est clairement un morphisme de groupes et est surjective. De plus, $G$ étant de type fini, il existe $(y_1, \dots, y_m)$ une famille génératrice finie de $G$. La surjectivité de $f$ assure alors que $(g(y_1), \dots, g(y_m))$ est une famille génératrice de $T(G)$. Ainsi, $\boxed{T(G) \text{ est de type fini}}$.

- On trouve l'énoncé précis du théorème de structure donné dans l'énoncé en utilisant I-3(b) pour passer de la somme directe au produit cartésien.

3. - L'unicité de l'exposant $n$ provient du fait que si

$$G = \mathbb{Z}^n \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_\ell\mathbb{Z},$$

  le groupe $T(G)$ est clairement $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_\ell\mathbb{Z}$, donc, en quotientant, $G/T(G) = \mathbb{Z}^n$ (cela reste vrai à isomorphisme près). Ainsi, $n$ est le rang de $G/T(G)$, groupe ne dépendant que de $G$. On en déduit l'unicité de $n$.

- Quitte à considérer $T(G)$, pour l'unicité des $d_i$, on peut se placer dans le cas où $G$ est un groupe fini. On démontre l'unicité des exposants $d_i$ par récurrence sur l'ordre de $G$.
  - ∗ Si l'ordre de $G$ est 1, $G = \{0\}$, et il n'y a pas grand chose à montrer.
  - ∗ Soit $n > 1$. Supposons l'unicité aquise pour tous les groupes d'ordre strictement inférieur à $n$. Soit $G$ d'ordre $n$. Supposons qu'on ait deux décompositions (qu'on réécrit sous forme de somme directe, afin de pouvoir voir chacun des termes comme sous-groupe de $G$) :

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_\ell\mathbb{Z} \simeq \mathbb{Z}/d'_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d'_{\ell'}\mathbb{Z},$$

    avec les relations de divisibilité imposées. Ces relations de divisibilité permettent de s'assurer que l'ordre maximal d'un élément de $G$ est $d_1$ dans la première décomposition et $d'_1$ dans la seconde. Ainsi, $d_1 = d'_1$. On considère alors $G/(\mathbb{Z}/d_1\mathbb{Z})$.
    Pour ce faire on remarque que si $G = H \oplus K$, alors le morphisme $x \mapsto \overline{0 + x}$ donne un isomorphisme de $K$ sur $G/H$. Ainsi

$$G/(\mathbb{Z}/d_1\mathbb{Z}) \simeq \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_\ell\mathbb{Z} \simeq \mathbb{Z}/d'_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d'_{\ell'}\mathbb{Z}.$$

    Comme $d_1 > 1$ (car 0 est le seul élément d'ordre 1), on en déduit que le cardinale du groupe $G/(\mathbb{Z}/d_1\mathbb{Z})$ est strictement plus petit que le cardinal de $G$, donc on peut lui appliquer l'hypothèse de récurrence, de laquelle il découle que $\ell = \ell'$ et pour tout $i \in [\![2, \ell]\!]$, $d_i = d'_i$.

- On déduit du principe de récurrence l'$\boxed{\text{unicité des constantes } n, \ \ell \text{ et } d_i \text{ dans la décomposition}}$.