Lycée Lakanal, Sceaux
MP – Mathématiques
A. Troesch

Pour le 20/11/2024, 21h00

DM n° 8 : structures algébriques

Corrigé 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, ℓ), où k est pair et ℓ 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
   $$\varphi((h,k)) = h + k.$$
   - φ 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.
   - φ est surjective, par définition même de $H_1 + H_2$
   - φ 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 $k \in [\![1, n]\!]$

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

En notant $X = \{x_i,\ i \in I\}$, on a donc

$$X \subset \bigoplus_{i\in J} \langle y_i \rangle .$$

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), on en déduit que

$$G = < X > \subset \bigoplus_{i\in J} \langle y_i \rangle, \qquad \text{puis:} \qquad \bigoplus_{i\in J} \langle y_i \rangle = G.$$

Comme J est fini et I est infini, on dispose de $i_0 \in I \backslash J$. 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 :

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

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 φ_i est bien à valeurs dans $\langle 2x_i\rangle$, et c'est de façon évidente un homomorphisme de groupes (même justification que pour φ). Par ailleurs :

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

En conclusion, φ_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 φ 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, toute base de G a même cardinal n.

Partie III – Groupes abéliens sans torsion

1. - $\mathbb{Q}$ est un groupe sans torsion. En effet, tout $x \in \mathbb{Q}$ non nul est d'ordre infini ($nx \neq 0$, pour tout $n \in \mathbb{Z}^*$)
   - $\mathbb{Q}/\mathbb{Z}$ 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 $\mathbb{Q}/\mathbb{Z}$.
   - $\mathbb{C}^*$ 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, 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) Soit X une famille génératrice de G. 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 $y \in \sum_{x\in X} \langle x \rangle$, on aurait unicité de la décomposition de x dans cette somme. 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, la somme $\bigoplus_{x\in X} \langle x \rangle$ est une somme directe de groupes monogènes infinis. On en déduit que 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

$$x = -\sum_{y\in X\backslash\{x\}} n_y y,$$

donc $x \in \bigoplus_{y\in X\backslash\{x\}} \langle y\rangle$.

On en déduit sans peine que $X\backslash\{x\}$ est encore une famille génératrice, dont le cardinal est strictement inférieur à celui de X. Cela contredit la minimalité du cardinal de X.

Ainsi, $\boxed{\text{pour tout } x \in X,\ n_x \neq 1.}$

(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 $\boxed{|n_x| < |n_y|}$.

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

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

Posons $x' = x + qy$ et $X' = \{x'\} \cup (X\backslash\{x\})$. 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 $z \in X'\backslash\{x', y\}$, $n'_z = n_z$, 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 $\boxed{\text{contredit le choix de } X}$, 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 φ_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 φ :

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

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 $\mathbb{Z}^m$. D'après la partie précédente, toute base de $\mathbb{Z}^m$ est donc aussi de cardinal m.
- Pour tout $x \in G$, puisque Φ est injective (donc son noyau est réduit à 0), $x^a = 0_G$ équivaut à $\Phi(x)^a = 0_{\mathbb{Z}^m}$. Ainsi, Φ préserve l'ordre, donc les $\Phi(x_i)$ sont d'ordre infini.
- Puisque Φ est injective, elle préserve les sommes directes. En effet, si E et f sont deux sous-groupes de G tels que $E \oplus F$ soit directe, alors soit $z \in \Phi(E) + \Phi(F)$, qu'on décompose de deux façons en

  $$z = x + y = x' + y',$$

  où $x, x' \in \Phi(E)$ et $y, y' \in \Phi(F)$. On écrit $x = \Phi(u)$, $x' = \Phi(u')$, $y = \Phi(v)$, $y' = \Phi(v')$, avec $u, u' \in E$ et $v, v' \in F$. Ainsi,

  $$\Phi(u + v) = \Phi(u) + \Phi(v) = x + y = z = x' + y' = \Phi(u' + v').$$

  Puisque Φ est injective, on en déduit que $u + v = u' + v'$. La somme $E \oplus F$ étant directe, $u = u'$ et $v = v'$, d'où $x = x'$ et $y = y'$. Ainsi la somme $\Phi(E) \oplus \Phi(F)$ est directe.
- On en déduit que la somme suivante est directe :

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

  L'égalité résulte du fait que

  $$\Phi(\langle x_i \rangle) = \{\Phi(nx), n \in \mathbb{Z}\} = \{n\Phi(x), n \in \mathbb{Z}\} = \langle \Phi(x_i) \rangle .$$

- Enfin, soit $y \in \mathbb{Z}^m$. Comme Φ est surjective, il existe $x \in G$ tel que $\Phi(x) = y$. Puisque $(x_1, \ldots, x_n)$ est une base de G, il existe $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ tels que

  $$x = \sum_{k=1}^{n} a_k x_k \qquad \text{donc:} \qquad y = \Phi(x) = \sum_{k=1}^{n} a_k \Phi(x_k).$$

  On en déduit que

  $$\mathbb{Z}^m = \bigoplus_{k=1}^{n} \langle \Phi(x_k) \rangle .$$

- Ainsi, $(\Phi(x_1), \ldots, \Phi(x_n))$ est une base de $\mathbb{Z}^m$. D'après le premier point, $m = n$.
  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 d_1.

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 ψ_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 $\psi'_{|K} = \psi$, donc si ψ' prolonge ψ 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 au lemme de Zorn). Notons (K, ψ) un tel élément maximal.
   - Si $K \neq G$, considérons un élément $y \in G \backslash K$, et montrons qu'on peut prolonger ψ 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) $\mathbb{U}_{d_1}$, d_1 étant l'ordre de x, donc l'exposant du groupe G. On note $\psi' : K \to H \to \mathbb{U}$ la composée de ψ et de cette injection. En particulier, l'image de ψ' est incluse dans $\mathbb{U}_{n_0}$.

     Pour prolonger ψ, on va commencer par prolonger ψ', 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 $\tilde{\psi'}(by) = \psi'(x_0)$, 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 λ, λ' 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 $k'-k = \alpha x_0$, donc $\psi'(k')-\psi'(k) = \alpha\psi'(x_0)$. 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 $\tilde{\psi'}(ay) = 0$, donc $\tilde{\psi'}(y)^a = 0$. Ainsi, l'ordre de $\tilde{\psi'}(y)$ dans $\mathbb{U}$ divise a. Or, l'ordre d_1 de x est par définition l'exposant du groupe G, donc est divisible par l'ordre de tout élément de G. Ainsi, a divise d_1, donc l'ordre de $\tilde{\psi'}(y)$ divise d_1 dans $\mathbb{U}$, ce qui implique que $\tilde{\psi'}(y)^{d_1} = 1$, donc $\tilde{\psi'}(y) \in \mathbb{U}_{d_1}$. 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 ψ, 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 ψ' 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

$$\psi(by) = kx = \frac{d_1 c'}{c}x = \frac{d_1 bc'}{a}x.$$

  On pose alors $y' = \frac{d_1 c'}{a}x$, 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, Φ 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 ψ étant l'identité sur H, on déduire de la première que $g = 0$. Ainsi, $\mathrm{Ker}(\Phi) = 0$.

  Par conséquent Φ est un morphisme injectif, 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 Φ 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 $(x_1, \dots, x_n)$. Alors $(\overline{x_1}, \dots, \overline{x_n})$ 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, $\boxed{G/T(G) \text{ est libre}}$ d'après la partie III.
2. Comme $G/T(G)$ est libre de type fini, on peut considérer $(\overline{x_1}, \dots, \overline{x_n})$ une base de $G/T(G)$, de représentants $x_1, \dots, x_n$ 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 $i \in [\![1, n]\!]$, $\boxed{\langle x_i \rangle \simeq \mathbb{Z}}$.
   - Montrons que 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 $(\overline{x_1}, \dots, \overline{x_n})$ 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 $(y_1, \ldots, y_m)$ une famille génératrice finie de G. La surjectivité de f assure alors que $(g(y_1), \ldots, g(y_m))$ 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 cardinal 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'$\boxed{\text{unicité des constantes } n, \ \ell \text{ et } d_i \text{ dans la décomposition}}$.

Corrigé du problème 2 – Théorèmes de Sylow

Partie I – Étude des sous-groupes de Sylow de $\mathbb{Z}/n\mathbb{Z}$

1. - On a $S = \{\overline{mk},\ k \in \mathbb{Z}\}$. En effet, l'inclusion directe est immédiate, et l'inclusion réciproque résulte du fait que si $k \in \mathbb{Z}$, et si r est le reste de la division euclidienne de k par p^α, on a l'existence de q tel que
$$k = p^\alpha q + r, \qquad \text{donc:} \qquad km = p^\alpha mq + rm \equiv rm \ [n].$$
Ainsi, $\overline{km} \in S$.

- Montrons que S est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$.
  * De façon évidente, $S \subset \mathbb{Z}/n\mathbb{Z}$, et $\overline{0} \in S$.
  * Soit $(x, y) \in S^2$. Il existe alors $(k, \ell) \in \mathbb{Z}^2$ tels que $x = \overline{mk}$ et $y = \overline{m\ell}$. On a alors $x - y = \overline{m(k-\ell)} \in S$.

  Ainsi, d'après la caractérisation des sous-groupes, S est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$.
- Soit $(k, \ell) \in [\![0, p^\alpha - 1]\!]$ tels que $k \neq \ell$, alors $|k - \ell| < p^\alpha$, donc $|m(k-\ell)| < n$, donc $mk \not\equiv m\ell[n]$. On en déduit que $\overline{mk} \neq \overline{m\ell}$.
- Ainsi, S est constitué d'exactement p^α éléments. $\boxed{S \text{ est donc un sous-groupe de Sylow de } \mathbb{Z}/n\mathbb{Z}}$.

2. Soit S' un p-sous-groupe de Sylow de $\mathbb{Z}/n\mathbb{Z}$, et soit $x \in S'$.
   (a) L'élément x étant un élément du groupe S' d'ordre p^α, on déduit du théorème de Lagrange que l'ordre de x divise p^α, donc, p étant premier, $\boxed{\text{l'ordre de } x \text{ est } p^\beta, \text{ pour un certain entier naturel } \beta \leqslant \alpha}$.
   (b) On en déduit que $\overline{p^\beta x} = 0$, donc si k est un représentant dans $\mathbb{Z}$ de x, il existe $\ell \in \mathbb{Z}$ tel que $p^\beta k = \ell n = \ell p^\alpha m$, donc $k = m\ell p^{\alpha-\beta}$, et comme $\alpha - \beta \geqslant 0$, $\boxed{x = \overline{k} \in S}$.
3. On en déduit que $S' \subset S$, et comme par définition, S et S' ont même cardinal fini, $S' = S$.
   Ainsi, $\boxed{\mathbb{Z}/n\mathbb{Z} \text{ admet un unique sous-groupe de Sylow, } S.}$

Remarque : Toute cette partie est en fait conséquence directe de la description générale des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$, vue en exercice : ce sont les $d\mathbb{Z}/n\mathbb{Z}$ où d divise n. Ces groupes sont de cardinal $\frac{n}{d}$. Le seul sous-groupe d'ordre p^α est donc celui obtenu pour $d = m$. Il correspond bien à la description élémentaire donnée dans cette partie.
Pour rappel, la description des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ s'obtient facilement à partir de la description des sous-groupes de $\mathbb{Z}$, qui sont les $a\mathbb{Z}$, $a \in \mathbb{N}$ (voir cours). En effet, en notant $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la projection canonique, qui est un morphisme de groupe, si G est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$, $\pi^{-1}(G)$ est un sous-groupe de $\mathbb{Z}$, donc de la forme $d\mathbb{Z}$. De plus, on doit avoir $\pi(n) = 0 \in G$, donc $n \in d\mathbb{Z}$, donc d est un diviseur de n. Enfin, en restreignant π à $d\mathbb{Z}$, on obtient un morphisme surjectif $d\mathbb{Z} \to G$, dont le noyau est $n\mathbb{Z}$. Avec le premier théorème d'isomorphisme démontré plus loin, on en déduit que $G \simeq d\mathbb{Z}/n\mathbb{Z}$, et on vérifie facilement que l'isomorphisme $\tilde{pi}$ obtenu en quotientant π correspond à l'inclusion de $d\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$.
Ce résultat peut aussi se montrer de façon élémentaire de la sorte : notant $G = \{\overline{x_1}, \dots, \overline{x_k}\}$, où les x_i sont des représentants des éléments 2 à 2 distincts de G, considérer d le pgcd des x_i, et montrer par double-inclusion que $G = d\mathbb{Z}/n\mathbb{Z}$ (on pourra adapter la preuve du cours de la description des sous-groupes de $\mathbb{Z}$, en considérant la division euclidienne par d).

Partie II – Actions de groupe, stabilisateurs, orbites

1. Quelques exemples.
   (a)
   - L'application donnant l'action de groupe est l'application de $H \times G$ dans G donnée par $h \cdot g = hg$ (où le point représente l'action de groupe, et le produit sans point représente la multiplication dans G).
   - On a bien, pour tout $(h, h') \in H^2$, et $g \in G$,

   $$h \cdot (h' \cdot g) = h \cdot (h'g) = h(h'g) = (hh')g = (hh') \cdot g,$$

   l'avant-dernière égalité découlant de l'associativité dans G.
   - On a également $e_H \cdot g = e_H g = e_G g = g$.

   Ainsi, $(h, g) \mapsto hg$ est une action du groupe H sur le groupe G.
   L'orbite d'un élément $g \in G$ est l'ensemble $\boxed{\{h \cdot g \mid h \in H\} = Hg}$, classe à droite modulo H.
   (b) $\boxed{\text{La translation à droite ne définit pas une action}}$ si le groupe H n'est pas abélien, car en général, si on appelle φ l'application désignant cette loi de composition externe définie sur G :

   $$\varphi(hh', g) = g(hh'),$$

   alors que

   $$\varphi(h, \varphi(h', g)) = g(h'h).$$

   Pour avoir le premier axiome définissant une action de groupe, il faudrait avoir $ghh' = gh'h$, ce qui n'est pas vrai en toute généralité.
   Pour régler le problème de l'inversion des deux termes, on peut faire précéder la multiplication à droite par h d'une opération qui justement inverse l'ordre des termes d'un produit, par exemple l'inversion : $\boxed{\psi : (h, g) \mapsto gh^{-1}}$ définit une action de groupe puisque pour tout $(h, h') \in H^2$ et tout $g \in G$:
   - $\psi(e, g) = ge = g$

- $\psi(hh', g) = g(hh')^{-1} = gh'^{-1}h^{-1} = \psi(h, \psi(h', g))$.

On peut aussi modifier la définition d'une action de groupe, en définissant une action de groupe à droite par $(g, x)\ in G \times X \mapsto x \cdot g$, et en remplaçant le premier axiome par $x \cdot (gg') = (x \cdot g) \cdot g'$.

(c) Vérifions que la conjugaison définit bien une action du groupe G sur lui-même. Ici encore on désigne avec un point l'action de groupe, et sans point le produit danbs G. Pour tout $(g, g', x) \in G^3$:
- $e \cdot x = exe^{-1} = x$
- $(gg') \cdot x = (gg')x(gg')^{-1} = gg'xg'^{-1}g^{-1} = g \cdot (g'xg'^{-1}) = g \cdot (g' \cdot x)$.

Ainsi, $\boxed{\text{la conjugaison définit bien une action de } G \text{ sur lui-même.}}$

(d) i. On note e le neutre de G. Soit H un sous-groupe de G, $g \in G$, et $H' = \{gxg^{-1},\ x \in H\}$. Montrons que H' est un sous-groupe de G :
- Puisque H est un sous-groupe de G, $e \in H$, donc $geg^{-1} \in H'$, soit $e \in H'$.
- Soit x' et y' dans H'. Il existe donc x et y dans H tels que $x' = gxg^{-1}$ et $y' = gyg^{-1}$. On a alors :

$$x'y'^{-1} = gxg^{-1}(gyg^{-1})^{-1}) = gxg^{-1}gy^{-1}g^{-1} = gxy^{-1}g^{-1}.$$

Or, H étant un sous-groupe de G, $xy^{-1} \in H$, donc $gxy^{-1}g^{-1} \in H'$, soit $x'y'^{-1} \in H'$.

Ainsi, d'après la caractérisation des sous-groupes, H' est un sous-groupe de G, donc $\boxed{gHg^{-1} \in X}$.

ii.
- D'après la question précédente, l'application $(g, H) \mapsto gHg^{-1}$ est bien définie de $G \times X$ dans X.
- Soit $H \in X$, on a évidemment $eHe^{-1} = H$
- Soit $H \in X$, $g, g' \in G$. On a :

$$(gg') \cdot H = \{gg'x(gg')^{-1},\ x \in H\} = \{g(g'xg'^{-1})g^{-1},\ x \in H\} = \{gyg^{-1}, y \in g'Hg'^{-1}\} = g \cdot (g' \cdot H).$$

Ainsi, $\boxed{(g, H) \mapsto gHg^{-1} \text{ est une action du groupe } G \text{ sur } X}$.

2. Soit $x \in X$, et $\mathrm{Stab}(x)$ le stabilisateur de x. Montrons que $\mathrm{Stab}(x)$ est un sous-groupe de G.
- On a, par définition, $\mathrm{Stab}(x) \subset G$
- On a $e \cdot x = x$, par définition d'une action de groupe, donc $e \in H_x$.
- Soit $(g, h) \in \mathrm{Stab}(x)^2$. On a

$$(h^{-1}h) \cdot x = e \cdot x = x \qquad \text{et} \qquad (h^{-1}h) \cdot x = h^{-1} \cdot (h \cdot x) = h^{-1} \cdot x,$$

puisque $h \in H_x$. Ainsi, $h^{-1} \cdot x = x$, puis

$$(gh^{-1}) \cdot x = g \cdot (h^{-1} \cdot x) = g \cdot x = x,$$

puisque $g \in \mathrm{Stab}(x)$. On en déduit que $gh^{-1} \in \mathrm{Stab}(x)$.

D'après la caractérisation des sous-groupes, $\boxed{\mathrm{Stab}(x) \text{ est donc un sous-groupe de } G}$.

3. (a) Montrons que $\mathcal{R}$ est une relation d'équivalence :
- Soit $x \in X$, on a $e \times x = x$, donc $x \in \omega(x)$, donc $x\mathcal{R}x$, d'où la reflexivité de $\mathcal{R}$.
- Soit $(x, y) \in X$ tel que $x\mathcal{R}y$. On a alors $y \in \omega(x)$, donc il existe $g \in G$ tel que $g \cdot x = y$, donc

$$g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x,$$

donc $x \in \omega(y)$, d'où $y\mathcal{R}x$, d'où la symétrie de $\mathcal{R}$.
- Soit $(x, y, z) \in X$ tel que $x\mathcal{R}y$ et $y\mathcal{R}z$. On a alors $y \in \omega(x)$ et $z \in \omega(y)$, d'où l'existence de g et h dans G tels que $y = g \cdot x$ et $z = h \cdot y$, d'où $z = h \cdot (g \cdot x) = (hg) \cdot x$. Comme G est un groupe, $hg \in G$, donc $z \in \omega(x)$, d'où $x\mathcal{R}z$. D'où la transitivité de $\mathcal{R}$.

On déduit des trois points précédents que $\boxed{\mathcal{R} \text{ est une relation d'équivalence}}$.

(b) Par définition même de $\mathcal{R}$, les classes d'équivalence pour la relation $\mathcal{R}$ sont exactement les orbites de X sous l'action de G. Ainsi, $\boxed{\text{l'ensemble des orbites forme une partition de } X}$.

4. Soit G un groupe opérant sur un ensemble X. Soit $x \in X$.

(a) Soit $\varphi : g \mapsto g \cdot x$, de G dans $\omega(x)$. Soit $(g, g') \in G$ tels que $g'^{-1}g \in \mathrm{Stab}(x)$. Alors

$$(g'^{-1}g) \cdot x = x \qquad \text{donc:} \qquad g' \cdot x = g' \cdot ((g'^{-1}g) \cdot x) = (g'g'^{-1}) \cdot (g \cdot x) = e \cdot (g \cdot x) = g \cdot x.$$

Réciproquement, si $g' \cdot x = g \cdot x$, alors

$$(g'^{-1}g) \cdot x = g'^{-1} \cdot (g \cdot x) = g'^{-1} \cdot (g' \cdot x) = (g'^{-1}g') \cdot x = \mathrm{e} \cdot x = e,$$

donc $g'^{-1}g \in \mathrm{Stab}(x)$. Ainsi, $\boxed{g'^{-1}g \in \mathrm{Stab}(x) \text{ ssi } \varphi(g) = \varphi(g')}$.

(b) Soit $x \in X$. L'application $\varphi : G \mapsto \omega(x)$ définie par $g \mapsto g \cdot x$ est surjective, par définition d'une orbite. Soit $y \in \omega(x)$, et g tel que $y = g \cdot x$. D'après la question précédente,

$$\varphi^{-1}(\{y\}) = \{g' \in G \mid g^{-1}g' \in \mathrm{Stab}(x)\}.$$

Or, par régularité de g, $g^{-1}g' \in \mathrm{Stab}(x)$ équivaut à $g' \in g\mathrm{Stab}(x)$. Ainsi, $\varphi^{-1}(\{y\}) = g\mathrm{Stab}(x)$, dont le cardinal est égal à $|\mathrm{Stab}(x)|$ (d'après le cours, les classes de congruence modulo un sous-groupe ont toutes même cardinal). Ainsi, d'après le lemme des bergers, l'image récirproque de tout point ayant même cardinal, on a $|G| = |\mathrm{Stab}(x)| \cdot |\omega(x)|$, soit : $\boxed{|\omega(x)| = \dfrac{|G|}{|\mathrm{Stab}(x)|}}$.

On peut aussi remarquer que l'application φ étant constante sur chaque classe $g\mathrm{Stab}(x)$, elle passe au quotient, définissant une application (pas un morphisme) de $(G/\mathrm{Stab}(x))_g$ vers $\omega(x)$. L'équivalence de la question précédente permet de montrer l'injectivité, la surjectivité résultant celle de φ.

5. (a) Comme l'ensemble des orbites forme une partition de X, le cardinal de X est la somme des cardinaux des orbites. Or $\sum_{i=1}^{n} |\Omega_i|$ est la somme des cardinaux des orbites non réduites à un point, et $|X_G|$ est la somme des cardinaux des orbites réduites à un point (chaque orbite étant de cardinal 1, et ces orbites étant exactement les singletons dont l'unique élément est un point fixe de l'action). Ainsi, on a bien :

$$\boxed{|X| = |X_G| + \sum_{i=1}^{n} |\Omega_i|}.$$

(b) Si G est d'ordre p^α, les Ω_i ont un cardinal strictement supérieur à 1, et divisant p^α d'après 4(b). Ainsi, leur cardinal est p^β pour un certain $\beta \in [\![1, \alpha]\!]$. On en déduit que pour tout $i \in [\![1, n]\!]$, $|\Omega_i| \equiv 0\ [p]$.
Ainsi, en réduisant l'égalité de la question précédente modulo p, on obtient :

$$\boxed{|X_G| \equiv |X|\ [p]}.$$

(c) Le centre $Z(G)$ est égal à l'ensemble des points fixes de G sous l'action de G sur lui-même par conjugaison : $g \cdot x = gxg^{-1}$. Ainsi, d'après la question précédente, $|Z(G)| \equiv |G| \equiv 0\ [p]$.
Comme par ailleurs $Z(G)$ est non vide (car il contient le neutre), son cardinal est au moins p, donc $\boxed{Z(G) \text{ n'est pas réduit au groupe trivial}}$.

Partie III – Démonstration des théorèmes de Sylow par Wielandt

1. Soit $E \in X$, et $g \in G$. Alors, g étant régulier, $x \mapsto g \cdot x$ est injective, et surjective de E dans $g \cdot E$, par définition de $g \cdot E$. Ainsi, il s'agit d'une bijection de E sur $g \cdot E$, donc $|g \cdot E| = |E| = p^\alpha$. On en déduit que $g \cdot E \in X$.
La preuve que la translation à gauche définit une $\boxed{\text{action de } G \text{ sur } X}$ est alors la même que la démonstration de la question 1(d).
2. Soit $E \in X$, et $\mathrm{Stab}(E)$ son stabilisateur par l'action définie dans la question précédente. Soit $x \in E$. Pour tout $a \in \mathrm{Stab}(E)$, $a \cdot E = E$, donc $ax \in E$. Considérons l'application $\varphi_x : \mathrm{Stab}(E) \to E$ définie par $a \mapsto ax$. Par régularité de x dans G, φ_x est injective. Par conséquent, $\boxed{|\mathrm{Stab}(E)| \leqslant |E| = p^\alpha.}$
3. (a) Si de plus, $|\mathrm{Stab}(E)| = p^\alpha$, alors l'application φ_x est une injection entre deux ensembles finis de même cardinal, donc une bijection. On en déduit que

$$E = \mathrm{Im}(\varphi_x) = \{ax \mid a \in \mathrm{Stab}(E)\} = \boxed{\mathrm{Stab}(E) \cdot x}.$$

Le choix de $x \in E$ dans la question précédente était arbitraire.

(b) Supposons qu'il existe $S \in Y$ et $x \in G$ tels que $E = Sx$. Par stabilité de S, tout élément $g \in S$ est dans le stabilisateur de E : $gE = gSx = Sx = E$. Ainsi, $S \subset \mathrm{Stab}(E)$.
Comme S est de cardinal p^α et $\mathrm{Stab}(E)$ de cardinal au plus p^α, cette inclusion est nécessairement une égalité : $\boxed{S = \mathrm{Stab}(E)}$, puis $\boxed{|\mathrm{Stab}(E)| = p^\alpha}$.

(c) Soit $S \neq S'$ dans Y. Considérons cette fois l'action sur E, définie par $(X, g) \mapsto Xg^{-1}$. On montre sans problème qu'il s'agit d'une action, comme en III-1. Pour éviter la confusion, notons $\mathrm{Stab}'(X)$ le stabilisateur de X sous cette action. En adaptant les arguments amenant III-3, on montre de même que si $E = xS$ pour

un élément x de G et un sous-groupe de Sylow S, alors $\mathrm{Stab}'(E) = S$ (en plus de la stabilité par produit de S, on utilise ici aussi la stabilité par inverse).

Supposons que deux sous-groupes de Sylow S et S' soient dans une même orbite sous l'action de G.

Il existe donc x dans G tel que $S' = xS$. On a aussi évidemment $S' = eS'$. La remarque précédente appliquée à ces deux égalités amènent, pour la première, $\mathrm{Stab}(S') = S$, et pour la seconde, $\mathrm{Stab}(S') = S'$. On en déduit que $S = S'$.

Ainsi, par contraposée, $\boxed{\text{deux sous groupes de Sylow distincts ne peuvent pas être dans la même orbite}}$.

On pouvait aussi s'en sortir de façon plus élémentaire, en remarquant que si S et S' sont dans la même orbite, il existe g tel que $S' = g \cdot S$, et comme le neutre e est dans S', il existe $g' \in S$ tel que $gg' = e$. Bien sûr, $g' = g^{-1}$, donc $g^{-1} \in S$, puis $g \in S$, puis $S' = g \cdot S = S$.

4. Puisque les orbites forment une partition de X, en notant Ω l'ensemble des orbites, on obtient :

$$|X| = \sum_{\omega \in \Omega} |\omega|.$$

Or :

- Dans un premier temps, on peut remarquer que le cardinal de $\mathrm{Stab}(E)$ est le même pour tout élément E d'une même orbite ω.

  D'après III-2 et II-4(b), pour toute classe ω telle que pour $E \in \omega$, $|\mathrm{Stab}(E)| \neq p^\alpha$, on a $v_p(\mathrm{Stab}(E)) < \alpha$, donc d'après II-4(b), $|\omega|$ est divisible par p. Ainsi, en notant Ω' l'ensemble des classes telles que pour $E \in \omega$, $\mathrm{Stab}(E)$ est de cardinal p^α, on a :

$$|X| \equiv \sum_{\omega \in \Omega'} |\omega| \ [p].$$

- Toujours d'après II-4(b), pour tout élément ω de Ω', le stabilisateur des éléments de ω étant de cardinal p^α, on a $|\omega| = m$. Ainsi,

$$|X| \equiv m|\Omega'| \ [p].$$

- Tout ω de Ω' contient un sous-groupe de Sylow (question 3(a) avec $S = \mathrm{Stab}(E)$) et un seul (question 3(c)). Réciproquement, d'après 3(b), l'orbite ω d'un sous-groupe de Sylow S est dans Ω'. Ainsi, tout sous-groupe de Sylow appartient à un élément ω de Ω'.

  on en déduit qu'il y a autant de sous-groupes de Sylow que d'orbites ω dans Ω' ; ainsi $|Y| = |\Omega'|$, puis

$$\boxed{|X| \equiv m|Y| \ [p]}.$$

5. Le cardinal de X ne dépend pas de la structure de groupe de G mais seulement de son cardinal (il s'agit du nombre de sous-ensembles de G ayant p^α élément). En particulier, ce cardinal est le même que celui de l'ensemble X' associé au groupe $\mathbb{Z}/n\mathbb{Z}$. En appliquant le résultat précédent au groupe $\mathbb{Z}/n\mathbb{Z}$, possédant un unique sous-groupe de Sylow d'après la partie 1, il vient donc :

$$|X| = |X'| \equiv m \ [p].$$

On revient donc au groupe G initial. On déduit de la question précédente que

$$m \equiv m|Y| \ [p],$$

et comme m est premier avec p^α, donc aussi avec p, m est inversible modulo p, donc

$$\boxed{|Y| \equiv 1 \ [p]}.$$

Partie IV – Quatre lemmes

1. **Lemme de Cauchy**

(a) Montrons que la loi donnée définit bien une action de $\mathbb{Z}/p\mathbb{Z}$ sur E

- Tout d'abord, soit $\ell \in [\![0, p-1]\!]$ et $(x_1, \cdots, x_p) \in E$. On a

$$\overline{\ell} \cdot (x_1, \cdots, x_p) = (x_{\ell+1}, \cdots x_p, x_1, \cdots x_\ell).$$

Or,

$$(x_1 \cdots x_\ell)(x_{\ell+1} \cdots x_p) = e,$$

donc

$$x_1 \cdots x_\ell = (x_{\ell+1} \cdots x_p)^{-1},$$

donc

$$(x_{\ell+1} \cdots x_p) \cdot (x_1 \cdots x_\ell) = e.$$

On en déduit que $\overline{\ell} \cdot (x_1, \cdots, x_p)$ est encore un élément de E.

- Ici, contrairement à la définition et à tous les exemples traités ci-dessus, le groupe donnant l'action est noté additivement. Il faut faire attention à transcrire convenablement les propriétés requises pour l'action dans ce cadre. Tout d'abord, $0 \cdot (y_1, \cdots, y_p) = (y_{1+0}, \cdots y_{n+0}) = (y_1, \cdots y_p)$.
- La deuxième condition est aussi vérifiée :

$$\alpha \cdot (\beta \cdot (y_1, \ldots, y_p)) = a \cdot (y_{1+\beta}, \cdots, y_{p+\beta}) = (y_{1+\beta+\alpha}, \ldots, y_{p+\beta+\alpha}) = (\alpha + \beta) \cdot (y_1, \ldots, y_n).$$

Il s'agit donc bien d'une $\boxed{\text{action de groupe}}$.

(b) Les points fixes sont les points dont toutes les coordonnées sont égales.

Ainsi, il s'agit des p-uplets $\boxed{(x, \ldots, x) \text{ tels que } x^p = 1}$.

Il y en a donc autant que de solutions de l'équation $x^p = 1$.

(c) D'après II-5(b) (avec $n = 1$), en notant $G_p = \{x \mid x^p = 1\}$, on a donc $|E| \equiv |G_p|\ [p]$. Or, un élément de E est déterminé par le choix quelconque des $p-1$ première coordonnées, imposant la dernière de façon unique :

$$y_p = (y_{p-1} \cdots y_1)^{-1}.$$

Par conséquent, $|E| = n^{p-1} \equiv 0\ [p]$. Puisque p divise n, $\boxed{|G_p| \equiv 0\ [p]}$.

(d) L'ensemble G_p est l'ensemble des éléments de G d'ordre divisant p, donc d'ordre 1 ou p. Il n'y a qu'un élément d'ordre 1 (le neutre), donc le nombre n_p d'éléments d'ordre p vérifie :

$$\boxed{n_p \equiv -1 \equiv p - 1\ [p]}.$$

Remarque : Le lemme de Cauchy étant très utile, il peut être intéressant de savoir faire rapidement sa preuve, mais en l'extrayant du contexte hors-programme des actions de groupe. On peut introduire la relation sur E définie par permutation circulaire des composantes du p-uplet. Si le p-uplet $X = (x_1, \ldots, x_p)$ n'est pas constitué de variables toutes égales, alors sa classe d'équivalence est de cardinal p. En effet, si ce n'est pas le cas, il existe une permutation circulaire non triviale (en décalant chaque coordonnée de k, avec $k \in [\![1, p-1]\!]$) laissant $(x_1, \ldots, x_p)$ invariant donc, avec les indices vus modulo p, pour tout $n \in \mathbb{Z}$, $x_{n+k} = x_n$, et en itérant (dans un sens et dans l'autre), $x_{n+\alpha k} = x_n$, pour tout $\alpha \in \mathbb{Z}$. Comme k est premier avec p, il existe une relation de Bezout $uk + vp = 1$. On a alors, pour tout $n \in \mathbb{Z}$, $x_n = x_{n+uk} = x_{n+1-vp} = x_{n+1}$, par p-périodicité de (x_n), ce qui signifie bien que les x_i sont tous égaux. On termine alors de même que ci-dessus, en réduisant modulo p l'égalité entre le cardinal de E et la somme des cardinaux des classes d'équivalence, ne restant dans cette somme que les classes d'équivalence de cardinal 1, correspondant aux p-uplets $(x, \ldots, x)$, avec $x^p = 1$. Le nombre de ces p-uplets est alors congru à 0 modulo p ; il s'agit aussi du nombre d'éléments x de G dont l'ordre divise p, donc est égal à 1 ou p. Comme e est le seul élément d'ordre 1, il reste bien $p-1$ modulo p éléments d'ordre p.

2. **Image réciproque d'un sous-groupe**
   - Par définition, $f^{-1}(K) \subset G$.
   - Puisque $1_H \in K$ (car K est un sous-groupe), et puisque $f(1_G) = 1_H$ (car f est un homomorphisme de groupes), on a bien $1_G \in f^{-1}(K)$.
   - Soit $(x, y) \in f^{-1}(K)$. On a donc $f(x) \in K$ et $f(y) \in K$. On a alors, par le fait que f est un homomorphisme de groupes, et par stabilité de K :

$$f(xy^{-1}) = f(x)f(y)^{-1} \in K.$$

   Donc $xy^{-1} \in f^{-1}(K)$.

   On déduit alors de la caractérisation des sous-groupes que $\boxed{f^{-1}(K) \text{ est un sous-groupe de } G}$.

3. **Groupes quotients**

(a) Les classes à gauche et à droite sont les mêmes. Or la partition des classes d'équivalences détermine de façon unique une relation d'équivalence. Ainsi, les relations $\boxed{\equiv_g \text{ et } \equiv_d \text{ sont identiques}}$. On notera simplement $\equiv$ cette relation.

(b) Soit $(x, x', y, y') \in G^4$ tels que $x \equiv x'\ [H]$ et $y \equiv y'\ [H]$. On a alors

$$x \in Hx' = x'H \qquad \text{et} \qquad y \in Hy',$$

Soit h et h' tels que $x = x'h$ et $y = h'y'$. On a alors $xy = x'hh'y'$
Or $x'hh' \in x'H = Hx'$, il existe donc $h'' \in H'$ tel que $x' = h''x'$, puis $xy = h''x'y'$. Ainsi, $xy \in Hx'y'$, d'où $xy \equiv x'y'\ [H]$.
Ainsi, $\boxed{\equiv \text{ est une congruence pour la loi du groupe } G}$

(c)
- Soit C, D et E trois classes modulo H, et x, y, z des représentants dans G de ces classes. Alors, par définition, et par associativité dans G :

$$(C \times D) \times E = (\overline{xy})\overline{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{x}(\overline{yz}) = C \times (D \times E).$$

D'où l'associativité de la loi définie sur G/H.
- On a $H = \overline{1_G}$. On a alors, pour toute classe C, de représentant x dans G :

$$H \times C = \overline{1_G} \times \overline{x} = \overline{1_G x} = \overline{x} = C.$$

Ainsi, il y a dans G/H un élément neutre, égal à $H = \overline{1_G}$.
- Soit $C \in G/H$, représentée par un élément $x \in G$. On a alors

$$x^{-1}x = 1_G = xx^{-1} \qquad \text{donc:} \qquad \overline{x^{-1}} \times \overline{x} = \overline{1_G} = \overline{x} \times \overline{x^{-1}}.$$

Ainsi, $\overline{x^{-1}}$ est un symétrique de C dans G/H

On a bien vérifié tous les axiomes d'une structure de groupe : $\boxed{G/H \text{ est bien muni d'une structure de groupe}}$.
On peut remarquer que la loi de groupe est explicitement donnée par $(aH) \cdot (bH) = (ab)H$, ce qui est commode pour les manipulations. De plus, cette définition correspond aussi au produit terme à terme des éléments de aH et de bH (vérification facile).

4. **Premier théorème d'isomorphisme**.

(a)
- $\mathrm{Ker}(f) = f^{-1}(\{e\})$ est un sous-groupe de G d'après la question (3).
- Montrons que $\mathrm{Ker}(f)$ est distingué dans G. Il suffit pour cela de montrer que si $g \in G$ et $h \in \mathrm{Ker}(f)$, alors $ghg^{-1} \in \mathrm{Ker}(f)$. Soit donc $g \in G$ et $h \in \mathrm{Ker}(f)$. On a alors :

$$f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)1_H f(g)^{-1} = f(g)f(g)^{-1} = 1_H.$$

Ainsi, $\boxed{\mathrm{Ker}(f) \text{ est un sous-groupe distingué de } G.}$

(b) Soit $x \equiv y\ [\mathrm{Ker}(f)]$, on a donc $xy^{-1} \in \mathrm{Ker}(f)$, d'où :

$$f(xy^{-1}) = 1_H \qquad \text{soit:} \qquad f(x)f(y)^{-1} = 1_H \qquad \text{donc:} \qquad f(x) = f(y).$$

Ainsi, $\boxed{f \text{ est constante sur chaque classe d'équivalence modulo } \mathrm{Ker}(f)}$. Elle induit donc une application $\overline{f} : G/\mathrm{Ker}(f) \longrightarrow H$

(c)
- Soit C et D deux classes modulo $\mathrm{Ker}(f)$, représentées par x et y respectivement. Supposons que $\overline{f}(C) = \overline{f}(D)$, soit $f(x) = f(y)$. On a alors

$$f(xy^{-1}) = f(x)f(y)^{-1} = 1_H, \qquad \text{donc:} \qquad xy^{-1} \in \mathrm{Ker}(f).$$

On en déduit que $x \equiv y\ [H]$, puis $C = D$. Donc $\overline{f}$ est injective.
- Soit $h \in H$. Puisque par hypothèse, f est surjective, il existe $x \in G$ tel que $f(x) = h$, donc $\overline{f}(\overline{x}) = h$, d'où la surjectivité de $\overline{f}$.

$\boxed{\text{La fonction } \overline{f} \text{ est injective et surjective, donc bijective}}$.

(d) On a donc $|G/\mathrm{Ker}(f)| = |H|$. Or, on a vu dans le cours (cf démonstration du théorème de Lagrange) que

$$|G/\mathrm{Ker}(f)| = \frac{|G|}{|\mathrm{Ker}(f)|}.$$

On obtient donc la relation : $\boxed{|G| = |\mathrm{Ker}(f)| \times |H|.}$

Partie V – Une démonstration par récurrence du premier théorème de Sylow

1. On suppose dans cette question que G est abélien.

   (a) D'après le lemme de Cauchy, puisque p divise n, il existe un élément x d'ordre p dans G. Soit $H = \{x^i,\ i \in \mathbb{Z}\}$ le sous-groupe monogène engendré par x. H est donc d'ordre p. Par ailleurs, G étant abélien, tout sous-groupe de G est évidemment distingué !

   Ainsi, $\boxed{\text{il existe bien un sous-groupe distingué } H \text{ d'ordre } p}$.

   (b) Soit $m \in \mathbb{N}$, premier avec p.

   Soit, pour tout α dans $\mathbb{N}$, la propriété $\mathcal{P}(\alpha)$: Tout groupe abélien G d'ordre $p^\alpha m$ admet un p-sous-groupe de Sylow.

   Le cas $\alpha = 0$ est trivial, un p-sous-groupe de Sylow étant dans ce cas d'ordre $p^0 = 1$. Le sous-groupe $\{1_G\}$ convient.

   Soit $\alpha \in \mathbb{N}$. On suppose que la propriété $\mathcal{P}(\alpha)$ est vraie. Soit G un groupe abélien d'ordre $p^{\alpha+1}m$. D'après la question précédente (puisque $\alpha + 1 > 0$), G admet un sous-groupe distingué H d'ordre p. Soit alors $f : G \longrightarrow G/H$ l'application qui à x associe sa classe $\overline{x}$ modulo H (projection canonique). Puisque G/H est de cardinal $p^\alpha m$ et est abélien, on peut lui appliquer l'hypothèse de récurrence : il existe un p-sous-groupe de Sylow S de G/H. On considère alors $S' = f^{-1}(S)$. D'après IV-2, S' est un sous-groupe de G/H et f se restreint en un morphisme de groupe surjectif $\tilde{f}$ de S' sur S. Par ailleurs, puisque $\mathrm{Ker}(f) \subset S'$, on a $\mathrm{Ker}(\tilde{f}) = \mathrm{Ker}(f) = H$. Ainsi, en appliquant IV-4(d) à $\tilde{f}$, il vient :

   $$|S'| = |H| \times |S| \qquad \text{donc:} \qquad |S'| = p \times p^\alpha = p^{\alpha+1}.$$

   On en déduit que S' est un p-sous-groupe de Sylow de G. On a bien prouvé $\mathcal{P}(\alpha + 1)$.

   Par conséquent, $\mathcal{P}(0)$ est vraie, et pour tout α dans $\mathbb{N}$, $\mathcal{P}(\alpha)$ entraîne $\mathcal{P}(\alpha + 1)$. D'après le principe de récurrence, $\mathcal{P}(\alpha)$ est vraie pour tout α dans $\mathbb{N}$.

   Ainsi, $\boxed{\text{tout groupe abélien admet un } p\text{-sous-groupe de Sylow.}}$

2. (a)
   - De façon évidente, $Z(G) \subset G$ et $1_G \in Z$.
   - Soit $(x, y) \in Z(G)^2$. On a alors, pour tout $g \in G$,

     $$(xy)g = x(yg) = (yg)x = y(gx) = (gx)y = g(xy).$$

     Ainsi, $xy \in Z(G)$
   - Soit $x \in Z(G)$. On a alors, pour tout $g \in G$

     $$g = (xx^{-1})g = x(x^{-1}g) = (x^{-1}g)x.$$

     D'un autre côté :

     $$g = g(x^{-1}x) = (gx^{-1})x.$$

     Ainsi, $(x^{-1}g)x = (gx^{-1})x$, et x étant régulier, $x^{-1}g = gx^{-1}$. On en déduit que $x^{-1} \in Z(G)$.

   Ainsi, $\boxed{Z(G) \text{ est un sous-groupe de } G}$. De plus, tout élément de $Z(G)$ commute avec tout élément de G, donc en particulier avec tout autre élément de $Z(G)$. Donc $\boxed{Z(G) \text{ est commutatif}}$.

   Puisque tout élément de $Z(G)$ commute avec tout élément de G, pour tout $z \in Z(G)$, pour tout $g \in G$, $gzg^{-1} = gg^{-1}z = z \in Z(G)$, donc $\boxed{Z(G) \text{ est distingué dans } G}$.

   (b) Supposons que $|Z(G)|$ soit non divisible par p. Les éléments de $Z(G)$ sont les points fixes par l'action de G sur lui-même par conjugaison. Ainsi, d'après II-5(a), en notant Ω' l'ensemble des orbites non réduites à un point pour cette action, on a :

   $$|G| = |Z(G)| + \sum_{\omega \in \Omega'} |\omega|.$$

   Si toutes les orbites $\omega \in \Omega'$ sont de cardinal divisible par p, puisque p divise $|G|$, on obtient : $0 \equiv |Z(G)|\ [p]$, d'où une contradiction.

   Ainsi, $\boxed{\text{il existe au moins une classe } \omega \text{ de cardinal différent de 1 et premier avec } p.}$

   (c) Soit, pour tout n dans $\mathbb{N}$, la propriété $\mathcal{P}(n)$: Tout groupe d'ordre n admet un p-sous-groupe de Sylow.

   La propriété est triviale pour $n = 1$.

   Soit $n > 1$. On suppose que $\mathcal{P}(1), \ldots, \mathcal{P}(n-1)$ sont vrais. Soit G un groupe d'ordre n, et Z son centre. On écrit $n = p^\alpha m$, où p et m sont premiers entre eux. Si $m = 1$, le résultat est trivial (G est un p-sous-groupe de Sylow de lui-même). Supposons donc $m > 1$.

- Supposons $|Z|$ premier avec p. Dans ce cas, il existe une orbite ω non réduite à un point, de cardinal premier avec p, donc divisant m. Soit $x \in \omega$ et $\mathrm{Stab}(x)$ le stabilisateur de x. Alors $\mathrm{Stab}(x)$ est un sous-groupe de G, et d'après II-4, son cardinal est $p^\alpha k$, où $k = \frac{m}{|\omega|}$. Comme $|\omega| \neq 1$, $p^\alpha k < n$, et on peut donc appliquer l'hypothèse de récurrence à $\mathrm{Stab}(x)$, qui admet un p-sous-groupe de Sylow, donc un sous-groupe S de cardinal p^α. Ce sous-groupe est aussi sous-groupe de G, de cardinal p^α. Il s'agit donc d'un p-sous-groupe de Sylow de G.
- Supposons $|Z|$ non premier avec p. On note $|Z| = p^\beta q$, où p et q sont premiers entre eux ; on a alors $1 \leqslant \beta \leqslant \alpha$. Soit T un p-sous-groupe de Sylow T du groupe abélien Z (existe par la question 1, Z étant abélien, ce qui permet aussi de régler le cas éventuel où $Z = G$, cas dans lequel l'hypothèse de récurrence est inutilisable). Le groupe T est d'ordre p^β. par ailleurs, T est distingué dans G (même démonstration que pour Z). On peut donc munir G/T d'une structure de groupe.

  La projection $f : G \longrightarrow G/T$, qui à x associe sa classe $\overline{x}$ modulo T est alors un morphisme de groupe surjectif, de noyau $\mathrm{Ker}(f) = T$.

  Par ailleurs $|G/T| = p^{\alpha-\beta}m$. Comme $\beta > 0$, on peut appliquer l'hypothèse de récurrence à G/T : soit U un p-sous-groupe de Sylow de G/T, donc de cardinal $p^{\alpha-\beta}$. On considère alors $S = f^{-1}(U)$. La restriction à S de f est surjective sur U et de noyau T, donc d'après le premier théorème d'isomophisme,

  $$|S| = |U| \times |T| = p^\alpha.$$

  Ainsi, S est un sous-groupe de Sylow de G.

On a bien prouvé, dans tous les cas, que G admet un p-sous-groupe de Sylow.

Par conséquent, $\mathcal{P}(n-1)$ est vraie, et pour tout n dans 1, $\mathcal{P}(n-1), \ldots, \mathcal{P}(n-1)$ entraînent $\mathcal{P}(n)$. D'après le principe de récurrence forte, $\mathcal{P}(n)$ est vraie pour tout n dans $\mathbb{N}$.

Ainsi, $\boxed{\text{tout groupe fini admet un } p\text{-sous-groupe de Sylow}}$.

Partie VI – Démonstration des deuxième et troisième théorèmes de Sylow

1. Soit S un p-sous-groupe de Sylow de G. Soit H un p-sous-groupe de G. On fait opérer H sur l'ensemble $X = (G/S)_g$ des classes à gauche xS par translation : $h \cdot (xS) = (hx) \cdot S$.
   (a) On a, d'après II-5(a) :
   $$|X| = |X_H| + \sum_{o m \in \Omega'} |\omega|,$$
   où Ω' est l'ensemble des orbites non réduites à un point. Or, d'après II-4(b), pour tout $\omega \in \Omega'$, $|\omega|$ divise $|H|$, donc est une puissance de p. Comme $|\omega| \neq 1$, on en déduit que $|\omega| \equiv 0\ [p]$. Ainsi,
   $$\boxed{|X_H| \equiv |X| = \frac{|G|}{|S|} = m \mod [p]}.$$
   (b) Comme m n'est pas divisible par p, ceci implique qu'il existe au moins un point fixe, donc une classe xS telle que pour tout $h \in H$, $h(xS) = xS$, puis $\boxed{h(xSx^{-1}) = xSx^{-1}}$.
   (c) Il n'est pas dur de voir que xSx^{-1} est un sous-groupe de G, et que son cardinal est p^α. C'est donc un sous-groupe de Sylow. On a déjà justifié que dans ce cas, son stabilisateur pour l'action à gauche est lui-même (partie III). Or, le résultat précédent montre que tout $h \in H$ est dans ce stabilisateur.

   Ainsi, $\boxed{H \text{ est un sous-groupe du sous-groupe de Sylow } xSx^{-1}}$.
2. Soit S et S' deux sous-groupes de Sylow. On applique le résultat précédent avec $H = S'$. On en déduit l'existence de $x \in G$ tel que $S' \subset xSx^{-1}$, et pour des raisons de cardinalité, on en déduit que $\boxed{S' = xSx^{-1}}$.

   Ainsi, les p-sous-groupes de Sylow sont deux à deux conjugués.
3. (a) Les p-Sylow étant deux à deux conjugués, et le conjugué d'un p-Sylow étant encore un p-Sylow, Ω_S est très précisément $\boxed{\text{l'ensemble } Y \text{ des } p\text{-sous-groupes de Sylow}}$.
   (b) Ainsi, d'après II-3(b), $\boxed{|Y| = |\Omega_S| = \frac{|G|}{|\mathrm{Stab}(S)|}}$, le stabilisateur étant ici pris au sens de la conjugaison (ne pas s'embrouiller dans les différentes actions considérées).

   Ceci permet de conclure de façon immédiate que $\boxed{|Y| \text{ divise } n = |G|}$.

   Le dernier point ($|Y| \equiv 1\ [p]$) a été démontré en partie III.