Groupes abéliens de type fini

Le théorème chinois donne des exemples de groupes abéliens finis qui se décomposent en un produit de groupes cycliques plus simples. Par exemple $\mathbf{Z}/6\mathbf{Z}$ est isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$. D'autre part $(\mathbf{Z}/2\mathbf{Z})^2$ est un groupe abélien d'ordre 4 qui n'est pas cyclique puisque tous ses éléments sont d'ordre au plus 2. Il n'est donc pas isomorphe à $\mathbf{Z}/4\mathbf{Z}$. Un des problèmes que l'on va étudier ici est celui de l'existence et de l'unicité de la décomposition, à isomorphisme près, d'un groupe abélien fini en un produit de groupes cycliques.

1. Définitions et notations

On suppose connues les définitions des mots ou expressions *groupe*, *groupe abélien (ou commutatif)*, *morphisme de groupes*, *noyau, image d'un morphisme de groupes*. Le mot *entier* désigne un élément de l'ensemble des entiers relatifs $\mathbf{Z}$.
La loi d'un groupe abélien G sera toujours notée additivement et l'élément neutre sera désigné par 0. L'opposé d'un élément a de G est noté $-a$ et si n est un entier naturel, na se définit par récurrence : $0a := 0$ et $na := a + (n-1)a$. On pose alors $(-n)a := -(na)$. Autrement dit, on vient de définir une action de l'anneau $\mathbf{Z}$ sur le groupe abélien G.
On dira que deux groupes G et G' sont *isomorphes* s'il existe deux morphismes de groupes $f : G \longrightarrow G'$ et $g : G' \longrightarrow G$ tels que $f \circ g = \mathrm{Id}_G$ et $g \circ f = \mathrm{Id}_{G'}$. Pour cela il faut et il suffit que f soit un morphisme de groupes bijectif (le vérifier). Un morphisme de groupes est *injectif* si son *noyau* est réduit à 0 (le vérifier).
On considère un groupe abélien G, un élément a de G et tous les na pour n entier ; plus précisément on considère l'application

$$\begin{array}{ccc} \mathbf{Z} & \longrightarrow & G \\ n & \longmapsto & na. \end{array}$$

On vérifie que c'est un morphisme de groupes. Son noyau est un sous-groupe de $\mathbf{Z}$. Il existe donc un entier d, appelé l'**ordre** de a, caractérisé par l'une des propriétés suivantes

(1) $na = 0$ dans G (on dit que n annule a dans G) si et seulement si n est un multiple de d.
(2) d est le plus petit des entiers qui annulent a dans G.
(3) $da = 0$ et aucun diviseur strict de d n'annule a.

Exercice 1. ▶ On se donne un groupe abélien G et un élément a de G.
Montrer que l'ordre de a est l'ordre du sous-groupe (cyclique) engendré par a dans G.
Soit p un nombre premier. Montrer que a est d'ordre p si et seulement si $pa = 0$ et $a \neq 0$ dans G.
Montrer que a est d'ordre 12 dans G, si et seulement si $12a = 0$ et $6a \neq 0$ et $4a \neq 0$ dans G. ◀

Définition 1.1. *On dit qu'un groupe abélien G est de* type fini *s'il existe une* famille génératrice finie *de G, c'est-à-dire un entier r et une famille $(a_1, \ldots, a_r)$ d'éléments de G tel que tout élément de G est une combinaison linéaire à coefficients entiers d'éléments du système $(a_1, \ldots, a_r)$.*

Précisément, pour tout g dans G, il existe des entiers $n_1, \ldots, n_k$ tels que $g = \sum_{i=1}^{r} n_i a_i$. Une telle écriture n'a aucune raison d'être unique.
On peut traduire ce qui précède comme suit : le groupe G est engendré par $(a_1, \ldots, a_r)$ si et seulement si le morphisme de groupes

$$\begin{array}{ccc} \mathbf{Z}^r & \longrightarrow & G \\ (n_1, \ldots, n_r) & \longmapsto & \displaystyle\sum_{i=1}^{r} n_i a_i \end{array}$$

est surjectif.
On a donc obtenu la formulation équivalente suivante : *le groupe G est un groupe abélien de type fini si et seulement si il existe un entier r et un morphisme surjectif de $\mathbf{Z}^r$ sur G.*

Exemple 1.2. Un groupe engendré par un élément est

(1) soit réduit à l'élément neutre,
(2) soit égal à $\mathbf{Z}$,
(3) soit cyclique et fini.

On convient que le système vide engendre le groupe réduit à l'élément neutre 0.

Exercice 2. ▶ Montrer que l'ensemble

$$G := \{a + b\sqrt{2} \mid a, b \in \mathbf{Z}\}$$

est un sous-groupe de $\mathbf{R}$, engendré par le système $(1, \sqrt{2})$ et ne peut pas être engendré par un seul élément de G.
Montrer que l'application

$$\begin{array}{ccc} \mathbf{Z}^2 & \longrightarrow & G \\ (a, b) & \longmapsto & a + b\sqrt{2} \end{array}$$

est un isomorphisme de groupe.
Montrer que le groupe additif des rationnels $\mathbf{Q}$ n'est pas de type fini. Indication : un ensemble fini de rationnels a un dénominateur commun. ◀

2. Groupes abéliens libres de type fini

On dit qu'un groupe abélien G est *libre de type fini* s'il existe un entier naturel r tel que G est *isomorphe* à $\mathbf{Z}^r$.

Exemple 2.1. Le groupe $\mathbf{Z}^r$. Pour j de 1 à r, on note e_j l'élément dont la j-ème coordonnée vaut 1 et les autres 0. Vérifier que tout élément x de $\mathbf{Z}^r$ a une écriture unique

$$x = \sum_{i=1}^{r} x_i e_i.$$

Le système $(e_1, \dots, e_r)$ est donc un système générateur. Il est aussi $\mathbf{Z}$-*libre* au sens suivant : si $0 = \sum_{i=1}^{r} x_i e_i$ alors tous les x_i sont nuls. On l'appelle $\mathbf{Z}$-*base canonique* de $\mathbf{Z}^r$.
Attention ! L'analogie avec les notions correspondantes de la catégorie des espaces vectoriels a ses limites. Par exemple :

- Montrer que $(2, 3)$ est une partie génératrice de $\mathbf{Z}$. Quels sont les systèmes libres qu'elle contient ?
- Montrer que tout système libre extrait de $(2, 3)$ n'engendre pas $\mathbf{Z}$ et en déduire que *l'analogue du théorème de la base incomplète est faux pour les groupes libres.*

Un morphisme de groupes de $\mathbf{Z}^r$ dans $\mathbf{Z}^s$ est $\mathbf{Z}$-linéaire. Il est déterminé par sa matrice (à coefficients entiers) dans les bases canoniques de $\mathbf{Z}^r$ et $\mathbf{Z}^s$.

Exercice 3. ► Soit G un groupe abélien de type fini. Montrer que de tout système générateur, on peut extraire un système $\mathbf{Z}$-libre maximal, éventuellement vide (voir 3.8 pour la suite).
Que se passe-t-il lorsque G est fini ?
Si $G = \mathbf{Z}^r$, montrer qu'un système libre maximal a r éléments. Donner un exemple où un tel système libre maximal ne se complète pas en une base de G. ◄

Exercice 4. ► On donne deux vecteurs (a, b) et (c, d) dans $\mathbf{Z}^2$. On désigne par L le sous-groupe qu'ils engendrent.
Montrer que $L = \mathbf{Z}^2$ si et seulement si $|ad - bc| = 1$.
Montrer que si $(a', b'), (c', d')$ est une autre $\mathbf{Z}$-base de L, alors $|ad - bc| = |a'd' - c'd'|$. Généraliser les énoncés précédents aux sous-groupes de $\mathbf{Z}^r$. ◄

Exercice 5. ► On considère le sous-ensemble de $\mathbf{R}$

$$A := \{a + b\sqrt{2} + c\sqrt{3} \mid a, b, c \in \mathbf{Z}\}.$$

Montrer que c'est un groupe libre. ◄

Exercice 6. ► On considère le sous-ensemble de $\mathbf{C}$ (entiers de Gauss)

$$\mathbf{Z}[i] := \{a + ib \mid a, b \in \mathbf{Z}\}.$$

Montrer que c'est un groupe libre. ◄

Proposition 2.2. *Soient r et s deux entiers naturels. Les deux groupes $\mathbf{Z}^r$ et $\mathbf{Z}^s$ sont isomorphes si et seulement si $r = s$.*

Démonstration. Supposons qu'il existe un morphisme injectif de groupes

$$\varphi : \mathbf{Z}^r \longrightarrow \mathbf{Z}^s,$$

que l'on peut prolonger en un morphisme injectif, noté $\widetilde{\varphi}$, de $\mathbf{Z}^r$ dans $\mathbf{Q}^s$. Considérons dans *l'espace vectoriel* $\mathbf{Q}^s$ une relation linéaire à coefficients rationnels

$$\sum_{j=1}^{r} \lambda_j \widetilde{\varphi}(e_j) = 0.$$

entre les images $\widetilde{\varphi}(e_1), \dots, \widetilde{\varphi}(e_r)$ des éléments de la $\mathbf{Z}$-base canonique de $\mathbf{Z}^r$.
En multipliant les rationnels λ_j par un dénominateur commun d on obtient un élément $\sum_j d\lambda_j e_j$ dans $\mathbf{Z}^r$ dont l'image par $\widetilde{\varphi}$, donc par φ est nulle. Comme φ est injective, c'est que $\sum_j d\lambda_j e_j$ est nul dans $\mathbf{Z}^r$. On en conclut que les $d\lambda_j$, $1 \leq j \leq r$ sont tous nuls.
La famille $(\widetilde{\varphi}(e_1), \dots, \widetilde{\varphi}(e_r))$ est libre dans $\mathbf{Q}^s$. Il s'ensuit que $r \leq s$.
Si $\mathbf{Z}^r$ et $\mathbf{Z}^s$ sont isomorphes, on a donc $r = s$. □

Si L est libre de type fini, il existe donc un *unique* entier naturel r tel que L est isomorphe à $\mathbf{Z}^r$. On l'appelle le *rang* de L. Un système de générateurs de L comportant r éléments est appelé une $\mathbf{Z}$-base de L. *Attention ! la notion de $\mathbf{Z}$-base n'a de sens que pour un groupe libre.*
Un produit de deux groupes libres de rangs respectifs r et s est libre de rang $r + s$.

Exercice 7. ► Reprendre la démonstration de la proposition 2.2 et montrer que pour un morphisme φ injectif (resp. surjectif) de $\mathbf{Z}^r$ dans $\mathbf{Z}^s$, alors le rang de la matrice A de φ dans les $\mathbf{Z}$-bases canoniques est r (resp. s) et que $r \leq s$ (resp. $r \geq s$).
Lorsque $r = s$, montrer que le morphisme φ est injectif (resp. bijectif) si et seulement si le déterminant de sa matrice A est non nul (resp. inversible dans $\mathbf{Z}$). En déduire que le groupe des matrices inversibles dans $\mathcal{M}_r(\mathbf{Z})$ est l'ensemble des matrices de déterminant 1 ou -1. On le note $\mathrm{GL}(n, \mathbf{Z})$. ◄

Théorème 2.3. *Un sous-groupe d'un groupe libre de rang r est libre. Son rang s est au plus égal à r.*

Exemple 2.4. Les sous groupes de $\mathbf{Z}$ sont les ensembles $n\mathbf{Z}$, $n \in \mathbf{N}$. Ils sont de rang 1, sauf 0, de rang 0. On voit donc qu'il peut exister un sous groupe, distinct du groupe, de même rang que le groupe (comparer avec les espaces vectoriels et leur dimension).

Démonstration. Considérons un groupe libre L de rang r, une $\mathbf{Z}$-base $\mathcal{B} = (e_1, \dots, e_r)$ de L et un sous-groupe M de L. Pour j de 1 à r, on désigne par L_j le sous-groupe libre de L engendré par $(e_1, \dots, e_j)$ et par M_j le sous-groupe de L_j intersection de M et L_j.
La démonstration se fait par récurrence sur r. Pour $r = 0$ il n'y a rien à prouver. (Pour $r = 1$ on part d'un groupe

L isomorphe à $\mathbf{Z}$. Les sous-groupes de $\mathbf{Z}$ sont engendrés par un élément, donc libres de rang 0 ou 1.)
Supposons maintenant $r \geq 1$. Par hypothèse de récurrence, M_{r-1} est libre de rang au plus égal à $r-1$. Tout élément x de M se décompose de manière unique sur la $\mathbf{Z}$-base $\mathcal{B}$ en $x = x_1e_1 + \ldots + x_{r-1}e_{r-1} + x_re_r$. Considérons l'application

$$\begin{array}{ccc} M & \longrightarrow & \mathbf{Z} \\ x & \longmapsto & x_r. \end{array}$$

Son noyau est le sous-groupe M_{r-1}. Son image est un sous-groupe de $\mathbf{Z}$, qui est donc engendré par un entier a_r. Si $a_r = 0$ c'est que $M = M_{r-1}$ et M est libre de rang au plus égal à $r-1$. Si a_r n'est pas nul on choisit un élément z dans M tel que $z_r = a_r$ (il y en a au moins un) et on considère le produit $M_{r-1} \times \mathbf{Z}$ et le morphisme

$$\begin{array}{ccc} M_{r-1} \times \mathbf{Z} & \longrightarrow & M \\ (x, n) & \longmapsto & x + nz \end{array}$$

qui est injectif et surjectif (le vérifier). Le groupe M est isomorphe à $M_{r-1} \times \mathbf{Z}$ libre de rang au plus égal à r. □

2.5. **Conséquences.** Soit G un groupe abélien de type fini. Il existe donc un morphisme surjectif $\pi : \mathbf{Z}^r \longrightarrow G$. Le noyau K de ce morphisme est un groupe libre de type fini de rang $s \leq r$. Les éléments de K sont associés aux relations entre les générateurs de G. Précisément pour toute relation

$$\sum_{i=1}^{r} \lambda_i a_i = 0 \text{ dans } G$$

entre les générateurs de G, le vecteur $(\lambda_1, \ldots, \lambda_r)$ se décompose de manière unique sur la $\mathbf{Z}$-base de K.
Soit H un sous-groupe de G. Alors $L = \pi^{-1}(H)$ est un sous-groupe de $\mathbf{Z}^r$, donc libre de rang $r' \leq r$. La restriction de π à L est un morphisme surjectif de L sur H qui est donc de type fini.

Exercice 8. ► Soit a et b deux entiers non tous les deux nuls. Soit H le sous groupe de $\mathbf{Z}^2$ formé des éléments (na, nb) pour n dans $\mathbf{Z}$. Quel est le rang de H ?
On considère le sous-ensemble $\overline{H}$ de $\mathbf{Z}^2$ formé des éléments *proportionnels* à (a, b). Montrer que c'est un sous-groupe de $\mathbf{Z}^2$. Décrire une $\mathbf{Z}$-base de $\overline{H}$. Existe-t-il une $\mathbf{Z}$-base de $\mathbf{Z}^2$ obtenue en complétant une $\mathbf{Z}$-base de $\overline{H}$? Décrire le quotient $\mathbf{Z}^2/\overline{H}$, puis le quotient $\mathbf{Z}^2/H$. ◄

Exercice 9. ► On considère dans $\mathbf{Z}^4$ le sous ensemble G suivant :

$$G := \{x \in \mathbf{Z}^4 \mid x_1 + 2x_2 + 3x_3 = 0,\ 2x_2 + 5x_4 = 0\}.$$

Montrer que c'est un groupe libre de rang 2. En donner une $\mathbf{Z}$-base. ◄

Exercice 10. ► On considère un polynôme P unitaire de degré $d > 0$ à coefficients entiers. On suppose P irréductible dans $\mathbf{Q}[X]$. Soit α une racine complexe de P. On considère le sous-ensemble suivant de $\mathbf{C}$

$$\mathbf{Z}[\alpha] :=$$
$$\{a_0 + a_1\alpha + \ldots + a_k\alpha^k \mid k \in \mathbf{N}, a_0, a_1, \ldots, a_k \in \mathbf{Z}\}.$$

Montrer successivement que $\mathbf{Z}[\alpha]$ est un sous-groupe de $\mathbf{C}$, de type fini, sans torsion, libre de rang d (voir exercice 6 pour un exemple). ◄

Exercice 11. ► On se donne un groupe abélien libre de type fini L. On appelle *forme* $\mathbf{Z}$*-linéaire* un morphisme $f : L \longrightarrow \mathbf{Z}$.
Montrer que son image est un idéal de $\mathbf{Z}$, donc engendré par un élément. Si f n'est pas le morphisme nul, ce générateur est un entier non nul. Montrer que l'ensemble de tous les morphismes de L dans $\mathbf{Z}$ est un groupe abélien L', lui aussi libre de même rang que L. Si on se donne une $\mathbf{Z}$-base de L, montrer que les fonctions coordonnées dans cette base sont des éléments de L' qui forment une $\mathbf{Z}$-base de L' (dite duale). ◄

On précise ici le théorème 2.3.

Théorème 2.6. *On considère un groupe abélien libre L de rang r et un sous-groupe M non réduit à $\{0\}$. Il existe une $\mathbf{Z}$-base $\mathcal{B}$ de L, des éléments $(e_1, \ldots, e_s)$ de $\mathcal{B}$ et des entiers $a_1, \ldots, a_s$ non nuls tels que*

(1) *Les éléments $(a_1e_1, \ldots, a_se_s)$ forment une $\mathbf{Z}$-base de M.*
(2) *Les a_i sont ordonnés pour la relation de divisibilité $a_1 \mid a_2 \mid \ldots \mid a_s$.*
(3) *La famille d'entiers $(a_1, \ldots, a_s)$ ne dépendent que de la donnée de M dans L. On les appelle* facteurs invariants de M dans L.

Le quotient L/M est isomorphe au produit

$$\mathbf{Z}^{r-s} \times \mathbf{Z}/a_1\mathbf{Z} \times \ldots \times \mathbf{Z}/a_s\mathbf{Z}.$$

Démonstration. La démonstration se fait par récurrence sur le rang de M.
Existence. On note L' comme dans l'exercice 11 l'ensemble des formes $\mathbf{Z}$-linéaires sur L. On remarque que par restriction, toute forme f induit une forme de M dans $\mathbf{Z}$. L'image $f(M)$ est aussi un idéal, contenu dans $f(L)$. Parmi tous les éléments de L', il en est dont la restriction à M n'est pas identiquement nulle. On choisit une forme f telle que l'idéal $f(M)$ est engendré par un élément positif non nul a_1 le plus petit possible (un tel entier existe puisqu'un ensemble d'entiers naturels non vide a un plus petit élément). On choisit également un élément x_1 de M tel que $f(x_1) = a_1$. Considérons une $\mathbf{Z}$-base $\mathcal{B}_0$ de L. Toute forme $\mathbf{Z}$-linéaire prend sur x_1 une valeur qui est un multiple de a_1 (sinon on pourrait en trouver une qui prend une valeur non nulle inférieure). En particulier, les formes coordonnées pour une $\mathbf{Z}$-base $\mathcal{B}_0$ ont cette propriété, ce qui montre que les coordonnées

de x_1 dans la $\mathbf{Z}$-base $\mathcal{B}_0$ sont divisibles par a_1. Il existe donc un élément e_1 de L tel que $x_1 = a_1 e_1$ et $f(e_1) = 1$. Montrons que L est isomorphe au produit $\mathbf{Z} \times \ker f$. Pour cela considérons le morphisme

$$\begin{array}{rcl} \phi : \mathbf{Z} \times \ker f & \longrightarrow & L \\ (a, x) & \longmapsto & ae_1 + x. \end{array}$$

On se donne y dans L. Vérifier que l'équation en α

$$f(y - \alpha e_1) = 0$$

a pour unique solution $\alpha = f(y)$. En déduire que ϕ est bijectif.
Noter que $\ker f$ est un groupe libre de rang $\mathrm{rg} L - 1$.
De manière analogue, montrer que le morphisme

$$\begin{array}{rcl} \varphi : \mathbf{Z} \times (M \cap \ker f) & \longrightarrow & M \\ (a, x) & \longmapsto & ax_1 + x. \end{array}$$

est aussi un isomorphisme et que $M \cap \ker f$ est un sous-groupe de $\ker f$ libre de rang $s-1$. Si $s = 1$ on a terminé. Sinon, par hypothèse de récurrence, on peut trouver une $\mathbf{Z}$-base $\mathcal{B}_1$ de $\ker f$, une partie $(e_2, \ldots, e_s)$ de $\mathcal{B}_1$ et des entiers $a_2, \ldots, a_s$ tels que $(a_2 e_2, \ldots, a_s e_s)$ est une $\mathbf{Z}$-base de $M \cap \ker f$. On termine la preuve en prenant pour $\mathcal{B}$ la $\mathbf{Z}$-base obtenue en adjoignant e_1 à $\mathcal{B}_1$.
Unicité. Le sous-groupe M est donc libre de type fini. Se donner un tel groupe, c'est se donner une famille génératrice $\mathcal{V}$ de t éléments de L. Leurs coordonnées dans une base $\mathcal{B}_0$ de L sont les colonnes d'une matrice A de $\mathcal{M}_{r,t}(\mathbf{Z})$.
L'existence d'une base $\mathcal{B}$ de L avec les propriétés du théorème équivaut à l'existence

(1) d'une matrice P inversible dans $\mathcal{M}_r(\mathbf{Z})$ (la matrice de passage de la base $\mathcal{B}$ à la base $\mathcal{B}_0$),
(2) d'une matrice Q de $\mathcal{M}_{t,s}(\mathbf{Z})$ (la matrice des coordonnées des vecteurs de la famille $(a_1 e_1, \ldots, a_s e_s)$ sur la famille génératrice $\mathcal{V}$),
(3) d'une matrice R de $\mathcal{M}_{t,s}(\mathbf{Z})$ (la matrice des coordonnées des vecteurs de la famille $\mathcal{V}$ sur la base $(a_1 e_1, \ldots, a_s e_s)$),

telles que le produit PAQ est la matrice

$$PAQ = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & & a_s \\ 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

Montrer que le pgcd des coefficients de A divise le pgcd des coefficients de PA, puis qu'ils sont égaux. Montrer la propriété analogue pour A et AQ (Remarquer que si $AQ = A'$, alors $A'R = A$). Conclure que le plus petit des invariants de A est le pgcd de ses coefficients.

Plus généralement, on se donne un entier $n \leq s$, un sous-ensemble I de n éléments extraits de $\{1, \ldots, r\}$ et un sous ensemble J à n éléments extarits de $\{1, \ldots, s\}$. On note A_I la matrice $n \times s$ extraite de A et formée des lignes de A dont l'indice est dans I. On note Q_J la matrice $s \times n$ extraite de Q et formée des colonnes de Q dont l'indice appartient à J. On considère alors le produit $B_{IJ} = A_I Q_J$ dans $\mathcal{M}_n(\mathbf{Z})$. Remarquer que toute colonne du produit B_{IJ} est combinaison linéaire des colonnes de A_I. En déduire que le déterminant $\det(B_{IJ})$ appartient à l'idéal engendré par les $n \times n$ mineurs de A_I donc à l'idéal engendré par les $n \times n$ mineurs de A. Montrer enfin que l'idéal de $\mathbf{Z}$ engendré par les $n \times n$ mineurs de A est égal à l'idéal engendré par les $n \times n$ mineurs de AQ.
Formuler et montrer la propriété analogue pour A et PA lorsque P est dans $GL(s, \mathbf{Z})$. Conclure que le n-ème invariant de A est le pgcd de ses $n \times n$ mineurs. □

Exercice 12. ► Application : L est $\mathbf{Z}^2$ et M le sous-groupe engendré par les vecteurs $(3, 2)$ et $(-1, 2)$. Trouver les facteurs invariants de M dans L.
Même question pour N engendré dans L par $(6, 4)$ et $(-2, 4)$. ◄

Exercice 13. ► On considère le groupe $G = (\mathbf{Z}/4\mathbf{Z})^2$. Montrer qu'une matrice de $\mathcal{M}_2(\mathbf{Z}/4\mathbf{Z})$ est inversible dans $\mathcal{M}_2(\mathbf{Z}/4\mathbf{Z})$ si et seulement si son déterminant est inversible dans $\mathbf{Z}/4\mathbf{Z}$. On note $GL(2, \mathbf{Z}/4\mathbf{Z})$ le groupe de ces matrices. Quel est l'ordre de $GL(2, \mathbf{Z}/4\mathbf{Z})$? Est-il abélien ? Montrer qu'un automorphisme de G est déterminé par la donnée des images des générateurs $(1, 0)$ et $(0, 1)$ de G et en déduire que le groupe des automorphismes de G est isomorphe à $GL(2, \mathbf{Z}/4\mathbf{Z})$. Comparer avec le groupe des automorphismes de $\mathbf{Z}/16\mathbf{Z}$. ◄

Si G est un groupe abélien de type fini engendré par une famille finie $(g_1, \ldots, g_r)$, il existe un morphisme surjectif

$$\begin{array}{rcl} \mathbf{Z}^r & \longrightarrow & G \\ (n_1, \ldots, n_r) & \longmapsto & \displaystyle\sum_{i=1}^{r} n_i g_i. \end{array}$$

Le noyau de ce morphisme est un sous-groupe M de $\mathbf{Z}^r$, donc libre. Le quotient $\mathbf{Z}^r/M$ est isomorphe à G. On désigne par $(a_1, \ldots, a_s)$ les facteurs invariants de M dans L. On obtient alors par le théorème 2.6 que G est isomorphe à

$$\mathbf{Z}/a_1\mathbf{Z} \times \ldots \times \mathbf{Z}/a_s\mathbf{Z} \times \mathbf{Z}^{r-s}$$

Exercice 14. ► On considère le groupe $G = (\mathbf{Z}/4\mathbf{Z})^2$. Montrer qu'une matrice de $\mathcal{M}_2(\mathbf{Z}/4\mathbf{Z})$ est inversible dans $\mathcal{M}_2(\mathbf{Z}/4\mathbf{Z})$ si et seulement si son déterminant est inversible dans $\mathbf{Z}/4\mathbf{Z}$. On note $GL(2, \mathbf{Z}/4\mathbf{Z})$ le groupe de ces matrices. Quel est l'ordre de $GL(2, \mathbf{Z}/4\mathbf{Z})$? Est-il abélien ? Montrer qu'un automorphisme de G est déterminé par la donnée des images des générateurs $(1, 0)$ et

$(0,1)$ de G et en déduire que le groupe des automorphismes de G est isomorphe à $GL(2,\mathbf{Z}/4\mathbf{Z})$. Comparer avec le groupe des automorphismes de $\mathbf{Z}/16\mathbf{Z}$. ◄

3. Groupes abéliens de torsion

Un élément g d'un groupe abélien est dit de *torsion* s'il est d'ordre fini, autrement dit s'il engendre un sous-groupe cyclique fini, autrement dit encore s'il existe un entier non nul n tel que $ng = 0$.
Un groupe abélien est dit de torsion si tous ses éléments sont de torsion. S'il existe un entier *non nul* n tel que $nG = \{0\}$ on dit que n est un *exposant* pour G.

Exemple 3.1. Tout élément du groupe cyclique $\mathbf{Z}/n\mathbf{Z}$ a pour ordre un diviseur de n. Il est donc annulé par n.

Exercice 15. ► On considère un groupe abélien G et deux de ses éléments x et y d'ordres respectifs m et n premiers entre eux. Montrer que $x+y$ est d'ordre mn.
On suppose maintenant que les ordres de x et y ont un pgcd égal à d. Montrer qu'il existe deux entiers m' et n' premiers entre eux, m' diviseur de m, n' diviseur de n, tels que $d = m'n'$. En déduire que l'ensemble des ordres des éléments de G est stable par ppcm.
Montrer enfin que si G a un exposant fini e il existe un élément de G d'ordre e. ◄

Proposition 3.2. *Un groupe abélien est de type fini et de torsion si et seulement si il est fini.*

Démonstration. Si G est un groupe abélien fini, il est de type fini et chacun de ses éléments est d'ordre fini donc de torsion. Il existe un entier (par exemple le *ppcm* des ordres des éléments ou encore l'ordre du groupe) qui annule tous les éléments de G.
Supposons maintenant que G est abélien de type fini et de torsion. Choisissons des générateurs $g_1, \ldots, g_r$ de G. Ils sont d'ordre fini. Notons d le *ppcm* des ordres des $g_1, \ldots, g_r$. Si x est un élément de G, il existe des entiers $x_1, \ldots, x_r$ tels que

$$x = x_1 g_1 + \ldots + x_r g_r.$$

On a donc $dx = x_1 dg_1 + \ldots + x_r dg_r = 0$. On en conclut que d annule tous les éléments de G. □

Exercice 16. ► Pour n entier naturel, on considère le groupe $G := (\mathbf{Z}/2\mathbf{Z})^n$. Quel est l'ordre de G ? Quel est l'ordre d'un élément non nul de G ? Quel est le plus petit exposant de G ?
Mêmes questions avec le groupe $\mathbf{Z}/2^n\mathbf{Z}$. ◄

Exercice 17. ► Le groupe $\mathbf{Q}/\mathbf{Z}$. Montrer que tout élément de $\mathbf{Q}/\mathbf{Z}$ est représenté par un unique rationnel de $\mathbf{Q} \cap [0,1[$. Par qui sont repésentés les entiers ? Vérifier alors que $\mathbf{Q}/\mathbf{Z}$ est de torsion et infini. Il n'est donc pas de type fini.
Montrer que, pour tout $n \geq 1$ entier, il a un seul sous-groupe d'ordre n, qui est cyclique. Le décrire. ◄

Théorème 3.3. *Soit G un groupe abélien et d un entier non nul tel que $dG = 0$ (autrement dit, tous les éléments de G ont un ordre qui divise d). On suppose de plus que $d = d_1 d_2$ avec d_1, d_2 premiers entre eux et on note G_{d_1} (resp. G_{d_2}) le sous-groupe des éléments de G annulés par d_1 (resp. d_2). Alors G est isomorphe au produit des deux sous-groupes $G_{d_1} \times G_{d_2}$.*

Comparer l'énoncé et la preuve du théorème avec ceux du théorème des noyaux. Considérer d'autre part l'exemple $G = \mathbf{Z}/d\mathbf{Z}$ et le théorème chinois.

Lemme 3.4. *Soit G un groupe abélien fini. On note son ordre $|G|$. Soit p un nombre premier qui divise $|G|$. Alors G contient un élément d'ordre p.*

Démonstration. On note e un exposant de G et on montre d'abord par récurrence sur l'ordre de G qu'il divise une puissance de e.
Si $|G| = 1$, alors $G = \{0\}$ et il n'y a rien à prouver. Supposons que $|G| > 1$ et considérons un élément non nul x de G. Son ordre n (qui est l'ordre du groupe cyclique H engendré par x) divise e. D'autre part e est aussi un exposant du groupe quotient G/H. Par hypothèse de récurrence, l'ordre de G/H divise une puissance de e. Il en est de même de l'ordre de G puisque $|G| = |H|\,|G/H| = n\,|G/H|$.
Considérons maintenant un nombre premier p qui divise l'ordre de G. Il existe alors un élément x de G dont l'ordre est divisible par p, sinon l'exposant de G ne serait pas divisible par p. Si l'ordre de x est pq alors qx est d'ordre p. □

Comme conséquence du théorème 3.3, on obtient que si G est un groupe abélien fini d'ordre d, dont la décomposition en facteurs premiers est $d = \prod_{i=1}^{\ell} p_i^{n_i}$, alors G est isomorphe au produit $G_1 \times \ldots \times G_\ell$ où G_i est le sous-groupe des éléments annulés par $p_i^{n_i}$, $i = 1, \ldots, \ell$ (ce sous-groupe n'est pas réduit à 0 à cause du lemme).

Exemple 3.5. Pour n entier naturel, on considère le groupe $G = \mathbf{Z}/p^n\mathbf{Z}$. Pour k de 0 à n, on note G_k l'ensemble des éléments de G divisibles par p^k dans G. On note u le morphisme de multiplication par p de G dans lui-même. Montrer que

(1) G_k est l'image du morphisme u^k.
(2) G_k est le sous-groupe des éléments d'ordre au plus p^{n-k}.
(3) G_k est le noyau du morphisme u^{n_k}.

Vérifier que $G_n = \{0\}$, que $G_0 = G$ et que $G^\times = G_0 \backslash G_1$. Quel est l'ordre de G_k ?
À la multiplication par p agissant sur $\mathbf{Z}/p^n\mathbf{Z}$, on associe un schéma

$$G_n = \{0\} \longleftarrow G_{n-1} \longleftarrow \ldots \longleftarrow G_1 \longleftarrow G_0 = G$$

où les flèches représentent l'action de la multiplication par p. On résume souvent cette information dans un tableau formé d'une seule ligne et de n colonnes

$$\square\,\square\,\ldots\,\square\,\square$$

en omettant $\{0\}$ et en convenant que l'action est le décalage vers la gauche : le carré le plus à gauche représente donc le noyau de la multiplication par p sur G.

Théorème 3.6. *Soit p un nombre premier, n un entier et G un groupe abélien fini d'ordre p^n. Il existe une unique partition de n en $N_1+\ldots+N_s$, $N_1 \geq N_2 \geq \ldots \leq N_s$ et un isomorphisme de G avec le produit de groupes*

$$\mathbf{Z}/p^{N_1}\mathbf{Z} \times \ldots \times \mathbf{Z}/p^{N_s}\mathbf{Z}.$$

Démonstration. La démonstration se fait par récurrence sur n. Pour $n = 0$ le groupe G est réduit à l'élément neutre et il n'y a rien à démontrer.
Supposons maintenant $n > 0$. Dans le groupe G, d'ordre p^n, l'ordre de tout élément est une puissance de p. Considérons un élément x d'ordre maximum p^r et le sous-groupe cyclique H qu'il engendre. Le quotient G/H est d'ordre p^{n-r}. Par hypothèse de récurrence, il existe une unique partition de $n-r$ en $N_2+\ldots+N_s$, $N_2 \geq \ldots \leq N_s$ et un isomorphisme de G/H avec le produit $\mathbf{Z}/p^{N_2}\mathbf{Z} \times \ldots \times \mathbf{Z}/p^{N_s}\mathbf{Z}$. En particulier, il existe un morphisme surjectif $\pi : G \longrightarrow \mathbf{Z}/p^{N_2}\mathbf{Z} \times \ldots \times \mathbf{Z}/p^{N_s}\mathbf{Z}$ dont le noyau est H.
Nous allons maintenant construire un isomorphisme de G avec $\mathbf{Z}/p^r\mathbf{Z} \times (\mathbf{Z}/p^{N_2}\mathbf{Z} \times \ldots \times \mathbf{Z}/p^{N_s}\mathbf{Z})$. On note que p^r étant l'ordre maximum d'un élément de G, r est plus grand ou égal à N_2. On résout d'abord le problème suivant :

Lemme 3.7. *Sous les hypothèses du théorème, étant donné un élément y d'ordre p^m dans G/H, il existe un élément $\tilde{y}$ de G dont la classe modulo H est y et de même ordre que y.*

Démonstration. Choisissons un z dans G dont la classe modulo H est y. Comme $p^m y$ est nul dans G/H, $p^m z$ appartient à H et s'écrit donc ax avec a entier inférieur à p^r. En mettant p en facteur, on a $a = p^s q$ avec $s \leq r$ et q non divisible par p. Finalement $p^m z = p^s q x$. L'élément $p^s q x$ est d'ordre p^{r-s} et z est d'ordre p^{m+r-s}. Comme p^r est l'ordre maximum d'un élément de G on a $m+r-s \leq r$ et donc $m \leq s$. On en déduit que

$$\tilde{y} := z - p^{s-m}x$$

est annulé par p^m. L'ordre de $\tilde{y}$ est donc p^m. En effet, s'il était inférieur, sa classe y serait annulée par un entier inférieur à p^m. □

On termine la preuve du théorème : pour tout j de 2 à s, il existe donc un élément y_j de G d'ordre p^{N_j} dont l'image par π a pour i-ème composante 1 si $i = j$ et 0 sinon. Remarquons que le morphisme

$$\begin{aligned} \sigma : \mathbf{Z}/p^{N_2}\mathbf{Z} \times \ldots \times \mathbf{Z}/p^{N_s}\mathbf{Z} &\longrightarrow G \\ (a_2, \ldots, a_s) &\longmapsto a_2 y_2 + \ldots + a_s y_s \end{aligned}$$

est injectif : sa composée avec le morphisme quotient $G \longrightarrow G/H$ est un isomorphisme.
L'isomorphisme recherché ϕ de $\mathbf{Z}/p^r\mathbf{Z} \times (\mathbf{Z}/p^{N_2}\mathbf{Z} \times \ldots \times \mathbf{Z}/p^{N_s}\mathbf{Z})$ sur G est alors donné par :

$$\phi(b, a_2, \ldots, a_s) = bx + \sigma(a_2, \ldots, a_s).$$

Vérifier que ϕ est surjectif en utilisant que sa composée avec la surjection canonique $G \longrightarrow G/H$ est surjective. Vérifier ensuite que ϕ est injective en étudiant l'intersection de H avec le sous-groupe de G engendré par $(y_2, \ldots, y_s)$ (*i.e.* l'image de σ).
On pose $N_1 := r$ et $y_1 := x$. Il nous reste maintenant à démontrer l'unicité de la partition $n = N_1+N_2+\ldots+N_s$, $N_1 \geq \ldots \geq N_s$. Sa donnée est équivalente à celle du tableau suivant justifié à gauche, dont la j-ème ligne à N_j cases.

$$\begin{array}{l} \square\,\square\,\square\,\square\,\square\,\square \\ \square\,\square\,\square\,\square\,\square \\ \square \\ \square \end{array}$$

On peut considérer que la j-ème ligne représente l'action de la multiplication par p sur le sous-groupe engendré par y_j, d'ordre p^{N_j} (voir exemple 3.5). La première colonne à gauche représente donc le noyau de la multiplication par p sur G. On en déduit que le nombre de lignes, c'est-à-dire s, est déterminé par ce noyau. Vérifiez par exemple que

$$p\,s = |p^{n-1}G|.$$

De manière analogue, le noyau de la multiplication par p^k sur G est représenté par les k premières colonnes. Si on désigne par s_k le nombre de lignes de longueur au moins k (c'est-à-dire la hauteur de la k-ème colonne), vérifiez que $s_1 = s$ et

$$(p^k - p^{k-1})s_k = |p^{n-k}G| - |p^{n-k+1}G|.$$

□

En résumé, si on se donne un groupe abélien fini G d'ordre d, on considère d'abord la décomposition en facteurs premiers $d = \prod_{i=1}^{\ell} p_i^{n_i}$. D'après le théorème 3.3 le groupe G a une décomposition en un produit $G_1 \times \ldots \times G_\ell$ où chaque G_i, d'après le théorème 3.6, a lui-même une décomposition associée à une unique partition $N_i = N_{i,1} + N_{i,2} + \ldots + N_{i,s_i}$, $N_{i,1} \geq N_{i,2} \geq \ldots \geq N_{i,s_i}$. La décomposition de G ainsi obtenue est appelée **décomposition primaire** de G.

En écrivant les entiers sous forme d'un tableau justifié à droite

$$\begin{array}{c} p_1^{N_{1,s_1}} \mid \ldots \mid \ldots \mid \ldots \mid \ldots \mid p_1^{N_{1,2}} \mid p_1^{N_{1,1}} \\ p_2^{N_{2,s_2}} \mid \ldots \mid \ldots \mid p_2^{N_{2,2}} \mid p_2^{N_{2,1}} \\ \vdots \\ p_\ell^{N_{\ell,s_\ell}} \mid \ldots \mid p_\ell^{N_{\ell,2}} \mid p_\ell^{N_{\ell,1}} \end{array}$$

et en recombinant suivant les colonnes de ce tableau, on obtient, en appliquant le théorème chinois, une décomposition de G en un produit

$$\mathbf{Z}/a_1\mathbf{Z} \times \ldots \times \mathbf{Z}/a_s\mathbf{Z}.$$

où a_j est le produit des entiers non nuls situés sur la j-ème colonne du tableau et, par suite, $a_1 \mid a_2 \mid \ldots \mid a_s$. Comme le tableau ne dépend que de G, la suite $a_1, a_2, \ldots, a_s$ est entièrement déterminée par G. Les **facteurs invariants** du groupe G sont les éléments de cette suite.

Exercice 18. ► Combien y a-t-il de classes de groupes abéliens d'ordre 4 à isomorphisme près ? Les décrire. Soit G un groupe abélien d'ordre 4. Donner un critère simple qui permette de déterminer la classe de G.
Même question avec les groupes abéliens d'ordre p (resp. p^2) lorsque p est un nombre premier.
Décrire tous les groupes abéliens d'ordre 15.
Décrire toutes les classes à isomorphisme près de groupes abéliens ou non d'ordre 4. ◄

Exercice 19. ► Donner la décomposition primaire des groupes suivants

$$(\mathbf{Z}/54\mathbf{Z}) \times (\mathbf{Z}/26\mathbf{Z}) \times (\mathbf{Z}/15\mathbf{Z}),$$
$$(\mathbf{Z}/55\mathbf{Z}) \times (\mathbf{Z}/36\mathbf{Z}) \times (\mathbf{Z}/120\mathbf{Z}),$$
$$(\mathbf{Z}/30\mathbf{Z}) \times (\mathbf{Z}/48\mathbf{Z}) \times (\mathbf{Z}/54\mathbf{Z}) \times (\mathbf{Z}/26\mathbf{Z})$$

En déduire leurs facteurs invariants. ◄

Exercice 20. ► Soit G un groupe abélien de type fini. Montrer que l'ensemble T des éléments de torsion de G est un sous-groupe de G. Montrer que le quotient de G par T est un groupe sans torsion, c'est-à-dire qui ne contient aucun élément de torsion. ◄

Théorème 3.8. *Un groupe abélien de type fini est isomorphe au produit de son sous-groupe de torsion (fini) par un groupe libre. En particulier, un groupe abélien de type fini sans torsion est libre.*

Démonstration. Considérons un groupe G engendré par un système fini de générateurs $(g_1, \ldots, g_r)$. Considérons également un sous-système $\mathbf{Z}$-libre maximal (voir exercice 3). Quitte à renuméroter les générateurs, on peut supposer que le système $(g_1, \ldots, g_s)$, $s \leq r$, est $\mathbf{Z}$-libre, ce qui revient à dire que le sous-groupe L engendré par $(g_1, \ldots, g_s)$ est libre de rang s. Pour tout entier j de $s+1$ à r on a un entier non nul a_j et une relation :

$$a_j g_j \in L.$$

Notons a le ppcm (non nul) des entiers a_j $s < j \leq r$. L'application

$$\begin{array}{ccc} G & \longrightarrow & L \\ x & \longmapsto & ax \end{array}$$

est évidemment surjective et son noyau est le sous-groupe T des éléments de torsion de G. En effet si ax est nul, c'est que x est de torsion. Réciproquement, si x est de torsion, ax est dans $L \cap T = \{0\}$ donc nul. Vérifier alors que l'application

$$\begin{array}{ccc} G/T & \longrightarrow & L \\ \bar{x} & \longmapsto & ax. \end{array}$$

est bien définie et injective. Le groupe G/T s'identifie à un sous-groupe de L qui est libre d'après le théorème 2.3. Or nous avons aussi un morphisme injectif de L dans G/T induit par l'application quotient. D'après la proposition 2.2, on en conclut que L et G/T sont libres et de même rang. Choisissons des éléments $x_1, \ldots, x_s$ de G dont les classes $\bar{x}_1, \ldots, \bar{x}_s$ forment une $\mathbf{Z}$-base de G/T et considérons le morphisme

$$\begin{array}{ccc} \phi : T \times \mathbf{Z}^s & \longrightarrow & G \\ (x, n_1, \ldots, n_s) & \longmapsto & x + \sum_{i=1}^{s} n_i x_i. \end{array}$$

Remarquer que si $x + \sum_{i=1}^{s} n_i x_i = y$ est vraie dans G alors $\sum_{i=1}^{s} n_i \bar{x}_i = \bar{y}$ est vraie dans G/T. En déduire que le morphisme ϕ est bijectif. □