Groupes abéliens finis, groupes abéliens de type fini

1 Introduction

Dans le cas d'un groupe abélien (*i.e.* commutatif), il est courant de noter la loi de composition interne additivement (l'élément neutre étant 0). Cela se justifie par l'intervention de la structure de groupe abélien dans d'autres structures algébriques comme les anneaux, les modules ou les espaces vectoriels, qui par convention sont tous des groupes abéliens additifs. On peut d'ailleurs remarquer que la notion de groupe abélien coïncide avec celle de $\mathbb{Z}$-module [...].

1.1 Somme directe de sous-groupes

Soient $H_1, \ldots, H_n$ des sous-groupes du groupe abélien G. On dit que G est *somme directe de* $H_1, \ldots, H_n$, et on écrit

$$G \ = \ H_1 \oplus \cdots \oplus H_n$$

si tout élément de G s'écrit de manière unique sous la forme $h_1 + \cdots + h_n$, où pour tout i, $h_i \in H_i$. On définit de manière analogue la somme directe d'une famille infinie de sous-groupes, mais avec la condition que dans la somme $\sum h_i$, tous les h_i sauf un nombre fini soient nuls.

Si G s'écrit comme la somme directe d'une famille finie de sous-groupes, alors G est en fait isomorphe au produit direct de ces sous-groupes. Mais ce n'est plus vrai pour une somme directe infinie [...].

Si H est un sous-groupe de G, on dit que H est un *facteur direct* s'il existe un autre sous-groupe H' tel que $G = H \oplus H'$. Dans ce cas, H' est appelé un *supplémentaire de* H. Contrairement à ce qui se passe dans le cadre de la théorie des espaces vectoriels, un sous-groupe donné n'a pas nécessairement de supplémentaire, comme le montre l'exercice qui suit.

Exercice 1.1 *Montrer que si le groupe abélien G est la somme directe de deux de ses sous-groupes H et H', alors $H \cap H' = \{0\}$. En déduire qu'aucun sous-groupe non trivial de $\mathbb{Z}$ n'est un facteur direct de $\mathbb{Z}$.*

Lorsque H est un facteur direct de G, il n'y a pas en général unicité du supplémentaire H'. Mais H' est dans ce cas déterminé à un isomorphisme près : il est isomorphe au groupe quotient G/H.

Exercice 1.2 *Prouver l'affirmation ci-dessus.*

2 Groupes abéliens finis

On propose ici d'étudier la structure des groupes abéliens finis, en vue notamment d'obtenir le théorème fondamental énoncé ci-dessous.

Théorème 2.1 *Tout groupe abélien fini est isomorphe à un produit direct du type*

$$\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z},$$

où r est un entier positif, et $m_1, \ldots, m_r$ sont des entiers supérieurs ou égaux à 2 tels que $m_1|m_2|\cdots|m_r$.

De plus, les entiers $r, m_1, \ldots, m_r$ vérifiant ces conditions sont déterminés de façon unique par le groupe G.

2.1 Composantes p-primaires d'un groupe abélien fini

Un entier m est appelé *exposant d'un groupe G* (pas nécessairement abélien) si pour tout $g \in G$, $mg = 0$ (ou $g^m = 1$ si la loi est notée multiplicativement). L'ordre d'un groupe fini est toujours un exposant de ce groupe.

Soit G un groupe abélien fini. Pour tout entier premier p divisant $|G|$, on note G_p l'ensemble des éléments de G dont l'ordre est une puissance de p. G_p se nomme *composante p-primaire de G*. Il est aisé de vérifier que G_p est un sous-groupe de G [...].

Théorème 2.2 *Tout groupe abélien fini G s'écrit comme somme directe*

$$G \;=\; \bigoplus_{p \text{ premier},\, p\,|\,|G|} G_p.$$

Preuve — Si G a comme exposant une puissance d'un nombre premier p, il est clair que $G = G_p$. Sinon, on peut trouver un exposant m de G qui s'écrit $m = m_1m_2$, où m_1 et m_2 sont deux entiers premiers entre eux. Par Bezout, il existe des entiers u_1 et u_2 tels que $u_1m_1 + u_2m_2 = 1$, d'où $G = m_1u_1G + m_2u_2G \subset m_1G + m_2G \subset G$, et on peut en déduire que

$$G \;=\; m_1G + m_2G.$$

Montrons que cette somme est directe. Supposons $0 = m_1x + m_2y$; comme $mx = 0$, on a $m_2(m_2y) = 0$, mais aussi $m_1(m_2y) = my = 0$. Comme m_1 et m_2 sont premiers entre eux, cela entraîne $m_2y = 0$[1], puis $m_1x = 0$. Ainsi on a

$$G \;=\; m_1G \oplus m_2G.$$

Notons maintenant pour n entier, $G_{(n)} \stackrel{\text{déf}}{=} \{x \in G \;/\; nx = 0\}$. Il est clair que $m_2G \subset G_{(m_1)}$. Réciproquement, si $g \in G_{(m_1)}$, on peut écrire $g = u_1m_1g + u_2m_2g = m_2u_2g$, donc $g \in m_2G$. On a donc $m_2G = G_{(m_1)}$, et de même $m_1G = G_{(m_2)}$. On obtient finalement

$$G \;=\; G_{(m_1)} \oplus G_{(m_2)}.$$

G_{m_i} admettant m_i comme exposant, une induction sur le nombre de facteurs premiers d'un exposant de G donne le résultat annoncé. ❏

[1]on utilise ici le fait que si m et n sont premiers entre eux, et vérifient $mx = nx = 0$, alors $x = 0$ [...].

Tout groupe abélien fini s'écrit donc comme la somme directe de ses composantes p-primaires G_p. En se rappelant le lemme de Cauchy qui affirme que pour tout p premier divisant l'ordre d'un groupe fini, on peut trouver un élément de ce groupe d'ordre p, on voit que pour tout p premier divisant $|G|$, G_p est un p-groupe (c'est-à-dire un groupe d'ordre une puissance de p). En fait, on voit immédiatement que G_p est un p-Sylow de G, et c'est même l'unique p-Sylow puisque G est abélien. Ceci prouve que la décomposition présentée dans le théorème ci-dessus est *l'unique* écriture de G comme une somme directe de p-groupes abéliens, avec des entiers premiers deux à deux distincts.

Exercice 2.1 *Retrouver l'unicité de l'écriture de G comme une somme directe de p-groupes abéliens, avec des entiers premiers deux à deux distincts, sans utiliser les théorèmes de Sylow.*

2.2 Décomposition d'un groupe abélien fini en somme directe de groupes cycliques

La seconde étape dans l'analyse de la structure des groupes abéliens finis consiste à démontrer le résultat suivant.

Théorème 2.3 *Tout groupe abélien fini s'écrit comme somme directe de groupes cycliques.*

Commençons par un lemme dont on se servira dans la suite.

Lemme 2.4 *Si le groupe abélien G est engendré par les n éléments $x_1, \dots, x_n$, et si $a_1, \dots, a_n$ sont n entiers premiers entre eux, alors il existe une famille génératrice de G à n éléments dont l'un est $a_1x_1 + \cdots + a_nx_n$.*

Preuve — Puisque les entiers $a_1, \dots, a_n$ sont premiers entre eux, on peut trouver une matrice $A \in \mathscr{M}_n(\mathbb{Z})$ de déterminant 1, et dont le premier vecteur ligne est $(a_1, \dots, a_n)$ (à vérifier en exercice, par récurrence sur n). Soit $Y = (y_1, \dots, y_n) \in G^n$ défini par la relation $Y = AX$, où X est le vecteur colonne de composantes $x_1, \dots, x_n$. En particulier, on a $y_1 = a_1x_1 + \cdots + a_nx_n$. Comme $\det A = 1$, A^{-1} est encore une matrice à coefficients entiers. Or, $X = (A^{-1}A)X = A^{-1}Y$. On en déduit que chaque x_i est une combinaison linéaire à coefficients entiers des y_j. Comme la famille $(x_1, \dots, x_n)$ est génératrice, la famille $(y_1, \dots, y_n)$ l'est également. ❏

Preuve du théorème 2.3 — On prouve le résultat par récurrence sur n, où n est le cardinal minimum d'une famille génératrice de G. Si $n = 1$, c'est évident ; supposons que $n \geq 2$, et que l'on sait déjà que tout groupe abélien fini engendré par $(n-1)$ éléments est somme directe de groupes cycliques. Prenons une famille génératrice $(x_1, \dots, x_n)$ de G, où x_1 est d'ordre k minimum (autrement dit, aucune famille génératrice de taille n ne comporte un élément d'ordre strictement plus petit que k). Alors $H \stackrel{\text{déf}}{=} < x_2, \dots, x_n >$ est un sous-groupe strict de G, auquel on peut appliquer l'hypothèse de récurrence : H est somme directe de groupes cycliques. Pour terminer la démonstration, il suffit donc de montrer que $G = < x_1 > \oplus H$. Comme G est déjà somme de $< x_1 >$ et H, il ne reste plus qu'à vérifier que $< x_1 > \cap H = \{0\}$. Supposons par l'absurde qu'il existe z non nul dans $< x_1 > \cap H$, que l'on peut donc écrire sous la forme

$$z = a_1x_1 = a_2x_2 + \cdots + a_nx_n.$$

Puisque $z \neq 0$, on peut toujours supposer que $|a_1|$ est strictement inférieur à l'ordre k de x_1. Soit d le pgcd de $(a_1, \dots, a_n)$, et soit $g \stackrel{\text{déf}}{=} -(a_1/d)x_1 + (a_2/d)x_2 + \cdots + (a_n/d)x_n$. Alors g

est d'ordre strictement inférieur à k (car $dg = 0$, et $d \leq |a_1| < k$), mais le lemme précédent affirme que l'on peut trouver une famille génératrice de G à n éléments dont l'un est g : ceci contredit la minimalité de k. ❏

Dans le cas où G est un p-groupe abélien, les groupes cycliques intervenant dans la décomposition de G sont forcément d'ordre une puissance de p, ce qui prouve que tout p-groupe abélien est isomorphe à un produit direct de groupes de la forme $\mathbb{Z}/p^{r_j}\mathbb{Z}$. On va voir dans la suite que ces p^{r_j} sont uniques (à l'ordre près).

Théorème 2.5 *Soit p un nombre premier, et G un p-groupe abélien. Il existe une unique suite d'entiers $(r_1, r_2, \ldots, r_s)$ avec $1 \leq r_1 \leq \cdots \leq r_s$, telle que G soit isomorphe au produit*

$$\mathbb{Z}/p^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_s}\mathbb{Z}.$$

G est dit de type $(p^{r_1}, \ldots, p^{r_s})$.

Preuve — Comme on l'a remarqué ci-dessus, l'existence d'une telle suite $(r_1, r_2, \ldots, r_s)$ est donnée par le théorème 2.3 : on sait que G s'écrit comme une somme directe de groupes cycliques

$$G \ = \ <x_1> \oplus \cdots \oplus <x_s>,$$

où chaque x_j est d'ordre p^{r_j}, et on peut toujours les ordonner de sorte à ce que $1 \leq r_1 \leq \cdots \leq r_s$. Voyons maintenant pourquoi une telle suite (r_j) est unique pour un p-groupe abélien donné. Soit $n \geq 0$ un entier. On considère le sous-groupe

$$p^n G \ = \ \{p^n g \ / \ g \in G\},$$

que l'on peut écrire

$$p^n G \ = \ <p^n x_1> \oplus \cdots \oplus <p^n x_s>,$$

où l'on remarque que $<p^n x_j>$ est réduit à $\{0\}$ si $r_j \leq n$, isomorphe à $\mathbb{Z}/p^{r_j - n}\mathbb{Z}$ si $r_j > n$. De même, on a

$$p^{n+1} G \ = \ <p^{n+1} x_1> \oplus \cdots \oplus <p^{n+1} x_s> .$$

Rappelons ici que si $G_1, \ldots, G_s$ sont des groupes, et si pour tout $j \in \{1, \ldots, s\}$ N_j est un sous-groupe distingué de G_j, alors $N_1 \times \cdots \times N_s \lhd G_1 \times \cdots \times G_s$, et

$$(G_1 \times \cdots \times G_s)/(N_1 \times \cdots \times N_s) \ \simeq \ (G_1/N_1) \times \cdots \times (G_s/N_s).$$

En appliquant ce résultat avec $G_j \stackrel{\text{déf}}{=} <p^n x_j>$ et $N_j \stackrel{\text{déf}}{=} <p^{n+1} x_j>$, on obtient

$$\begin{aligned} p^n G / p^{n+1} G \ &\simeq \ \bigoplus_{1 \leq j \leq s} <p^n x_j> / <p^{n+1} x_j> \\ &\simeq \ \bigoplus_{j,\ r_j > n} (\mathbb{Z}/p^{r_j - n}\mathbb{Z})/(\mathbb{Z}/p^{r_j - n - 1}\mathbb{Z}) \\ &\simeq \ (\mathbb{Z}/p\mathbb{Z})^{k_n}, \end{aligned}$$

où $k_n \stackrel{\text{déf}}{=} |\{j \in \{1, \ldots, s\} \ / \ r_j > n\}|$. Ainsi, le nombre d'indices j tels que $r_j > n$ est uniquement déterminé par l'ordre du groupe $p^n G / p^{n+1} G$. Comme c'est vrai pour tout $n \geq 0$, il n'y a qu'une suite (r_j) possible une fois G donné. ❏

2.3 Structure des groupes abéliens finis

Des théorèmes 2.2 et 2.5 découle directement le théorème qui suit, décrivant complètement la structure de tout groupe abélien fini.

Théorème 2.6 *Si G est un groupe abélien fini, il existe une unique suite d'entiers premiers $p_1 < \cdots < p_k$, et pour chaque j entre 1 et k une unique suite croissante d'entiers supérieurs ou égaux à 1 $(r_1^j, \dots, r_{s_j}^j)$ tels que G soit isomorphe au produit de groupes cycliques*

$$\mathbb{Z}/p_1^{r_1^1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_1^{r_{s_1}^1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{r_1^k}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{r_{s_k}^k}\mathbb{Z}.$$

Le groupe G est alors dit de type $(p_1^{r_1^1}, \dots, p_1^{r_{s_1}^1}, \dots, p_k^{r_1^k}, \dots, p_k^{r_{s_k}^k})$.

Le théorème 2.1 énoncé au début s'en déduit facilement en utilisant le résultat très classique rappelé ci-dessous.

Théorème 2.7 (Lemme chinois) *Si m et n sont deux entiers premiers entre eux, le produit $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est isomorphe au groupe cyclique $\mathbb{Z}/mn\mathbb{Z}$.*

2.4 Dual d'un groupe abélien fini

Soit G un groupe abélien fini. On appelle *dual* de G l'ensemble noté $\widehat{G}$ des morphismes de G dans le groupe multiplicatif des nombres complexes non nuls. $\widehat{G}$ est muni naturellement d'une structure de groupe par la loi de composition interne $(\varphi, \psi) \longmapsto \varphi\psi$ où $\varphi\psi(x) \overset{\text{déf}}{=} \varphi(x)\psi(x)$. Les éléments de $\widehat{G}$ sont appelés les *caractères* de G.

Exercice 2.2 *Montrer que si φ est un caractère d'un groupe abélien fini G, on a $|\varphi(g)| = 1$ pour tout $g \in G$.*

Théorème 2.8 *Si G est un groupe abélien fini, $\widehat{G}$ est isomorphe à G.*

Preuve — Grâce au théorème 2.1, on peut toujours supposer que G est de la forme

$$G = \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}. \tag{1}$$

Pour tout $j \in \{1, \dots, r\}$, soit $x_j \overset{\text{déf}}{=} (0, \dots, 0, 1, 0, \dots, 0)$ l'élément de G dont toutes les composantes sont nulles sauf la j-ième. Soit $\varphi \in \widehat{G}$. Puisque x_j est d'ordre m_j dans G, $\varphi(x_j)$ est une racine m_j-ième de l'unité, et il existe donc un unique $k_j \in \mathbb{Z}/m_j\mathbb{Z}$ tel que $\varphi(x_j) = e^{2\pi i k_j/m_j}$. On en déduit que si $g = (g_1, \dots, g_r) \in G$,

$$\varphi(g) = e^{2\pi i k_1 g_1/m_1} \times \cdots \times e^{2\pi i k_r g_r/m_r}. \tag{2}$$

Inversement, si on se donne $(k_1, \dots, k_r) \in G$, la formule (2) définit toujours un élément de $\widehat{G}$; on note désormais $\varphi_{(k_1,\dots,k_r)}$ cet élément. Il est immédiat alors que $(k_1, \dots, k_r) \longmapsto \varphi_{(k_1,\dots,k_r)}$ est un isomorphisme de G sur $\widehat{G}$. ❑

Pour $x \in G$, considérons le morphisme E_x de $\widehat{G}$ dans $\mathbb{C}^*$ défini par $E_x(\varphi) \overset{\text{déf}}{=} \varphi(x)$. On appelle *évaluation* l'aplication $E \ : \ x \longmapsto E_x$.

Théorème 2.9 *L'évaluation E est un isomorphisme entre G et son bidual $\widehat{\widehat{G}}$.*

Preuve — Il est clair que l'évaluation est un morphisme de G dans son bidual $\widehat{\widehat{G}}$. Montrons que E est injective. Comme précédemment, on peut toujours supposer que G est de la forme (1). Soit alors $g = (g_1, \ldots, g_r) \in G$, $g \neq 0$, puis soit $j \in \{1, \ldots, r\}$ tel que $g_j \neq 0$. Alors $E_g(\varphi_{x_j}) = \varphi_{x_j}(g) = e^{2\pi i g_j/m_j} \neq 1$ (voir les notations de la preuve précédente), et donc E_g n'est pas l'élément neutre de $\widehat{\widehat{G}}$ (l'application constamment égale à 1). Ainsi, $\operatorname{Ker} E = \{0\}$, et E est injective. Or, les groupes G et $\widehat{\widehat{G}}$ sont de même cardinal, et donc E est aussi surjective. ❑

Soit maintenant H un sous-groupe du groupe abélien fini G. On pose

$$H^\circ \overset{\text{déf}}{=} \left\{ \varphi \in \widehat{G} \;/\; \forall h \in H,\ \varphi(h) = 1 \right\}.$$

Si $\varphi \in H^\circ$, on a $H \subset \operatorname{Ker} \varphi$, et donc la propriété universelle du groupe quotient prouve qu'il existe un unique $\tilde{\varphi} \in \widehat{(G/H)}$ tel que $\varphi = \tilde{\varphi} \circ \pi_H$, où π_H est la surjection canonique de G sur G/H. On vérifie très facilement que $\varphi \longmapsto \tilde{\varphi}$ est un isomorphisme entre H° et $\widehat{(G/H)}$. Ainsi, pour tout sous-groupe H de G, on peut trouver dans $\widehat{G}$ (qui est isomorphe à G d'après le théorème 2.8) un sous-groupe H° isomorphe à $\widehat{(G/H)}$, donc au groupe quotient G/H. On obtient donc le théorème qui suit.

Théorème 2.10 *Si H est un sous-groupe du groupe abélien fini G, il existe un sous-groupe de G isomorphe à G/H.*

Attention, cela ne veut pas dire pour autant que H est toujours un facteur direct de G !

Exercice 2.3 *Trouver un groupe abélien fini G et un sous-groupe H de G qui ne soit pas facteur direct.*

Exercice 2.4 *Trouver un contre-exemple prouvant que le théorème 2.10 n'est plus vrai si on retire l'hypothèse G* abélien, *même si on suppose $H \lhd G$.*

Si K est un sous-groupe de $\widehat{G}$, on note

$$K^\perp \overset{\text{déf}}{=} \{ x \in G \;/\; \forall \varphi \in K,\ \varphi(x) = 1 \}.$$

Théorème 2.11 *Pour tout sous-groupe H du groupe abélien fini G, on a*

$$H = (H^\circ)^\perp.$$

Preuve — Il est clair que $H \subset (H^\circ)^\perp$. Pour montrer l'égalité, il suffit donc de vérifier que ces deux ensembles ont même cardinal. Or, pour tout sous-groupe K de $\widehat{G}$, on a un isomorphisme entre $K^\perp$ et $\widehat{G}/K$ [...]. On a donc $|K^\perp| = |G|/|K|$. Dans le cas où $K = H^\circ$, $|K| = |G|/|H|$, d'où

$$\left|(H^\circ)^\perp\right| = |H|.$$

❑

Application à l'étude d'un casse-tête.

Avant de passer à l'étude des groupes abéliens de type fini, on propose d'illustrer les résultats précédents par l'étude du jeu suivant (on peut y jouer sur internet à l'adresse `http://www.univ-rouen.fr/LMRS/Vulgarisation/Rverso/rverso.html`). Sur chaque case d'une grille 3×3, on place un pion dont une face est blanche, l'autre noire. Dans la configuration initiale, toutes les faces blanches sont visibles. Il est possible de retourner les pions, mais pas n'importe comment : seul un retournement simultané des 3 pions d'une même rangée est autorisé (une *rangée* est une ligne, une colonne ou une diagonale). Une configuration est dite *accessible* si on peut l'obtenir à partir de la configuration initiale en respectant cette règle. Combien y a-t-il de configurations accessibles ? Comment reconnaître facilement si une configuration donnée est accessible ou non ?

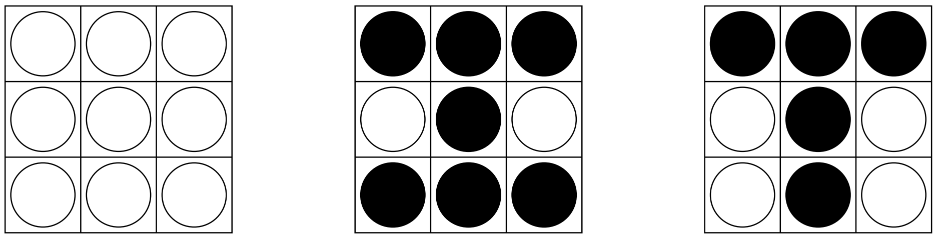


FIG. 1 – La position de départ, et deux autres configurations. Sont-elles accessibles ?

Pour répondre à ces questions, voici quelques indications. On note X l'ensemble des 2^9 configurations de pions sur la grille. Soit G le sous-groupe de $\mathbf{S}(X)$ engendré par les 9 retournements d'un des 9 pions de la grille.

- Vérifier que G est un groupe abélien fini. Quelle est son type ?
- Décrire les éléments du dual de G.
- Montrer que si H est un sous-groupe de G, il existe k parties $P_1, \dots, P_k$ de l'ensemble des 9 cases telles H soit l'ensemble des $g \in G$ vérifiant :

$$\textit{pour tout } j \in \{1, \dots, k\}, \textit{ le nombre de pions retournés par } g \textit{ dans } P_j \textit{ est pair.} \tag{3}$$

  Donner la valeur minimum de k en fonction de l'ordre de H.

On note maintenant H le sous-groupe de G engendré par les 8 transformations qui consistent à retourner simultanément tous les pions d'une même rangée.

- Donner un morphisme "naturel" de $(\mathbb{Z}/2\mathbb{Z})^8$ dans G dont H est l'image. Quel est le noyau de ce morphisme ? En déduire l'ordre et le type de H.
- Donner le k minimum et trouver des parties $P_1, \dots, P_k$ qui permettent de caractériser H comme en (3).
- En déduire une description simple des configurations accessibles.

3 Groupes abéliens de type fini

Un groupe (abélien ou non) est dit *de type fini* s'il existe une partie *finie* du groupe qui l'engendre.

Exercice 3.1 *Montrer qu'un groupe abélien de type fini est toujours dénombrable. $\mathbb{Q}$ est-il un groupe abélien de type fini ?*

Les groupes abéliens finis sont évidemment des exemples de groupes abéliens de type fini. Le but de la suite est d'obtenir pour les groupes abéliens de type fini un résultat de structure étendant le théorème 2.1.

3.1 Groupes abéliens libres

Une partie F du groupe abélien G est dite *libre* si pour tout choix d'un nombre fini d'éléments $f_1, \dots, f_n$ de F, une égalité de la forme $z_1 f_1 + \cdots + z_n f_n = 0$ où les z_j sont des entiers ne peut avoir lieu que si tous les z_j sont nuls. Cela signifie donc que les éléments de F ne sont pas liés par une relation non triviale.

Le groupe abélien G est dit *libre* s'il possède une partie libre qui l'engendre. Une telle partie libre et génératrice est appelée une *base* de G.

Exercice 3.2 *Vérifier que $B \subset G$ est une base de G si et seulement si tout élément de G s'écrit de manière unique sous la forme $\sum_{b \in B} z_b b$ où les entiers z_b sont nuls sauf pour un nombre fini d'éléments de B.*

Il n'y a bien sûr pas unicité de la base d'un groupe abélien libre, mais on dispose d'un résultat analogue à ce qui se passe dans les espaces vectoriels, énoncé dans le théorème suivant.

Théorème 3.1 *Toutes les bases d'un groupe abélien libre G ont même cardinal, appelé le* rang *de G.*

Preuve — On ne va démontrer ce résultat que dans le cas où G admet une base finie, $B = (b_1, \dots, b_n)$. On peut alors écrire

$$G = \mathbb{Z}b_1 \oplus \mathbb{Z}b_2 \oplus \cdots \oplus \mathbb{Z}b_n.$$

Considérons le sous-groupe de G

$$2G \stackrel{\text{déf}}{=} \{2g \;/\; g \in G\} = 2\mathbb{Z}b_1 \oplus \cdots \oplus 2\mathbb{Z}b_n.$$

Le groupe quotient $G/2G$ est alors isomorphe au groupe $\mathbb{Z}b_1/2\mathbb{Z}b_1 \times \cdots \times \mathbb{Z}b_n/2\mathbb{Z}b_n$ [...], donc isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$. On en déduit que l'ordre du groupe $G/2G$ vaut

$$[G : 2G] = 2^n.$$

Soit maintenant B' une autre base de G, et supposons que B' contienne au moins m éléments, où m est un entier positif (on ne suppose même pas ici que cette autre base soit finie). Alors le groupe $G/2G$ contient au moins 2^m éléments [...], d'où $2^m \leq 2^n$, *i.e.* $m \leq n$. Ainsi $|B'| \leq |B|$, et par symétrie $|B'| = |B|$. ❏

Remarque : pour montrer le théorème 3.1 dans le cas où G admet une base infinie B, une méthode possible consiste à vérifier qu'alors le cardinal de G est égal au cardinal de B [...].

Comme on le verra dans la suite (voir le théorème 3.6), un groupe libre de type fini est de rang fini. On en déduit le corollaire suivant.

Théorème 3.2 *Si G est un groupe abélien libre de type fini, il existe un unique entier r tel que G soit isomorphe à $\mathbb{Z}^r$.*

Le résultat énoncé dans l'exercice qui suit est un lemme important qui servira plusieurs fois dans la suite.

Exercice 3.3 *Soit $f : G \longrightarrow G'$ un morphisme surjectif de groupes abéliens, où l'on suppose de plus que G' est libre. Prouver alors que $\operatorname{Ker} f$ est un facteur direct de G, et qu'il existe F sous-groupe de G, isomorphe à G', tel que*

$$G = \operatorname{Ker} f \oplus F.$$

Une application directe de cet exercice donne une condition suffisante pour qu'un sous-groupe d'un groupe abélien soit un facteur direct.

Proposition 3.3 *Soit H un sous-groupe du groupe abélien G. Si G/H est libre, alors H est un facteur direct de G. De plus, tout supplémentaire de H est libre, car isomorphe à G/H.*

Exercice 3.4 *La condition donnée dans la proposition précédente est-elle nécessaire pour que H soit un facteur direct du groupe abélien G ?*

Théorème 3.4 *Tout sous-groupe d'un groupe abélien libre G est un groupe abélien libre, et son rang est inférieur ou égal à celui de G.*

Preuve — Là aussi, on se restreint au cas où G est de rang fini, et on procède par récurrence sur le rang de G. Si G est de rang 1, c'est un résultat bien connu sur $\mathbb{Z}$.

Supposons le résultat prouvé pour tout groupe de rang $n-1$ ($n \geq 2$), et soit G un groupe abélien libre de rang n, de base $(b_1, \ldots, b_n)$. On considère le morphisme f de G sur $\mathbb{Z}$ défini par $f(z_1b_1 + \cdots + z_nb_n) \stackrel{\text{déf}}{=} z_n$. Soit H un sous-groupe de G ; alors $H' \stackrel{\text{déf}}{=} \operatorname{Ker} f_{|_H} = \operatorname{Ker} f \cap H$ est contenu dans le groupe $\mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_{n-1}$. Par hypothèse de récurrence, H' est donc un groupe libre de rang inférieur ou égal à $n-1$. Puis, l'image G' de $f_{|_H}$ est un sous-groupe (libre !) de $\mathbb{Z}$, et d'après l'exercice 3.3, il existe un sous-groupe F de H, isomorphe à G', tel que $H = F \oplus H'$. F étant de rang au plus 1, H est libre et de rang au plus n. ❏

Remarque : contrairement à ce que l'on connaît dans la théorie des espaces vectoriels de dimension finie, un sous-groupe strict d'un groupe abélien libre de type fini peut être de même rang. Ainsi, $2\mathbb{Z}$ est un sous-groupe de rang 1 de $\mathbb{Z}$, qui n'est pas $\mathbb{Z}$ tout entier.

3.2 Groupes abéliens de torsion

Un groupe G (pas nécessairement abélien) est dit *de torsion* si tout élément de G est d'ordre fini ; il est dit *sans torsion* si tout élément (autre que l'élément neutre) est d'ordre infini, et il est dit *mixte* s'il possède à la fois des éléments d'ordre fini (différents du neutre) et des éléments d'ordre infini.

Il est immédiat que tout groupe fini est de torsion, mais il existe aussi des groupes de torsion infinis ($\mathbb{Q}/\mathbb{Z}$ par exemple). Un problème difficile posé par Burnside en 1902, s'énonce ainsi : tout groupe de type fini et de torsion est-il fini ? Ce n'est qu'en 1964 que les mathématiciens Golod et Shafarevich ont répondu négativement à cette question. Cependant, dans le cadre des groupes abéliens, il est facile de voir que la réponse au problème de Burnside est oui.

Théorème 3.5 *Soit G un groupe abélien de type fini. G est de torsion si et seulement si c'est un groupe fini.*

Preuve — laissée en exercice...

Il est également facile de voir que tout groupe abélien libre est sans torsion. Dans le cadre des groupes abéliens de type fini, la réciproque est vraie aussi.

Théorème 3.6 *Soit G un groupe abélien de type fini. G est sans torsion si et seulement si G est libre. Dans ce cas, le rang de G est majoré par le cardinal de toute partie génératrice de G.*

Preuve — Il suffit de démontrer que si G est abélien, de type fini, et sans torsion, alors G admet une base (car l'autre implication est claire). On va prouver ce résultat par récurrence sur le cardinal d'une partie génératrice finie de G. Si $G \neq \{0\}$ est monogène et sans torsion, la famille formée d'un élément générateur est une base de G, qui est donc libre de rang 1.

Soit maintenant un entier $r \geq 1$, et supposons déjà montrée la propriété suivante : tout groupe abélien sans torsion engendré par r éléments est libre, de rang au plus r. Soit G un groupe abélien sans torsion, engendré par $r+1$ éléments $g_1, \ldots, g_{r+1}$. Si la famille $(g_1, \ldots, g_{r+1})$ est libre, elle constitue une base de G qui est donc libre de rang $r+1$. Sinon, on dispose d'une relation du type

$$z_1 g_1 + \cdots + z_{r+1} g_{r+1} \;=\; 0, \tag{4}$$

où les z_j sont des entiers non tous nuls, qui va permettre de montrer que G possède une partie génératrice de cardinal au plus r, et donc d'utiliser l'hypothèse de récurrence. On peut déjà supposer que les entiers $(z_1, \ldots, z_{r+1})$ sont premiers entre eux : sinon, il suffit de mettre leur PGCD en facteur dans la relation (4), puis de simplifier par ce PGCD, ce qui est légitime car G est sans torsion.

Si l'un des entiers z_j vérifie $|z_j| = 1$, par exemple $|z_{r+1}| = 1$, alors il suffit de $g_1, \ldots, g_r$ pour engendrer G. Sinon, le minimum des $|z_j|$ sur les indices j tels que $z_j \neq 0$ est strictement supérieur à 1 ; supposons que $|z_{r+1}|$ soit ce minimum. Puisque le PGCD des z_j est 1, l'un des autres coefficients (par exemple z_r) n'est pas multiple de z_{r+1}. Par division euclidienne de z_r par $|z_{r+1}|$, on peut donc trouver un entier q tel que $0 < |z_r - q z_{r+1}| < |z_{r+1}|$. Posons maintenant $g'_{r+1} \stackrel{\text{déf}}{=} g_{r+1} + q g_r$; la famille $(g_1, \ldots, g_r, g'_{r+1})$ est encore génératrice de G, et vérifie la relation non triviale

$$z_1 g_1 + \cdots + z_{r-1} g_{r-1} + (z_r - q z_{r+1}) g_r + z_{r+1} g'_{r+1} \;=\; 0,$$

dont les coefficients sont toujours premiers entre eux, mais où la plus petite valeur absolue non nulle a strictement diminué. Itérant ce procédé autant de fois qu'il faut, on aboutit à une relation de type (4), où l'un des coefficients est de valeur absolue 1, ce qui prouve alors que G est engendré par une famille de r éléments. ❑

Exercice 3.5 *Dans le théorème précédent, l'hypothèse "G est de type fini" est essentielle : montrer par exemple que $\mathbb{Q}$ est un groupe abélien sans torsion qui n'admet pas de base.*

Exercice 3.6 *Soit G un sous-groupe de $(\mathbb{R}, +)$, finiment engendré, et tel qu'il existe un entier $k \geq 2$ vérifiant : pour tout $x \in G$, x/k est toujours un élément de G. Montrer que $G = \{0\}$.*

Sous-groupe de torsion

Théorème 3.7 *Soit G un groupe abélien. L'ensemble $T(G)$ des éléments de G qui sont d'ordre fini est un sous-groupe de G, appelé* sous-groupe de torsion *de G. Le groupe quotient $G/T(G)$ est sans torsion. En particulier, si G est de type fini, $G/T(G)$ est libre de type fini.*

Preuve — T(G) contient évidemment 0, et si x et y sont dans $T(G)$, il existe deux entiers m et n tels que $mx = ny = 0$, d'où $mn(x-y) = 0$, et donc $x - y \in T(G)$. Ceci prouve que $T(G)$ est un sous-groupe de G. Soit maintenant $\dot{x} = x + T(G)$ un élément de $G/T(G)$, d'ordre fini, et soit $n \geq 1$ tel que $n\dot{x} = 0$. Cela signifie $nx + T(G) = T(G)$, et donc $nx \in T(G)$. Ceci entraîne que x lui-même est d'ordre fini dans G, autrement dit $x \in T(G)$. Ainsi, $\dot{x} = 0$ dans $G/T(G)$ et $G/T(G)$ est sans torsion. Si de plus G est de type fini, $G/T(G)$ reste de type fini [...], et le théorème 3.6 prouve que $G/T(G)$ est libre. ❏

Exercice 3.7 *Trouver un exemple de groupe (non abélien) pour lequel l'ensemble des éléments d'ordre fini n'est pas un sous-groupe.*

Le théorème qui suit constitue l'ultime étape dans l'étude de la structure des groupes abéliens de type fini.

Théorème 3.8 *Si G est un groupe abélien de type fini, G est la somme directe de deux sous-groupes F et H, où F est fini et H est libre de type fini. Dans cette décomposition, le sous-groupe F est uniquement déterminé, et H est déterminé à un isomorphisme près.*

Preuve — Supposons tout d'abord que $G = F \oplus H$, où F et H satisfont aux conditions de l'énoncé. Comme F est un groupe fini, F est de torsion et donc $F \subset T(G)$. Puis soit $g \in T(G)$, que l'on écrit $g = g_F + g_H$, où $g_F \in F$ et $g_H \in H$. Comme $T(G)$ est un sous-groupe, $g_H = g - g_F$ est de torsion ; mais puisque H est libre, $g_H = 0$ et $g = g_F \in F$. On a donc finalement $F = T(G)$, et H doit être isomorphe à $G/T(G)$.

Posons donc $F \stackrel{\text{déf}}{=} T(G)$, et montrons l'existence de H. D'après le théorème 3.7, le groupe quotient $G/T(G)$ est libre de type fini, donc $T(G)$ est un facteur direct (proposition 3.3). $T(G)$ admet ainsi un supplémentaire H, isomorphe à $G/T(G)$: H remplit donc toutes les conditions voulues. ❏

3.3 Épilogue

La synthèse des théorèmes 3.8, 2.1 et 3.2 s'énonce sous la forme d'un théorème général de structure des groupes abéliens de type fini.

Théorème 3.9 *Tout groupe abélien de type fini est isomorphe à un produit du type*

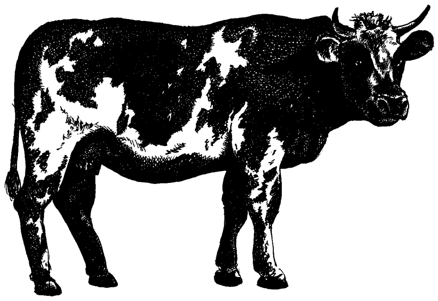
$$\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z} \times \mathbb{Z}^s,$$

où r et s sont des entiers positifs ou nuls, et $m_1, \ldots, m_r$ sont des entiers supérieurs ou égaux à 2 tels que $m_1 | m_2 | \cdots | m_r$.

De plus, les entiers $r, s, m_1, \ldots, m_r$ vérifiant ces conditions sont déterminés de façon unique par le groupe G.

Pour terminer ce chapitre, on propose au lecteur de s'amuser à résoudre l'exercice qui suit, application inattendue de certains résultats rencontrés ici.

Exercice 3.8 *Un paysan possède un troupeau de 25 vaches, et il a remarqué la propriété suivante : quelle que soit la vache qu'il retire, il peut partager les 24 vaches qui restent en 3 sous-troupeaux de 8 vaches, tous les trois de même poids total. Prouver que toutes ses vaches ont le même poids.*



Références

[1] Alain Bouvier et Denis Richard. *Groupes – observation, théorie, pratique.* Hermann, 1994.

[2] Josette Calais. *Éléments de Théorie des Groupes.* Puf, 1998.

[3] J.J. Rotman. *An Introduction to the Theory of Groups.* Graduate Texts in Mathematics. Springer-Verlag, 1995.