THÉORIE DES GROUPES 2024 - 25, SOLUTIONS 5

Exercise 1. À faire vous-même.

Exercise 2. (1) Tout élément d'un groupe fini est de torsion, donc $\mathrm{Tors}(A) = A$.

(2) Aucun élément sauf 0 n'est d'ordre fini, donc son groupe de torsion est trivial.

(3) Soit $[q] \in \mathbb{Q}/\mathbb{Z}$ un élément quelconque représenté par $q = \frac{a}{b} \in \mathbb{Q}$. Alors

$$b[q] = [bq] = [a] = [0] \in \mathbb{Q}/\mathbb{Z}$$

puisque $a \in \mathbb{Z}$. Ainsi, tout élément est de torsion et $\mathrm{Tors}(\mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$.

(4) Soit $x \in \mathbb{C}^\times$ et écrivons-le en forme polaire $x = re^{i\theta}$ avec $r > 0$ et $\theta \in [0, 2\pi)$. Alors $x^n = r^n e^{in\theta} = 1$ si et seulement si $r = 1$ et $n\theta = 0 \bmod 2\pi$, c'est-à-dire $x = e^{2\pi ik/n}$ pour $k \in \mathbb{Z}$. Ce sont les racines n-ièmes de l'unité μ_n. Ainsi

$$\mathrm{Tors}(\mathbb{C}^\times) = \mu_\infty = \bigcup_{n \in \mathbb{N}_{>0}} \mu_n.$$

(5) Nous savons que les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z} \cong \mathbb{Z}$, qui sont libres, donc sans torsion.

(6) Nous avons vu dans le cours que les sous-groupes d'un groupe abélien libre fini sont abéliens libres, ce qui montre que leur sous-groupe de torsion est trivial.

Exercise 3. Étant donné que G est de type fini, il existe un ensemble fini de générateurs pour G. Soit $g_1, g_2, \dots, g_k$ un ensemble de générateurs pour G, de sorte que tout élément de G peut s'écrire comme une combinaison linéaire entière de ces générateurs :

$$g = n_1 g_1 + n_2 g_2 + \cdots + n_k g_k,$$

où $n_1, n_2, \dots, n_k \in \mathbb{Z}$.

Puisque $\mathrm{Tors}(G) = G$, tout élément de G est un élément de torsion. Cela implique que pour chaque générateur $g_i \in G$, il existe un entier positif m_i minimal tel que $m_i \cdot g_i = 0$ (m_i est l'ordre de g_i).

Puisque G est engendré par l'ensemble fini $\{g_1, g_2, \dots, g_k\}$ et que chaque g_i a un ordre fini m_i, il n'y a qu'un nombre fini de combinaisons possibles des générateurs $g_1, g_2, \dots, g_k$ avec des coefficients entiers n_i modulo m_i, ce qui implique que G lui-même est fini.

Exercise 4. **(1) $\implies$ (2)** : Pour tout $i \in I$, définissons $e_i \in \mathbb{Z}^{\oplus I}$ comme :

$$e_i := (a_j)_{j \in I} \in \mathbb{Z}^{\oplus I}, \text{ où } a_j = 1 \text{ si } j = i \text{ et } a_j = 0 \text{ si } j \neq i.$$

Il est facile de montrer en utilisant la définition des sommes directes que l'ensemble $\{e_i\}_{i \in I}$ est une base de $\mathbb{Z}^{\oplus I}$. Maintenant, si $A \cong \mathbb{Z}^{\oplus I}$, alors l'image homomorphe des e_i est une base pour

A.
(2) $\implies$ **(1)** : Fixons une base $(a_k)_{k\in I}$ de A, alors tout élément $x \in A$ peut être écrit de manière unique comme

$$x = \sum_{k\in I} n_k a_k$$

pour certains $n_k \in \mathbb{Z}$. Considérons la fonction suivante, qui est bien définie en raison de l'unicité mentionnée ci-dessus

$$\varphi : A \to \mathbb{Z}^{\oplus I}, \sum_{k\in I} n_k a_k \mapsto (n_k)_{k\in I}.$$

Il est facile de vérifier que φ est un isomorphisme de groupes abéliens.

Exercise 5. (1) Supposons d'abord que G est abélien libre. L'exercice précédent nous dit qu'il existe un ensemble I et une base $B = \{a_i \mid i \in I\} \subset G$ telle que tous les éléments $x \in G$ peuvent être écrits de manière unique sous forme de sommes finies

$$x = \sum_{k\in I} n_k a_k$$

où presque tous les n_k sont égaux à 0. Soit A un autre groupe abélien avec une fonction d'ensemble $f : B \to A$. Prouvons l'existence de φ en définissant

$$\begin{aligned} \varphi : G &\to A \\ x = \sum_{k\in I} n_k a_k &\mapsto \sum_{k\in I} n_k f(a_k) \end{aligned}$$

Cela est bien défini puisque presque tous les n_k sont nuls (c'est une somme finie). C'est clairement un homomorphisme de groupes (à vérifier par vous-même) et $\varphi(i(a_k)) = \varphi(a_k) = f(a_k)$ pour tout $a_k \in B$ de sorte que $\varphi \circ i = f$. Pour prouver l'unicité, supposons qu'il existe deux homomorphismes $\varphi, \varphi' : G \to A$ prolongeant f. Alors pour tout $x = \sum_{k\in I} n_k a_k \in G$ nous avons

$$\begin{aligned} \varphi'(x) = \varphi'(\sum_{k\in I} n_k a_k) &= \sum_{k\in I} n_k \varphi'(a_k) \\ &= \sum_{k\in I} n_k f(a_k) \\ &= \sum_{k\in I} n_k \varphi(a_k) = \varphi(\sum_{k\in I} n_k a_k) = \varphi(x) \end{aligned}$$

ce qui prouve que $\varphi = \varphi'$ (nous avons utilisé le fait que φ et φ' sont linéaires et prolongent f).

(2) Supposons maintenant que G satisfait à la propriété universelle des groupes abéliens libres. Nous allons montrer que G est en effet libre abélien en montrant que $G \cong \mathbb{Z}^{\oplus B}$ pour B l'ensemble donné par la propriété universelle de G. Notez que l'idée de la preuve suivante est toujours utilisée lors du traitement des propriétés universelles, que vous rencontrerez (probablement) à nouveau dans le futur.

Soit $f : B \to \mathbb{Z}^{\oplus B}$ donné par l'inclusion de la base, c'est-à-dire $f : b \mapsto e_b \in \mathbb{Z}^{\oplus B}$ défini dans la preuve de l'exercice précédent (e_b est une généralisation de $e_i \in k^n$ en algèbre linéaire). En utilisant la propriété universelle de G, l'application f se prolonge en un morphisme $\varphi : G \to \mathbb{Z}^{\oplus B}$ de telle sorte que le triangle suivant commute

$$\begin{tikzcd} B \arrow[r, "i"] \arrow[dr, "f"'] & G \arrow[d, "\varphi"] \\ & \mathbb{Z}^{\oplus B}. \end{tikzcd}$$

Puisque $\mathbb{Z}^{\oplus B}$ est libre abélien avec comme base $f : B \subset \mathbb{Z}^{\oplus B}$, il satisfait à la propriété universelle (prouvée dans le premier point) des groupes abéliens libres. Ainsi, nous pouvons prolonger $i : B \to G$ le long de $f : B \to \mathbb{Z}^{\oplus B}$ pour obtenir $\varphi' : \mathbb{Z}^{\oplus B} \to G$ de sorte que le triangle suivant commute:

$$\begin{tikzcd} B \arrow[r, "f"] \arrow[dr, "i"'] & \mathbb{Z}^{\oplus B} \arrow[d, "\varphi'"] \\ & G. \end{tikzcd}$$

Nous allons maintenant prouver que φ et φ' sont inverses l'une de l'autre en appliquant deux fois de plus la propriété universelle des groupes abéliens libres. D'abord, nous l'appliquons à G et elle nous dit qu'il existe un unique $\psi : G \to G$ tel que le triangle suivant commute

$$\begin{tikzcd} B \arrow[r, "i"] \arrow[dr, "i"'] & G \arrow[d, "\psi"] \\ & G. \end{tikzcd}$$

Puisque l'identité $\mathrm{id}_G : G \to G$ fait l'affaire, toute telle ψ doit être l'identité. Mais pour $\psi = \varphi' \circ \varphi$ nous avons que $\psi \circ i = \varphi' \circ \varphi \circ i = \varphi' \circ f = i$, où nous utilisons la commutativité des deux premiers triangles. Comme expliqué, par unicité de telles applications, nous devons avoir que $\varphi' \circ \varphi = \mathrm{id}_G$. De manière similaire, nous pouvons utiliser la propriété universelle de $\mathbb{Z}^{\oplus B}$ pour montrer que $\varphi \circ \varphi' = \mathrm{id}_{\mathbb{Z}^{\oplus B}}$. Cela montre que $G \cong \mathbb{Z}^{\oplus B}$, ce qui termine la preuve.

Exercise 6. Puisque F est libre avec comme base $\{e_1, e_2, e_3\}$, nous pouvons appliquer la propriété universelle de l'exercice 5 avec $B = \{e_1, e_2, e_3\}$, $G = F$ et $A = \mathbb{Z}^2$. Cela nous dit qu'il existe un unique homomorphisme de groupes $\varphi : F \to \mathbb{Z}^2$ qui prolonge f. L'image d'un homomorphisme de groupes est toujours un sous-groupe du codomaine. Puisque nous avons vu dans les cours que les sous-groupes des groupes abéliens libres finis sont libres abéliens finis, cela répond positivement à la question.

Exercise 7. Nous utiliserons constamment le fait que tout sous-groupe de $\mathbb{Z}^k$ est libre de rang $l \leq k$. Dans chaque cas, nous désignerons le groupe abélien en question par A.

(1) Comme $\{(1, 1)\}$ est un ensemble générateur de A et est linéairement indépendant, c'est une base pour A et donc le rang de A est 1.

(2) Le rang de A est encore 1 puisque $B = \{(1,2)\}$ est une base pour A. L'ensemble B est linéairement indépendant et génère A car $(-3,-6) = (-3) \cdot (1,2)$.
(3) On vérifie que $\{1, \sqrt{2}, \sqrt{3}\}$ forme une base pour A et donc le rang de A est 3.
(4) Le rang de A est 3 puisque les trois éléments génèrent A et sont linéairement indépendants, ce qui peut être constaté en observant que le déterminant de la matrice suivante est non nul

$$\begin{pmatrix} 1 & 2 & 1 \\ 5 & 3 & -9 \\ 1 & 8 & 34 \end{pmatrix}.$$

(5) Remarquez que l'ensemble $B = \{(1,5,1),(2,3,8)\}$ est linéairement indépendant et génère A puisque $(1,-9,13) = (-3) \cdot (1,5,1) + 2 \cdot (2,3,8)$. Donc, le rang de A est 2.

Exercise 8. Soit $\varphi : \mathbb{Z}^n \to \mathbb{Z}^m$ un isomorphisme de groupes abéliens. Fixons un nombre premier p et considérons le sous-groupe suivant de $\mathbb{Z}^m$:

$$H := \{(a_1, ..., a_m) \in \mathbb{Z}^m \mid a_i \in p\mathbb{Z}\}.$$

Remarquons que $\mathbb{Z}^m/H \cong (\mathbb{Z}/p\mathbb{Z})^m$.

Nous laissons comme un petit exercice au lecteur de montrer que

$$\varphi^{-1}(H) = \{(a_1, ..., a_n) \in \mathbb{Z}^n \mid a_i \in p\mathbb{Z}\}$$

et $\mathbb{Z}^n/\varphi^{-1}(H) \cong (\mathbb{Z}/p\mathbb{Z})^n$.
Puisque φ est en particulier un homomorphisme surjectif, le théorème de correspondance ainsi que le troisième théorème d'isomorphisme impliquent que φ induit un isomorphisme

$$\overline{\varphi} : \mathbb{Z}^n/\varphi^{-1}(H) \to \mathbb{Z}^m/H.$$

Nous avons donc un isomorphisme de groupes abéliens

$$\overline{\varphi} : (\mathbb{Z}/p\mathbb{Z})^n \to (\mathbb{Z}/p\mathbb{Z})^m.$$

qui est automatiquement $\mathbb{Z}/p\mathbb{Z}$-linéaire puisqu'il s'agit d'un morphisme de groupes abéliens. Puisque les espaces vectoriels isomorphes doivent avoir la même dimension, on obtient que $m = n$.

Exercise 9. La même preuve que dans la Proposition 11 des notes de cours s'applique pour montrer que $\mathbb{Q}^{>0}$ n'est pas de type fini. Pour montrer qu'il est libre, nous montrons que l'ensemble $B = \{p_i \mid p_i \text{ est un nombre premier}\}$ des nombres premiers forme une base. Soit $q = \frac{a}{b}$ écrit sous forme irréductible, avec $a, b \in \mathbb{N}_*$. Décomposons a et b comme un produit de puissances de nombres premiers. Remarquons que les nombres premiers apparaissant dans chaque décomposition sont distincts puisque la fraction $\frac{a}{b}$ a été choisie irréductible. En utilisant ces décompositions, nous obtenons q comme un produit fini de puissances d'éléments de B (les puissances sont négatives pour les premiers apparaissant dans la décomposition de b). S'il existait plus d'une décomposition de q comme un produit de puissances de nombres premiers, cela donnerait des décompositions distinctes de a ou de b (ou des deux) comme produit de puissances de nombres premiers, en séparant les puissances positives et négatives. Par unicité de la décomposition des nombres naturels (vue en algèbre linéaire 2), nous obtenons une contradiction.

Nous avons montré que B est une base du groupe abélien $\mathbb{Q}^{>0}$, ce qui signifie qu'il est libre par l'exercice 4.

Exercise 10. Nous nous référons au diagramme de la série pour la notation. Supposons que F soit un groupe abélien libre de type fini, alors fixons une base $e_1, e_2, ..., e_n$ pour F. Puisque ϕ est surjective, nous pouvons choisir des pré-images $g_1, ..., g_n$ dans G de $\psi(e_1), ..., \psi(e_n)(H)$. Il découle de la propriété universelle des groupes abéliens libres que nous pouvons définir une application $\alpha : A \to G$, rendant le diagramme commutatif en envoyant simplement e_i sur g_i. Ainsi, A est projectif.
Réciproquement, supposons que A soit un groupe abélien de type fini, alors soit $a_1, ..., a_n$ un ensemble générateur quelconque. Nous obtenons alors un homomorphisme de groupes surjectif $\phi : \mathbb{Z}^n \to A$ défini en envoyant la base usuelle e_i sur a_i. Soit K le noyau de l'homomorphisme ϕ. Maintenant, K est un groupe abélien libre puisque nous savons, d'après les cours, que les sous-groupes des groupes abéliens libres de type fini sont libres. Nous obtenons donc une suite exacte courte

$$0 \to K \to \mathbb{Z}^n \xrightarrow{\phi} A \to 0.$$

Soit $\psi : A \to A$ l'application identité, la projectivité de A implique qu'il existe une application $\alpha : A \to \mathbb{Z}^n$ telle que $\phi \circ \alpha = \mathrm{id}_A$. Ainsi, la suite exacte ci-dessus se scinde à droite. Par conséquent, A est un sous-groupe de $\mathbb{Z}^n$ et est donc un groupe abélien libre.

Exercise 11. Considérons la suite exacte courte

$$0 \to 2\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

La suite induite des sous-groupes de torsion est

$$0 \to 0 \to 0 \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

qui n'est clairement pas exacte en raison de l'échec de la surjectivité de l'application $0 \to \mathbb{Z}/2\mathbb{Z}$.