TD3 : Groupes abéliens de type fini

Exercices ⋆ : à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices ⋆⋆ : seront traités en classe en priorité.
Exercices ⋆⋆⋆ : plus difficiles.

Exercice 1 : ⋆

Montrer que les groupes $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ et $\mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ sont isomorphes.

Solution de l'exercice 1. On utilise le lemme chinois pour voir que les deux groupes sont isomorphes au groupe

$$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z} \times /Z/9\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z})\,.$$

Cette écriture est la décomposition en composantes p-primaire. On peut aussi écrire la décomposition en facteurs invariants de ces deux groupes, et l'on trouve :

$$\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/900\mathbb{Z}\,.$$

Exercice 2 : ⋆

Montrer qu'un groupe abélien fini non cyclique possède un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ pour un certain nombre premier p.

Solution de l'exercice 2. Le théorème du cours assure qu'un tel groupe G est isomorphe à un produit $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$, avec $d_i \geq 2$ et $d_i | d_{i+1}$. Comme G n'est pas cyclique, on a $r \geq 2$. Il existe un facteur premier p de d_1, alors p divise tous les d_i, et $\mathbb{Z}/p\mathbb{Z}$ est isomorphe à un sous-groupe de chacun des $\mathbb{Z}/d_i\mathbb{Z}$ (c'est le sous-groupe de p-torsion). Alors le sous-groupe de p-torsion de G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^r$, qui contient clairement un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 3 : ⋆

a) Combien y a-t-il de groupes abéliens de cardinal 360 ? Faire la liste complète de ces groupes.

b) Plus généralement, pour tout entier n, combien y a-t-il de groupes abéliens de cardinal n ?

Solution de l'exercice 3.

a) On écrit la décomposition en facteurs premiers de $360 = 2^3.3^2.5$. Alors si G est un groupe de cardinal 360, $T_2(G)$ est un groupe abélien de cardinal 2^3, il y a donc 3 classes d'isomorphisme de tels groupes, à savoir $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^3$. De même, il y a exactement deux classes d'isomorphisme possibles pour $T_3(G)$, à savoir $\mathbb{Z}/9\mathbb{Z}$ et $(\mathbb{Z}/3\mathbb{Z})^2$, et $T_5(G)$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Par conséquent, il y a exactement $3.2 = 6$ classes d'isomorphisme de groupes abéliens d'ordre 360, dont les décompositions p-primaires et en facteurs invariants sont les suivantes :

$$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/360\mathbb{Z}$$

$$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$$

$$(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$$

$$\mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z}$$

$$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}$$

$$(\mathbb{Z}/2\mathbb{Z})^3 \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}\,.$$

b) On utilise la classification des classes d'isomorphisme de groupes abéliens finis. Notons $n = {p_1}^1 \dots {p_r}^r$ la décomposition de n en facteurs premiers. Alors on sait que la classe d'isomorphisme d'un groupe abélien d'ordre n est caractérisée par ses facteurs invariants $(d_1, \dots, d_s)$ qui sont des entiers > 1 tels que $d_i | d_{i+1}$ et $d_1 \dots d_s = n$. Par conséquent, chaque d_i se décompose $d_i = {p_1}^{i,1} \dots {p_1}^{i,r}$, avec les contraintes suivantes : pour tout j, $\alpha_{i;j} \leq \alpha_{i+1;j}$ (pour tout i) et $\sum_{i=1}^{s} \alpha_{i;j} = \alpha_j$.
Par conséquent, le nombre de choix possibles pour les a_i est exactement $\prod_{j=1}^{r} p(\alpha_j)$, où $p(\alpha)$ désigne le nombre de partitions de α, i.e. le nombre de façons d'écrire l'entier α comme une somme croissante d'entiers strictement positifs.

Exercice 4 :

a) Le nombre de classes de conjugaison dans $\mathfrak{S}_5$ est le même que le nombre de groupes abéliens de cardinal 32 à isomorphisme près. Pourquoi ?

b) Généraliser au nombre de classes de conjugaison dans $\mathfrak{S}_n$.

Solution de l'exercice 4.

a) Les deux ensembles en question sont naturellement en bijection avec l'ensemble des partitions de 5.

b) Soit p un nombre premier. Notons G_n l'ensemble des classes d'isomorphisme de groupes abéliens de cardinal p^n, P_n l'ensemble des partitions de l'entier n et C_n l'ensemble des classes de conjugaison dans $\mathfrak{S}_n$. On dispose des applications suivantes

$$\varphi : P_n \to G_n$$

et

$$\psi : P_n \to C_n$$

où pour toute partition $(n_1, \dots, n_r)$ de n, $\varphi((n_1, \dots, n_r))$ est la classe d'isomorphisme de $\prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$ et $\psi((n_1, \dots, n_r))$ est la classe de conjugaison de la permutation $(1, 2, \dots, n_1)(n_1 + 1, \dots, n_1 + n_2) \dots (n_1 + \dots + n_{r-1} + 1, \dots, n)$. On voit alors facilement que φ et ψ sont des bijections, donc $|C_n| = |G_n|$, i.e. il y a autant de classes de conjugaison dans $\mathfrak{S}_n$ que de classes d'isomorphisme de groupes abéliens d'ordre p^n.

Exercice 5 : ⋆

Soit G un groupe abélien fini. Montrer qu'il existe dans G un élément d'ordre égal à l'*exposant de G* (c'est-à-dire au ppcm des ordres des éléments de G).

Solution de l'exercice 5.

— On commence par une preuve "élémentaire" : montrons d'abord que pour tous $x, y \in G$ d'ordres respectifs m et n premiers entre eux, le produit xy est d'ordre $m.n$. Il est clair que $(xy)^{mn} = 1$ donc l'ordre de xy divise mn. Soit maintenant $k \geq 1$ tel que $(xy)^k = 1$. En élevant à la puissance n, on obtient $x^{kn} = 1$, donc m divise kn. Or m et n sont premiers entre eux, donc m divise k. Par symétrie, on a aussi que n divise k, donc mn divise k, donc xy est d'ordre mn.
On décompose l'exposant de G en facteurs premiers : $\exp(G) = {p_1}^1 \dots {p_r}^r$, avec les p_i premiers distincts. Par définition de l'exposant de G, pour tout $1 \leq i \leq r$, il existe $g_i \in G$ dont l'ordre est divisible par ${p_i}^i$, disons égal à ${p_i}^i.m_i$. Alors $g_i^{m_i}$ est d'ordre ${p_i}^i$, et on a vu qu'alors l'élément $g := g_1^{m_1} \dots g_r^{m_r} \in G$ est d'ordre exactement ${p_1}^1 \dots {p_r}^r = \exp(G)$.
— Une preuve moins élémentaire : le théorème de classification des groupes abéliens finis assure qu'il existe des entiers $2 \leq d_1 | \dots | d_s$ tels que G soit isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z}$. Il est alors clair que $\exp(G) = d_r$ et que l'élément $(0, \dots, 0, 1) \in \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z}$ est d'ordre d_r.

Exercice 6 : ⋆

Soit G un groupe et soient H et K des sous-groupes de G. On suppose que :

a) $H \triangleleft G$ et $K \triangleleft G$;

b) $HK = G$;

c) $H \cap K = e$.

Montrer que G est isomorphe à $H \times K$.

Solution de l'exercice 6. Montrons d'abord que H et K commutent. Soient $h \in H$ et $k \in K$. Comme H est distingué dans G, on a $kh^{-1}k^{-1} \in H$, donc $hkh^{-1}k^{-1} \in H$. De même, K est distingué dans G, donc $hkh^{-1} \in K$, donc $hkh^{-1}k^{-1} \in K$. Donc $hkh^{-1}k^{-1} \in H \cap K = \{e\}$, donc $hk = kh$.
Montrons maintenant que pour tout $g \in G$, il existe un unique couple $(h, k) \in H \times K$ tel que $g = hk$. L'existence est assurée par l'hypothèse b). Pour l'unicité, soient $h, h' \in H$ et $k, k' \in K$ tels que $hk = h'k'$. Alors $kk'^{-1} = h^{-1}h'$ est dans $H \cap K$, donc l'hypothèse c) assure que $kk'^{-1} = h^{-1}h' = e$, donc $h = h'$ et $k = k'$, d'où l'unicité.
On considère alors l'application $\varphi : H \times K \to G$ définie par $\varphi(h, k) := hk$. Le fait que H et K commutent assure que φ est un morphisme de groupes. L'existence et l'unicité prouvée plus haut assurent que φ est une bijection. Donc G est bien isomorphe au groupe $H \times K$.

Exercice 7 : ⋆⋆

Soit K un corps et soit $G \subset K^*$ un sous-groupe fini d'ordre n. On va montrer que G est un groupe cyclique.

a) Montrer que l'ordre de tout élément de G divise n.

b) Soit d un diviseur de n et $x \in G$ d'ordre d. Soit H le sous-groupe cyclique de G engendré par x. Montrer que tout élément d'ordre d est dans H.

c) On note $N(d)$ le nombre d'éléments de G d'ordre d. Montrer que $N(d) = 0$ ou $\varphi(d)$, et que $\sum_{d|n;\ d>0} N(d) = n$.

d) Conclure.

En particulier, si p est un nombre premier, $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, et si K est un corps fini, K^* est un groupe cyclique.

Solution de l'exercice 7.

a) C'est le théorème de Lagrange.

b) Considérons le polynôme $P = X^d - 1 \in K[X]$. Comme K est un corps, le polynôme P a au plus d racines dans K. Or tout élément du groupe H est d'ordre divisant d, donc tous les éléments de H sont des racines de P. Or le cardinal de H est égal à l'ordre de x, c'est-à-dire à d. Donc H contient toutes les racines de P dans K.

Soit maintenant $y \in G$ d'ordre d. Alors y est racine de P, donc y est dans H.

c) Supposons $N(d) \neq 0$. Alors il existe $x \in G$ d'ordre d. La question b) assure que tout les éléments d'ordre d dans G sont exactement les éléments d'ordre d dans $\langle x \rangle$ qui est un groupe cyclique d'ordre d. Or un groupe cyclique d'ordre d a exactement $\varphi(d)$ éléments d'ordre d, donc $N(d) = \varphi(d)$.

En outre, on peut partitionner G selon l'ordre des éléments, i.e. G est la réunion disjointe, pour d divisant n (par la question a)), des ensembles G_d formés des éléments d'ordre d. En calculant les cardinaux, on trouve donc $|G| = \sum_{d|n} |G_g|$, i.e. $n = \sum_{d|n} N(d)$.

d) La question c) assure que $n = \sum_{d|n} N(d)$. Or on sait que $n = \sum_{d|n} \varphi(d)$. Donc $\sum_{d|n} N(d) = \sum_{d|n} \varphi(d)$. Or pour tout $d|n$, $N(d) \leq \varphi(d)$, donc on a bien pour tout $d|n$, $N(d) = \varphi(d)$. En particulier, $N(n) = \varphi(n) > 0$, donc il existe un élément d'ordre n dans G, i.e. G est cyclique.

Exercice 8 : ⋆⋆

Si A est un anneau, on note $A^\times$ le groupe (multiplicatif) des éléments inversibles de A.

a) Soit G un groupe monogène. Montrer que le groupe des automorphismes de G est en bijection avec l'ensemble des générateurs de G.

b) Montrer que pour tout $n \in \mathbb{N}$, on a un isomorphisme de groupes $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

c) Soit p un nombre premier impair et soit $\alpha \geq 1$. Quel est l'ordre de $1+p$ dans $(\mathbb{Z}/p^{\alpha}\mathbb{Z})^{\times}$? En déduire que $(\mathbb{Z}/p^{\alpha}\mathbb{Z})^{\times} \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.

d) Expliciter $(\mathbb{Z}/2^{\alpha}\mathbb{Z})^{\times}$ pour $\alpha \geq 1$.

e) En déduire $(\mathbb{Z}/n\mathbb{Z})^{\times}$ pour $n \in \mathbb{N}$.

Solution de l'exercice 8.

a) Soit G_0 l'ensemble des générateurs de G et soit g_0 un élément de G_0. Alors si φ est un automorphisme de G, l'image de φ est engendrée par $\varphi(g_0)$; ce qui veut dire que $\varphi(g_0)$ est un générateur de G. On définit alors une application (ensembliste) $\begin{array}{ccc} \mathrm{Aut}\, G & \to & G_0 \\ \varphi & \mapsto & \varphi(g_0) \end{array}$. Comme g_0 est générateur, l'application est bijective.

b) Dans $\mathbb{Z}$, montrons par récurrence sur $k \geq 1$ qu'il existe λ_k premier à p vérifiant $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$. L'étape d'initialisation pour $k=1$ est claire via la formule du binôme, puisque p divise $\binom{p}{2}$. Montrons l'hérédité : soit $k \geq 1$, on a $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$ par hypothèse de récurrence, donc on obtient $(1+p)^{p^{k+1}} = 1 + p^{k+2}(\lambda_k + \sum_{i=2}^{p} \binom{p}{i} \lambda_k^i p^{(i-1)(k+1)-1})$ et le résultat est montré par récurrence.
En particulier, $1+p$ est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^{\alpha}\mathbb{Z})^{\times}$.
En utilisant l'exercice 7, on sait que $(\mathbb{Z}/p\mathbb{Z})^{\times}$ est cyclique, d'ordre $p-1$. Notons x_0 un générateur de $(\mathbb{Z}/p\mathbb{Z})^{\times}$ et prenons un relèvement x_1 de x_0 dans $(\mathbb{Z}/p^{\alpha}\mathbb{Z})^{\times}$. L'ordre de x_1 est le la forme $(p-1)p^s$ pour un certain $s \leq \alpha$, de sorte que $x := x_1^{p^s}$ est d'ordre $p-1$. Comme x et $1+p$ ont des ordres premiers entre eux et comme le groupe $(\mathbb{Z}/p^{\alpha}\mathbb{Z})^{\times}$ est abélien, on a vu que $x(1+p)$ est donc d'ordre $p^{\alpha-1}(p-1) = \varphi(p)$ et $(\mathbb{Z}/p^{\alpha}\mathbb{Z})^{\times}$ est donc cyclique.

c) Remarquons d'abord que $(\mathbb{Z}/2\mathbb{Z})^{\times} = \{1\}$ et $(\mathbb{Z}/4\mathbb{Z})^{\times} \simeq \mathbb{Z}/2\mathbb{Z}$. Supposons maintenant $\alpha \geq 2$. Par une récurrence semblable à celle effectuée au b), on montre que 5 est d'ordre $2^{\alpha-2}$ dans $(\mathbb{Z}/2^{\alpha}\mathbb{Z})^{\times}$. Observons maintenant le morphisme surjectif $\pi : (\mathbb{Z}/2^{\alpha}\mathbb{Z})^{\times} \to (\mathbb{Z}/4\mathbb{Z})^{\times}$: son noyau est exactement $\langle 5 \rangle$, et $\pi(-1) = -1$. Par conséquent, les sous-groupes $\langle 5 \rangle$ et $\langle -1 \rangle$ vérifient les hypothèses de l'exercice 6, donc $\langle 5 \rangle \times \langle -1 \rangle \cong (\mathbb{Z}/2^{\alpha}\mathbb{Z})^{\times}$. On obtient donc finalement $(\mathbb{Z}/2^{\alpha}\mathbb{Z})^{\times} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

d) Si $n = \prod_p p^{v_p}$ est la décomposition en facteurs premiers de n, alors le lemme chinois nous donne

$$(\mathbb{Z}/n\mathbb{Z})^{\times} \simeq (\mathbb{Z}/2^{v_2}\mathbb{Z})^{\times} \times \prod_{p \neq 2;\ v_p \geq 1} \big(\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{v_p-1}\mathbb{Z}\big).$$

Exercice 9 :

Déterminer les entiers $n \in \mathbb{Z}$ pour lesquels $(\mathbb{Z}/n\mathbb{Z})^{\times}$ est cyclique.

Solution de l'exercice 9. Si $n = \prod_p p^{v_p}$ est la décomposition en facteurs premiers de n, la question d) de l'exercice 8 assure que

$$(\mathbb{Z}/n\mathbb{Z})^{\times} \simeq (\mathbb{Z}/2^{v_2}\mathbb{Z})^{\times} \times \prod_{p \neq 2;\ v_p \geq 1} \big(\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{v_p-1}\mathbb{Z}\big).$$

En remarquant qu'un groupe cyclique ne peut pas contenir plus d'un élément d'ordre 2, on conclut que $(\mathbb{Z}/n\mathbb{Z})^{\times}$ est cyclique si et seulement si $n = p^{\alpha}$ ou $2p^{\alpha}$ avec p un nombre premier impair et $\alpha \geq 0$ ou $n = 4$.

Exercice 10 : ⋆⋆

Décomposer le groupe $G = (\mathbb{Z}/187\mathbb{Z})^{\times}$ sous la forme donnée par le théorème de structure des groupes abéliens de type fini.

Solution de l'exercice 10. Comme $187 = 11.17$, l'exercice 8 assure que

$$G \cong (\mathbb{Z}/11\mathbb{Z})^{\times} \times (\mathbb{Z}/17\mathbb{Z})^{\times} \cong \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/80\mathbb{Z}\,.$$

Les facteurs invariants de G sont donc 2 et 80.

Exercice 11 : ⋆⋆

a) On considère $H := \{(a,b) \in \mathbb{Z}^2 : a-b \text{ est divisible par } 10\}$. Montrer que H est un sous-groupe de $\mathbb{Z}^2$, calculer son rang, en donner une base et décrire le quotient $\mathbb{Z}^2/H$.

b) On note H le sous-groupe de $\mathbb{Z}^2$ engendré par $(2,5)$, $(5,-1)$ et $(1,-2)$. Déterminer une base de H et décrire le quotient $\mathbb{Z}^2/H$.

c) On note H le quotient de $\mathbb{Z}^3$ par le sous-groupe engendré par les vecteurs $(4,8,10)$ et $(6,2,0)$. Déterminer la structure du groupe H.

Solution de l'exercice 11.

a) Il est clair que H est un sous-groupe de $\mathbb{Z}^2$. Soit $(a,b) \in \mathbb{Z}^2$. Alors $(a,b) \in H$ si et seulement s'il existe $k \in \mathbb{Z}$ tel que $b = a + 10k$. Cela assure que $H = \{(a, a+10k) : (a,k) \in \mathbb{Z}^2\} = \mathbb{Z}(1,1) \oplus \mathbb{Z}(0,10)$, donc que H est de rang 2, de base $(1,1)$ et $(0,10)$. Alors $(1,1)$ et $(0,1)$ forment une base de $\mathbb{Z}^2$ adaptée à l'inclusion $H \subset \mathbb{Z}^2$, ce qui assure que $\mathbb{Z}^2/H \cong \mathbb{Z}/10\mathbb{Z}$.

b) On applique l'algorithme de réduction des matrices à coefficients entiers pour montrer que des opérations élémentaires sur les colonnes de la matrice obtenue en inscrivant les trois vecteurs donnés en colonne, à savoir

$$\begin{pmatrix} 2 & 5 & 1 \\ 5 & -1 & -2 \end{pmatrix},$$

aboutissent à la matrice

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 9 & -2 \end{pmatrix}.$$

Cela assure que $(1,-2)$ et $(0,9)$ forment une base de H. Donc H est de rang 2, et $((1,-2);(0,1))$ est une base adaptée à l'inclusion $H \subset \mathbb{Z}^2$, ce qui assure que $\mathbb{Z}^2/H \cong \mathbb{Z}/9\mathbb{Z}$.

c) En réduisant la matrice correspondante, on voit qu'une base du sous-groupe $\mathbb{Z}(4,8,10) + \mathbb{Z}(6,2,0)$ est donnée par $(-20,0,10)$ et $(6,2,0)$. Cela assure qu'une base adaptée à l'inclusion de ce groupe dans $\mathbb{Z}^3$ est donnée par les trois vecteurs $(-2,0,1)$, $(3,1,0)$ et $(1,0,0)$. Donc le quotient H est isomorphe à $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.

Exercice 12 :

Soit $n \geq 1$. Constuire dans $\mathbb{R}$ un sous-groupe isomorphe à $\mathbb{Z}^n$.

Solution de l'exercice 12. Soient $p_1, \ldots, p_n$ des nombres premiers distincts. Considrons le sous-groupe additif de $\mathbb{R}$ engendr par $\log(p_1), \ldots, \log(p_n)$. Si $a_1, \ldots, a_n \in \mathbb{Z}$ sont tels que $a_1 \log(p_1) + \cdots + a_n \log(p_n) = 0$, alors en prenant l'exponentielle on trouve $p_1^{a_1} \ldots p_n^{a_n} = 1$ donc $a_1 = \cdots = a_n = 0$. Donc ce sous-groupe est isomorphe à $\mathbb{Z}^n$.
Autre exemple : le groupe engendré par $2^{(2^{-i})}$, $1 \leq i \leq n$ convient aussi.
Autre exemple : le groupe engendré par les racines carrées des n premiers entiers positifs sans facteurs carrés $1, \sqrt{2}, \ldots, \sqrt{m}$ convient aussi.
Encore un autre exemple : si $\theta \in \mathbb{R}$ est un nombre transcendant (il en existe, par cardinalité), alors le sous-groupe engendré par $1, \theta, \ldots, \theta^{n-1}$ convient également (pour un exemple explicite, on pourra prendre $\theta = \pi$, mais la preuve de la transcendance est difficile, ou plus directement un nombre de Liouville comme $\theta = \sum_{k=0}^{+\infty} 10^{-k!}$).

Exercice 13 :

Soit $n \geq 1$ est un entier. Montrer que tout système libre maximal dans $\mathbb{Z}^n$ est de cardinal n.
Donner un exemple où un tel système n'est pas une base.

Solution de l'exercice 13. On peut voir $G = \mathbb{Z}^n$ comme un sous-groupe de $\mathbb{Q}^n$. Soit $e_1, \ldots, e_r$ un système libre maximal de G.

— Supposons $r > n$. Alors $e_1, \ldots, e_r$ n'est pas libre sur $\mathbb{Q}$ donc il existe $q_1, \ldots, q_r \in \mathbb{Q}$ tels que $q_1 e_1 + \cdots + q_r e_r = 0$. Quitte à multiplier par le PPCM des dénominateurs des $q_1, \ldots, q_r$, on peut supposer que $q_1, \ldots, q_r \in \mathbb{Z}$. Donc $e_1, \ldots, e_r$ n'est pas libre sur $\mathbb{Z}$.

— Supposons $r < n$. On vient de voir que $e_1, \dots, e_r$ est libre sur $\mathbb{Z}$ si et seulement si $e_1, \dots, e_r$ est libre sur $\mathbb{Q}$. Or si $r < n$, alors $e_1, \dots, e_r$ n'est pas une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}^n$, donc il existe $e_{r+1} \in G$ tel que $e_1, \dots, e_r, e_{r+1}$ soit libre sur $\mathbb{Q}$ donc sur $\mathbb{Z}$, et alors $e_1, \dots, e_r$ n'est pas maximal.

Enfin, le système $(2, 0, \dots, 0)$, $(0, 2, \dots, 0)$, …, $(0, \dots, 0, 2)$ est libre de cardinal n, donc maximal, mais ce n'est pas une base de $\mathbb{Z}^n$ puisque $(1, 0, \dots, 0)$ n'est pas dans le sous-groupe engendré (la somme des coordonnées d'un vecteurs du sous-groupe engendré est toujours paire).

Exercice 14 :

Soit $e_1 = (a_1, \dots, a_n) \in \mathbb{Z}^n$ un vecteur tel que le pgcd de ses coordonnées vaut 1. Montrer que l'on peut compléter e_1 en une base $(e_1, \dots, e_n)$ de $\mathbb{Z}^n$.

Solution de l'exercice 14. L'exercice équivaut à trouver une matrice dans $\mathrm{GL}_n(\mathbb{Z})$ dont la première ligne est formée des entiers $a_1, \dots, a_n$. On le montre par récurrence sur n. Soit d le pgcd de $a_1, \dots, a_{n-1}$ et notons $a'_i = a_i/d$ pour tout $1 \leq i \leq n-1$. Alors, par hypothèse de récurrence, il existe une matrice D de taille $(n-1) \times (n-2)$ telle que la matrice

$$\left(\begin{array}{ccc} a'_1 & \dots & a'_{n-1} \\ \hline & & \\ & D & \\ & & \end{array}\right)$$

appartienne à $\mathrm{GL}_{n-1}(\mathbb{Z})$. Par hypothèse, $\mathrm{pgcd}(a_n, d) = 1$ donc il existe $v, w \in \mathbb{Z}$ tels que $a_n v + dw = 1$. Alors la matrice

$$\left(\begin{array}{ccccc} da'_1 & \dots & da'_{n-1} & a_n \\ \hline & & & 0 \\ & & & 0 \\ & D & & 0 \\ & & & \vdots \\ & & & 0 \\ -va'_1 & \dots & -va'_{n-1} & w \end{array}\right)$$

convient.

Exercice 15 : ⋆⋆

Déterminer les facteurs invariants des matrices suivantes à coefficients dans $\mathbb{Z}$:

$$\begin{pmatrix} 2 & 4 \\ 4 & 11 \end{pmatrix}, \begin{pmatrix} 69 & -153 \\ 12 & -27 \end{pmatrix}, \begin{pmatrix} 12 & -6 & 2 \\ 75 & -41 & 13 \\ 19 & -3 & 3 \end{pmatrix}.$$

Solution de l'exercice 15. On peut le faire de deux façons différentes a priori : soit en calculant le PGCD des coefficients de la matrices, puis le PGCD des mineurs de taille 2, etc..., soit en appliquant l'algorithme de réduction des matrices à coefficients entiers via des opérations élémentaires sur les lignes et les colonnes (cette second méthode est sans doute la plus rapide dans le troisième exemple). Dans les deux cas, on trouve les résultats suivants, où $\sim$ désigne l'équivalence des matrices à coefficients entiers :

$$\begin{pmatrix} 2 & 4 \\ 4 & 11 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix},$$

$$\begin{pmatrix} 69 & -153 \\ 12 & -27 \end{pmatrix} \sim \begin{pmatrix} 3 & 0 \\ 0 & 9 \end{pmatrix},$$

$$\begin{pmatrix} 12 & -6 & 2 \\ 75 & -41 & 13 \\ 19 & -3 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 16 \end{pmatrix}.$$

Les facteurs invariants sont donc respectivement $(1, 6)$, $(3, 9)$ et $(1, 2, 16)$.

Exercice 16 :

a) Soit G un groupe abélien de type fini et soit $f : G \to G$ un morphisme surjectif. Montrer que f est un isomorphisme. Ceci est-il nécessairement vrai si l'on remplace surjectif par injectif ?

b) Soit G un groupe abélien libre de type fini et soit $f : G \to G$ un morphisme. Définir le déterminant $\det(f) \in \mathbb{Z}$ de f et montrer que f est injectif si et seulement si $\det(f) \neq 0$. Dans ce cas, montrer que l'on a $|\mathrm{Coker}(f)| = |\det(f)|$.

Solution de l'exercice 16.

a) Notons F le sous-groupe de torsion de G, de sorte que $\overline{G} := G/F$ est un groupe abélien libre de type fini, i.e. isomorphe à $\mathbb{Z}^n$. On voit alors que f induit un morphisme $f_{\mathsf{tors}} : F \to F$ et un morphisme surjectif $\overline{f} : \overline{G} \to \overline{G}$. On choisit une base $(e_1, \dots, e_n)$ de $\overline{G}$. Comme $\overline{f}$ est surjectif, pour tout $1 \leq i \leq n$, il existe $d_i \in \overline{G}$ tel que $f(d_i) = e_i$. On considère alors le morphisme $\overline{g} : \overline{G} \to \overline{G}$ défini par $\overline{g}(e_i) := d_i$ pour tout i. On voit alors que (d_i) est une base de $\overline{G}$. Par construction, on a $\overline{f} \circ \overline{g} = \mathrm{id}_{\overline{G}}$. Alors le calcul matriciel assure que l'on a aussi $\overline{g} \circ \overline{f} = \mathrm{id}_{\overline{G}}$, donc $\overline{f}$ est un isomorphisme. Comme $\overline{f}$ est injectif, on en déduit que $f_{\mathsf{tors}} : F \to F$ est surjectif, et comme F est fini, f_{tors} est un isomorphisme de F. Il est alors facile de conclure que f est un isomorphisme de G.

Variante : pour tout $n \geq 1$, on a une inclusion $\mathrm{Ker}(f^n) \subset \mathrm{Ker}(f^{n+1})$ et un isomorphisme $\mathrm{Ker}(f^{n+1})/\mathrm{Ker}(f^n) \cong \mathrm{Ker}(f)$. On peut montrer que la suite des noyaux $\mathrm{Ker}(f^n)$ est une suite croissante de sous-groupes de G. Or on voit facilement que $G \cong F \times \mathbb{Z}^n$ n'admet pas de suite croissante non stationnaire de sous-groupes, donc la suite des $\mathrm{Ker}(f^n)$ est stationnaire : il existe $n \geq 1$ tel que $\mathrm{Ker}(f^n) = \mathrm{Ker}(f^{n+1})$. On en déduit donc que $\mathrm{Ker}(f) = 0$, ce qui conclut la preuve.

La conclusion n'est plus valable si l'on remplace surjectif par injectif. Par exemple, le morphisme de multiplication par 2 dans $\mathbb{Z}$ est injectif, mais son image est le sous-groupe strict $2\mathbb{Z} \subset \mathbb{Z}$, donc ce n'est pas un isomorphisme.

b) On définit $\det(f)$ comme le déterminant de la matrice de f (à coefficents dans $\mathbb{Z}$) dans une base quelconque de G sur $\mathbb{Z}$. En effet, la formule classique de changement de bases assure que ce déterminant est bien défini (il ne dépend pas de la base choisie). Cela revient à définir $\det(f)$ comme le déterminant de l'endomorphisme $\widetilde{f}$ de $\mathbb{Q}^n$ induit par f via un isomorphisme $G \cong \mathbb{Z}^n$ (correspondant au choix d'une base de G).

Supposons $\det(f) \neq 0$. Alors l'application linéaire correspondante $\widetilde{f} : \mathbb{Q}^n \to \mathbb{Q}^n$ est de déterminant non nul, donc elle est injective, ce qui assure que sa restriction à $\mathbb{Z}^n$ est injective, donc f est injective.

Réciproquement, supposons que $\det(f) = 0$. Alors il existe $x \in \mathbb{Q}^n$ non nul tel que $\widetilde{f}(x) = 0$. Or il existe $m \in \mathbb{Z} \setminus \{0\}$ tel que $mx \in \mathbb{Z}^n$. On a alors $f(mx) = m\widetilde{f}(x) = 0$, et $mx \neq 0$, donc f n'est pas injective sur $\mathbb{Z}^n$.

On suppose désormais que $\det(f) \neq 0$. Le théorème de réduction des matrices à coefficients entiers assure qu'il existe deux bases (x_i) et (y_i) de G et $(d_1, \dots, d_n)$ des entiers positifs tels que $\mathrm{Mat}_{\underline{x};\underline{y}}(f) = \mathrm{diag}(d_1, \dots, d_n)$. En particulier, on a $\det(f) = \pm d_1 \dots d_n$ et l'image de f est engendrée par les vecteurs $(d_1 y_1, \dots, d_n y_n)$. Comme $(y_1, \dots, y_n)$ est une base de G, on voit que $\mathrm{Coker}(f) := G/\mathrm{Im}\,(f) \cong \prod_{i=1}^n \mathbb{Z}/d_i\mathbb{Z}$. Donc en particulier, on a $|\mathrm{Coker}(f)| = |d_1 \dots d_n|$, d'où le résultat.

Exercice 17 : ⋆⋆⋆

Soient $A_1, \dots, A_n$ des groupes abéliens de type fini et $f_i : A_i \to A_{i+1}$ des morphismes de groupes. On dit que la suite

$$0 \to A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} \dots \xrightarrow{f_{n-1}} A_n \to 0$$

est exacte si f_1 est injectif, f_{n-1} est surjectif, et pour tout $1 \leq i \leq n-2$, $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$.
Montrer que si la suite est exacte, alors $\sum_{i=1}^n (-1)^i \mathrm{rang}(A_i) = 0$.

Solution de l'exercice 17. On remarque qu'une telle suite exacte se découpe en des suites exactes courtes de la forme

$$0 \to \mathrm{Im}\,(f_{i-1}) = \mathrm{Ker}(f_i) \to A_i \xrightarrow{f_i} \mathrm{Im}\,(f_i) = \mathrm{Ker}(f_{i+1}) \to 0\,,$$

et qu'il suffit donc de démontrer la formule souhaitée pour un telle suite exacte courte. On suppose donc $n = 3$.
On sait que le rang d'un groupe abélien G de type fini est le cardinal maximal d'une famille libre de G, i.e. le plus grand entier n tel que G admette un sous-groupe (ou un quotient) isomorphe à $\mathbb{Z}^n$.
On note r_i le rang de A_i. Il existe donc un sous-groupe de B_i de A_i isomorphe à $\mathbb{Z}^{n_i}$. Si $(e_1, \dots, e_{n_3})$ est une base de B_3, on peut trouver pour tout $1 \leq j \leq n_3$ un élément $d_j \in A_2$ tel que $f_2(d_j) = e_j$. Alors le sous-groupe de A_2 engendré par $f_1(B_1)$ et par les d_j est isomorpheà $\mathbb{Z}^{r_1+r_3}$: en effet, si $(c_1, \dots, c_{n_1})$ est une base de B_1, pour tous $(\lambda_1, \dots, \lambda_{n_1}, \mu_1, \dots, \mu_{n_3}) \in \mathbb{Z}^{n_1+n_3}$ tels que $\sum_i \lambda_i f_1(c_i) + \sum_j \mu_j d_j = 0$, on a (après application de f_2) $\sum_j \mu_j e_j = 0$ dans A_3, donc tous les μ_j sont nuls, donc $\sum_i \lambda_i f_1(c_i) = 0$, donc par injectivité de f_1, $\sum_i \lambda_i c_i = 0$, donc tous les λ_i sont nuls, donc la famille $(f_1(c_1, \dots, f_1(c_{n_1}), d_1, \dots, d_{n_3})$ est bien libre. On a donc $r_2 \geq r_1 + r_3$. Le théorème de la base adaptée assure que $f_1(A_1) \cap B_2$ est un sous-groupe abélien libre de rang s_1, tel que le quotient soit de rand $r_2 - s_1$ (pas forcément libre). Donc $s_1 \leq r_1$ et $r_2 - s_1 \leq r_3$, donc $r_2 \leq r_1 + r_3$. Donc finalement $r_2 = r_1 + r_3$, ce qui conclut la preuve.

Exercice 18 : ⋆⋆⋆

On se propose de redémontrer le théorème de structure des groupes abéliens finis.
On appelle caractère d'un groupe abélien fini G tout morphisme $G \to \mathbb{C}^*$.

a) Si H est un sous-groupe d'un groupe abélien fini G, montrer que tout caractère de H se prolonge en un caractère de G.

b) Soit G un groupe abélien fini. On note H un sous-groupe de G engendré par un élément de G d'ordre maximal. Montrer que l'on a un isomorphisme $G \cong H \times G/H$.

c) Conclure.

Solution de l'exercice 18.

a) On monter le résultat par récurrence sur $n := [G : H]$. C'est clair si $n = 1$. Supposons donc $n > 1$ et le résultat vrai pour tous les sous-groupes H' de G tels que $[G : H'] < n$. Soit $\chi : H \to \mathbb{C}^*$ un caractère de H. Choisissons $x \in G \setminus H$, et notons $m \geq 2$ l'entier minimal tel que $x^m \in H$. On note enfin $H' := \langle H, x \rangle$. Comme $x^m \in H$, $a := \chi(x^m) \in \mathbb{C}^*$ a bien un sens. On sait que a admet (au moins) une racine m-ième, choisissons-en une que l'on note a_0. On pose alors $\chi' : H' \to \mathbb{C}^*$ défini par $\chi'(hx^k) := \chi(h)a_0^k$. Vérifions que χ' est bien défini et que c'est un caractère de H'. Tout d'abord, supposons que $hx^k = h'x^{k'}$, avec $h, h' \in H$ et $k, k' \in \mathbb{Z}$. Alors $h^{-1}h' = x^{k-k'}$, donc $k - k'$ est multiple de m. Notons par exemple $k - k' = mr$. Alors on a

$$\chi(h')a_0^{k'} = \chi(hx^{mr})a_0^{k'} = \chi(h)\chi(x^{mr})a_0^{k'} = \chi(h)a_0^{k'+mr} = \chi(h)a_0^k\,,$$

ce qui assure que χ' est bien défini. Montrons maitenant que c'est un morphisme de groupes : soient $h, h\text{“} \in H$ et $k, k' \in \mathbb{Z}$. On a alors

$$\chi'(hx^k h'x^{k'}) = \chi'(hh'x^{k+k'}) = \chi(hh')a_0^{k+k'} = \chi(h)\chi(h')a_0^{k+k'} = \chi(h)a_0^k\chi(h')a_0^{k'} = \chi'(hx^k)\chi'(h'x^{k'})\,,$$

donc χ' est un caractère de H'.
Enfin, il est clair par construction que $\chi'_{|H} = \chi$.
L'hypothèse de récurrence assure alors que χ' se prolonge en un caractère de G, car $[G : H'] < [G : H]$, donc χ se prolonge bien en un caractère de G.

b) Notons d l'ordre du sous-groupe cyclique H et $\pi : G \to G/H$ la projection canonique. Il est clair qu'il existe un caractère surjectif (et même un isomorphisme) $\chi : H \to \mu_d(\mathbb{C})$, où $\mu_d(\mathbb{C})$ désigne le sous-groupe de $\mathbb{C}^*$ formé des racines d-ièmes de l'unité. La question a) assure alors que χ se prolonge en un caractère $\chi' : G \to \mathbb{C}^*$. Remarquons que par définition de H, l'exposant de G est égal à d, ce qui assure que χ' est un morphisme à valeurs dans $\mu_d(\mathbb{C})$. En particulier, on dispose d'un morphisme de groupes surjectif

$$\varphi := \chi^{-1} \circ \chi' : G \to H\,.$$

Alors le morphisme

$$\psi : G \to H \times G/H$$

défini par $\psi(g) := (\varphi(g), \pi(g))$. Alors $\mathrm{Ker}(\psi) = \mathrm{Ker}(\varphi) \cap \mathrm{Ker}(\pi) = \mathrm{Ker}(\chi') \cap H$. Or $\chi'_{|H} = \chi$ est injectif, donc $\mathrm{Ker}(\psi) = \{e\}$, donc ψ est injectif, donc par cardinalité, ψ est un isomorphisme.

c) La question b) jointe à une récurrence simple sur $|G|$ assure que tout groupe abélien fini G est isomorphe à un produit de groupes cycliques de la forme

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots, \mathbb{Z}/d_r\mathbb{Z}$$

avec $d_1 \geq 2$ et $d_i | d_{i+1}$ pour tout i.
Il reste à montrer l'unicité d'une telle écriture. Cela peut se faire assez facilement avec une récurrence sur r, ou alors en suivant la preuve du cours.