Groupes abéliens de type fini

Travaux dirigés du 16 et du 19 décembre 2025

Préambule. Prolongement de morphismes entre groupes abéliens

Soient G, H, D des groupes abéliens avec $H \subseteq G$, D divisible, et $f : H \to D$ un morphisme de groupes. On va montrer qu'il existe un morphisme de groupes $\widetilde{f} : G \to D$ qui prolonge f.

1. Montrer le résultat si G est engendré par H et un élément $g \in G$.
   Tout élément de G s'écrit donc sous la forme hg^n pour certains $h \in H$ et $n \in \mathbb{Z}$, par commutativité de G. Cette écriture n'est pas nécessairement unique. En effet, considérons $K = \left\{n \in \mathbb{Z} \mid g^n \in H\right\}$; c'est un sous-groupe de $\mathbb{Z}$, donc de la forme $d\mathbb{Z}$ avec $d \geq 0$. Ainsi, si on a $hg^n = h'g^m$ avec $h, h' \in H$ et $n, m \in \mathbb{Z}$, on a $h^{-1}h' = g^{n-m}$ puis $n \equiv m \bmod d$ et $h' = h\left(g^d\right)^{\frac{n-m}{d}}$ avec $g^d \in H$. Comme g^d est dans H, il y a un sens à considérer $f\left(g^d\right) \in D$, et par divisibilité de G on peut choisir un élément $x \in D$ tel que $x^d = f\left(g^d\right)$ (si $d = 0$ on a $f\left(g^d\right) = f(1) = 1$ et on peut prendre $x = 1$). On a tout fait pour que l'application
   $$\widetilde{f} : G \to D, hg^n \mapsto f(h)x^n$$
   soit bien définie : si on a $hg^n = h'g^m$ avec $h, h' \in H$ et $n, m \in \mathbb{Z}$, on a vu $n \equiv m \bmod d$ et $h' = h\cdot\left(g^d\right)^{\frac{n-m}{d}}$ avec $g^d \in H$, de sorte qu'en appliquant f à cette dernière égalité on trouve $f\left(h'\right) = f(h)\left(x^d\right)^{\frac{n-m}{d}}$ puis $f(h)x^n = f\left(h'\right)x^m$. Enfin, il est clair que $\widetilde{f}$ ainsi définie est un morphisme de groupes tel que $\widetilde{f}_{|H} = f$.
2. Montrer le résultat si G est de type fini.
   Quand G est de type fini, disons $G = \langle b_1\rangle\langle b_2\rangle\cdots\langle b_r\rangle$ (car G est commutatif), on conclut en prolongeant f successivement à chaque sous-groupe $H_i := H\langle b_1\rangle\langle b_2\rangle\cdots\langle b_i\rangle$ pour $i = 1, \ldots, r$.
3. Montrer le cas général avec le lemme de Zorn.
   Pour un G général, on peut encore conclure par le lemme de Zorn. En effet, soit X l'ensemble des couples (H', f') avec H' un sous-groupe de G contenant H et $f' : H' \to D$ un morphisme prolongeant f. On munit X d'une relation d'ordre en posant $\left(H', f'\right) \leq \left(H'', f''\right)$ si on a $H' \subseteq H''$ et $f''_{|H'} = f'$. On constate que $(X, \leq)$ est inductif. Si (H', f') est maximal, alors on a $H' = G$. En effet, sinon il existe $g \in G - H'$ et on peut prolonger f' à $H'\langle b\rangle$ par le premier cas étudié plus haut, ce qui contredit la maximalité de (H', f').
4. Donner un contre-exemple si D n'est plus divisible.
   Si on prend $G = \mathbb{Z}/4\mathbb{Z}$ et $H = D = \mathbb{Z}/2\mathbb{Z}$, alors pour tout morphisme $\varphi : G \to D$ on a $\varphi(\overline{2}) = \varphi(2.\overline{1}) = 2\varphi(\overline{1}) = 0$. Ainsi, l'identité $f : H \to D$, $x \mapsto x$, ne se prolonge pas à G.

Problème. Structure des groupes abéliens de type fini

On se propose de classifier les groupes abéliens de type fini à isomorphisme près. On commence par étudier le cas fini ; soit donc G est un groupe abélien fini. On définit l'*exposant* de G, noté $\exp(G)$, comme le plus petit entier $e \geq 1$ vérifiant $g^e = 1$ pour tout $g \in G$.

1. Montrer que $\exp(G)$ est le PPCM des ordres des éléments de G.
   En effet, pour $e \in \mathbb{Z}$ on a $g^e = 1$ pour tout $g \in G$ si et seulement si $\operatorname{ord} g \mid e$ pour pour $g \in G$.
2. Montrer qu'il existe un élément $x \in G$ d'ordre $\exp(G)$.
   Soit $e = \exp G$, de décomposition en facteurs premiers $e = \prod_i p_i^{\alpha_i}$. Comme e est le PPCM des ordres des éléments de G, pour tout i il existe un élément $g_i \in G$ d'ordre de la forme $p_i^{\alpha_i} m_i$ avec $p_i \nmid m_i$. En particulier, $g_i^{m_i}$ est d'ordre exactement $p_i^{\alpha_i}$. Le produit g des $g_i^{m_i}$ convient.
3. Montrer qu'il existe un morphisme de groupes $\chi : G \to \mathbb{C}^\times$ qui envoie x sur $e^{2i\pi/\exp(G)}$.
   Le groupe cyclique $\langle x\rangle$ est d'ordre $\exp(G)$. On peut donc trouver un morphisme (en fait, un caractère) $\chi_0 : \langle x\rangle \to \mathbb{C}^\times$ envoyant x sur $e^{2i\pi/\exp(G)}$. Par prolongement des morphismes, on peut trouver un morphisme (un caractère) $\chi : G \to \mathbb{C}^\times$ prolongeant χ_0.
4. Montrer que le noyau de χ est un complément de $\langle x\rangle$ dans G.
   On pose $a := \exp(G)$. Soit $g \in G$. On a $g^a = 1$ car a est l'exposant de G, donc $\chi(g)^a = 1$, puis $\chi(g) \in \mu_a$. Il existe donc $k \in \mathbb{Z}$ tel que $\chi(g) = \chi\left(x^k\right)$, puis $gx^{-k} \in \ker\chi$. On a montré $G = \langle x\rangle\ker\chi$. Comme d'autre part on a $\langle x\rangle \cap \ker\chi = \{1\}$ car on a
   $$\chi\left(x^k\right) = 1 \Longleftrightarrow \chi_0\left(x^k\right) = 1 \Longleftrightarrow e^{2ik\pi/a} = 1 \Longleftrightarrow k \equiv 0 \bmod a \Longleftrightarrow x^k = 1,$$
   c'est une situation de produit direct interne et donc $G \simeq \langle x\rangle \times \ker\chi$.

5. En déduire qu'il existe un entier n et des entiers $a_1, \dots, a_n > 1$ tels que

$$a_1 \mid a_2 \mid \cdots \mid a_n \quad \text{et} \quad G \simeq \prod_{i=1}^{n} \mathbb{Z}/a_i\mathbb{Z}$$

(on convient qu'un produit vide de groupes est le groupe trivial).

On conclut par récurrence sur $|G|$ car on a $\langle x \rangle \simeq \mathbb{Z}/a\mathbb{Z}$ et car l'exposant du sous-groupe $\ker \chi$ divise nécessairement a. (L'exposant d'un sous-groupe divise toujours l'exposant du groupe.)

On note $\min(G)$ le nombre minimal de générateurs de G.

6. Si $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$ avec p premier, montrer que $n = \min(G)$.

Une famille engendre G si et seulement si elle engendre le $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $(\mathbb{Z}/p\mathbb{Z})^n$, donc $n = \min(G)$.

7. En déduire que dans le cas général, on a $n = \min(G)$.

Le groupe G est engendré par les n éléments e_i avec $e_i = (0, \dots, 0, \overline{1}, 0, \dots, 0)$ (le $\overline{1}$ à la place i). On a donc $\min(G) \leq n$. D'autre part, pour p premier divisant a_1 on a $p \mid a_i$ pour tout i et on peut donc considérer un morphisme surjectif $f : G \to (\mathbb{Z}/p\mathbb{Z})^n$ en considérant coordonnée par coordonnée le morphisme naturel

$$\mathbb{Z}/a_i\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z},\ n \bmod a_i \mapsto n \bmod p$$

(bien défini car $p \mid a_i$). Cette surjection envoie les familles génératrices de G sur des familles génératrices de $(\mathbb{Z}/p\mathbb{Z})^n$, donc $\min(G) \geq \min\big((\mathbb{Z}/p\mathbb{Z})^n\big) = n$.

On a donc l'unicité de n. Pour montrer l'unicité du n-uplet $(a_1 \dots, a_n)$, on va considérer l'ensemble A_n des suites finies $a = (a_1, \dots, a_n)$ de $\mathbb{N}^*$ avec $a_1 \mid a_2 \mid \cdots \mid a_n$. Pour $a \in A_n$ on pose

$$G_a := \prod_{i=1}^{n} \mathbb{Z}/a_i\mathbb{Z}.$$

On suppose $a, b \in A_n$ et $G_a \simeq G_b$, on veut montrer $a = b$. On raisonne par récurrence sur $\sum_{i=1}^{n}(a_i + b_i)$. Si $a_1 = b_1 = 1$, on conclut par récurrence sur n. Sinon, quitte à échanger a et b, on peut supposer $a_1 > 1$. Soit p premier divisant a_1, et donc tous les a_i. On regarde les sous-groupes de p-torsion.

8. Montrer que $(\mathbb{Z}/m\mathbb{Z})[p] = \{0\}$ sauf si $p \mid m$, auquel cas on a $(\mathbb{Z}/m\mathbb{Z})[p] \simeq \mathbb{Z}/p\mathbb{Z}$ et $(\mathbb{Z}/m\mathbb{Z})/(\mathbb{Z}/m\mathbb{Z})[p] \simeq \mathbb{Z}/(m/p)\mathbb{Z}$.

Pour $k \in \mathbb{Z}$ on a $p\overline{k} = \overline{0}$ dans $\mathbb{Z}/m\mathbb{Z}$ si et seulement si $m \mid kp$. Si $p \nmid m$, cela équivaut à $k \equiv 0 \bmod m$, et donc $(\mathbb{Z}/m\mathbb{Z})[p] = \{0\}$. Si $p \mid m$, cela équivaut à $k \equiv 0 \bmod m/p$. On a donc $(\mathbb{Z}/m\mathbb{Z})[p] \simeq \mathbb{Z}/p\mathbb{Z}$, et le groupe quotient $(\mathbb{Z}/m\mathbb{Z})/(\mathbb{Z}/m\mathbb{Z})[p]$, qui est engendré par l'image de $\overline{1}$ dans $(\mathbb{Z}/m\mathbb{Z})/(\mathbb{Z}/m\mathbb{Z})[p]$, est donc isomorphe à $\mathbb{Z}/(m/p)\mathbb{Z}$.

9. En déduire $\big|G_a[p]\big| = p^n$, et $\big|G_b[p]\big| = p^r$ où r est le nombre d'entiers $1 \leq i \leq n$ tels que $p \mid b_i$.

La p-torsion d'un produit est le produit des p-torsions, ce qui conclut.

10. Montrer $G_a[p] \simeq G_b[p]$ et $G_a/G_a[p] \simeq G_b/G_b[p]$.

Un (iso)morphisme induit un (iso)morphisme entre les p-torsions, ce qui conclut.

11. Conclure.

De l'identité de gauche on déduit $r = n$ puis $p \mid b_i$ pour tout i. Mais on constate que $G_a/G_a[p]$ et $G_b/G_b[p]$ sont respectivement isomorphes à $G_{a'}$ et $G_{b'}$ avec $a'_i = a_i/p$ et $b'_i = b_i/p$ pour tout i. Par récurrence on en déduit $a' = b'$, puis $a = b$.

On a donc l'unicité des a_i, que l'on appelle les *facteurs invariants* de G. On s'intéresse maintenant au cas, plus général, où le groupe abélien G est de type fini, c'est-à-dire que le $\mathbb{Z}$-module correspondant est de type fini.

12. Si $r \geq 0$, montrer qu'on a $\min(\mathbb{Z}^r) = r$. En particulier, le rang d'un $\mathbb{Z}$-module libre est bien défini.

L'inégalité $\min(\mathbb{Z}^n) \leq n$ est claire. En considérant le morphisme $\mathbb{Z}^n \to (\mathbb{Z}/2\mathbb{Z})^n$ de réduction modulo 2 sur chaque coordonnée, qui est surjectif, on a l'inégalité opposée $\min(\mathbb{Z}^n) \geq \min((\mathbb{Z}/2\mathbb{Z})^n) = n$. La seconde assertion s'en déduit car $G \simeq G'$ implique $\min(G) = \min\big(G'\big)$.

On regarde le *sous-groupe de torsion* de G

$$G_{\text{tor}} := \{g \in G \mid \exists m \geq 1, g^m = 1\} = \bigcup_{m \geq 1} G[m].$$

On va montrer que G_{tor} est fini et qu'il existe un unique entier $r \geq 0$ tel que $G \simeq G_{\text{tor}} \times \mathbb{Z}^r$; on pourra donc se ramener à la classification des groupes abéliens finis. En particulier, un groupe abélien de type fini sans torsion est libre.

13. Montrer qu'un groupe abélien qui se surjecte dans $\mathbb{Z}$ par un morphisme f est isomorphe à $\mathbb{Z}\times\ker f$.
Par surjectivité de f, il existe $h\in G$ tel que $f(h)=1$. L'élément h est d'ordre infini, car $h^n=0$ implique $0=nf(h)=n\in\mathbb{Z}$. On a donc $H:=\langle h\rangle\simeq\mathbb{Z}$. Vérifions que G est produit direct interne de H et de $\ker f$. On vient juste de montrer $H\cap\ker f=\{0\}$. Vérifions $G=H\ker f$. Soit $g\in G$. Posons $n:=f(g)\in\mathbb{Z}$, on a alors $f(g)=n=f(h^n)$ et donc $gh^{-n}\in\ker f$.

14. En déduire que si G admet un élément d'ordre infini, il existe un groupe abélien de type fini G' tel que $G\simeq G'\times\mathbb{Z}$.
Supposons qu'il existe $g\in G$ d'ordre infini. Choisissons un isomorphisme $f:\langle g\rangle\xrightarrow{\sim}\mathbb{Z}$. D'après le préambule, on peut étendre f en un morphisme $\widetilde{f}:G\to\mathbb{Q}$, car $\mathbb{Q}$ est divisible. Mais $\widetilde{f}(G)$ est un sous-groupe de type fini de $\mathbb{Q}$, donc de la forme $\mathbb{Z}\lambda$ pour un certain $\lambda\in\mathbb{Q}$. On a $\lambda\neq0$ car $\widetilde{f}(G)$ contient $f(G)=\mathbb{Z}$. Quitte à diviser $\widetilde{f}$ par λ, on a donc trouvé un morphisme surjectif $G\to\mathbb{Z}$. On conclut par la question précédente.

15. En déduire qu'il existe $r\le\min(G)$ et G' groupe abélien fini tels que $G\simeq G'\times\mathbb{Z}^r$.
Posons $N=\min(G)$. Si on a $G\simeq G'\times\mathbb{Z}^n$ alors $N=\min(G')+\min(\mathbb{Z}^n)\le\min(\mathbb{Z}^n)=n$. On en déduit que l'on peut itérer au plus N fois la première étape, i.e. qu'il existe $n\le N$ tel que $G\simeq G'\times\mathbb{Z}^n$ et tel que tous les éléments de G' sont d'ordre fini. Mais alors on a aussi $\min\left(G'\right)\le\min(G)<\infty$, donc G' est de type fini, et comme ses éléments sont d'ordre fini il est alors nécessairement fini (on utilise ici que G' est abélien !).

16. Montrer que si A et B sont des groupes abéliens avec A fini et B libre de rang fini, on a
$$(A\times B)_{\mathrm{tor}}=A\times\{0\}\quad\text{et}\quad(A\times B)/(A\times B)_{\mathrm{tor}}\simeq B.$$
On a $G_{\mathrm{tor}}=A_{\mathrm{tor}}\times B_{\mathrm{tor}}$ avec $A_{\mathrm{tor}}=A$ et $B_{\mathrm{tor}}=\{0\}$, donc $G_{\mathrm{tors}}=A\times\{0\}$. On conclut car le morphisme de projection $G\to B,(a,b)\mapsto b$, est surjectif de noyau G_{tors}.

17. En déduire qu'on a $G'\simeq G_{\mathrm{tor}}$ et $r=\min(G/G_{\mathrm{tor}})$, d'où l'unicité de r que l'on appelle le *rang* de G.
Puisque $G\simeq G'\times\mathbb{Z}^r$ on a $G_{\mathrm{tor}}\simeq(G'\times\mathbb{Z}^r)_{\mathrm{tor}}=G'\times\{0\}\simeq G'$, et aussi $G/G_{\mathrm{tor}}\simeq(G'\times\mathbb{Z}^r)/(G'\times\mathbb{Z}^r)_{\mathrm{tor}}\simeq\mathbb{Z}^r$, ce qui conclut.

Pour finir, on présente quelques applications de la classification des groupes abéliens finis.

18. Déterminer, à isomorphisme près, les groupes abéliens d'ordre 2025, en précisant leurs facteurs invariants.
Observons d'abord que pour une suite d'entiers $a_1,a_2,\dots,a_n$ on a
$$a_1\,|\,a_2|\cdots|\,a_n\Leftrightarrow \mathrm{v}_p(a_1)\le\mathrm{v}_p(a_2)\le\cdots\le\mathrm{v}_p(a_n)\ \text{pour tout } p \text{ premier},$$
où v_p désigne la valuation p-adique. Revenons au problème. On a $2025=3^45^2$. Les facteurs invariants possibles d'un groupe abélien d'ordre 5^2 sont $(5,5)$ et $\left(5^2\right)$. Les facteurs invariants possibles d'un groupe abélien d'ordre 3^4 sont $(3,3,3,3)$, $\left(3,3,3^2\right)$, $\left(3,3^3\right)$, $\left(3^2,3^2\right)$ et $\left(3^4\right)$. Les facteurs invariants possibles d'un groupe abélien d'ordre 2025 sont donc
$$\left(3,3,3\cdot5,3\cdot5\right),\left(3,3\cdot5,3^2\cdot5\right),\left(3\cdot5,3^3\cdot5\right),\left(3^2\cdot5,3^2\cdot5\right),\left(5,3^4\cdot5\right),$$
$$\left(3,3,3,3\cdot5^2\right),\left(3,3,3^2\cdot5^2\right),\left(3,3^3\cdot5^2\right),\left(3^2,3^2\cdot5^2\right)\text{ et }\left(3^4\cdot5^2\right).$$
Autrement dit, ce sont exactement
$$(3,3,15,15),(3,15,15),(3,15,45),(15,135),(45,45),(5,405),(3,3,3,75),(3,3,225),(3,675),(2025).$$
En particulier, il y a exactement 10 groupes abéliens non isomorphes d'ordre 2025.

19. Déterminer tous les sous-groupes de $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$.
Soit $G=\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. Observons que les éléments d'ordre 4 de G sont $(0,\pm1)$ et $(1,\pm1)$. Les deux premiers (inverses l'un de l'autre) engendrent le même sous-groupe $H_1=\{0\}\times\mathbb{Z}/4\mathbb{Z}$, et les deux second engendrent de même un même sous-groupe $\simeq\mathbb{Z}/4\mathbb{Z}$, à savoir $H_2=\{(n \bmod 2, n \bmod 4)\mid n\in\mathbb{Z}\}\subseteq G$. Soit H un sous-groupe de G, que l'on peut supposer $\neq G$, donc d'ordre divisant 4. Si H contient un élément d'ordre 4, alors H contient le groupe cyclique engendré par cet élément, et coïncide donc avec H_1 ou H_2 pour des raisons de cardinalité. Sinon, tout élément h de H vérifie $2h=0$, et donc H est inclus dans le sous-groupe $H_3=\{(x,y)\mid x\in\mathbb{Z}/2\mathbb{Z},y\in2\mathbb{Z}/4\mathbb{Z}\}\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Mais H_2 est un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel de dimension 2, et ses sous-groupes sont ses sous-espaces. Il a donc H_2 lui-même, ses trois droites, engendrées respectivement par $(1,0)$, $(0,2)$ et $(1,2)$, et le groupe trivial $\{0\}$. Le groupe G a donc exactement $1+3+4=8$ sous-groupes.

20. Déterminer, à isomorphisme près, les groupes abéliens G qui ont un sous-groupe H avec $H\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\simeq G/H$.
Un tel groupe G est d'ordre 16. Comme on le suppose abélien, il est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^4$, $(\mathbb{Z}/2\mathbb{Z})^2\times\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/16\mathbb{Z}$. Mais G n'a pas d'élément d'ordre 8 . En effet, pour tout $g\in G$ on a $g^2=1$ dans G/H, donc $g^2\in H$, puis $\left(g^2\right)^2=g^4=1$ car $h^2=1$ pour tout $h\in H$. Cela élimine $G\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ et $G\simeq\mathbb{Z}/16\mathbb{Z}$. Les autres cas sont possibles : pour $G=(\mathbb{Z}/2\mathbb{Z})^4$ on peut prendre $H=\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\{0\}\times\{0\}$, pour $G=(\mathbb{Z}/2\mathbb{Z})^2\times\mathbb{Z}/4\mathbb{Z}$ on peut prendre $H=\mathbb{Z}/2\mathbb{Z}\times\{0\}\times2\mathbb{Z}/4\mathbb{Z}$, et pour $G=\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ on peut prendre $H=2\mathbb{Z}/4\mathbb{Z}\times2\mathbb{Z}/4\mathbb{Z}$.

21. Soit G un groupe abélien fini. Montrer que pour tout diviseur d de $|G|$ il existe un sous-groupe de G d'ordre d.
    Soient $a_1, \ldots, a_n$ les facteurs invariants de G. Soit d un diviseur de G. En utilisant la première observation de la solution de la question 18, il n'est pas difficile de voir que l'on peut trouver, pour tout $i = 1, \ldots, n$, un diviseur d_i de a_i, tels que $d = d_1 d_2 \cdots d_n$. On a $G \simeq \prod_i C_i$ avec C_i cyclique d'ordre a_i. On sait que C_i a un sous-groupe (cyclique) D_i d'ordre d_i. On en déduit que le sous-groupe $\prod_i D_i$ convient.