# Groupe abélien de type fini - correction des exercices

Marc Abboud

24 janvier 2021

**Exercice 1.** Montrer que $\mathbf{Q}$ et $\mathbf{Q}/\mathbf{Z}$ ne sont pas de type fini.

**Correction.** Si $Q$ était de type fini, on aurait un nombre fini de générateurs $e_1 = \frac{p_1}{q_1} \cdots e_r \frac{p_r}{q_r}$ avec $p_i \wedge q_i = 1$. On aurait donc $\mathbf{Q} \subset \mathbf{Z}e_1 + \cdots + \mathbf{Z}e_r$. Soit $q$ un nombre premier qui ne divise aucun des $q_i$, tout rationnel serait de la forme

$$x = \sum_i \lambda_i e_i = \frac{N}{q_1 \cdots q_r}$$

avec $\lambda_i$ et $N$ des entiers. On voit que $q$ ne divise pas le dénominateur de $x$ pour tout $x \in \mathbf{Q}$. Mais alors $1/q \notin \mathbf{Q}$ et c'est absurde.

La même preuve fonctionne aussi pour $\mathbf{Q}/\mathbf{Z}$, on peut aussi dire que $\mathbf{Q}/\mathbf{Z}$ est de torsion et infini donc il ne peut pas être de type fini.

**Exercice 2.** Montrer que tout sous-groupe de $\mathbf{Z}^r$ est de type fini. En déduire que pour tout groupe abélien de type fini, tout sous-groupe est de type fini.

**Correction.** On procède par récurrence sur $r$. On sait que si $r = 1$ c'est vrai car tous les sous-groupes de $\mathbf{Z}$ sont de la forme $d\mathbf{Z}$ avec $d$ entier. Supposons le résultat vrai pour un entier $r \geq 1$. Soit $H$ un sous-groupe de $\mathbf{Z}^{r+1}$, montrons que $H$ est de type fini. Soit $\pi : \mathbf{Z}^{r+1} \to \mathbf{Z}^r$ le morphisme de groupes d'oubli de la dernière coordonnée. Ce morphisme est surjectif et son noyau est $(0, \cdots, 0, 1)\mathbf{Z}$ qui est isomorphe à $\mathbf{Z}$. Par récurrence, il existe $h_1, \cdots, h_s \in H$ tels que $\pi(H)$ est engendré par $\pi(h_1), \cdots, \pi(h_s)$. Maintenant, $H \cap \ker \pi$ est un sous-groupe de $\mathbf{Z}$ donc est engendré par un élément $h_0$. On montre que $h_0, \cdots, h_s$ est une partie génératrice de $H$. En effet, soit $h \in H$, il existe $\lambda_1, \cdots, \lambda_s \in \mathbf{Z}$ tels que $\pi(h) = \sum \lambda_i \pi(h_i)$. Donc, $h - \sum_i \lambda_i h_i \in \mathbf{H} \cap \ker \pi$ et est donc de la forme $\lambda_0 h_0$.

**Exercice 3.** Donner les générateurs de $\mathbf{Z}/n\mathbf{Z}$ et montrer qu'ils forment un groupe isomorphe à $(\mathbf{Z}/n\mathbf{Z})^\times$.

**Correction.** On sait qu'un entier $a$ est un générateur de $\mathbf{Z}/n\mathbf{Z}$, s'il existe $u \in \mathbf{Z}$ tel que $au \equiv 1 \mod n$. Donc les générateurs de $\mathbf{Z}/n\mathbf{Z}$ sont les nombres premiers avec $n$ et ceux sont bien ce qui sont inversibles pour la multiplication.

**Exercice 4.** Soit $G$ un groupe et $H, K$ des sous groupes tels que

1. $H$ et $K$ sont distingués dans $G$.
2. $G = HK$.
3. $H \cap K = \{e\}$.

Montrer que $G$ est isomorphe à $H \times K$. Montrer que le résultat est aussi vrai si on suppose $G$ fini et qu'on remplace l'hypothèse 3 par $|G| = |H|\,|K|$.

**Correction.** L'hypothèse (1) et (3) donnent que les éléments de $H$ et $K$ commutent entre eux. En effet si $h \in H, k \in K$, le commutateur de $h$ et $k$, $[h, k] := hkh^{-1}k^{-1}$ appartient à $H \cap K$ car les deux sous-groupes sont distingués.

On pose alors le morphisme de groupes

$$\varphi : (h, k) \in H \times K \mapsto hk \in G.$$

C'est un morphisme de groupe justement parce que les éléments de $H$ et $K$ commutent entre eux. Il est surjectif par l'hypothèse (2) et il est injectif car si $hk = e$, alors $h = k^{-1}$ et on a $h \in H \cap K$, donc $h = k = e$. Ainsi, $\varphi$ est un isomorphisme.

Si on remplace l'hypothèse (2) par l'égalité sur les cardinaux, on a toujours que $\varphi$ est injectif avec (3) et $\varphi$ est un isomorphisme par égalité des cardinaux.

**Exercice 5.** Soit $\mathbf{k}$ un corps fini, on cherche à montrer que le groupe abélien $\mathbf{k}^\times$ est cyclique. Si on utilise le théorème de structure des groupes abéliens, le résultat est assez rapide à démontrer. Voici une preuve qui ne l'utilise pas. On note $N$ le cardinal de $\mathbf{k}^\times$.

1. Soit $d$ un entier divisant $N$ et $x$ un élément d'ordre $d$. Montrer que le sous groupe engendré par $x$ est de cardinal $d$.
2. Quel est le nombre maximal de solutions de l'équation $t^d - 1 = 0$ dans $\mathbf{k}^\times$ ?
3. En déduire que si $y$ est un autre élément d'ordre $d$, alors $y \in < x >$.
4. Soit $N(d)$ le nombre d'élément d'ordre $d$ dans $\mathbf{k}^\times$, montrer que l'on a $N(d) = 0$ ou bien $N(d) = \varphi(d)$ avec $\varphi$ l'indicatrice d'Euler.
5. Montrer que $N = \sum_{d/N} N(d)$ et conclure.
6. En déduire que $(\mathbf{Z}/p\mathbf{Z})^\times$ est isomorphe à $\mathbf{Z}/(p-1)\mathbf{Z}$.

**Correction.**

1. Le sous-groupe engendré par $x$ est isomorphe à $\mathbf{Z}/d\mathbf{Z}$, il est de cardinal $d$.
2. Le polynôme $t^d - 1$ est de degré $d$ et il est défini sur un corps. Il n'a donc au plus que $d$ racines.
3. Le sous-groupe engendré par $x$ est de taille $d$ et toutes les puissances de $x$ sont racines de $t^d - 1$, on a donc trouvé toutes les racines du polynôme. Si $y^d = 1$, alors $y$ est racine de $t^d - 1$ donc appartient au sous-groupe engendré par $x$.
4. Supposons que $N(d) \neq 0$ et soit $x$ d'ordre $d$. Tous les éléments $y$ d'ordre $d$ dans $\mathbf{k}^\times$ sont dans le sous-groupe engendré par $x$ qui est isomorphe à $\mathbf{Z}/d\mathbf{Z}$. Les éléments d'ordre $d$ dans $\mathbf{Z}/d\mathbf{Z}$ sont exactement les générateurs de $\mathbf{Z}/d\mathbf{Z}$ et il y en a $\varphi(d)$.
5. On sait que $N = \sum_{d|N} \varphi(d)$ (exercice d'arithmétique classique). Maintenant, tout élément de $\mathbf{k}^\times$ a un ordre $d$ divisant $N$ donc par dénombrement, $N = \sum_{d|N} N(d)$. On a donc
$$N = \sum_{d|N} N(d) \geq \sum_{d|N} \varphi(d) = N$$
Il n'y a donc que des égalités et $N(N) = \varphi(N) \neq 0$ donc $\mathbf{k}^\times$ a un élément d'ordre $N$ et est donc cyclique.
6. Comme $\mathbf{Z}/p\mathbf{Z}$ est un corps, $(\mathbf{Z}/p\mathbf{Z})^\times$ est un groupe cyclique de cardinal $p-1$.

**Exercice 6.**

1. Montrer que tout sous-groupe d'un groupe cyclique est cyclique.
2. Soit $n$ un entier naturel et $d$ divisant $n$. Montrer que $\mathbf{Z}/n\mathbf{Z}$ possède un unique sous-groupe de taille $d$.

**Correction.**

1. Un groupe $G$ est cyclique si et seulement s'il existe un morphisme de groupe surjectif $\mathbf{Z} \twoheadrightarrow G$. Soit $G$ un groupe cyclique et $H$ un sous-groupe de $G$. On note $\varphi : \mathbf{Z} \twoheadrightarrow G$ un morphisme de groupes surjectif, l'image réciproque $\varphi^{-1}(H)$ est un sous-groupe de $\mathbf{Z}$ donc de la forme $d\mathbf{Z}$ qui est isomorphe à $\mathbf{Z}$. On a donc un morphisme surjectif $\mathbf{Z} \to d\mathbf{Z} \to H$ et $H$ est cyclique.
2. Soit $H \subset \mathbf{Z}/n\mathbf{Z}$ un sous-groupe de taille $d$. On sait que $H$ est cyclique par la question précédente. On va montrer que $H$ est en fait engendré par l'entier $\frac{n}{d}$. Soit $a$ un élément de $H$, il est d'ordre $d$ aussi. Donc $da$ est divisible par $n$, et $\frac{n}{d}$ divise $a$, ainsi $H \subset < \frac{n}{d} >$ et on obtient le résultat par égalité des cardinaux.

**Exercice 7.** Montrer que $\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) \simeq (\mathbf{Z}/n\mathbf{Z})^\times$.

**Correction.** Pour commencer, tout élément $a \in (\mathbf{Z}/n\mathbf{Z})^\times$ définit un automorphisme par $\varphi_a : x \in \mathbf{Z}/n\mathbf{Z} \mapsto ax \in \mathbf{Z}/n\mathbf{Z}$. Ce qui donne une flèche $\Psi : (\mathbf{Z}/n\mathbf{Z})^\times \to \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})$.

Réciproquement, soit $\varphi \in \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})$, et $a := \varphi(1)$. Comme 1 est un générateur, $a$ en est un aussi donc $a \in (\mathbf{Z}/n\mathbf{Z})^\times$. Comme $\varphi$ est un morphisme de groupe, on a $\varphi = \varphi_a$. Le morphisme inverse de $\Psi$ est donné par $\Psi(\varphi) = \varphi(1)$.

**Exercice 8.** Le but de cet exercice est de décrire les groupes $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ pour $p$ premier et $\alpha$ un entier.

1. On suppose d'abord que $p$ est impair. On sait que $(\mathbf{Z}/p\mathbf{Z})^\times$ est cylique par l'exercice 5. Soit $\alpha \geq 2$, montrer par récurrence que pour tout $k \geq 1$ il existe $\lambda_k$ premier à $p$ tel que $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$. En déduire que $1+p$ est d'ordre $p^{\alpha-1}$ dans $(\mathbf{Z}/p^{\alpha-1}\mathbf{Z})^\times$.
2. En considérant la projection $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times \twoheadrightarrow (\mathbf{Z}/p\mathbf{Z})^\times$ montrer qu'il existe un élément $v$ d'ordre $p-1$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$.
3. En déduire que $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times \simeq \mathbf{Z}/p^{\alpha-1}(p-1)\mathbf{Z}$.
4. On suppose maintenant $p = 2$, traiter le cas $\alpha = 1, 2$.
5. Soit $\alpha \geq 3$, montrer que 5 est d'ordre $2^{\alpha-2}$, en déduire que le noyau de la projection $\pi : (\mathbf{Z}/2^\alpha\mathbf{Z})^\times \twoheadrightarrow (\mathbf{Z}/4\mathbf{Z})^\times$ est le sous-groupe engendré par 5.
6. Montrer que $\pi(-1) = -1$ et que $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times$ est isomorphe au produit $< 5 > \times < -1 >$. En déduire que $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{\alpha-2}\mathbf{Z}$.

**Correction.**

1. Pour $k = 1$, on a $(1+p)^p = 1 + p^2 + \binom{2}{p}p^2 + Up^3$ avec $U$ un entier. Comme $\binom{2}{p} = \frac{p(p-1)}{2}$ et que $\frac{p-1}{2}$ est un entier ($p$ est impair c'est important), on a
$$(1+p)^p = 1 + p^2\left(1 + p(\frac{p-1}{2} + U)\right)$$
donc le résultat est vrai pour $k = 1$.
Supposons le résultat vrai pour un entier $k \geq 1$, on a par récurrence
$$(1+p)^{p^{k+1}} = (1 + \lambda_k p^{k+1})^p = 1 + p^{k+2}\lambda_k + \binom{2}{p}\lambda_k^2 p^{2k} + Vp^{3k}$$
avec $V$ un entier. De la même manière, $\binom{2}{p}$ est un entier divisible par $p$, donc on en déduit la forme souhaitée.
Maintenant, on voit que $u = 1+p$ vérifie $u^{p^{\alpha-1}} = 1 \mod p^\alpha$ et que $u^{p^k} - 1$ n'est pas divisible par $p^\alpha$ pour $k < \alpha - 1$.
2. On note $\pi$ la projection. On sait par l'exercice précédent que $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique de taille $p-1$. Soit $y \in (\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ tel que $\pi(y)$ soit un générateur. L'ordre de $y$ est de la forme $p^s m$ avec $m$ divisant $p-1$. On a nécessairement $m = p-1$ car $\pi(y)^{p^s} = \pi(y)$. Donc $v := y^{p^s}$ est d'ordre $p-1$.
3. On en déduit l'isomorphisme en utilisant l'exercice 4 avec $H$ le sous-groupe engendré par $1+p$ et $K$ le sous groupe engendré par $v$.
4. Pour $\alpha = 1$ le groupe est trivial, pour $\alpha = 2$, on trouve $\mathbf{Z}/2\mathbf{Z}$.
5. La preuve est similaire à celle de la question 1. Vu que $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times$ est de cardinal $2^{\alpha-1}$ on sait que le noyau de $\pi$ est de cardinal $2^{\alpha-2}$, comme 5 est dans le noyau et que le sous-groupe qu'il engendre est de cardinal $2^{\alpha-2}$ on a égalité.
6. On utilise encore l'exercice 4 avec le sous-groupe engendré par 5 et $-1$. On voit que le groupe n'est pas cyclique dès que $\alpha \geq 3$.

**Exercice 9.** Trouver les entiers $n$ tels que $(\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique.

**Correction.** On écrit la décomposition de $n$ en facteurs premiers $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. On a par le théorème chinois

$$H := (\mathbf{Z}/n\mathbf{Z})^\times \simeq (\mathbf{Z}/p_1^{\alpha_1}\mathbf{Z})^\times \times \dots \times (\mathbf{Z}/p_r^{\alpha_r}\mathbf{Z})^\times$$

Si $n$ est une puissance de 2, alors on voit que $n = 2, 4$ par la fin de l'exercie précédent. On suppose maintenant que $n$ a au moins un diviseur premier impair.

Si $n$ possède 2 diviseurs premiers impairs distincts $q$ et $p$, alors par l'exercice précédent et le théorème chinois, $H$ possède un sous-groupe isomorphe à $\mathbf{Z}/(p-1)\mathbf{Z} \times \mathbf{Z}/(q-1)\mathbf{Z}$ qui n'est pas cyclique car $p-1$ et $q-1$ sont tous les deux pairs. $H$ ne peut donc pas être cyclique dans ce cas.

Donc $n$ est de la forme $n = 2^\alpha p^\beta$ avec $p$ premier impair. Si $\alpha \geq 2$, alors $H$ possède un sous-groupe isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/(p-1)\mathbf{Z}$ qui n'est pas cyclique car $p-1$ est pair, donc $H$ ne peut pas être cyclique.

Finalement les seuls solutions sont

$$n = 2, 4, p^\alpha, 2p^\alpha$$

**Exercice 10.** Soit $G$ un groupe et $x, y \in G$ d'ordre $m$ et $n$ respectivement. Si $m$ et $n$ sont premiers entre eux et que $x$ et $y$ commutent, alors $xy$ est d'ordre $mn$.

**Correction.** On a $(xy)^{mn} = e$ l'élément neutre, donc l'ordre de $xy$ divise $mn$. Soit $d$ l'ordre de $xy$, on a $x^d = y^{-d}$. Donc $x^d$ appartient au sous-groupe engendré par $y$ et son ordre doit diviser $m$. Mais l'ordre de $x^d$ doit aussi diviser $n$, comme $m$ et $n$ sont premiers entre eux, on a que cet ordre vaut 1 et $x^d = y^{-d} = 1$. Ainsi, $n$ et $m$ divise $d$ et on a $d = mn$ par le lemme de gauss.

**Proposition 0.1.** *Soit $G$ un groupe fini abélien et $N$ le maximum des ordres des éléments de $G$. Alors, tous les éléments de $g$ ont un ordre divisant $N$ et l'exposant de $G$ est égal à $N$.*

**Exercice 11.** Retrouver le fait que pour $\mathbf{k}$ un corps fini, le groupe $\mathbf{k}^\times$ est cyclique.

**Correction.** Soit $G = \mathbf{k}^\times$, $G$ est un groupe abélien fini, soit $e$ son exposant. On a $|G| = |\mathbf{k}| - 1$, par la proposition précédente $G$ possède un élément d'ordre $e$ donc $e$ divise $|\mathbf{k}| - 1$ et $e \leq |\mathbf{k}| - 1$. Par la proposition, tout élément de $G$ a un ordre divisant $e$, donc est racine du polynôme $X^e - 1$ sur le corps $\mathbf{k}$, qui a au plus $e$ racines dans $\mathbf{k}$, comme tous les éléments de $\mathbf{k}^\times$ sont racines, on a $e \geq |k| - 1$ ce qui donne l'égalité. $G$ possède un élément d'ordre $|k| - 1$ et $G$ est cyclique.

**Exercice 12.** Montrer qu'un produit de groupe $G_1 \times \dots \times G_s$ est cyclique si et seulement si chaque $G_i$ est cyclique et les cardinaux des $G_i$ sont deux à deux premiers entre eux.

**Correction.** Le sens indirect est juste une application du lemme chinois.

Pour le sens direct, le fait que chaque $G_i$ est cyclique est automatique car si on a un morphisme de groupe $G \twoheadrightarrow H$ avec $G$ cyclique, alors $H$ est aussi cyclique. On a $|G| = |G|_1 \times \dots \times |G|_s$ et l'exposant de $G$ est le ppcm des $|G|_i$. Pour que $G$ soit cyclique, il faut et il suffit par la proposition que l'exposant de $G$ soit égal à son cardinal, donc les $|G|_i$ doivent être premiers entre eux. soit égal à son cardinal

**Exercice 13.** Soit $G$ un groupe et $Z$ son centre. On suppose que le quotient $G/Z$ est cyclique. Montrer que $G$ est abélien. En utilisant ce résultat, classifier tous les groupes de cardinal $p^2$ pour $p$ premier.

**Correction.** Soit $g \in G$ un élément qui engendre le quotient $G/Z$, alors tout élément de $G$ s'écrit $g^k z$ avec $k \in \mathbf{Z}$ et $z \in Z$. Il est clair alors que $G$ est abélien.

Si $G$ est un groupe d'ordre $p^2$, montrons qu'il est abélien. S'il ne l'est pas, alors il possède un centre non trivial de taille $p$, mais alors le quotient de $G$ par son centre est un groupe de taille $p$ qui est nécessairement isomorphe à $\mathbf{Z}/p\mathbf{Z}$. Par l'exercice, $G$ est alors abélien c'est absurde.

Donc $G$ est isomorphe à $\mathbf{Z}/p^2\mathbf{Z}$ ou $\mathbf{Z} \times p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$.

**Exercice 14.** Donner le plus petit entier $n$ tel qu'il existe un groupe de taille $n$ non commutatif.

**Correction.** On voit que le groupe des permutations d'un ensemble à trois éléments $\mathfrak{S}_3$ est non commutatif et de cardinal 6. Montrons que 6 est la solution. Soit $G$ un groupe de taille 2,3,4 ou 5, alors $G$ est de cardinal $p$ ou $p^2$ avec $p$ premier donc il est abélien par l'exercice précédent.

**Exercice 15.** Soit $G$ un groupe abélien fini non cyclique. Montrer qu'il existe un nombre premier $p$ tel que $G$ possède un sous-groupe $H$ isomorphe à $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$.

**Correction.** On utilise le théorème de structure des groupes abéliens finis. Comme $G$ n'est pas cyclique, $G$ a au moins deux facteurs invariants $d_1$, $d_2$ avec $d_1|d_2$ et $d_1 > 1$. Soit $p$ un nombre premier qui divise $d_1$ (et $d_2$), $G$ possède un sous-groupe isomorphe à $\mathbf{Z}/d_1\mathbf{Z} \times \mathbf{Z}/d_2\mathbf{Z}$. Par le lemme de Cauchy, $\mathbf{Z}/d_1\mathbf{Z}$ et $\mathbf{Z}/d_2\mathbf{Z}$ possède un élément d'ordre $p$ que l'on note respectivement $x_1$ et $x_2$, alors le groupe engendré par $(x_1, x_2)$ est isomorphe à $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$.

**Exercice 16.** Donner tous les groupes abéliens de cardinal 360 à isomorphisme près. Plus généralement, combien y'a t'il de groupes abéliens de taille $n$ à isomorphisme près ?

**Correction.** On factorise $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec les $p_i$ des nombres premiers deux à deux distincts. Soit $G$ un groupe de taille $n$, $G$ est produit de ses sous-groupes de $p_i$-torsions. Il suffit donc de classifier les groupes abéliens de taille $p^\alpha$ pour $p$ premier.

Soit $H$ un groupe abélien de taille $p^\alpha$, on applique le théorème de structure des groupes abéliens finis à $H$, alors $H$ est isomorphe à

$$H \simeq \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_r\mathbf{Z}$$

avec $d_1|\cdots|d_r$. Comme $H$ est de cardinal $p^\alpha$, on a $d_i = p^{\beta_i}$ avec $\beta_i \leq \alpha$.

On obtient alors un $r$-uplet d'entiers $(\beta_1, \cdots, \beta_r)$ avec $\beta_i \leq \beta_{i+1}$ tel que $\sum \beta_i = \alpha$. Un tel uplet s'appelle une *partition* de l'entier $\alpha$. On note $p(\alpha)$ le nombre de partition de $\alpha$. Deux partitions distinctes donnent deux groupes de taille $p^\alpha$ non isomorphe, il y a donc $p(\alpha)$ groupe abélien de taille $p^\alpha$ à isomorphisme près.