# Correction du TD n°1 : Groupes et groupes cycliques

## Exercice 1. Vrai/Faux, première édition

Pour chaque affirmation qui suit, démontrer sa véracité ou trouver un contre-exemple :

1. Le groupe $\mathbb{Z}$ est produit de deux groupes non triviaux.
2. Soit $G$ un groupe. Si $G$ a un nombre fini de sous-groupes, alors $G$ est fini.

### Correstion de l'exercice 1

1. **Faux.**
   L'intersection de deux sous-groupes non triviaux de $\mathbb{Z}$ est non trivial. Supposons que
   $$\mathbb{Z} \xrightarrow[\iota]{\sim} G \times H.$$
   Les sous-groupes $\iota^{-1}(G \times \{e\})$ et $\iota^{-1}(\{e\} \times H)$ sont d'intersection triviale. Il en découle que l'un des deux est trivial, i.e. que $G$ ou $H$ est trivial.
2. **Vrai.**
   Soit $G$ un groupe avec un nombre fini de sous-groupes. Un élément d'ordre infini de $G$ correspond à un sous-groupe isomorphe à $\mathbb{Z}$. Le groupe $G$ admettrait alors une infinité de sous-groupes, correspondant aux $n\mathbb{Z}$ pour $n \geq 1$. Nous avons démontré que tout élément de $G$ est d'ordre fini. Les sous-groupes $\langle g \rangle$ pour $g \in G$ sont donc finis, en nombre fini [1]. Puisque ces sous-groupes recouvrent $G$, le groupe $G$ est fini.

## Exercice 5. Groupes finis monogènes

On rappelle (ou alors reprouvez-le !) que les sous-groupes de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$ pour $n \in \mathbb{N}$. Rappelons également que pour un élément $g$ d'un groupe $G$, l'application
$$\mathbb{Z} \to G, \quad n \mapsto g^n$$
est un morphisme de groupes. S'il n'est pas injectif, on appelle ordre de $g$ et on écrit $\omega(g)$ l'entier naturel tel que le noyau s'écrive $\omega(g)\mathbb{Z}$.

1. Vérifier que
   $$\omega(g) = \min\{n \in \mathbb{N}_{\geq 1} \mid g^n = 1\} = \gcd\{n \in \mathbb{N}_{\geq 1} \mid g^n = 1\}.$$
2. Déduire que $g^n = 1 \Leftrightarrow \omega(g) | n$.

Soit $n \geq 2$ et $\zeta_n \in \mathbb{C}$ une racine primitive $n$-ième de l'unité (i.e. un élément de $(\mathbb{C}^\times, \times)$ d'ordre $n$). On appelle $\mu_n$ le sous-groupe des racines $n$-ièmes de l'unité.

3. Vérifier que
   $$\mathbb{Z}/n\mathbb{Z} \to \mu_n, \quad a + n\mathbb{Z} \mapsto \zeta_n^a$$
   est un isomorphisme de groupes.

Par la suite, nous cherchons à retrouver les premiers résultats d'arithmétique en choisissant la meilleure vision entre $\mathbb{Z}/n\mathbb{Z}$ et $\mu_n$. Il sera souvent pratique de se donner une intuition avec $\mu_n$ est parfois nécessaire de raisonner sur $\mathbb{Z}/n\mathbb{Z}$.

1. Mais à ce stade, rien ne garantit qu'il n'y ai pas des redondances infinies.

4. Soit $d|n$, a-t-il des éléments d'ordre $d$ dans $\mu_n$ ?
5. Soit $k \in \mathbb{Z}$. Quel est l'ordre de $k + n\mathbb{Z}$ dans $n\mathbb{Z}$ ?
6. Prouver le théorème des restes chinois avec votre point de vue préféré, puis avec l'autre point de vue.
7. Démontrer que tout sous-groupe d'un groupe cyclique est cyclique.

**Correction de l'exercice 5**

1. Demandez-vous quels sont l'élément strictement positif le plus petit de $\omega(g)\mathbb{Z}$ et le PGCD de ses éléments.
2. En utilisant la première question

$$\begin{aligned} g^n = 1 &\Leftrightarrow n \text{ appartient au noyau} \\ &\Leftrightarrow n \in \omega(g)\mathbb{Z} \\ &\Leftrightarrow \omega(g)|n \end{aligned}$$

3. L'application est bien définie car $\zeta_n^n = 1$ donc $\zeta_n^{a+nk} = \zeta_n^a$. On vérifie que c'est un morphisme de groupes. On vérifie qu'elle est injective en regardant son noyau et $\zeta_n^a = 1$ ssi $a \in n\mathbb{Z}$ par définition de l'ordre. Puisque la source et le but ont même cardinal, c'est un isomorphisme.
4. La question se reformule en : y a-t-il des racines primitives $d$-ièmes de l'unité dans $\mu_n$ ? En écrivant $n = d'd$, tout $\zeta \in \mu_d$ vérifie $\zeta_n = \zeta^{d'd} = (\zeta^d)^{d'} = 1$. Ainsi, $\mu_d \subset \mu_n$ et la réponse est oui.
5. Nous cherchons à décire $\{l \in \mathbb{Z} \,|\, l(k + n\mathbb{Z}) = n\mathbb{Z}\}$. Cet ensemble se réécrit $\{l \in \mathbb{Z} \,|\, lk \in n\mathbb{Z}\}$. En utilisant une relation de Bézout entre $k$ et $n$, il se réécrit $\{l \in \mathbb{Z} | \, l \gcd(k, n) \in n\mathbb{Z}\}$. Ainsi l'ordre de $k$ est ${}^{n}/_{\gcd k, n}$.
6. Soient $(a, b) \in \mathbb{N}_{\geq 1}$ premiers entre eux. Le point de vue arithmétique revient à considérer le morphisme de groupes donné par les réductions modulo $a$ et $b$

$$\mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, \;\; k + ab\mathbb{Z} \mapsto (k + a\mathbb{Z}, k + b\mathbb{Z}).$$

   Tout élément $k + ab\mathbb{Z}$ dans son noyau vérifie $a|k$ et $b|k$. Puisqu'ils sont premiers entre eux, le théorème de Gauss affirme que $ab|k$. Le morphisme est donc injectif et un argument de cardinalité conclut.

   L'autre point de vue revient à considérer le morphisme de groupes

$$\mu_a \times \mu_b \to \mu_{ab}, \;\; (\zeta, \xi) \mapsto \zeta\xi.$$

   Il est correctement défini puisque $(\zeta\xi)^{ab} = (\zeta^a)^b(\xi^b)^a = 1$. Ce morphisme est injectif : si $(\zeta, \xi)$ appartient au noyau alors $(\zeta\xi)^a = 1$, soit $\xi^a = 1$. Ainsi $\omega(\xi)|a$. Comme il divise $b$ par définition, il divise leur PGCD. Ainsi $\xi = 1$ et pour des raisons analogues $\zeta = 1$. Un argument de cardinalité conclut.

   Pour relier les deux morphismes, il faut choisir des racines primitives $\zeta_a$ et $\zeta_b$ puis prendre (prouver que l'on peu prendre) $\zeta_a\zeta_b$ pour racine primitive $ab$-ième.
7. Intiutivement dans $\mu_n$, on peut se convaincre qu'un sous-groupe est engendré par son élément de plus petit ordre. Donnons une preuve arithmétique. Nous considérons $H < {}^{\mathbb{Z}}/_{n\mathbb{Z}}$ et son image réciproque par

$$\mathbb{Z} \to {}^{\mathbb{Z}}/_{n\mathbb{Z}}.$$

   C'est encore un sous-groupe de $\mathbb{Z}$, contenant $n\mathbb{Z}$. Ce noyau s'écrit donc $k\mathbb{Z}$ pour $k|n$. Nous en déduisons que $H = {}^{k\mathbb{Z}}/_{n\mathbb{Z}}$, engendré par $k$.

## Exercice 9. Ordre et conjugaison

Soit $G$ un groupe fini. On rappelle que deux éléments $g$ et $g'$ sont dits conjugués dans $G$ s'il existe $h \in G$ tels que $g' = hgh^{-1}$.

1. Démontrer que deux éléments conjugués dans $G$ sont de même ordre.
2. Deux éléments de même ordre dans $G$ sont-ils toujours conjugués ? Trouver tous les groupes abéliens finis pour lesquels la réponse est positive.

### Correction de l'exercice 9

1. On a caractérisé $\omega(g)$ comme générateur du sous-groupe $\{n \in \mathbb{Z} \,|\, g^n = 1\}$. Or,
$$\forall n,\ \ (hgh^{-1})^n = hg^n h^{-1}$$
donc les deux ensembles coïncident pour $g$ et $g'$.
2. Dans un groupe abélien, le seul élément conjugué à $g$ est lui-même. Il n'existe donc au plus un élément de chaque ordre. Or, si $g$ est d'ordre $n \geq 3$, il existe plusieurs éléments d'ordre $n$ dans $\langle g \rangle$. Pour le voir, regarder l'isomorphisme avec $\mu_n$ obtenu à l'exercice 5. Ainsi, $G$ contient le neutre et au plus un élément d'ordre 2. Les seuls groupes fonctionnant sont isomorphes à $\{1\}$ ou $\mathbb{Z}/2\mathbb{Z}$.

## Exercice 10. Ordre de certaines puissances $p$-ièmes

Soient $G$ un groupe, $H$ l'un de ses sous-groupes et $p$ un nombre premier. On pose $a \in G \backslash H$ tel que $a^p \in H$. Montrer que $\mathrm{ord}(a) = p\,\mathrm{ord}(a^p)$.

### Correction de l'exercice 10

Si $a$ est d'ordre infini, alors aucun $(a^p)^n$ ne peut être trivial donc $a^p$ aussi. Si $a$ est d'ordre fini, alors $(a^p)^{\mathrm{ord}(a)} = e$ donc $a^p$ est d'ordre fini et nous avons que
$$\mathrm{ord}(a^p) = \frac{\mathrm{ord}(a)}{\mathrm{pgcd}(\mathrm{ord}, p)}.$$
Si le PGCD vaut 1, les éléments $a$ et $a^p$ ont même ordre. L'inclusion des sous-groupes $\langle a^p \rangle \subseteq \langle a \rangle$ ainsi que l'égalité de leur cardinaux entraîne que $\langle a \rangle = \langle a^p \rangle \subset H$. Ceci est impossible. Ainsi, $\mathrm{pgcd}(\mathrm{ord}(a), p) = p$ et l'on obtient l'identité souhaitée.

On propose aussi une preuve plus conceptuelle. Rappelons que l'ordre de $a$ a été défini a partir du noyau du morphisme
$$\varphi_a : \mathbb{Z} \to G,\ \ n \mapsto a^n.$$
Puisque $e \in H$, le noyau de $\varphi_a$ est contenu dans $\varphi_a^{-1}(H)$. Les hypothèses donnent des informations sur le sous-groupe $\varphi_a^{-1}(H)$ de $\mathbb{Z}$. Puisque $a \notin H$, ce sous-groupe ne contient pas 1 et puisque $a^p \in H$, ce sous-groupe contient $p$. Il s'agit donc de $p\mathbb{Z}$.

Le diagramme suivant est commutatif :
$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi_a} & G \\ {\scriptstyle p\times -}\downarrow & \nearrow_{\varphi_{a^p}} & \\ \mathbb{Z} & & \end{array}$$
et puisque $\mathrm{Ker}(\varphi_a) \subseteq p\mathbb{Z}$, l'inclusion $p\mathrm{Ker}(\varphi_{a^g}) \subseteq \mathrm{Ker}(\varphi_a)$ est une égalité. L'identité sur les ordres s'en déduit.