Correction exercice 11 du TD 2

Exercice 11. Soit $n \in \mathbb{N}^*$. On note les éléments de $\mathbb{Z}/n\mathbb{Z}$ comme $[0]_n, [1]_n, \dots, [n-1]_n$.

1. Soit H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. Montrons qu'il est cyclique. Si on suppose que H n'est pas trivial (pas réduit à l'élément neutre), alors il existe un entier $1 \leq d < n$ tel que $[d]_n = d.[1]_n \in H$. On prend le plus petit entier naturel non-nul d vérifiant cette propriété. Comme H est un sous-groupe, on sait que $\langle [d]_n \rangle \subset H$. Vérifions l'inclusion inverse. Soit $p.[1]_n \in H$. On effectue la division euclidienne de p par d, on a $p = qd + r$ avec $0 \leq r < d$ et $p.[1]_n = qd.[1]_n + r.[1]_n$. On en déduit que $r.[1]_n \in H$ mais comme d est le plus petit entier non-nul vérifiant cette propriété, on obtient $r = 0$. Ainsi, on a montré que $p \in d\mathbb{Z}$ et $H \subset \langle [d]_n \rangle$. Au final, $H = \langle [d]_n \rangle$ est un sous-groupe cyclique.
   Par le théorème de Lagrange, $k = |H|$ divise n. On a donc $k.[d]_n = kd.[1]_n = [0]_n$. Ceci implique que n divise kd et on en déduit que $\frac{n}{k}$ divise d. On a alors $H = \langle [d]_n \rangle \subset \left\langle [\frac{n}{k}]_n \right\rangle$. Comme ces deux sous-groupes sont d'ordre k, ils sont égaux. Par minimalité de d, on a $\frac{n}{k} = d$. Autrement dit, d divise n et $k = \frac{n}{d}$.
2. Supposons qu'il existe un autre sous-groupe d'ordre $\frac{n}{d}$, notons le $K = \langle [l]_n \rangle$. On a alors $\frac{n}{d}.[l]_n = [0]_n = [n]_n$. Donc n divise $\frac{n}{d}.l$, c'est à dire d divise l. Comme $l \in d\mathbb{Z}$, on a $\langle [l]_n \rangle \subset \langle [d]_n \rangle$. Ce sont deux sous-groupes de même ordre, ils coïncident. Comme $\mathbb{Z}/n\mathbb{Z}$ est un groupe abélien, le sous-groupe $(d\mathbb{Z})/(n\mathbb{Z})$ de $\mathbb{Z}/n\mathbb{Z}$ est distingué, et le quotient $(\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z})$ est un groupe. Comme $\mathbb{Z}/n\mathbb{Z}$ est cyclique, engendré par $[1]_n$, l'image de la projection canonique $\pi : \mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z})$ est un groupe cyclique engendré par $\pi([1]_n)$. Comme π est surjective, on obtient que le quotient $(\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z})$ est un groupe cyclique. Son ordre est $\frac{n}{\frac{n}{d}} = d$ et il est donc isomorphe à $\mathbb{Z}/d\mathbb{Z}$. Notez qu'on peut aussi utiliser le « Troisième théorème d'isomorphisme » donné dans l'exercice précédent pour conclure.
3. Soit $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ un morphisme de groupe. Pour $[k]_n \in \mathbb{Z}/n\mathbb{Z}$ avec $1 \leq k < n$, on a
   $$\varphi([k]_n) = \varphi(k.[1]_n) = \varphi([1]_n + \ldots + [1]_n) = \varphi([1]_n) + \ldots + \varphi([1]_n) = k.\varphi([1]_n).$$
   Donc φ est entièrement caractérisé par $\varphi([1]_n)$. De plus, on a
   $$[0]_m = \varphi([0]_n) = \varphi([n]_n) = \varphi(n.[1]_n) = n.\varphi([1]_n).$$
4. On se donne $[l]_m \in \mathbb{Z}/m\mathbb{Z}$ tel que $n.[l]_m = [0]_m$. Montrons que l'application $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ définie par $\varphi([k]_n) = k.[l]_m$ est un morphisme de groupes. On vérifie d'abord que l'application est bien définie. Soit $[k]_n, [k']_n \in \mathbb{Z}/n\mathbb{Z}$ tel que $[k]_n = [k']_n$, on a alors $\varphi([k]_n) = \varphi([k']_n)$ car $\varphi([k]_n - [k']_n)) = [0]_m$. On vérifie à présent la compatibilité de φ avec la structure de groupes. Soit $[k]_n, [h]_n \in \mathbb{Z}/n\mathbb{Z}$. On a
   $$\begin{aligned} \varphi([k]_n + [h]_n) &= \phi([k+h]_n)) \\ &= (k+h).[l]_m \\ &= [(k+h).l]_m \\ &= [k.l]_m + [h.l]_m \\ &= k.[l]_m + h.[l]_m \\ &= \varphi([k]_n) + \varphi([h]_n). \end{aligned}$$
5. On sait que $\operatorname{Im}\varphi$ est un sous-groupe de $\mathbb{Z}/m\mathbb{Z}$ donc on a $\operatorname{Im}\varphi = \langle [d]_m \rangle$ avec d un diviseur de m (on choisit d minimal dans $\mathbb{N}^*$). De plus, on a $\varphi([1]_n) = [l]_m \in \langle [d]_m \rangle$. On en déduit que $l \in d\mathbb{Z}$. Autrement dit, d est un diviseur commun à m et l. Comme d est le plus petit entier naturel tel que $[d]_m$ soit un générateur de $\operatorname{Im}\varphi$, on trouve que $d = l \wedge m$.
   Par le théorème de factorisation canonique, on a un isomorphisme de groupes $(\mathbb{Z}/n\mathbb{Z})/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi$ et on en déduit que $\frac{n}{|\operatorname{Ker}\varphi|} = \frac{m}{l\wedge m}$. On obtient $|\operatorname{Ker}\varphi| = \frac{(l\wedge m)n}{m}$. Il existe un unique sous-groupe d'ordre $\frac{(l\wedge m)n}{m}$ dans $\mathbb{Z}/n\mathbb{Z}$, donc $\operatorname{Ker}\varphi = (\frac{m}{l\wedge m}\mathbb{Z})/n\mathbb{Z}$.