Correction séance 9 (5 avril)

† *Groupes abéliens finis*

Exercice 3 (**Théorème des restes chinois**).
1. Pour $k, n \in \mathbb{Z}$ on a $k[n] = 0 (= 0[n])$ si et seulement si n divise k. Le noyau du morphisme considéré est donc l'ensemble des entiers k qui sont divisibles à la fois par n et par m. Par définition, cet ensemble est $n\mathbb{Z} \cap m\mathbb{Z} = ppcm(n, m)\mathbb{Z}$.

2. Si n et m sont premiers entre eux, alors leur ppcm est égal à leur produit, de la question précédente on déduit alors que $\ker f = nm\mathbb{Z}$, et donc, par propriété universelle des quotients, on a l'unique morphisme désiré.

3. On sait par la question précédente que $\overline{f}$ est un morphisme injectif. Comme $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont tous deux de cardinal nm, on obtient que f est également surjectif, et donc un isomorphisme.

4. On pose $d := pgcd(n, m)$, $\ell := ppcm(n, m)$, et $n' := n/d$, $m' := m/d$. On a $\ell = \frac{mn}{d} = m'n = mn'$ et d est premier avec n', m'. On a donc par les questions précédentes

$$\begin{aligned}\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} &\simeq \mathbb{Z}/dn'\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ &\simeq \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ &\simeq \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/n'm\mathbb{Z} \\ &\simeq \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}\end{aligned}$$

soit le résultat voulu.

Pour des raisons de lisibilité, on notera exceptionnellement $\mathbb{Z}/m$ au lieu de $\mathbb{Z}/m\mathbb{Z}$ à partir de maintenant.

Exercice 4.
1. On a $36 = 4.9 = 2^2.3^2$, par le théorème des restes chinois, un groupe d'ordre 36 est produit d'un groupe d'ordre 4 par un groupe d'ordre 9, les partitions de 2 sont $1+1$ et 2, il y a donc deux groupes d'ordre 4 (resp. 9) :

$$\mathbb{Z}/4, \quad \mathbb{Z}/2 \times \mathbb{Z}/2 \qquad (resp. \mathbb{Z}/9, \quad \mathbb{Z}/3 \times \mathbb{Z}/3)$$

il y a donc 4 groupes abéliens d'ordre 36 :

- $\mathbb{Z}/4 \times \mathbb{Z}/9 = \mathbb{Z}/36$
- $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/9 = \mathbb{Z}/2 \times \mathbb{Z}/18$
- $\mathbb{Z}/4 \times \mathbb{Z}/3 \times \mathbb{Z}/3 = \mathbb{Z}/3 \times \mathbb{Z}/12$
- $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3 = \mathbb{Z}/6 \times \mathbb{Z}/6$

2. On a $72 = 8.9 = 2^3.9^2$, par le théorème des restes chinois, un groupe d'ordre 72 est produit d'un groupe d'ordre 8 par un groupe d'ordre 9, les partitions de 3 sont $1+1+1, 1+2, 3$, et les partitions de 2 sont $1+1$ et 2, il y a donc 3 groupes abéliens d'ordre 8 et deux groupes abéliens d'ordre 9 (ceux de la question précédente). On a donc 6 groupes abéliens d'ordre 72

- $\mathbb{Z}/8 \times \mathbb{Z}/9 = \mathbb{Z}/72$
- $\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/9 = \mathbb{Z}/2 \times \mathbb{Z}/36$
- $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/9 = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/18$
- $\mathbb{Z}/8 \times \mathbb{Z}/3 \times \mathbb{Z}/3 = \mathbb{Z}/3 \times \mathbb{Z}/24$

- $\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/3 \times \mathbb{Z}/3 = \mathbb{Z}/6 \times \mathbb{Z}/12$
- $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3 = \mathbb{Z}/2 \times \mathbb{Z}/6 \times \mathbb{Z}/6$

3. On a $180 = 4.5.9 = 2^2.5.2^2$, par le théorème des restes chinois, un groupe d'ordre 180 est produit d'un groupe d'ordre 4, d'un groupe d'ordre 5 et d'un groupe d'ordre 9. Les partitions de 2 sont $1+1$ et 2, et 1 est l'unique partition de 1. Il y a donc deux groupes abéliens, d'ordre 4 et deux groupes abéliens d'ordre 9, et un groupe abélien d'ordre 5, d'où au final 4 groupes d'ordre 180 :

- $\mathbb{Z}/4 \times \mathbb{Z}/9 \times \mathbb{Z}/5 = \mathbb{Z}/180$
- $\mathbb{Z}/4 \times \mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/5 = \mathbb{Z}/3 \times \mathbb{Z}/60$
- $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/9 \times \mathbb{Z}/5 = \mathbb{Z}/2 \times \mathbb{Z}/90$
- $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/5 = \mathbb{Z}/6 \times \mathbb{Z}/30$

Exercice 5. Utilisons le théorème des restes chinois pour décomposer M en produit de $\mathbb{Z}/p^n\mathbb{Z}$ avec p premier :

$$\begin{aligned} M &= \mathbb{Z}/5 \times \mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/9 \times \mathbb{Z}/3 \times \mathbb{Z}/4 \times \mathbb{Z}/9 \times \mathbb{Z}/4 \\ &= \mathbb{Z}/2 \times (\mathbb{Z}/4)^3 \times \mathbb{Z}/3 \times (\mathbb{Z}/9)^2 \times \mathbb{Z}/5 \end{aligned}$$

c'est la décomposition en modules indécomposables.
Pour déterminer les facteurs invariants, essayons de faire le plus grand module possible avec les restes chinois : c'est $\mathbb{Z}/4 \times \mathbb{Z}/9 \times \mathbb{Z}/5 = \mathbb{Z}/180$, on a donc

$$M = \mathbb{Z}/2 \times (\mathbb{Z}/4)^2 \times \mathbb{Z}/3 \times \mathbb{Z}/9 \times \mathbb{Z}/180$$

et on recommence la procédure sur les facteurs restants, :

$$\begin{aligned} M &= \mathbb{Z}/2 \times (\mathbb{Z}/4)^2 \times \mathbb{Z}/3 \times \mathbb{Z}/9 \times \mathbb{Z}/180 \\ &= (\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/3) \times (\mathbb{Z}/4 \times \mathbb{Z}/9) \times \mathbb{Z}/180 \\ &= \mathbb{Z}/2 \times (\mathbb{Z}/4 \times \mathbb{Z}/3) \times \mathbb{Z}/36 \times \mathbb{Z}/180 \\ &= \mathbb{Z}/2 \times \mathbb{Z}/12 \times \mathbb{Z}/36 \times \mathbb{Z}/180 \end{aligned}$$

Et voila les facteurs invariants.

Exercice 6. Par les restes chinois, on a

$$\mathbb{Z}/pq \times \mathbb{Z}/p2 = \mathbb{Z}/p \times \mathbb{Z}/q \times \mathbb{Z}/p^2 = \mathbb{Z}/p \times \mathbb{Z}/p^2q$$

les facteurs invariants de ce $\mathbb{Z}$-module sont donc p, p^2q, qui sont différents de p^3q, le seul facteur invariant de $\mathbb{Z}/p^3q$

Exercice 7 (Unicité dans la décomposition en facteurs invariants).
1. Soit $i \in [\![1, n]\!]$ et soit $x_i \in \mathbb{Z}/d_i$. Comme d_n est un multiple de d_i, on a $d_n.x_i \equiv 0[d_i]$. En général, un élément g de G s'écrit sous la forme $(x_1, \ldots, x_n)$ avec $x_i \in \mathbb{Z}/d_i$, on a donc

$$d_n.g = d_n.(x_1, \ldots, x_n) = (d_1x_1, \ldots, d_nx_n) = (0, \ldots, 0)$$

En revanche, si $1 \leqslant k < d_n$, on a $k.1 = k \not\equiv 0[d_n]$, donc $k.(0, \ldots, 0, 1) \neq (0, \ldots, 0)$ dans G, soit le résultat voulu.

2. On a montré dans la question précédente que d_n est le plus petit entier positif non nul qui agit par 0 sur le $\mathbb{Z}$-module G. En appliquant le même raisonnement à la deuxième décomposition, on trouve que δ_m est aussi le plus petit entier positif non nul qui agit par 0 sur le $\mathbb{Z}$-module G. Par unicité d'un tel entier, on en déduit que $\delta_m = d_n$.

3. On montre la propriété par récurrence sur $|G|$. Le cas $|G| = 1$ ou $|G| = 2$ étant immédiat. Soit $x = (0, \ldots, 0, 1)$ dans la décomposition $G = \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_n$. Dans l'isomorphisme $G = \mathbb{Z}/\delta_1 \times \cdots \times \mathbb{Z}/\delta_m$, on a $x = (a_1, \ldots, a_m)$.

Comme x est d'ordre $\delta_m = d_n$, et comme $\delta_1|\delta_2|\cdots|\delta_m$, on doit avoir $a_m \in \mathbb{Z}/\delta_m\mathbb{Z}$ est un générateur (sinon, l'ordre de x serait inférieur). On peut donc définir un morphisme

$$\mathbb{Z}/\delta_1 \times \cdots \times \mathbb{Z}/\delta_m \to \mathbb{Z}/\delta_1 \times \cdots \times \mathbb{Z}/\delta_m$$

qui envoie $(1,0,\ldots,0),(0,1,0,\ldots,0)\cdots(0,\ldots,0,1,0)$ sur eux-même, et qui envoie $(0,\ldots,0,1)$ sur x. Il s'agit bien d'un morphisme car x est d'ordre δ_m. Ce morphisme est surjectif car $(0,\ldots,0,a_m)$ est dans l'image et que a_m est un générateur de $\mathbb{Z}/\delta_m$. Par égalité des cardinaux, c'est un isomorphisme. On a donc une nouvelle façon d'écrire la décomposition $G = \mathbb{Z}/\delta_1 \times \cdots \times \mathbb{Z}/\delta_m\mathbb{Z}$, l'intérêt étant que le sous module $\mathbb{Z}/\delta_m\mathbb{Z}$ est maintenant engendré par x et identifié au sous-module $\mathbb{Z}/d_n\mathbb{Z}$ de la première décomposition. En quotientant G par $\langle x\rangle$, on trouve deux groupes isomorphes

$$\mathbb{Z}/d_1 \times \cdots \mathbb{Z}/d_{n-1} \simeq \mathbb{Z}/\delta_1 \times \cdots \times \mathbb{Z}/\delta_{m-1}$$

On conclut alors par hypothèse de récurrence.

Exercice 8. 1. On sait que $8 = 2^3$, les diviseurs de 8 sont donc $1,2,4,8$. Soit G un groupe d'ordre 8 et soient $(d_1,\ldots,d_n)$ ses diviseurs élémentaires. Si $d_n = 8$, alors $n = 1$ et $G \simeq \mathbb{Z}/8$. Si $d_n = 4$, alors $d_1 \cdots d_{n-1} = 2$, comme 2 est premier et que les diviseurs élémentaires sont différents de 1, on trouve $n = 2$, $d_1 = 2$ et $G = \mathbb{Z}/2 \times \mathbb{Z}/4$. Si $d_n = 2$, alors tous les d_i devant diviser 2, ils sont tous égaux à 2 et $G = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$. 2.a) D'abord, $G(\lambda)$ est un groupe abélien comme produit de groupes cycliques, donc abéliens. Son cardinal est donné par le produit des p^{λ_i}, autrement dit par $p^{\lambda_1+\cdots+\lambda_k} = p^n$.
b) Si $\lambda \neq \mu$ sont deux partitions distinctes, alors soit elles n'ont pas le même nombre de termes, soit elles ont le même nombre de termes mais au moins un de ces termes sont différents. Par construction, $G(\lambda)$ est décrit comme un produit de facteurs invariants (les p_i^λ se divisent successivement car la suite des λ_i est croissante). Comme une telle écriture est unique (pour un groupe à isomorphisme près), on a $G(\lambda) \neq G(\mu)$ si $\lambda \neq \mu$ car les deux groupes n'ont pas la même suite de facteurs invariants.
c) Dans les questions précédentes, on a vu que l'application $\lambda \mapsto G(\lambda)$ induit une application injective de l'ensemble des partitions de n vers l'ensemble des groupes abéliens d'ordre p^n. Réciproquement, si G est un groupe abélien d'ordre p^n, considérons les diviseurs élémentaires associés $d_1,\ldots,d_k$. Comme chacun des d_i est un diviseur de p^n, il est de la forme p^{λ_i} où $\lambda_i \leqslant n$. De plus, $d_i|d_{i+1}$ équivaut à $\lambda_i \leqslant \lambda_{i+1}$. Enfin, on a

$$d_1 \cdots d_k = p^{\lambda_1+\cdots+\lambda_k} = p^n = |G|$$

et donc $\lambda_1 + \cdots + \lambda_k = n$, la suite $\lambda := (\lambda_1,\ldots,\lambda_n)$ est donc une partition de n, et $G \simeq G(\lambda)$. L'application $\lambda \mapsto G(\lambda)$ est donc surjective, d'où le résultat.

3. Soit $\lambda = (\lambda_1,\ldots,\lambda_k)$ une partition de 7. On raisonne sur λ_k et sur k.
- Si $\lambda_k = 7$, alors $k = 1$ et $\lambda = (7)$.
- Si $\lambda_k = 6$, alors $\lambda' := (\lambda_1,\ldots,\lambda_{k-1})$ est une partition de 1. On a $\lambda' := (1)$ et $\lambda = (1,6)$.
- Si $\lambda_k = 5$, alors $\lambda' := (\lambda_1,\ldots,\lambda_{k-1})$ est une partition de 2. On a $\lambda' := (1,1)$ et $\lambda = (1,1,5)$ ou $\lambda' = (2)$ et $\lambda = (2,5)$.
- Si $\lambda_k = 4$, alors $\lambda' := (\lambda_1,\ldots,\lambda_{k-1})$ est une partition de 3. On a $\lambda' := (1,1,1)$ et $\lambda = (1,1,1,4)$ ou $\lambda' = (1,2)$ et $\lambda = (1,2,4)$ ou $\lambda' = (3)$ et $\lambda = (3,4)$.
- Si $\lambda_k = 3$, alors $\lambda' := (\lambda_1,\ldots,\lambda_{k-1})$ est une partition de 4 ne contenant que des entiers inférieurs ou égaux à 3. On a $\lambda' := (1,1,1,1)$ et $\lambda = (1,1,1,1,3)$ ou $\lambda' = (1,1,2)$ et $\lambda = (1,1,2,3)$ ou $\lambda' = (2,2)$ et $\lambda = (2,2,3)$ ou $\lambda' = (1,3)$ et $\lambda = (1,3,3)$.
- Si $\lambda_k = 2$, alors $\lambda' := (\lambda_1,\ldots,\lambda_{k-1})$ est une partition de 5 ne contenant que des entiers inférieurs ou égaux à 2. On a $\lambda' = (1,1,1,1,1)$ et $\lambda = (1,1,1,1,1,2)$ ou $\lambda' = (1,1,1,2)$ et $\lambda = (1,1,1,2,2)$ ou $\lambda' = (1,2,2)$ et $\lambda = (1,2,2,2)$.
- Si $\lambda_k = 1$, alors tous les λ_i sont égaux à 1 et $\lambda = (1,1,1,1,1,1,1)$.

On obtient au total 15 partitions de l'entier 7.

4. On rappelle que les puissances de 2 sont données par $1, 2, 4, 8, 16, 32, 64, 128$. On a donc la correspondance suivante entre partitions de 7 et groupes abéliens d'ordre 128.

(7)	$\mathbb{Z}/128\mathbb{Z}$
$(1,6)$	$\mathbb{Z}/2 \times \mathbb{Z}/64$
$(1,1,5)$	$(\mathbb{Z}/2)^2 \times \mathbb{Z}/32$
$(2,5)$	$\mathbb{Z}/4 \times \mathbb{Z}/32$
$(1,1,1,4)$	$(\mathbb{Z}/2)^3 \times \mathbb{Z}/16$
$(1,2,4)$	$\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/16$
$(3,4)$	$\mathbb{Z}/8 \times \mathbb{Z}/16$
$(1,1,1,1,3)$	$(\mathbb{Z}/2)^4 \times \mathbb{Z}/8$
$(1,1,2,3)$	$(\mathbb{Z}/2)^2 \times \mathbb{Z}/4 \times \mathbb{Z}/8$
$(2,2,3)$	$(\mathbb{Z}/4)^2 \times \mathbb{Z}/8$
$(1,3,3)$	$\mathbb{Z}/2 \times (\mathbb{Z}/8)^2$
$(1,1,1,1,1,2)$	$(\mathbb{Z}/2)^5 \times \mathbb{Z}/4$
$(1,1,1,2,2)$	$(\mathbb{Z}/2)^3 \times (\mathbb{Z}/4)^2$
$(1,2,2,2)$	$\mathbb{Z}/2 \times (\mathbb{Z}/4)^3$
$(1,1,1,1,1,1,1)$	$(\mathbb{Z}/2)^7$

Exercice 9.

1. C'est un fait général : les inversibles d'un anneau commutatif unitaire forment un groupe abélien. Le produit est une loi associative et commutative avec un élément neutre (par définition d'un anneau commutatif unitaire), donc $\mathbb{Z}/n$ muni de la multiplication forme un monoïde, et les éléments inversibles d'un monoïde forment toujours un groupe !

2. Il faut déjà commencer par déterminer l'ordre de ces groupes, il est connu que $|(\mathbb{Z}/n)^\times|$ est le nombre d'entiers de $[\![1, n-1]\!]$ qui sont premiers avec n, donc

- $(\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\}$
- $(\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\}$
- $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$
- $(\mathbb{Z}/16\mathbb{Z})^\times = \{1, 3, 5, 7, 9, 11, 13, 15\}$

Donc $(\mathbb{Z}/9\mathbb{Z})^\times$ est d'ordre 6, il n'y a qu'un seul groupe abélien d'ordre 6 : $\mathbb{Z}/6\mathbb{Z}$.
$(\mathbb{Z}/5\mathbb{Z})^\times$ est d'ordre 4, il y a donc deux possibilités, mais on a que 2 est d'ordre 4 dans $(\mathbb{Z}/5\mathbb{Z})^\times$, donc ce groupe est $\mathbb{Z}/4$ (en fait, le groupe des inversible d'un corps fini est toujours cyclique !)
$(\mathbb{Z}/8\mathbb{Z})^\times$ est lui aussi d'ordre 4, c'est $\mathbb{Z}/2 \times \mathbb{Z}/2$ car il ne contient que des éléments d'ordre 2 ($3^2 = 9 \equiv 1[8]$, $7^2 = 49 \equiv 1[8]$,...)
Enfin, $(\mathbb{Z}/16\mathbb{Z})^\times$ est d'ordre 8, ce qui laisse trois possibilités, en calculant directement, on voit que $\{1, 7, 9, 15\}$ sont d'ordre 2, et que $\{3, 5, 11, 13\}$ sont d'ordre 4, il n'y a pas d'éléments d'ordre 8, donc ce n'est pas $\mathbb{Z}/8$, et il y a des éléments d'ordre 4, donc ce n'est pas $(\mathbb{Z}/2)^3$ (qui ne contient que des éléments d'ordre 2), cela nous laisse donc seulement $(\mathbb{Z}/16)^\times \simeq \mathbb{Z}/2 \times \mathbb{Z}/4$.