Corrigé TD 1

Exercice 11.

1. On considère le morphisme

$$\begin{aligned}\varphi\colon \mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z}\\ k &\to \overline{k}\end{aligned}$$

Soit $F < \mathbb{Z}/n\mathbb{Z}$ un sous-groupe. Rappelons qu'alors $\varphi^{-1}(F)$ est un sous-groupe de $\mathbb{Z}$: pour tous $p,q \in \varphi^{-1}(F)$, on a $p-q \in \varphi^{-1}(F)$ car $\varphi(p-q) = \varphi(p) - \varphi(q) \in F$. Les sous-groupes de $\mathbb{Z}$ sont tous monogènes, en particulier il existe m tel que $\varphi^{-1}(F) = m\mathbb{Z}$. Finalement $F = \varphi\left(\varphi^{-1}(F)\right) = \langle\overline{m}\rangle$ est bien un groupe cyclique.

Soit G un groupe cyclique, et $H < G$ un sous-groupe. Il existe un isomorphisme $\pi\colon \mathbb{Z}/n\mathbb{Z} \to G$ pour un certain $n \geq 1$. Pour conclure que H est cyclique il suffit alors de remarquer que $\pi^{-1}(H) < \mathbb{Z}/n\mathbb{Z}$ est d'une part cyclique par ce qui précède, et d'autre part isomorphe à H via la restriction de π.

2. Soit H_d un sous-groupe d'ordre $d \geq 2$ de $\mathbb{Z}/n\mathbb{Z}$, et considérons $m \in \{1,\cdots,n-1\}$ minimal tel que $\overline{m} \in H_d$. Soit $\overline{k}$ un élément de H_d, on peut supposer $k \in \{0,\cdots,n-1\}$. On fait la division euclidienne $k = mq + r$, avec $q \geq 0$ et $0 \leq r < m$. Alors $\overline{r} = \overline{k} - q\overline{m} \in H_d$ et donc $r = 0$, sinon on contredirait la minimalité de m. On conclut que $H_d = \langle\overline{m}\rangle$, et plus précisément

$$H_d = \{\overline{qm};\ q \in \mathbb{N}, 0 \leq qm \leq n-1\}.$$

Comme H_d est supposé d'ordre d, on a également

$$H_d = \{\overline{qm};\ 0 \leq q \leq d-1\}.$$

Ainsi $\overline{dm} = \overline{0}$ et $(d-1)m < n$, d'où $md = n$. Finalement $m = \frac{n}{d}$ est uniquement déterminé et donc $H_d = \langle\overline{m}\rangle$ est l'unique sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$.

Alternativement (et plus directement), on pouvait aussi poser, pour d un diviseur de n :

$$H_d = \left\{\overline{k} \in \mathbb{Z}/n\mathbb{Z};\ d\overline{k} = \overline{0}\right\}.$$

On voit facilement que H_d est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. Il est d'ordre d car n divise dk si et seulement si k est un multiple de (l'entier) n/d. Enfin H_d est l'unique sous-groupe d'ordre d car si $\overline{k}$ appartient à un sous-groupe d'ordre d alors son ordre divise d et donc $d\overline{k} = 0$.

Exercice 12. 2. On considère G un groupe commutatif, et $a,b \in G$ avec $\text{ordre}(a) = m$ et $\text{ordre}(b) = n$. On veut montrer que $d = \text{ordre}(ab)$ divise $p = \text{PPCM}(m,n)$. Tout d'abord, puisque $p = ms = nt$ pour certains $s,t \in \mathbb{N}$, on a

$$(ab)^p = a^p b^p = (a^m)^s (b^n)^t = 1^s 1^t = 1.$$

On a donc $d \leq p$. Faisons la division euclidienne $p = dq + r$ avec $0 \leq r < d$. On a alors

$$(ab)^r = (ab)^p \left((ab)^d\right)^{-q} = 1.$$

On en déduit que $r = 0$ (sinon on contredirait la minimalité de d, dans la définition de l'ordre de ab), et finalement d divise p comme attendu.

Exercice 13. 1. Soit g un élément d'ordre d de G : en particulier d divise $n = \text{ordre}(g)$ par Lagrange. On remarque que chacun des d éléments g^i du groupe $\langle g \rangle$ satisfait $(g^i)^d = 1$, on en déduit qu'on épuise ainsi la liste des éléments de G avec puissance $d$ème triviale. En particulier tout élément d'ordre d doit être de la forme g^i, et on sait qu'il y a exactement $\varphi(d)$ générateurs distincts dans un groupe cyclique d'ordre d.

Finalement pour tout d diviseur de n, le nombre d'éléments d'ordre d dans G est ou bien 0 ou bien $\varphi(d)$.

On a donc

$$\begin{aligned} n &= |G| \\ &= \sum_{d|n} \#\{\text{éléments d'ordre } d \text{ dans } G\} \\ &\leq \sum_{d|n} \varphi(d) \end{aligned}$$

avec égalité si et seulement si $\#\{\text{éléments d'ordre } d \text{ dans } G\} = \varphi(d)$ pour tout d diviseur de n. Mais d'après l'exercice 11 (point 4), on est précisément dans le cas d'égalité, en particulier il y a $\varphi(n)$ éléments d'ordre n : soit g un tel élément d'ordre n, on a bien $G = \langle g \rangle$ cyclique comme attendu.

2. Le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ est d'ordre $p-1$. Pour tout d diviseur de $p-1$, il y a au plus d racines dans $\mathbb{Z}/p\mathbb{Z}$ pour le polynôme $X^d - \overline{1} \in \mathbb{Z}/p\mathbb{Z}[X]$ (car $\mathbb{Z}/p\mathbb{Z}$ est un corps). Par la question précédente, on en déduit que $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique.

Remarques :

- L'hypothèse p premier pour assurer que $\mathbb{Z}/p\mathbb{Z}$ soit un corps est essentielle : par exemple sur $\mathbb{Z}/6\mathbb{Z}$, le polynôme de degré 2 $(X-\overline{3})(X-\overline{4}) = X^2 - X = X(X-\overline{1})$ admet 4 racines...
- La conclusion F^* cyclique reste valable pour tout corps (commutatif) fini F, avec la même preuve.