Devoir à la maison n° 4 - MPI*

À rendre le lundi 10 novembre 2025

Étude du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$

On cherche dans ce problème à décrire le groupe des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

$\varphi : \mathbb{N}^* \to \mathbb{N}^*$ est l'indicatrice d'Euler, qui à tout $n \in \mathbb{N}^*$ associe le nombre d'éléments dans $[\![0, n-1]\!]$ qui sont premiers à n. On rappelle que pour $n \geqslant 2$, $\varphi(n)$ est aussi le cardinal du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

1. Une jolie formule.

Soit $n \in \mathbb{N}^*$.

a) Soit d est un diviseur de n. Montrer que pour tout $k \in [\![0, n-1]\!]$, on a

$$\overline{k} \text{ est d'ordre } d \quad \iff \quad \exists m \in [\![0, d-1]\!],\ m \wedge d = 1,\ k = m\frac{n}{d}$$

En déduire qu'il y a $\varphi(d)$ éléments d'ordre d dans le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

b) En déduire la formule :

$$\sum_{d|n} \varphi(d) = n$$

La somme portant sur l'ensemble des diviseurs de n.

2. cas de $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ est alors un corps (voir cours) et on va montrer que $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^*$ est un groupe cyclique, donc isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$.

On note $G = F_p^*$ et $n = p - 1$. G est donc un groupe d'ordre n.

a) Étudier le cas de $G = \mathbb{F}_7^* = \{\overline{1}, \overline{2}, \ldots, \overline{6}\}$: déterminer un élément d'ordre 6 et expliciter un isomorphisme $f : (\mathbb{Z}/6\mathbb{Z}, +) \mapsto (\mathbb{F}_7^*, \times)$.

b) Soit d un diviseur de n. On note $N(d)$ le nombre d'éléments de G d'ordre d.

(i) Montrer que si $x \in G$ est d'ordre d, et H le sous-groupe engendré par x, on a $y^d = \overline{1}$ pour tout $y \in H$.

(ii) En considérant le polynôme $X^d - \overline{1} \in \mathbb{F}_p[X]$, en déduire que H contient tous les éléments de G d'ordre d.

(iii) En déduire que $N(d) = 0$ ou $N(d) = \varphi(d)$.

c) En utilisant la formule obtenue à la question **1.b)** en déduire qu'on a en fait $N(d) = \varphi(d)$ pour tout diviseur d de n.

d) En déduire que G est cyclique.

3. Un petit lemme

Soient a et b des élements d'ordre p et q d'un groupe G. On suppose que a et b commutent et que p et q sont premiers entre eux. Montrer que ab est d'ordre pq.

4. Cas de $\mathbb{Z}/p^\alpha\mathbb{Z}$ avec $p \geqslant 3$ premier.

Soit p un nombre premier, avec $p \geqslant 3$, et soit $\alpha \geqslant 2$. On va montrer que le groupe multiplicatif $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, de cardinal $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ est encore cyclique, donc isomorphe au groupe additif $\mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.

a) Montrer que pour tout $i \in [\![1, p-1]\!]$, p est un diviseur de $\binom{p}{i}$.

b) Montrer par récurrence que pour tout $k \in \mathbb{N}^*$, on peut écrire $(1+p)^{p^k} = 1 + \lambda p^{k+1}$, avec $\lambda \in \mathbb{N}^*$ premier à p.

c) Déduire de la question précédente que $\overline{p+1}$ est d'ordre $p^{\alpha-1}$ dans le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

d) À l'aide du résultat obtenu à la question **2**, justifier de l'existence d'un élément y d'ordre $p-1$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

cDM *Indication : considérer le sous-groupe engendré par un élément x représenté par un élément d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$*

e) En se servant du lemme obtenu à la question **3.**, en déduire que $y(\overline{1+p})$ est d'ordre $p^{\alpha-1}(p-1)$ et conclure.

f) Exemple : déterminer un générateur du groupe $(\mathbb{Z}/81\mathbb{Z})^\times$.

5. Cas (presque) général : $\mathbb{Z}/n\mathbb{Z}$ avec $n \notin 8\mathbb{Z}$

On écrit la décomposition de n en facteurs premiers $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ en facteurs premiers, et on suppose dans un premier temps n impair (donc tous les p_i sont premiers impairs).

a) Montrer que $(\mathbb{Z}/n\mathbb{Z})^\times$ est isomorphe au groupe produit $\mathbb{Z}/\varphi(p_1^{\alpha_1})\mathbb{Z} \times \cdots \times \mathbb{Z}/\varphi(p_r^{\alpha_r})\mathbb{Z}$

b) En examinant les cas $(\mathbb{Z}/2\mathbb{Z})^\times$ et $(\mathbb{Z}/4\mathbb{Z})^\times$, montrer que le resultat de la question précédente persiste lorsque n est pair mais non multiple de 8.

c) Montrer que $(\mathbb{Z}/8\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z})^2$ (groupe de Klein)

On peut montrer de façon générale que pour $\alpha \geqslant 2$, $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$, non cyclique.