Devoir à la maison n° 4 - MPI*

À rendre le mercredi 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.

Un corrigé

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

1. Une jolie formule.

a) d étant un diviseur de n, écrivons d'abord $n = dl$, avec donc $l = \dfrac{n}{d}$. Soit $k \in [\![0, n-1]\!]$.

- $\underline{\Rightarrow}$: Supposons que $\overline{k}$ est d'ordre d. On a donc $d \cdot \overline{k} = \overline{dk} = 0$ et donc $n|dk$. Comme $n = dl$, on en déduit que $l|k$. Il existe donc $m \in [\![0, k-1]\!]$ tel que $k = ml = m\dfrac{n}{d}$. Si maintenant u est un diviseur commun à m et d, on peut écrire $m = m'u$ et $d = d'u$, avec $m', l' \in \mathbb{N}$ et on a alors $k = m'u\dfrac{n}{d'u} = m'l'$, avec $l' = \dfrac{n}{d'} = ul$. On a donc $d' \cdot \overline{k} = \overline{d'k} = \overline{m'n} = \overline{0}$. On en déduit $d' = d$ et donc $u = 1$: d'où $m \wedge d = 1$.
- $\underline{\Leftarrow}$: Supposons qu'il existe $m \in [\![0, d-1]\!]$, premier à d, tel que $k = m\dfrac{n}{d} = ml$. Alors on a déjà $d \cdot \overline{k} = \overline{dk} = \overline{mn} = \overline{0}$, et donc l'ordre d' de $\overline{k}$ divise d. Ecrivons alors $d = d'u$. La relation $d' \cdot \overline{k} = \overline{0}$ signifie que $n|d'k$, soit $ld'u|d'ml$, et donc $u|m$. u est donc un diviseur commun à d et m, et donc $u = 1$, et $d' = d$: $\overline{k}$ est bien d'ordre d.

On en déduit que l'ensemble $\{k \in [\![0, n-1]\!], \overline{k} \text{ est d'ordre } d\}$ est $\{ml, 0 \leqslant m \leqslant d-1, m \wedge d = 1\}$, de cardinal $\varphi(d)$: il y a donc bien $\varphi(d)$ éléments d'ordre d dans le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

b) S'achant que l'ordre d'un élément de $\mathbb{Z}/n\mathbb{Z}$ est forcément un diviseur de n, il suffit d'écrire $\mathbb{Z}/nZ$ comme la réunion disjointe :

$$\mathbb{Z}/n\mathbb{Z} = \bigcup_{d|n} \left\{x \in \mathbb{Z}/n\mathbb{Z} \mid x \text{ est d'ordre } d\right\}$$

On a donc bien

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

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

a) Les puissances strictement positives successives de 3, à savoir $3, 9, 27, \ldots$ donnent modulo 7 les classes $\overline{3}, \overline{2}, \overline{6}, \overline{4}, \overline{5}, \overline{1}, \ldots$. On voit donc que $\overline{3}$ est d'ordre 6, et donc générateur de $\mathbb{F}_7^*$. Ce groupe est donc cyclique et isomorphe à $\mathbb{Z}/6\mathbb{Z}$. Un isomorphisme de $\mathbb{Z}/6\mathbb{Z}$ sur $\mathbb{F}_7^*$ peut être explicitement donné par :

$$f : \overline{k} \mapsto \overline{3}^k,$$

b) (i) Soit $x \in G$ d'ordre d dans G, et H le sous-groupe engendré par x. On a donc $H = \{\overline{1}, x, \ldots, x^{d-1}\}$, et si $y = x^k \in H$, on a $y^d = (x^k)^d = (x^d)^k = \overline{1}$.

(ii) Le polynôme $X^d - \overline{1}$ ne peut pas avoir plus de d racines distinctes dans le corps $\mathbb{F}_p$ (chaque racine x permet de factoriser par $X - x$. Comme tout élément de H est déjà une racine, tout les éléments de G d'ordre d (qui sont donc des racines de ce polynôme) sont dans H.

(iii) Si G n'a aucun élément d'ordre d, on a bien $N(d) = 0$. Sinon, en considérant le groupe H de la question **(i)**, on voit que l'ensemble des éléments d'ordre d de G coincide avec l'ensemble des éléments d'ordre d du groupe H, donc l'ensemble de ses générateurs. Or $H \simeq \mathbb{Z}/d\mathbb{Z}$ qui a exactement $\varphi(d)$ générateurs. On a donc $N(d) = 0$ ou $N(d) = \varphi(d)$.

c) D'après ce qui précéde, on a toujours $N(d) \leqslant \varphi(d)$, et donc, en sommant sur l'ensemble des diviseurs de n :

$$\sum_{d|n} N(d) \leqslant \sum_{d|n} \varphi(d)$$

Or, G pouvant s'écrire comme la réunion des $\{x \in G \mid x \text{ est d'ordre } d\}$, pour tout $d|n$, les deux membres de l'inégalité ci-dessus sont en fait égaux à n, d'après la jolie formule de la question **1.**. Cela n'est possible qu'avec $N(d) = \varphi(d)$ pour tout $d|n$.

d) On a en particulier $N(n) = \varphi(n) > 0$, et G possède donc un diviseur d'ordre n : G est donc bien cyclique, isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

3. Un petit lemme

Notons e l'élement neutre de G. On a déja $(ab)^{pq} = a^p b^q = e$, donc l'ordre d de ab divise pq. Écrivons maintenant

$$e = (ab)^d = (ab)^{pd} = a^{pd} b^{pd} = b^{pd}$$

On a donc $q|pd$, mais comme q est premier à p, $q|d$ d'après le théorème de Gauss. Par symétrie du rôle de p et q on a aussi $q|d$ et donc $pq|d$ puisque $p \wedge q = pq$. D'où $d = pq$: ab est bien d'ordre pq.

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

a) Soit $i \in [\![1, p-1]\!]$. On a

$$i\binom{p}{i} = i\frac{p!}{i!(p-i)!} = p\frac{(p-1)!}{(i-1)!(p-1-(i-1))!} = p\binom{p-1}{i-1}$$

p est donc un diviseur de $i\binom{p}{i}$, mais comme p est premier à i, p divise $\binom{p}{i}$.

b) Pour $k = 1$, on a :

$$(1+p)^p = 1 + \sum_{i=1}^{p} \binom{p}{i} p^i$$

Pour tout $i \in [\![1, p]\!]$, p divise $\binom{p}{i}$ et p^i, donc p^2 divise $\binom{p}{i} p^i$. On peut donc bien écrire $(1+p)^p = 1 + \lambda p^2$, avec $\lambda \in \mathbb{N}^*$. Or pour $i \geqslant 2$, on a même p^3 qui divise $\binom{p}{i} p^i$, donc λ est de la forme $1 + qp$, avec $q \in \mathbb{N}^*$, donc premier à p.

Supposons maintenant cette propriété vérifiée pour un certain $k \geqslant 1$: il existe λ premier à p tel que $(1+p)^{p^k} = 1 + \lambda p^{k+1}$. On a donc :

$$(1+p)^{p^{k+1}} = \left((1+p)^{p^k}\right)^p = (1+\lambda p^{k+1})^p = 1 + \sum_{i=1}^{p} \binom{p}{i} \lambda^i p^{(k+1)i}$$

Pour tout $i \in [\![1, p]\!]$, p divise $\binom{p}{i}$ et p^{k+1} divise $p^{(k+1)i}$ donc p^{k+2} divise $\binom{p}{i} \lambda^i p^{(k+1)i}$. On peut donc écrire

$$(1+p)^{p^{k+1}} = 1 + \lambda' p^{k+2}$$

Mais on a en fait :

$$(1+p)^{p^{k+1}} = 1 + \lambda p^{k+2} + \sum_{i=2}^{p} \binom{p}{i} \lambda^i p^{(k+1)i}$$

Pour tout $i \geqslant 2$, p^{k+3} divise $\sum_{i=1}^{p} \binom{p}{i} \lambda^i p^{(k+1)i}$, et on peut donc écrire $\lambda' = 1 + q'p$, avec $q' \in \mathbb{N}^*$, on a donc bien λ' premier à p.

c) D'après la question précédente, on peut écrire $(p+1)^{p^{\alpha-1}} = 1 + \lambda p^\alpha$, avec $\lambda \in \mathbb{N}$ et on a donc $(p+1)^{p^{\alpha-1}} \equiv 1\ [p^\alpha]$, autrement dit $\overline{p+1}^{p^{\alpha-1}} = \overline{1}$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}$. L'ordre d de $\overline{p+1}$ divise donc $p^{\alpha-1}$ et s'écrit donc comme une puissance de p, soit $d = p^\beta$ avec $\beta \leqslant \alpha - 1$.

Or, toujours d'après la question précédente, on a $\overline{p+1}^{p^\beta} = \overline{1} + \overline{\lambda}\overline{p^{\beta+1}}$, avec λ premier à p, et donc $\overline{\lambda d \cdot p} = \overline{0}$. λ étant premier à p, il est premier à p^α, donc $\overline{\lambda}$ est inversible, et on en déduit $\overline{dp} = \overline{0}$, et donc que $p^{\alpha-1}$ divise d.

En conclusion, $\overline{p+1}$ est bien d'ordre $p^{\alpha-1}$ dans le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

d) D'après la question **2**, il existe $k \in [\![0, p-1]\!]$ tel que la classe $\overline{k}$ modulo p est d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Notons alors $x = \overline{k}$ la classe de k modulo p^α. x est un élément de $(Z/p^\alpha\mathbb{Z})^\times$ (puisque k est premier avec p, donc avec p^α) et on peut donc considérer le sous-groupe H engendré par x dans $(Z/p^\alpha\mathbb{Z})^\times$. Le cardinal de H est égal à l'ordre q de x dans ce groupe, et $x^q = 1$ implique que p^α divise $k^q - 1$, et donc qu'on a aussi $\overline{k}^q = \overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$. On en déduit que $p-1$ est un diviseur de q, et $y^{\frac{q}{p-1}}$ est donc d'ordre $p-1$ dans H, et donc également dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

e) Dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, $\overline{p+1}$ est d'ordre $p^{\alpha-1}$, et on vient de montrer l'exixtence de y d'ordre $p-1$. Comme $p-1$ et $p^{\alpha-1}$ sont premiers entre eux, on en déduit que $y(\overline{1+p})$ est d'ordre $p^{\alpha-1}(p-1) = \varphi(p^\alpha)$: il s'agit donc d'un générateur du groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, qui est donc bien cyclique.

f) On est dans le cas $p = 3$ et $\alpha = 4$. On a $\varphi(81) = 2 \times 3^3 = 54$. D'après les questions précédentes, $\overline{p+1} = 4$ est d'ordre 27. Pas besoin ici de chercher un élément y d'ordre 2, puisque $4 = 2^2$: On a immédiatement que $\overline{2}$ est d'ordre 54, et donc générateur de $(\mathbb{Z}/81\mathbb{Z})\times$.

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

On suppose ici dans un premier temps $n \geqslant 3$ impair, de décomposition $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ en facteurs premiers.

a) Puisque les $p_i^{\alpha_i}$ sont premiers entre eux deux à deux, on, d'après le théorème chinois, un isomorphisme d'anneau

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}$$

Cet isomorphisme induit un isomorphisme de groupes entre les groupes des éléments inversibles de ces deux anneaux. Or, dans l'anneau produit $\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}$, un élément $(x_1, \ldots, x_r)$ est inversible si, et seulement si x_i est inversible dans $\mathbb{Z}/p^{\alpha_i}$ pour tout i. On a donc finalement un isomorphisme de groupe :

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r})^\times \simeq \mathbb{Z}/\varphi(p_1^{\alpha_1})\mathbb{Z} \times \cdots \times \mathbb{Z}/\varphi(p_r^{\alpha_r})\mathbb{Z}$$

b) On a $(\mathbb{Z}/2\mathbb{Z})^\times = \{\overline{1}\}$, groupe trivial évidemment cyclique et isomorphe à $\mathbb{Z}/1\mathbb{Z} = \mathbb{Z}/\varphi(2)\mathbb{Z}$, et $(\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, \overline{3}\}$, groupe de cardinal 2 isomorphe bien sûr à $\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/\varphi(4)\mathbb{Z}$.

Le résultat de la question précédente persiste donc bien, si on ajoute le facteur 2^1 ou 2^2 dans la décomposition en facteurs premiers de n, donc si n est pair non multiple de $2^3 = 8$.

c) On a $(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$, de cardinal $4 = \varphi(8)$. Or $\overline{3}^2 = \overline{9} = \overline{1}$, $\overline{5}^2 = \overline{25} = \overline{1}$ et $\overline{7}^2 = \overline{49} = \overline{1}$: tous les élements autres que le neutre sont d'ordre 2, donc $(\mathbb{Z}/8\mathbb{Z})^\times$ n'est pas isomorphe au groupe cyclique $\mathbb{Z}/4Z$ mais au groupe de Klein $(\mathbb{Z}/2\mathbb{Z})^2$