**Agrégation Interne**

**L'anneau $\mathbb{Z}/n\mathbb{Z}$**

[1]

Ce problème est en relation avec les leçons d'oral suivantes :

- 101 : Groupes monogènes, groupes cycliques. Exemples.
- 103 : Congruences dans $\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$. Applications.

On pourra consulter les ouvrages suivants.


- F. Combes — *Algèbre et géométrie.* Bréal (2003).
- S. Francinou, H. Gianella, S. Nicolas : *Exercices de mathématiques. Oraux X-ENS. Algèbre 1.* Cassini (2001).
- S. Francinou, H. Gianella. *Exercices de mathématiques pour l'agrégation. Algèbre 1.* Masson (1994).
- X. Gourdon. *Les Maths en tête. Algèbre.* Ellipses.
- K. Madere. *Préparation à l'oral de l'agrégation. Leçons d'algèbre.* Ellipses (1998).
- P. Ortiz. *Exercices d'algèbre.* Ellipses (2004).
- D. Perrin. *Cours d'algèbre.* Ellipses (1996).
- A. Szpirglas. *Mathématiques L3. Algèbre.* Pearson (2009).


# 1 Énoncé

Pour tout entier naturel $n \geq 0$, on note $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ l'anneau des classes résiduelles modulo $n$.
Si $k$ est un entier relatif, on note $\overline{k} = k + n\mathbb{Z}$ la classe de $k$ dans $\mathbb{Z}_n$.
Pour tout couple $(a, b)$ d'entiers relatifs, on note $a \wedge b$ le pgcd de $a$ et $b$ et $a \vee b$ leur ppcm .

### – I – Ordre d'un élément dans un groupe

On se donne un groupe additif $(G, +)$ non nécessairement commutatif et on note 0 son élément neutre.
Le cardinal de $G$ est aussi appelé l'ordre de $G$.
Si $H$ est une partie non vide $G$, on note, pour tout $g \in G$ :

$$g + H = \{g + h \mid h \in H\}$$

Pour tout $g$ dans $G$, on note $\langle g\rangle = \{kg \mid k \in \mathbb{Z}\}$ le sous groupe de $G$ engendré par $g$.
Ce sous-groupe $\langle g\rangle$ est l'image du morphisme de groupes :

$$\begin{array}{rccc} \varphi_g : & \mathbb{Z} & \to & G \\ & k & \mapsto & kg \end{array}$$

L'ordre d'un élément $g$ de $G$ est l'élément $\theta(g) \in \mathbb{N}^* \cup \{+\infty\}$ défini par :

$$\theta(g) = \mathrm{card}(\langle g\rangle)$$

Si $\theta(g)$ est dans $\mathbb{N}^*$, on dit alors que $g$ est d'ordre fini, sinon on dit qu'il est d'ordre infini.

1. Rappeler la démonstration du théorème de Lagrange : pour tout sous-groupe $H$ d'un groupe fini $G$, l'ordre de $H$ divise l'ordre de $G$.

1. Le 22/09/2013

2. Montrer que :

$$(\theta(g) = +\infty) \Leftrightarrow (\forall k \in \mathbb{Z}^*,\ kg \neq 0) \Leftrightarrow (\langle g \rangle \text{ est infini isomorphe à } \mathbb{Z})$$

(dans ce cas, on dit que $\langle g \rangle$ est monogène infini) et :

$$\begin{aligned}(\theta(g) = n \in \mathbb{N}^*) &\Leftrightarrow (\langle g \rangle = \{rg \mid 0 \leq r \leq n-1\}) \\ &\Leftrightarrow (k \in \mathbb{Z} \text{ et } kg = 0 \text{ équivaut à } k \equiv 0 \mod (n)) \\ &\Leftrightarrow (n \text{ est le plus petit entier naturel non nul tel que } ng = 0)\end{aligned}$$

(dans ce cas, $\langle g \rangle$ est dit cyclique d'ordre $n$ et il est isomorphe à $\mathbb{Z}_n$).

3. Soient $n$ un entier naturel non nul, $d \in \mathbb{N}^*$ un diviseur de $n$ et $q = \dfrac{n}{d}$. Montrer que l'ensemble des éléments de $\mathbb{Z}_n$ d'ordre divisant $d$ est le groupe cyclique :

$$H = \langle \overline{q} \rangle = \left\{\overline{0}, \overline{q}, \cdots, (d-1)\overline{q}\right\}$$

engendré par $\overline{q}$, ce groupe étant d'ordre $d$.

4. Pour $n \geq 1$, on désigne par $\Gamma_n$ le groupe multiplicatif des racines complexes de l'unité.
   (a) Montrer que pour $n \geq 1$ et $m \geq 1$, on a $\Gamma_n \cap \Gamma_m = \Gamma_{n \wedge m}$.
   (b) Montrer que $(X^n - 1) \wedge (X^m - 1) = X^{n \wedge m} - 1$ dans $\mathbb{C}[X]$. Expliquer pourquoi ce résultat est encore vrai dans $\mathbb{R}[X]$.

## – II – Morphismes de groupes, d'anneaux de $\mathbb{Z}_n$ dans $\mathbb{Z}_m$

On s'intéresse dans cette parties aux morphismes de groupes et d'anneaux de $\mathbb{Z}_n$ dans $\mathbb{Z}_m$ pour tout couple $(n, m)$ d'entiers naturels.

Pour tout entier relatif $k$, on note respectivement $\overline{k}$ la classe de $k$ modulo $n$ et $\widehat{k}$ sa classe modulo $m$.

On suppose qu'un morphisme d'anneaux commutatifs unitaires $\varphi : \mathbb{A} \to \mathbb{B}$ est tel que $\varphi(1_{\mathbb{A}}) = 1_{\mathbb{B}}$.

On note $\mathrm{Hom}_{gr}(\mathbb{Z}_n, \mathbb{Z}_m)$ [resp. $\mathrm{Hom}_{Ann}(\mathbb{Z}_n, \mathbb{Z}_m)$] l'ensemble des morphismes de groupes [resp. d'anneaux] de $\mathbb{Z}_n$ dans $\mathbb{Z}_m$.

1. Étudier le cas $(n, m) = (0, 0)$.
2. Étudier le cas $n \geq 1$ et $m = 0$.
3. Étudier le cas $n = 0$ et $m \geq 1$.
4. Étudier le cas où $n \geq 1$, $m \geq 1$ sont premiers entre eux.
5. Étudier le cas où $n \geq 1$, $m \geq 1$ sont non premiers entre eux.
6. Montrer que pour tout entier $n \geq 2$, le groupe $(\mathrm{Aut}(\mathbb{Z}_n), \circ)$ des automorphismes du groupe additif $\mathbb{Z}_n$ est isomorphe au groupe $(\mathbb{Z}_n^\times, \cdot)$ des éléments inversibles de $\mathbb{Z}_n$.

## – III – Éléments inversibles de $\mathbb{Z}_n$, fonction indicatrice d'Euler

Pour tout entier $n \geq 2$, on note $\mathbb{Z}_n^\times$ le groupe multiplicatif des éléments inversibles de $\mathbb{Z}_n$.

La fonction indicatrice d'Euler est la fonction qui associe à tout entier naturel non nul $n$, le nombre, noté $\varphi(n)$, d'entiers compris entre 1 et $n$ qui sont premiers avec $n$ (pour $n = 1$, on a $\varphi(1) = 1$).

1. Soit $k$ un entier relatif. Montrer que les propriétés suivantes sont équivalentes :
   (a) $\overline{k}$ est inversible dans $\mathbb{Z}_n$ ;
   (b) $k$ est premier avec $n$ ;
   (c) $\overline{k}$ est un générateur de $(\mathbb{Z}_n, +)$.
2. Montrer que, pour tout entier relatif $k$ premier avec $n$, on a $k^{\varphi(n)} \equiv 1\ (n)$ (théorème d'Euler).

3. Soit $p$ un entier naturel premier. Montrer que pour tout entier relatif $k$ premier avec $n$, on a $k^{p-1} \equiv 1 \ (p)$ et pour tout entier relatif $k$, on a $k^p \equiv k \ (p)$ (petit théorème de Fermat).
4. Montrer que pour $n \geq 3$, $\varphi(n)$ est un entier pair.
5. Calculer le reste dans la division euclidienne de $5^{2008}$ par 11.
6.
   (a) Soient $a, b$ des entiers relatifs et $(n_k)_{1 \leq k \leq r}$ une suite finie d'entiers naturels non nuls.
   Monter que si $a \equiv b \mod (n_k)$ pour tout $k$ compris entre 1 et $r$, alors $a \equiv b \mod (n_1 \vee \cdots \vee n_r)$.

   (b) Montrer que pour tout entier relatif $a$ premier avec 561, on a $a^{560} \equiv 1 \ (561)$, alors que 561 n'est pas premier (on dit que 561 est un nombre de Carmichaël).
7. Montrer qu'il y a équivalence entre :
   (a) $n$ est premier ;

   (b) $\mathbb{Z}_n$ est un corps ;

   (c) $\mathbb{Z}_n$ est un intègre.
8. Montrer qu'un entier $p$ est premier si et seulement si $(p-1)! \equiv -1 \ (p)$ (théorème de Wilson).
9. Montrer qu'un entier $p$ supérieur ou égal à 2 est premier si, et seulement si, $(p-2)!$ est congru à 1 modulo $p$.
10. Montrer que les entiers $n$ et $m$ sont premiers entre eux si, et seulement si, les anneaux $\mathbb{Z}_{nm}$ et $\mathbb{Z}_n \times \mathbb{Z}_m$ sont isomorphes.
11. Montrer que si $\mathbb{A}, \mathbb{B}$ sont deux anneaux commutatifs unitaires et $\varphi$ est un isomorphisme d'anneaux de $\mathbb{A}$ sur $\mathbb{B}$, il réalise alors un isomorphisme de groupes de $\mathbb{A}^\times$ (groupe des éléments inversibles de $\mathbb{A}$) sur $\mathbb{B}^\times$.
12. Montrer que si $n$ et $m$ sont deux entiers naturels non nuls premiers entre eux, on a alors $\varphi(nm) = \varphi(n)\varphi(m)$.
13. Montrer que si $n \geq 2$ a pour décomposition en facteurs premiers $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec $2 \leq p_1 < \cdots < p_r$ premiers et les $\alpha_i$ entiers naturels non nuls, on a alors :
$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$
14. Pour tout entier $n \geq 2$, on note $\mathcal{D}_n$ l'ensemble des diviseurs positifs de $n$ et pour tout $d \in \mathcal{D}_n$, on note :
$$S_d = \left\{k \in \{1, \cdots, n\} \mid k \wedge n = \frac{n}{d}\right\}$$
Pour $d = n$, $S_n$ est l'ensemble des entiers $k$ compris entre 1 et $n$ premier avec $n$.

    (a) Montrer que les $S_d$, pour $d$ décrivant $\mathcal{D}_n$, forment une partition de $\{1, \cdots, n\}$ et que pour tout $d \in \mathcal{D}_n$ on a $\mathrm{card}(S_d) = \varphi(d)$.

    (b) Montrer que pour tout entier $n \geq 2$, on a :
$$n = \sum_{d \in \mathcal{D}_n} \varphi(d)$$
    (formule de Möbius).
15. Soit $p$ un nombre premier.
Pour tout $d \in \mathcal{D}_{p-1}$, on note $\psi(d)$ le nombre d'éléments d'ordre $d$ dans le groupe multiplicatif $\mathbb{Z}_p^\times$.

    (a) Montrer que $\psi(d) = \varphi(d)$ pour tout $d \in \mathcal{D}_{p-1}$.

    (b) Montrer que le groupe $\mathbb{Z}_p^\times$ est cyclique.

16. Soient $p$ un nombre premier impair et $\alpha$ un entier supérieur ou égal à 2. On se propose de montrer que le groupe multiplicatif $\mathbb{Z}_{p^\alpha}^\times$ est cyclique.
   (a) Montrer que pour tout entier $k$ compris entre 1 et $p-1$, $C_p^k$ est divisible par $p$.
   (b) Montrer qu'il existe une suite d'entiers naturels non nuls $(\lambda_k)_{k\in\mathbb{N}}$ tous premiers avec $p$ tels que :
$$\forall k \in \mathbb{N},\ (1+p)^{p^k} = 1 + \lambda_k p^{k+1}$$
   (c) Montrer que la classe résiduelle modulo $p^\alpha$, $\overline{1+p}$ est d'ordre $p^{\alpha-1}$ dans $\mathbb{Z}_{p^\alpha}^\times$.
   (d) Montrer que si $x = k + p\mathbb{Z}$ un générateur du groupe cyclique $\mathbb{Z}_p^\times$, alors $y = k^{p^{\alpha-1}} + p^\alpha\mathbb{Z}$ est d'ordre $p-1$ dans $\mathbb{Z}_{p^\alpha}^\times$.
   (e) En déduire que $\mathbb{Z}_{p^\alpha}^\times$ est cyclique.
17. Montrer que $\mathbb{Z}_2^\times$ et $\mathbb{Z}_{2^2}^\times$ sont cycliques.
18. On s'intéresse ici au groupe multiplicatif $\mathbb{Z}_{2^\alpha}^\times$ pour $\alpha \geq 3$.
   (a) Montrer qu'il existe une suite $(\lambda_k)_{k\in\mathbb{N}}$ d'entiers impairs tels que :
$$\forall k \in \mathbb{N},\ 5^{2^k} = 1 + \lambda_k 2^{k+2}$$
   (b) Montrer que la classe résiduelle de 5 modulo $2^\alpha$ est d'ordre $2^{\alpha-2}$ dans $\mathbb{Z}_{2^\alpha}^\times$.
   (c) On désigne par $\psi$ l'application qui à toute classe résiduelle modulo $2^\alpha$, $k + 2^\alpha\mathbb{Z}$, associe la classe résiduelle modulo 4, $k + 4\mathbb{Z}$. Montrer que cette application est bien définie, qu'elle induit un morphisme surjectif de groupes multiplicatifs de $\mathbb{Z}_{2^\alpha}^\times$ sur $\mathbb{Z}_4^\times$ et que son noyau est un groupe cyclique d'ordre $2^{\alpha-2}$.
   (d) Montrer que l'application :
$$\begin{array}{rccc} \pi : & \mathbb{Z}_{2^\alpha}^\times & \to & \mathbb{Z}_4^\times \times \ker(\psi) \\ & x & \mapsto & (\psi(x), \psi(x)\, x) \end{array}$$
   est un isomorphisme de groupes. En déduire que $\mathbb{Z}_{2^\alpha}^\times$ est isomorphe à $\mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$. Le groupe $\mathbb{Z}_{2^\alpha}^\times$ est-il cyclique ?

## – IV – Idéaux de $\mathbb{Z}_n = \dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

1. Soit $\varphi : \mathbb{A} \to \mathbb{B}$ un morphisme d'anneaux commutatifs, unitaires.
   (a) Montrer que pour tout idéal $J$ de $\mathbb{B}$, $\varphi^{-1}(J)$ est un idéal de $\mathbb{A}$.
   (b) On suppose que $\varphi$ est surjectif. Montrer que pour tout idéal $I$ de $\mathbb{A}$, $\varphi(I)$ est un idéal de $\mathbb{B}$, puis que l'application $\Phi$ qui associe à tout idéal $J$ de $\mathbb{B}$ l'idéal $\varphi^{-1}(J)$ de $\mathbb{A}$ réalise une bijection de l'ensemble des idéaux de $\mathbb{B}$ dans l'ensemble des idéaux de $\mathbb{A}$ qui contiennent $\ker(\varphi)$.
2. Soit $I$ un idéal de $\mathbb{A}$. Montrer qu'il y a une bijection entre les idéaux de $\dfrac{\mathbb{A}}{I}$ et les idéaux de $\mathbb{A}$ qui contiennent $I$.
3. 
   (a) Soient $\mathbb{A}$ un anneau principal et $I$ est un idéal non trivial de $\mathbb{A}$ (i. e. $I \neq \{0\}$ et $I \neq \mathbb{A}$). Montrer que tous les idéaux de $\dfrac{\mathbb{A}}{I}$ sont principaux. L'anneau $\dfrac{\mathbb{A}}{I}$ est-il principal ?
   (b) Montrer que, pour tout entier naturel $n$, les idéaux de l'anneau $\mathbb{Z}_n = \dfrac{\mathbb{Z}}{n\mathbb{Z}}$ sont ses sous-groupes additifs.
   (c) Déterminer tous les idéaux de $\mathbb{Z}_n$, où $n \geq 2$ est un entier.
4. Quels sont les idéaux premiers de $\mathbb{Z}_n = \dfrac{\mathbb{Z}}{n\mathbb{Z}}$ pour $n \geq 2$ ?