



Soit  $n$  un entier naturel supérieur ou égal à 2. On rappelle que la relation d'égalité modulo  $n$  est une relation d'équivalence. Pour tout  $i \in \llbracket 0, n-1 \rrbracket$ , on note  $\bar{i}$  la classe d'équivalence de  $i$ . On note alors  $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ .

On définit les lois internes  $+$  et  $\cdot$  par : pour  $\bar{i}, \bar{j} \in \mathbb{Z}/n\mathbb{Z}$ ,  $\bar{i} + \bar{j} = \overline{i+j}$  et  $\bar{i} \cdot \bar{j} = \overline{i \cdot j}$ . Plus précisément, si  $k$  est un représentant de  $\bar{i}$  et  $\ell$  un représentant de  $\bar{j}$ , alors  $\bar{i} + \bar{j}$  est la classe d'équivalence de  $k + \ell$ .

### 1. Premier contact avec $\mathbb{Z}/n\mathbb{Z}$ .

a) Montrer que les définitions de l'addition et de la multiplication ne dépendent pas des représentants choisis.

b) Montrer que  $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$  est un anneau commutatif.

c) Écrire les tables d'addition et de multiplication de  $\mathbb{Z}/2\mathbb{Z}$  et  $\mathbb{Z}/4\mathbb{Z}$ .

d) Parmi les anneaux précédents, déterminer ceux qui sont intègres ? ceux qui sont des corps ?

### 2. Isomorphismes.

a) Montrer que le groupe  $(\mathbb{Z}/n\mathbb{Z}, +)$  est isomorphe au groupe  $(\mathcal{U}_n, \cdot)$ , où  $\mathcal{U}_n$  désigne l'ensemble des racines  $n$ -èmes de l'unité.

b) On note  $\mathfrak{S}_3$  l'ensemble des bijections de  $\llbracket 1, 3 \rrbracket$  dans  $\llbracket 1, 3 \rrbracket$ . Les groupes  $(\mathbb{Z}/6\mathbb{Z}, +)$  et  $(\mathfrak{S}_3, \circ)$  sont-ils isomorphes ?

### 3. Éléments inversibles (pour la loi $\cdot$ ).

a) Soit  $x \in \mathbb{Z}$ . Montrer que  $x$  et  $n$  sont premiers entre eux si et seulement si  $\bar{x}$  est inversible dans  $\mathbb{Z}/n\mathbb{Z}$ .

b) Déterminer, en justifiant votre réponse, l'inverse de  $\bar{15}$  dans  $\mathbb{Z}/98\mathbb{Z}$ .

c) Soit  $p$  un nombre premier et  $\alpha \in \mathbb{N}^*$ . Déterminer le nombre d'éléments inversibles de  $\mathbb{Z}/p^\alpha\mathbb{Z}$ .

**4. Diviseurs de  $\bar{0}$ .** On dit que  $\bar{x}$  est un diviseur de  $\bar{0}$  si  $\bar{x} \neq \bar{0}$  et il existe  $\bar{y} \neq \bar{0}$  tel que  $\bar{x} \cdot \bar{y} = \bar{0}$ .

a) Soit  $x \in \mathbb{Z}^*$  tel que  $x \neq 0 \pmod{n}$ . Montrer que  $\bar{x}$  est un diviseur de  $\bar{0}$  dans  $\mathbb{Z}/n\mathbb{Z}$  si et seulement si  $x$  et  $n$  ne sont pas premiers entre eux.

b) Déterminer les diviseurs de  $\bar{0}$  dans  $\mathbb{Z}/30\mathbb{Z}$ .

**5.** Montrer que les assertions suivantes sont équivalentes.

(i)  $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$  est un corps.

(ii)  $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$  est un anneau intègre.

(iii)  $n$  est premier.

**6. Résolution d'une équation.** Dans cette question,  $n$  désigne un nombre premier.

a) Résoudre dans  $\mathbb{Z}/n\mathbb{Z}$  l'équation  $\bar{x}^2 - \bar{1} = \bar{0}$ .

b) En déduire que les seuls éléments de  $\mathbb{Z}/n\mathbb{Z}$  qui sont leur propre inverse sont  $\bar{1}$  et  $\overline{n-1}$ .

**7. Théorème de Wilson.**  $n$  est un nombre premier si et seulement si  $n$  divise  $1 + (n-1)!$ .

a) Montrer l'implication directe lorsque  $n = 2$ .

b) Soit  $n \geq 3$  un nombre premier. Montrer que  $\prod_{k=1}^{n-1} \bar{k} = \overline{n-1}$ .

c) En déduire le théorème de Wilson.