

Petit problème: Groupes $\mathbb{Z}/n\mathbb{Z}$ et applications

On admet que $(\mathbb{Z}, +)$ est un groupe abélien munit d'une division euclidienne.

Partie I: Etude des sous groupes de $(\mathbb{Z}, +)$

Soit K un sous-groupe de $\mathbb{Z}$ non réduit à $\{0\}$.

1. Montrer que $K \cap \mathbb{N}^* \neq \emptyset$ admet un plus petit élément, que l'on note n .
2. Montrer alors que $K = n\mathbb{Z}$.
3. En déduire que les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$, avec $n \in \mathbb{N}$.

Partie II: Construction du groupe $\mathbb{Z}/n\mathbb{Z}$

Dans toute la suite du problème, on désigne par n un entier naturel $n \geq 2$. On définit la relation $\mathcal{R}$ sur $\mathbb{Z}$ par $x\mathcal{R}y$ si et seulement si x et y ont même reste dans la division euclidienne par n .

1. Montrer que $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{Z}$.
2. Montrer que $x\mathcal{R}y \Leftrightarrow n|x - y$.
3. Soient x, y, z , et t quatres entiers, tels que $x \equiv y \pmod{n}$ et $z \equiv t \pmod{n}$.

(a) Montrer alors que $x + z \equiv y + t \pmod{n}$.

(b) Montrer que $x \times z \equiv y \times t \pmod{n}$.

On définit la classe d'équivalence de x modulo n par $\bar{x} = \{y \in \mathbb{Z}, x\mathcal{R}y\} = \{y \in \mathbb{Z}, x \equiv y \pmod{n}\}$. On désigne par $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences de la relation de congruence modulo n .

4. Montrer que $\bar{x} = x + n\mathbb{Z}$.
5. On définit la somme de deux classes modulo n par $\bar{x} + \bar{y} = \overline{x + y}$.
 - (a) Montrer que la définition de la classe de deux éléments ne dépend pas des représentants choisis.
 - (b) Montrer que l'opération somme dans $\mathbb{Z}/n\mathbb{Z}$ est associative.
 - (c) Montrer qu'elle admet un élément neutre que l'on précisera.
 - (d) Montrer que toute classe $\bar{x}$ est inversible et préciser la classe inverse.
 - (e) En déduire que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien.

Partie III: Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

Soit H un sous-groupe propre de $\mathbb{Z}/n\mathbb{Z}$.

1. On désigne par $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ l'application qui à $x \in \mathbb{Z}$ associe $\pi(x) = \bar{x}$. On appelle cette application la **projection canonique** de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$.
Montrer que π est un morphisme de groupes, et que cette application est surjective.
2. On désigne par $K = \pi^{-1}(H)$. Montrer que K est un sous-groupe de $\mathbb{Z}$.
3. En déduire que tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est engendré par un élément.
4. Soit $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ avec $x \neq 0$.
Montrer que l'ordre de $\bar{x}$ dans $\mathbb{Z}/n\mathbb{Z}$ est égal à $n/\text{pgcd}(x, n)$.