Lycée Saint-Louis — DM facultatif
MPSI

Devoir facultatif

Soit n et m deux entiers non nuls.

Groupe $\mathbb{Z}/n\mathbb{Z}$:

1. Montrer que la relation $\mathcal{R}$ définie sur $\mathbb{Z}$ par

$$\forall (k,k') \in \mathbb{Z}^2,\ \ k\mathcal{R}k' \Leftrightarrow k \equiv k'[n]$$

est une relation d'équivalence et déterminer le nombre de classes d'équivalence. On notera $\overline{k}$ la classe d'équivalence de l'entier relatif k et $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence

2. On définit sur $\mathbb{Z}/n\mathbb{Z}$ la loi $+$ par

$$\forall (k,k') \in \mathbb{Z}^2,\ \ \overline{k}+\overline{k'} = \overline{k+k'}$$

Montrer que cette loi est bien définie et qu'elle munit $\mathbb{Z}/n\mathbb{Z}$ d'une structure de groupe abélien.

3. Prouver que l'application $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ k \mapsto \overline{k}$ est un morphisme de groupe surjectif. Déterminer son noyau.
4. Vérifier que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe monogène i.e. engendré par un seul élément.

Généralisation :
Soit $(G,.)$ un groupe d'élément neutre $e$et H un sous-groupe de G.

1. Montrer que la relation $\mathcal{R}$ définie sur G par

$$\forall (x,x') \in G^2,\ \ x\mathcal{R}x' \Leftrightarrow xx'^{-1} \in H$$

est une relation d'équivalence. On note G/H l'ensemble des classe d'équivalence.

2. Soit $g \in G$, déterminer la classe d'équivalence $\overline{g}$ de G.
En particulier, que vaut $\overline{e}$?
3. Dans cette question, on suppose que G est fini.
   (a) Pour tout élément g de G, déterminer le cardinal de $\overline{g}$.
   (b) En déduire le théorème de Lagrange : le cardinal de H divise celui de G.
   (c) En déduire que l'ordre d'un élément g de G divise le cardinal de G.
4. Montrer que G/H muni de la loi induite

$$\forall (x,x') \in G^2,\ \ \overline{x}.\overline{x'} = \overline{x.x'}$$

est un groupe si et seulement si H est distingué dans G i.e. si et seulement si

$$\forall (x,h) \in G \times H,\ \ x.h.x^{-1} \in H$$

On dit que H est stable par conjugaison.

5. Déterminer les sous-groupes distingués d'un groupe commutatif. Établir un lien avec la première partie.
6. Montrer que si f est un morphisme de groupes défini sur G alors son noyau est un sous-groupe distingué.
7. Réciproquement, montrer que tout sous-groupe distingué est le noyau d'un morphisme de groupe.
8. Montrer que si f est un morphisme de groupes défini sur G fini alors $\mathrm{Card}G = \mathrm{Card}(\mathrm{Im}f) \times \mathrm{Card}(\mathrm{Ker}f)$.
9. Montrer que si G/H est de cardinal 2 alors H est distingué.

Propriétés de $\mathbb{Z}/n\mathbb{Z}$:

1. Soit $k \in \mathbb{N}$. Déterminer l'ordre de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$
2. En déduire une caractérisation des entiers k tels que $\overline{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$.
3. Montrer que si p est premier alors tout groupe de cardinal p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
4. Montrer que tout groupe de cardinal 4 est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
5. Montrer que les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont monogènes.
6. Prouver que dans $\mathbb{Z}/n\mathbb{Z}$, le théorème de Lagrange admet une réciproque : Pour tout entier d divisant n, il existe un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ de cardinal d. Montrer de plus que ce groupe est unique.

Anneau $\mathbb{Z}/n\mathbb{Z}$:

1. On définit sur $\mathbb{Z}/n\mathbb{Z}$ la loi . par

$$\forall (k,k') \in \mathbb{Z}^2,\ \ \overline{k}.\overline{k'} = \overline{kk'}$$

   Montrer que cette loi est bien définie et qu'elle munit $\mathbb{Z}/n\mathbb{Z}$ d'une structure d'anneau commutatif.

2. Déterminer les élément inversibles de $\mathbb{Z}/n\mathbb{Z}$. Que peut-on en déduire si n est premier ?

3. Montrer que les anneaux $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ sont isomorphes si et seulement si n et m sont premiers entre eux.

4. On définit l'indicatrice d'Euler ϕ par

$$\forall k \in \mathbb{N}^*,\ \ \phi(k) = \mathrm{Card}\,(\mathbb{Z}/k\mathbb{Z})^*$$

   (a) Montrer que si n et m sont premiers entre eux alors $\phi(nm) = \phi(n)\phi(m)$.

   (b) Pour tout entier p premier et pour tout entier k, calculer $\phi(p^k)$.

   (c) Soit $n = \prod p_i^{a_i}$ la décomposition canonique de n en produit de nombres premiers. Montrer que $\phi(n) = n\prod(1 - \frac{1}{p_i})$.

   (d) Prouver que

$$n = \sum_{d\in\mathbb{N}^*,\, d/n} \phi(d)$$