Algèbre et arithmétique 4
DEVOIR MAISON N° 1

Exercice 1 (*Le groupe* $(\mathbb{Z}/n\mathbb{Z})^*$)

Soit $n \geq 2$. On considère l'application :

$$\times_n : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},$$

définie par $\times_n(a,b) = \overline{ab}$; par exemple, $\times_5(2,3)$ est la classe de 6 modulo 5, c'est à dire $\overline{1}$.
1) Montrez que $\times_n$ passe au quotient modulo n, c'est à dire défini une application :

$$\overline{\times}_n : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}.$$

Ceci définit une multiplication sur $\mathbb{Z}/n\mathbb{Z}$, que l'on notera simplement $\times$.
2) On note $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des classes modulo n des entiers qui sont premiers à n. On rappelle (cours) que le cardinal de cet ensemble est noté $\varphi(n)$ (et coincide par ailleurs avec l'ensemble des générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$). Par exemple, $(\mathbb{Z}/6\mathbb{Z})^* = \{\overline{1}, \overline{5}\}$ et $(\mathbb{Z}/5\mathbb{Z})^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.
Montrez que en restriction à $(\mathbb{Z}/n\mathbb{Z})^*$, la multiplication définie précédemment est une loi interne.
3) Montrez que $(\mathbb{Z}/n\mathbb{Z})^*$ muni de la multiplication, est un groupe.
4) Montrez que l'ordre de $\overline{5}$ dans $(\mathbb{Z}/6\mathbb{Z}, +)$ est 6, et que son ordre dans le groupe $((\mathbb{Z}/6\mathbb{Z})^*, \times)$ est 2.
5) Quel est l'ordre de $\overline{3}$ dans $(\mathbb{Z}/7\mathbb{Z}, +)$? Et dans $((\mathbb{Z}/7\mathbb{Z})^*, \times)$?
6) Montrez que $((\mathbb{Z}/7\mathbb{Z})^*, \times)$ est isomorphe à $((\mathbb{Z}/6\mathbb{Z}), +)$. Explicitez l'isomorphisme en donnant l'image de chacun des éléments du groupe.

Exercice 2 (*Le groupe diédral* D_n)

Soit $n \geq 3$, $\mathcal{P}_n$ le polygône régulier à n côtés centré en 0, ayant pour sommet le point A_1 de coordonnées $(1,0)$; par exemple $\mathcal{P}_4$ est le carré de sommets $(1,0)$,$(0,1)$,$(-1,0)$ et $(0,-1)$.
1) Soit $O(2)$ l'ensemble des isométries linéaires de $\mathbb{R}^2$, c'est à dire des matrices 2*2 M qui vérifient ${}^tMM = I_2$. Montrez que $O(2)$ est un groupe, et que si on note D_n l'ensemble des transformations de $O(2)$ qui préservent $\mathcal{P}_n$, alors D_n est un sous-groupe de $O(2)$.
2) Soit $A_1, ..., A_n$ les sommets de $\mathcal{P}_n$ numérotés dans le sens trigonométrique. Soit ρ la rotation de centre 0 et d'angle $2\pi/n$. Quelle est l'image de A_i par ρ ? Quel est l'ordre de ρ ? Ecrire la matrice de ρ.
3) Montrez que l'on peut définir une application $\phi : \mathbb{Z}/n\mathbb{Z} \to D_n$, $\phi(\overline{k}) = \rho^k$, et que c'est un morphisme injectif. Notons Γ_n son image.
4) Soit s la symétrie d'axe Ox. Quel est l'ordre de s ? Ecrivez la matrice représentant s.
5) Soit M un élément quelconque de D_n. En remarquant que deux sommets de $\mathcal{P}_n$ adjacents ne peuvent être envoyés par une isométrie que sur deux autres sommets adjacents, montrez que soit M, soit sM, est dans Γ_n.
6) En conclure que Γ_n est d'indice 2 dans D_n, et l'ordre de D_n.
Décrire la signification géométrique pour un élément de D_n d'être ou non dans Γ_n.
7) Montrez que D_n n'est pas commutatif ; ou pourra calculer par exemple $s\rho s$.