Fiche de TD 6

$\mathbb{Z}/n\mathbb{Z}$ et groupe symétrique

exercices supplémentaires

Exercice 1 a) Montrer par récurrence sur $\alpha \in \mathbb{N}$ que :

$$\forall\, \alpha \in \mathbb{N},\ \forall\, k \in \mathbb{Z},\ (2k+1)^{2^\alpha} \in 1 + 2^{\alpha+2}\mathbb{Z}\ .$$

En déduire que $\forall\, n \in \mathbb{N}_{\geqslant 2},\ \forall\, x \in (\mathbb{Z}/2^n\mathbb{Z})^*,\ x^{2^{n-2}} = 1$ et que $(\mathbb{Z}/2^n\mathbb{Z})^*$ n'est pas cyclique si $n \geqslant 3$.

b) Montrer que $\forall\, \alpha \in \mathbb{N},\ 5^{2^\alpha} = 1 + 2^{\alpha+2}x_\alpha$ pour un certain entier impair x_α. En déduire l'ordre de 5 dans le groupe $(\mathbb{Z}/2^n\mathbb{Z})^*$. Montrer que

$$\forall\, n \in \mathbb{N}_{\geqslant 2},\ (\mathbb{Z}/2^n\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}\ .$$

c) Soit p premier impair. Montrer que

$$\forall\, \alpha \in \mathbb{N},\ \exists\, x_\alpha \in \mathbb{Z} \text{ premier à } p,\ (1+p)^{p^\alpha} = 1 + p^{\alpha+1}x_\alpha\ .$$

En déduire l'ordre de $1+p$ dans le groupe $(\mathbb{Z}/p^n\mathbb{Z})^*$.

d) Montrer que le morphisme de groupes $(\mathbb{Z}/p^n\mathbb{Z})^* \mapsto (\mathbb{Z}/p\mathbb{Z})^*$ est surjectif et en déduire qu'il existe un élément d'ordre $p-1$ dans le groupe $(\mathbb{Z}/p^n\mathbb{Z})^*$.

e) En déduire que pour tout nombre premier impair p, le groupe $(\mathbb{Z}/p^n\mathbb{Z})^*$ est cyclique.

Exercice 2 a) Soit $a \in \mathbb{Z}/n\mathbb{Z}$. Montrer que le morphisme de groupes

$$\phi_a : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ k \mapsto ak$$

est un isomorphisme si et seulement si $a \in (\mathbb{Z}/n\mathbb{Z})^*$.

b) Montrer que $(\mathbb{Z}/n\mathbb{Z})^* \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, $a \mapsto \phi_a$ est un isomorphisme de groupes.

c) Pour tout $a \in (\mathbb{Z}/11\mathbb{Z})^*$, décomposer ϕ_a en produit de cycles à supports disjoints dans $\mathfrak{S}_{10} = \mathfrak{S}_{\{\overline{1},\overline{2},\ldots,\overline{10}\}}$.

d) Soient $x_1, x_2, x_3 = (1,0), (0,1), (1,1) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

On pose pour tout $\sigma \in \mathfrak{S}_3$, $(a_\sigma, c_\sigma) = x_{\sigma(1)}$, $(b_\sigma, d_\sigma) = x_{\sigma(2)} \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Montrer que l'application $\mathfrak{S}_3 \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, $\sigma \mapsto \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix}$ est un isomorphisme de groupes.