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 :

$$\forall\, \alpha \in \mathbb{N}_{>}0,\ \forall\, k \in \mathbb{Z},\ (2k+1)^{2^\alpha} \in 1 + 2^{\alpha+2}\mathbb{Z}\ .$$

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 $n \geqslant 3$. C'est évident si $\alpha = 1$ car $(2k+1)^2 = 1 + 4k(k+1) = 1 \bmod 8$ car $k(k+1)$ est pair. Si $(2k+1)^{2^\alpha} = 1 + 2^{\alpha+2}m$, $m \in \mathbb{Z}$, alors

$$(2k+1)^{2^{\alpha+1}} = (1 + 2^{\alpha+2}m)^2 = 1 + 2^{\alpha+3}m + 2^{2\alpha+4}m^2 = 1 \bmod 2^{\alpha+3}$$

car $2\alpha + 4 \geqslant \alpha + 3$.

En particulier, si $x \in (\mathbb{Z}/2^n\mathbb{Z})^*$, $x = 2k+1$ pour un certain k car x est impair. Donc $x^{2^{n-2}} = 1 \bmod 2^n$. Donc il n'y a pas d'éléments d'ordre $2^{n-1} = \varphi(2^n) = |(\mathbb{Z}/2^n\mathbb{Z})^*|$ dans $(\mathbb{Z}/2^n\mathbb{Z})^*$ qui n'est donc pas cyclique.

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

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

Par récurrence sur $\alpha \in \mathbb{N}$. C'est évident pour $\alpha = 0$. Et si $5^{2^\alpha} = 1 + 2^{\alpha+2}x_\alpha$ pour un x_α impair, alors

$$\begin{aligned} 5^{2^{\alpha+1}} &= (5^{2^\alpha})^2 = 1 + 2^{\alpha+3}x_\alpha + 2^{2\alpha+4}x_\alpha^2 \\ &= 1 + 2^{\alpha+3}\underbrace{(x_\alpha + 2^{\alpha+1}x_\alpha^2)}_{\text{impair}}\ . \end{aligned}$$

Donc si $n \geqslant 3$, $5^{2^{n-2}} = 1 \bmod 2^n$ et $5^{2^{n-3}} = 1 + 2^{n-1}x_{n-3} \neq 1 \bmod 2^n$ car x_{n-3} est impair. Donc 5 est d'ordre 2^{n-2}. Comme $5 = 1 \bmod 4$, $5^k = 1 \bmod 4 \neq -1 \bmod 2^n$ si $n \geqslant 2$ (car $4|2^n$). Comme 5 est d'ordre 2^{n-2} et -1 d'ordre 2 dans $(\mathbb{Z}/2^n\mathbb{Z})^*$, l'application

$$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}, +) \longrightarrow (\mathbb{Z}/2^n\mathbb{Z})^*, .)$$

$$(\epsilon, k) \longmapsto (-1)^\epsilon 5^k$$

est bien définie et c'est un morphisme de groupes. C'est injectif car :

$$(-1)^\epsilon 5^k = 1 \Leftrightarrow 5^k = (-1)^\epsilon$$

$$\Rightarrow (-1)^\epsilon = 1$$

(car $5^k \neq -1 \bmod 2^n$). Donc $\epsilon = 0 \bmod 2$ et $5^k = 1 \bmod 2^n \Rightarrow k = 0 \bmod 2^{n-2}$ car 5 est d'ordre 2^{n-2} dans $(\mathbb{Z}/2^n\mathbb{Z})^*$.

Comme $|\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}| = |(\mathbb{Z}/2^n\mathbb{Z})^*| = 2^{n-1}$, c'est un isomorphisme.

c) Soit p premier impair. Montrer que

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

En déduire l'ordre de $1+p$ dans le groupe $(\mathbb{Z}/p^n\mathbb{Z})^*$. Par récurrence sur $\alpha \in \mathbb{N}$. Si $\alpha = 0$, c'est évident. Si $(1+p)^{p^\alpha} = 1 + p^{\alpha+1} x_\alpha$ avec $x_\alpha = 1 \bmod p$, alors :

$$(1+p)^{p^{\alpha+1}} = ((1+p)^{p^\alpha})^p = (1 + p^{\alpha+1} x_\alpha)^p$$

$$= 1 + p^{\alpha+2} x_\alpha + \binom{p}{2} p^{2\alpha+2} x_\alpha^2 + \ldots + p^{p\alpha+p} x_\alpha^p$$

$$1 + p^{\alpha+2} \underbrace{(x_\alpha + p(p^{\alpha-1}\binom{p}{2} x_\alpha^2 + \ldots + p^{(p-1)\alpha+p-3} x_\alpha^p))}_{= x_\alpha \bmod p = 1 \bmod p}$$

car $p \geqslant 3$.

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 $(\mathbb{Z}/p^n\mathbb{Z})^*$. Si x est premier à p, alors $x \in (\mathbb{Z}/p^n\mathbb{Z})^*$. Donc $x \bmod p^n$ est un antécédent de $x \bmod p$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique. Donc il existe $x \in \mathbb{Z}$ tel que $x \bmod p$ est d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^*$. Mais alors dans $(\mathbb{Z}/p^n\mathbb{Z})^*$, $x^d = 1 \bmod p^n \Rightarrow x^d = 1 \bmod p \Rightarrow p-1 | d$. Donc x est d'ordre $(p-1)k$ pour un entier k. Donc x^k est d'ordre $p-1$.

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

Soient $a \in (\mathbb{Z}/p^n\mathbb{Z})^*$ d'ordre $p^{\alpha-1}$ (par exemple $a = 1+p$) et $b \in (\mathbb{Z}/p^n\mathbb{Z})^*$ d'ordre $p-1$. Alors

$$(ab)^d = 1 \Leftrightarrow a^d b^d = 1$$

$$\Rightarrow a^d = b^{-d} \in \langle a \rangle \cap \langle b \rangle = 1$$

car l'ordre divise $\text{pgcd}(p^{n-1}, p-1) = 1$. Donc $a^d = b^d = 1 \Rightarrow p^{n-1} | d$ et $p-1 | d$

$$\Rightarrow |(\mathbb{Z}/p^n\mathbb{Z})^*| = \varphi(p^n) = p^{n-1}(p-1) \,|\, d$$

donc ab est d'ordre au moins $|(\mathbb{Z}/p^n\mathbb{Z})^*|$ donc

$$\langle ab\rangle = (\mathbb{Z}/p^n\mathbb{Z})^*$$

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.