Sujet 2

Exercice 1 :

1) $\sigma = \underbrace{(1\ 2\ 3\ 8)}_{\text{ordre } 4}(4)\underbrace{(5\ 7\ 6)}_{\text{ordre } 3}$

$\sigma^{2027} = (1\,2\,3\,8)^{2027}\,(5\,7\,6)^{2027}$, mais $2027 \equiv 3\ [4]$, $2027 \equiv 2\ [3]$.

$= (1\,2\,3\,8)^{3}\,(5\,7\,6)^{2}$

$= (1\,8\,3\,2)(5\,6\,7)$

2) a) $\tau = (1\,2)(3\,4)$ d'où $\varepsilon(\tau) = \varepsilon(12) \times \varepsilon(34)$

$= (-1) \times (-1) = 1$

donc $\tau \in \mathcal{A}_5$

b) $\tau = (1\,6\,4)(2\,3\,5)$, $\varepsilon(\tau) = \varepsilon(164) \times \varepsilon(235)$

$= (-1)^2 \times (-1)^2 = 1$

d'où $\tau \in \mathcal{A}_6$

c) $\tau = \sigma^{2026}$, $\varepsilon(\tau) = \varepsilon(\sigma)^{2026} = 1$ car 2026 pair

donc $\tau \in \mathcal{A}_8$.

Exercice 2 :

1) a) Non, par exemple pour $x=2$, on veut $2 \times u \times 2 = 2$ i.e. $2u = 1$, impossible dans $\mathbb{Z}$

b) Oui, il suffit de prendre $u = x^{-1}$: $\forall x \in K^*,\ x x^{-1} x = x$.

Cela reste vrai pour $x = 0$ (tout u convient)

c) Soit $v \in \mathcal{L}(E)$. Considérons $y_1, .., y_r$ une base de $\mathrm{Im}(v)$ et $e_1, .., e_r$ t.q. $v(e_i) = y_i$. La famille $(e_1, .., e_r)$ est alors libre. On peut compléter $(e_1, .., e_r)$ par $(e_{r+1}, .., e_n)$ une base de $\ker(v)$ (c'est en fait le théorème du rang, voir la preuve si vous voulez plus de détails)

On pose alors $u(y_i) = e_i$ pour $i \in [\![1; r]\!]$

$u(y_i) = 0$ sinon (où on a complété la base de $\mathrm{Im}(v)$)

Alors, $\forall i \in [\![1; n]\!]$:

$$v \circ u \circ v(e_i) = \begin{cases} v \circ u(0) = 0 = v(e_i) & \text{si } i > r \\ v \circ u(y_i) = v(e_i) = y_i & \text{si } i \leq r. \end{cases}$$

d'où $v \circ u \circ v = v$.

2) On utilise la méthode proposée ci-dessus pour trouver U.

L'image de A est donnée par ses colonnes. La colonne nulle nous donne un vecteur (générateur) de $\ker(A)$.

On pose donc $U = \begin{pmatrix} 0 & & 0 \\ & \ddots & \\ 0 & & 0 \end{pmatrix}$ [si $y_i = Ae_i$, $Uy_i = e_i$]

Un calcul donne $AUA = A$.

3) Regardons déjà ce qu'il se passe pour des petites valeurs de n.

$\mathbb{Z}/2\mathbb{Z}$ → corps donc régulier

$\mathbb{Z}/3\mathbb{Z}$ → ——————

$\mathbb{Z}/4\mathbb{Z}$ → $2u2 \equiv 2\ [4]$ ssi $4u \equiv 2\ [4]$ impossible car $4u \equiv 0\ [4]$

$\mathbb{Z}/6\mathbb{Z}$ → régulier car pour $x \wedge 6 = 1$, x inversible, $x=2$, $4u \equiv 2\ [6]$, $u=2$ convient, $x=3$, $9u \equiv 3\ [6]$ $u=-1$ convient.

$\mathbb{Z}/8\mathbb{Z}$ → pas régulier $x=4$, $16u \not\equiv 4\ [8]$.

On peut donc supposer que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est régulier ssi n ne possède pas de facteurs carrés.

En effet, si $n = mp^2$, prenons $x = p$. On cherche u t.q. $up^2 \equiv p\ [m]$

ie $m \mid p(up-1)$ i.e. $\exists k \in \mathbb{Z}$ t.q. $km = p(up-1)$.

Modulo p^2, cela donne $0 \equiv -p\ [p^2]$, impossible.

Maintenant, si $n = p_1 \times .. \times p_r$.

Pour x premier à n, on a x inversible dans $(\mathbb{Z}/n\mathbb{Z})$, donc $u = x^{-1}$ convient. Il reste le cas où $x = m \times p$, avec $m \wedge n = 1$ ($p = p_1^{\nu_{p_1}(x)} \times .. \times p_r^{\nu_{p_r}(x)}$)

On cherche u t.q. $ux^2 \equiv x\ [n]$ ie $n \mid x(ux-1)$ ie $\exists k \in \mathbb{Z}$ t.q. $km = x(ux-1)$ d'où $km = mp(ump-1)$.

Il suffit donc de prendre u l'élément inverse de mp modulo le produit des p_i qui ne sont pas dans la décomposition de x (u existe bien car mp serait premier avec le produit de ces p_i). On aurait alors $ump - 1 \equiv 0\ [\prod_{p_i \nmid x} p_i]$ ie $\prod_{p_i \nmid x} p_i \mid ump - 1$ d'où $n \mid x(ux-1)$