Ex1 1) $ax \equiv b\ [n] \Leftrightarrow \exists l \in \mathbb{Z}$ t.q. $ax = b + ln$

$\Leftrightarrow \exists l \in \mathbb{Z}$ t.q $ax - ln = b$

D'après cours on sait que $ax - ln = b$ admet des solutions ssi $a \wedge n$ divise b
La démonstration est demandée.

2)

126	2
63	7
9	3x3

$126 = 2 \times 3^2 \times 7$

230	2
	5
23	23

$230 = 2 \times 5 \times 23$

Donc $126 \wedge 230 = 2$. D'après la question précédente $126x \equiv 2\ [230]$ admet des solutions : $126x \equiv 2\ [230] \Leftrightarrow \exists l \in \mathbb{Z}$ t.q $126x - 230\,l = 2$

$\Leftrightarrow \exists l \in \mathbb{Z}$ t.q $63x - 115\,l = 1$

$$\begin{array}{r|l} 115 & 63 \\ -63 & 1 \\ \hline 52 & \end{array}$$

$115 - 63 = 52$

$$\begin{array}{r|l} 63 & 52 \\ -52 & 1 \\ \hline 11 & \end{array}$$

$63 - 52 = 11 \Rightarrow 63 - (115 - 63) = 11 \Rightarrow 2 \times 63 - 115 = 11$

$$\begin{array}{r|l} 52 & 11 \\ -44 & 4 \\ \hline 8 & \end{array}$$

$52 - 4 \times 11 = 8 \Rightarrow (115 - 63) - 4 \times (2 \times 63 - 115) = 8$

$\Rightarrow 5 \times 115 - 9 \times 63 = 8$

$$\begin{array}{r|l} 11 & 8 \\ -8 & 1 \\ \hline 3 & \end{array}$$

$11 - 8 = 3 \Rightarrow (2 \times 63 - 115) - (5 \times 115 - 9 \times 63) = 3$

$\Rightarrow 11 \times 63 - 6 \times 115 = 3$

$3 \times 3 - 8 = 1 \Rightarrow 3(11 \times 63 - 6 \times 115) - (5 \times 115 - 9 \times 63) = 1$

$\Rightarrow \boxed{42 \times 63 - 23 \times 115 = 1}$

Donc l'ensemble des solutions de $63x - 115\ell = 1$ est

$$\{(x,\ell) = (42+115k,\ 23+63k)\ /\ k \in \mathbb{Z}\}$$

Donc l'ensemble des solutions de $126x \equiv 2\ [230]$ est $\{42+115k\ /\ k \in \mathbb{Z}\}$

Ex2 1) $\sigma = \underbrace{(1\,6)}_{\tau_1}\underbrace{(1\,5\,4\,7)}_{\tau_2}\underbrace{(2\,1\,3\,7)}_{\tau_3}\underbrace{(1\,3\,6)}_{\tau_4}$

1) la signature est un morphisme de gpe $\varepsilon : (S_8, \circ) \longrightarrow (\{\pm 1\}, \times)$

D'après signature d'un k-cycle est $(-1)^{k+1}$

$$\varepsilon(\sigma) = \varepsilon(\tau_1) \times \varepsilon(\tau_2) \times \varepsilon(\tau_3) \times \varepsilon(\tau_4) = (-1)^3 \times (-1)^5 \times (-1)^5 \times (-1)^4 = -1$$

2) on calcule $\sigma(1) = \tau_1\tau_2\tau_3\tau_4(1) = \tau_1\tau_2\tau_3(3) = \tau_1\tau_2(7) = \tau_1(1) = 6$

$\sigma(2) = \tau_1\tau_2\tau_3\tau_4(2) = \tau_1\tau_2\tau_3(2) = \tau_1\tau_2(1) = \tau_1(5) = 5$

$\sigma(3) = \tau_1\tau_2\tau_3\tau_4(3) = \tau_1\tau_2\tau_3(6) = \tau_1\tau_2(6) = \tau_1(6) = 1$

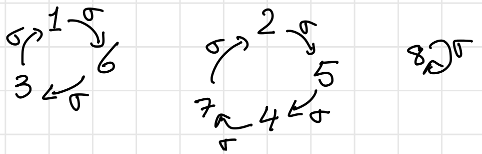
$\sigma(4) = \tau_1\tau_2\tau_3\tau_4(4) = \tau_1\tau_2\tau_3(4) = \tau_1\tau_2(4) = \tau_1(7) = 7$

$\sigma(5) = \tau_1\tau_2\tau_3\tau_4(5) = \tau_1\tau_2\tau_3(5) = \tau_1\tau_2(5) = \tau_1(4) = 4$

$\sigma(6) = \tau_1\tau_2\tau_3\tau_4(6) = \tau_1\tau_2\tau_3(1) = \tau_1\tau_2(3) = \tau_1(3) = 3$

$\sigma(7) = \tau_1\tau_2\tau_3\tau_4(7) = \tau_1\tau_2\tau_3(7) = \tau_1\tau_2(2) = \tau_1(2) = 2$

$\sigma(8) = 8$



$\sigma = (1\,6\,3)(2\,5\,4\,7)$

3) $(1\,6\,3)$ et $(2\,5\,4\,7)$ sont des cycles disjoints Donc

$$\mathrm{ord}(\sigma) = \mathrm{ppcm}(\mathrm{ord}(1\,6\,3),\ \mathrm{ord}(2\,5\,4\,7)) = \mathrm{ppcm}(3,4) = 12$$

$\mathrm{ord}(\sigma^{2025})$: <u>Méthode 1</u> $\mathrm{ord}(\sigma^k) = \dfrac{\mathrm{ord}(\sigma)}{\mathrm{ord}(\sigma)\wedge k}$

$$\mathrm{ord}(\sigma^{2025}) = \frac{12}{12\wedge 2025} = 4$$

<u>Méthode 2</u> $2025 = 12\times 168 + 9 \Rightarrow \sigma^{2025} = \sigma^{12\times 168}\circ\sigma^9 = \sigma^9$

$(1\,6\,8)$ et $(2\,5\,4\,7)$ étant des cycles disjoints, ils commutent. Donc

$\sigma^9 = (1\,6\,8)^9(2\,5\,4\,7)^9 = (2\,5\,4\,7) \Rightarrow$

$$\mathrm{ord}(\sigma^{2025}) = \mathrm{ord}(\sigma^9) = \mathrm{ord}((2\,5\,4\,7)) = 4$$

4) $26 = 2\times 12 + 2 \Rightarrow \sigma^{26} = (\sigma^{12})^2\circ\sigma^2 = \sigma^2$

$= (1\,6\,8)(2\,5\,4\,7)(1\,6\,8)(2\,5\,4\,7)$

$= (1\,8\,6)(2\,4)(5\,7)$

Ex 3 1) • Soient $g_1 = e^{\frac{k\pi}{4}i}$ et $g_2 = e^{\frac{l\pi i}{4}} \in G$

$g_1 g_2 = e^{\frac{(k+l)\pi}{4}i}$ Soit $k+l = 8q+r$ avec $0\leq r<8$ la div. eucl de $k+l$ par 8

$g_1 g_2 = e^{(8q+r)\frac{\pi}{4}i} = e^{\frac{r\pi}{4}i} \in G$ ✓

• Soit $g = e^{k\pi/4\, i}$ si $k=0 \Rightarrow g=1$ et $g^{-1} = 1\in G$

si $0<k<8 \Rightarrow 0<8-k<8$ et $g\times e^{(8-k)\frac{\pi i}{4}} = 1 \Rightarrow g^{-1}\in G$ aussi!

$G = \langle e^{\pi i/4}\rangle$. G est cyclique donc générateurs de G sont $(e^{\pi i/4})^k$ avec

$k\wedge 8 = 1 \Rightarrow k = 1, 3, 5, 7$

2)

$$
\begin{array}{r|l}
X^8 - 1 & X^6 - 1 \\ \cline{2-2}
-(X^8 - X^2) & X^2 \\ \cline{1-1}
X^2 - 1 &
\end{array}
\qquad\qquad
\begin{array}{r|l}
X^6 - 1 & X^2 - 1 \\ \cline{2-2}
-(X^6 - X^4) & X^4 + X^2 + 1 \\ \cline{1-1}
X^4 - 1 & \\
-(X^4 - X^2) & \\ \cline{1-1}
X^2 - 1 & \\
-(X^2 - 1) & \\ \cline{1-1}
0 &
\end{array}
$$

$$\Rightarrow P \wedge Q = X^2 - 1$$

3) les racines complexes de P sont $e^{\frac{k\pi i}{4}}$ avec $k = 0, 1, \dots, 7$

$$\Rightarrow P = (X-1)(X-e^{\pi i/4})(X-e^{\pi i/2})(X-e^{\frac{3\pi i}{4}})(X+1)(X-e^{5\pi i/4})(X-e^{\frac{3\pi i}{2}})(X-e^{\frac{7\pi}{4}i})$$

$$= (X-1)(X+1)(X-i)(X+i)(X-e^{\pi i/4})(X-e^{7\pi i/4})(X-e^{3\pi i/4})(X-e^{5\pi i/4})$$

$$e^{\pi i/4} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, \quad e^{7\pi i/4} = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}, \quad e^{\frac{3\pi i}{4}} = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, \quad e^{\frac{5\pi i}{4}} = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$$

$$(X-i)(X+i) = X^2+1, \quad (X-e^{\pi i/4})(X-e^{7\pi i/4}) = (X^2 + \sqrt{2}X + 1)$$

$$(X-e^{3\pi i/4})(X-e^{5\pi i/4}) = (X^2 - \sqrt{2}X + 1)$$

$$P = (X-1)(X+1)(X^2+1)(X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1)$$

décomp de P comme produit des polynômes irréductibles!

Les racines complexes sont $e^{\frac{k\pi i}{3}}$ $k = 0, 1, 2, 3, 4, 5$

$$Q = (X-1)(X-e^{\pi i/3})(X-e^{2\pi i/3})(X+1)(X-e^{4\pi i/3})(X-e^{5\pi i/3})$$

$$e^{\pi i/3} = \frac{1}{2} + i\frac{\sqrt{3}}{2}, \quad e^{\frac{2\pi i}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}, \quad e^{\frac{4\pi i}{3}} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}, \quad e^{\frac{5\pi i}{3}} = \frac{1}{2} - i\frac{\sqrt{3}}{2}$$

$$Q = (X-1)(X+1)(X-e^{\pi i/3})(X-e^{5\pi i/3})(X-e^{2\pi i/3})(X-e^{4\pi i/3})$$

$$= (X-1)(X+1)(X^2+X+1)(X^2-X+1)$$

décomposition de Q comme produit des polynômes irréductibles.

$$P \wedge Q = (X-1)(X+1)$$

Ex 4 1a) Soient $x, y \in H$

$$f^2(xy) = f\circ f(xy) = f(f(x)f(y)) = f^2(x) f^2(y) = xy$$

Donc $xy \in H$

- Soit $x \in H$

$$f^2(x^{-1}) = f(f(x^{-1})) = f(f(x)^{-1}) = f(x^{-1}) = f(x)^{-1} = x^{-1}$$

1b) Soit $x \in S$ Donc $f(x) = x^{-1}$

$$f^2(x) = f(f(x)) = f(x^{-1}) = f(x)^{-1} = (x^{-1})^{-1} = x \Rightarrow x \in H \checkmark$$

- Soient $x, y \in S$ $f(xy) = f(x) f(y) = x^{-1} y^{-1} \underset{\uparrow}{=} (yx)^{-1} = (xy)^{-1}$

G commutatif

Donc $xy \in S \checkmark$

- Soit $x \in S$ $f(x^{-1}) = f(x)^{-1} = (x^{-1})^{-1} = x \Rightarrow x^{-1} \in S \checkmark$

Ex4 2) $x \in S \Leftrightarrow f(x) = -x \Leftrightarrow 2x = -x \Leftrightarrow 3x = \bar{0}$

Donc $S = \{\bar{0}, \bar{2}, \bar{4}\}$

$x \in H \Leftrightarrow f^2(x) = x \Leftrightarrow f(2x) = x \Leftrightarrow 4x = x \Leftrightarrow 3x = \bar{0}$

Donc $H = S$

3a) Soient $x, y \in G$

- $f(x) f(y) = (\tau x \tau^{-1})(\tau y \tau^{-1}) = \tau x y \tau^{-1} = f(xy) \checkmark$

- $f(x) = f(y) \Leftrightarrow \tau x \tau^{-1} = \tau y \tau^{-1}$

$\Leftrightarrow \tau^{-1}(\tau x \tau^{-1})\tau = \tau^{-1}(\tau y \tau^{-1})\tau \Leftrightarrow x = y$ Donc f injectif $\checkmark$

- $f(\tau x \tau^{-1}) = \tau^{-1}(\tau x \tau^{-1})\tau = x$ Donc f est surjectif. $\checkmark$

3b) $\forall x \in G$ $f^2(x) = f(f(x)) = f(\tau x \tau^{-1}) = \tau^2 x (\tau^{-1})^2$

$\tau = (12)$ Donc $\tau^2 = id$, $\tau^{-1} = (12)$ donc $(\tau^{-1})^2 = id$. Donc $f^2(x) = x \Rightarrow x \in H$

$H \subset G$ et $G \subset H \Rightarrow H = G$

3c) $S_3 = \{id, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$

$f(id) = id \Rightarrow id \in S_3$

$f((1\,2)) = \tau (1\,2)\, \tau^{-1} = (1\,2)(1\,2)(1\,2) = (1\,2) = (1\,2)^{-1} \Rightarrow (1\,2) \in S$

$f((2\,3)) = (1\,2)(2\,3)(1\,2) = (1\,3) \Rightarrow (1\,3) \notin S$

$f((1\,3)) = (1\,2)(1\,3)(1\,2) = (2\,3) \Rightarrow (2\,3) \notin S$

$f((1\,2\,3)) = (1\,2)(1\,2\,3)(1\,2) = (1\,3\,2) = (1\,2\,3)^{-1} \Rightarrow (1\,2\,3) \in S$

$f((1\,3\,2)) = (1\,2)(1\,3\,2)(1\,2) = (1\,2\,3) = (1\,3\,2)^{-1} \Rightarrow (1\,3\,2) \in S$

$S = \{id, (1\,2), (1\,2\,3), (1\,3\,2)\}$

3d) D'apres le thm de Lagrange si S est un ss-gpe de G, cardinal de S divise le cardinal de G. Mais $card(S) = 4 \nmid card(G) = 6$