

• $G = (\mathbb{Z}/22\mathbb{Z})^*$ groupe mult.

$$1. |G| = \varphi(22) = \varphi(2 \times 11) = \varphi(2) \varphi(11) \\ = 1 \times 10 = 10$$

$$2. \overline{7} \text{ g n rateur de } G \Leftrightarrow \langle \overline{7} \rangle = |G| \\ \Leftrightarrow \text{ord}(\overline{7}) = |G| = 10$$

• th (Lagrange) : $\text{ord}(\overline{7})$ divise 10
donc c'est 1, 2, 5 ou 10

$\overline{7}$ d'ordre 1 : non

$\overline{7}$ d'ordre 2 : $\overline{7}^2 = \overline{49} = \overline{5} \neq \overline{1}$ non

$\overline{7}$ d'ordre 5 : $\overline{7}^5 = (\overline{7}^2)^2 \overline{7} = (\overline{5})^2 \times \overline{7} \\ = \overline{3} \times \overline{7} = \overline{21} \neq \overline{1}$ non

donc $\overline{7}$ d'ordre 10 et c'est un g n rateur

3. à faire $\left[\begin{array}{l} G \text{ cyclique engendré par } g, \text{ abs } G \\ \text{ sous-groupes de } G \text{ sur } \langle g^a \rangle \text{ avec } a|10 \end{array} \right.$
- 4.

↳ Générateurs de $(\mathbb{Z}/22\mathbb{Z})^*$

$(\mathbb{Z}/22\mathbb{Z})^*$ est cyclique d'ordre 10

$$\text{donc } (\mathbb{Z}/22\mathbb{Z})^* \simeq \mathbb{Z}/10\mathbb{Z}$$

$$\overline{7}^a \longleftarrow \overline{a}$$

Donc le nombre de générateurs de G

$$= \text{nombre de générateurs de } \mathbb{Z}/10\mathbb{Z} = \varphi(10) = 4$$

↳ 1, 3, 7, 9 générateurs de $\mathbb{Z}/10\mathbb{Z}$

Conclusion: générateurs de $(\mathbb{Z}/22\mathbb{Z})^*$

$$\text{sur } \overline{7}, \overline{7}^3, \overline{7}^7, \overline{7}^9$$

5. $\text{Aut}(G)$?

$f \in \text{Aut}(G)$, g g  n  rateur de G ssi

$f(g)$ g  n  rateur de G .

g g  n  rateur de G

De plus, une fois connu $f(g)$, f est compl  tement

d  termin   : $\forall a \in G$, il existe $s \in \mathbb{Z}$ tel que $a = g^s$

$$\text{d'o   } \underbrace{f(a)} = f(g)^s$$

Si $g = \overline{7}$ et donc $f \in \text{Aut}(G)$ sont

d  termin  s par $f(\overline{7}) = \overline{7}, \overline{7}^3, \overline{7}^7, \overline{7}^9$
id

4 auto : f_1, f_3, f_7, f_9 avec $f_i(\overline{7}) = \overline{7}^i$

$$|\text{Aut}(G)| = 4$$

$\mathcal{H}$: A d'ordre 4 abs

$$A \simeq \mathbb{Z}/4\mathbb{Z} \text{ ou } A \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

6. Table de mult. de $\text{Aut}(G)$

0	f_1	f_3	f_7	f_9
f_1	f_1	f_3	f_7	f_9
f_3	f_3	f_9	f_1	f_7
f_7	f_7	f_1	f_9	f_3
f_9	f_9	f_7	f_3	f_1

21 42

$$21 \ 42 = \{0, 1, 2, 3\}$$

$\uparrow$ $\uparrow$ $\downarrow$
 ordre 1 ordre 2 ordre 4

$$f_3 \circ f_3(7) = f_3(7^3)$$

$$= (7^3)^3 = 7^9$$

$$f_3 \circ f_7(7) = f_3(7^7)$$

$$= 7^{21} = 7^1$$

$$f_a \circ f_b = f_{ab \pmod{6}}$$