

Groupe $(\mathbb{Z}/22\mathbb{Z})^*$

$$1. \quad |(\mathbb{Z}/22\mathbb{Z})^*| = \varphi(22) = \varphi(2 \times 11) \\ = \varphi(2)\varphi(11) = (2-1)(11-1) = 10$$

2. Montrer $\overline{7}$ est générateur de $(\mathbb{Z}/22\mathbb{Z})^*$

$\overline{7}$ est générateur si ordre $\overline{7} = 10$

$$\overline{7} \neq \overline{1} : \text{ordre} \neq 1 \quad \overline{7}^2 = \overline{49} = \overline{5} \neq \overline{1} :$$

Idee : Par le th. de Lagrange, l'ordre de $\overline{7}$ ordre $\neq 2$

en ~~1, 2, 5~~ ou 10

Il reste à montrer que l'ordre $\bar{7} \neq 5$

$$\begin{aligned}\text{On a } \bar{7}^5 &= \bar{7}^{2 \times 2 + 1} = (\bar{7}^2)^2 \bar{7} & \bar{7} \\ &= \bar{5}^2 \times \bar{7} = \bar{3} \times \bar{7} = \bar{21} \neq \bar{7}\end{aligned}$$

donc $\bar{7}$ n'est pas d'ordre 5, donc $\bar{7}$ est d'ordre 10

et c'est un générateur $\leadsto (\mathbb{Z}/22\mathbb{Z})^*$ est
cyclique

3. En exercice

$G = \langle g \rangle$ sous-groupes $\langle g^s \rangle$ avec $s|n$

$$(n=161)$$

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

On sait que $(\mathbb{Z}/22\mathbb{Z})^* \simeq \mathbb{Z}/10\mathbb{Z}$

et même $\mathbb{Z}/10\mathbb{Z} \rightarrow (\mathbb{Z}/22\mathbb{Z})^*$

$$\overline{a} \mapsto \overline{7}^a \quad \begin{array}{l} \text{--- mod } 10 \\ \text{--- mod } 22 \end{array}$$

est bien définie et c'est un isomorphisme

En particulier, $\overline{7}^a$ est un générateur

sn $\bar{a}$ est g n rateur de $\mathbb{Z}/10\mathbb{Z}$

ssi $\bar{a} = \bar{1}, \bar{3}, \bar{7}, \bar{9}$ (entier entre 0 et 9
premier avec 10)

G n rateurs de $(\mathbb{Z}/22\mathbb{Z})^*$: $\bar{7}, \bar{7}^3, \bar{7}^7, \bar{7}^9$

5. $\text{Aut}((\mathbb{Z}/22\mathbb{Z})^*)$

Proposition: Soit G un groupe cyclique engendr 
par g . Soit $f: G \rightarrow G$ un automorphisme

alors f est un automorphisme sur

$f(g)$ est un générateur. $\square$

$$f : \underbrace{(\mathbb{Z}/22\mathbb{Z})^*}_G \rightarrow (\mathbb{Z}/22\mathbb{Z})^* \text{ morphisme}$$

• f est complètement déterminé par $f(\bar{7})$:
En effet, soit $\bar{x} \in G$ alors il existe $a \in \mathbb{Z}$
tel que $\bar{x} = \bar{7}^a$ d'où $f(\bar{x}) = f(\bar{7}^a)$
 $= f(\bar{7})^a$