G cyclique d'ordre n

Soit $d \geq 1$. On note $N_G(d)$ le nombre d'éléments d'ordre d dans G.

- Si $d \nmid n$: alors $N_G(d) = 0$ [th. de Lagrange]
- Si $d | n$: On considère sans perte de généralité que $G = \mathbb{Z}/n\mathbb{Z}$

Pour $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$, l'ordre de $\bar{m}$ est $\frac{n}{(n,m)}$

Notons $n = de$, $\bar{m}$ est d'ordre d ssi $(n,m) = e$

$$N_G(d) = \#\{0 \leq m < n \mid (n,m) = e\}$$

Mais $(n,m) = (de, m) = e$ ssi $e | m$ et

$$(d, m/e) = 1 \hookrightarrow k = \frac{m}{e}$$

$$N_G(d) = \#\{0 \leq k < d \mid (d,k) = 1\}$$

$$= \phi(d) \leftarrow \text{ne dépend pas de } n$$

2. En déduire $\sum_{d|n} \phi(d) = n$

On note $U_n(d) = \{ \bar{m} \in \mathbb{Z}/n\mathbb{Z} \mid \bar{m} \text{ d'ordre } d \}$

← ens. vide

On a $U_n(d) = \emptyset$ si $d \nmid n$

$\# U_n(d) = \phi(d)$ si $d \mid n$

← union disjointe

donc $$\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d \mid n} U_n(d)$$

or $$\underbrace{|\mathbb{Z}/n\mathbb{Z}|}_{n} = \sum_{d \mid n} \phi(d)$$

p premier

p premier $(\mathbb{Z}/p\mathbb{Z})^*$ cyclique : $n = p-1$

$$\boxed{d \mid n : \# U_n(d) \leq \phi(d)}$$

$$p-1 = \sum_{d \mid n} \# U_n(d) \underset{=}{\leq} \sum_{d \mid n} \phi(d) = n = p-1$$

• $\mathrm{Aut}\left(\left(\mathbb{Z}/22\mathbb{Z}\right)^*\right)$ ≠ $G = \left(\mathbb{Z}/22\mathbb{Z}\right)^*$

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

$= (2-1)\times(11-1) = 10$ → ordres possibles : 1, 2, 5, 10

2. Montrer $\langle \bar{7} \rangle = G \iff \text{ordre}(\bar{7}) = 10$

$\bar{7}$ n'est pas d'ordre 1

$\bar{7}^2 = \overline{49} = \bar{5} \neq \bar{1}$ donc $\bar{7}$ n'est pas d'ordre 2

$\bar{7}^5 = \bar{7}\times\left(\bar{7}^2\right)^2 = \bar{7}\times\bar{5}^2 = \bar{7}\times\overline{25} = \bar{7}\times\bar{3}$

$= \overline{21} \neq \bar{1}$ donc $\bar{7}$ n'est pas d'ordre 5

$= \overline{-1}$

Conclusion : $\bar{7}$ est d'ordre 10

et donc G est cyclique avec $G = \langle \bar{7} \rangle$

3. $\varphi : \mathbb{Z}/10\mathbb{Z} \simeq G$

$t \longmapsto \bar{7}^t$

Sous-groupes de $\mathbb{Z}/10\mathbb{Z}$: 1 d'ordre 1 $\{e\}$
1 d'ordre 2
1 d'ordre 5
1 d'ordre 10 G

4. Générateurs de G

$g \in G$ disons $g = \bar{7}^t$

alors g est générateur ssi A est générateur
ssi A est inversible
ssi $t \in \{1, 3, 7, 9\} \subseteq \mathbb{Z}/10\mathbb{Z}$

donc les générateurs de $(\mathbb{Z}/22\mathbb{Z})^*$ sont

$\bar{7}^1 = \bar{7}$, $\bar{7}^3 = \overline{13}$, $\bar{7}^7 = \bar{7}^5 \times \bar{7}^2 = -\bar{1} \times \bar{5} = -\bar{5}$
$= \overline{17}$

$\bar{7}^9 = \bar{7}^7 \times \bar{7}^2 = -\bar{5} \times \bar{5} = -\overline{25} = -\bar{3} = \overline{15}$

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

$f \in \mathrm{Aut}((\mathbb{Z}/22\mathbb{Z})^*)$ alors $f_1(\bar{7}) = \bar{7}$ — $f = id$
ou
$f_3(\bar{7}) = \bar{7}^3$
ou
$f_7(\bar{7}) = \bar{7}^7$
ou
$f(\bar{7}) = \bar{7}^9$

Aut envoie générateur sur générateur

6. $|\mathrm{Aut}(G)| = 4$ $\qquad f_i(\bar{7}) = \bar{7}^i \quad i \in \{1,3,7,9\}$

th : groupe d'ordre 4 est iso. à $\mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Table de multiplication de $\mathrm{Aut}(G)$

$\circ$	f_1 0	f_3 1	f_7 3	f_9 2
f_1 0	f_1 0	f_3 1	f_7 3	f_9 2
f_3 1	f_3 1	f_9 2	f_1 0	f_7 3
f_7 3	f_7 3	f_1 0	f_9 2	f_3 1
f_9 2	f_9 2	f_7 3	f_3 1	f_1 0

$$(f_3 \circ f_3)(\bar{7}) = f_3(f_3(7)) = f_3(7^3) = f_3(7)^3 = (7^3)^3 = 7^9 = f_9(7)$$

$$f_7(f_3(\bar{7})) = f_7(\bar{7})^3 = \bar{7}^{21} = \bar{7}^1 = f_1(\bar{7})$$

modulo

donc $s : \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(G)$

$s(0) = f_1 \quad s(1) = f_3 \quad s(2) = f_9 \quad s(3) = f_7$

est un isomorphisme donc $G \simeq \mathbb{Z}/4\mathbb{Z}$