

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

① Posons $G = (\mathbb{Z}/22\mathbb{Z})^*$

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

$$(\mathbb{Z}/22\mathbb{Z})^* = \{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$$

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

c'est-à-dire ordre $7 = |G| = 10$

Par le théorème de Lagrange, l'ordre de 7

divise 10, donc c'est 1, 2, 5 ou 10.

On a ordre $7 \neq 1$ car $7 \neq 1$

or $7^2 = 49 = 5 \neq 1$ donc ordre $7 \neq 2$

or $7^5 = 7 \times (7^2)^2 = 7 \times 5^2 = 7 \times 7^2 = 7 \times 5$

$= \overline{21}$ et d'un ordre $\overline{7} \neq 5$
 $(= \overline{-1})$
 donc ordre $\overline{7} = 10$ et donc $\overline{7}$ est générateur

et G est cyclique engendré par $\overline{7}$

3. —

4. Puisque G est cyclique d'ordre 10,

$$\text{on a } G \simeq \mathbb{Z}/10\mathbb{Z}$$

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

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

$$\text{générateur} \longleftrightarrow \text{générateur}$$

Générateurs de $\mathbb{Z}/10\mathbb{Z}$: m avec $(m, 10) = 1$

$$\hookrightarrow \text{nombre de générateurs } \varphi(10) = \varphi(2) \varphi(5)$$

$$= (2-1)(5-1) = 4$$

$$\hookrightarrow (\mathbb{Z}/10\mathbb{Z})^* = \{ \overline{1}, \overline{3}, \overline{7}, \overline{9} \}$$

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

$$\bar{7}, \bar{7}^3, \bar{7}^7 \text{ et } \bar{7}^9$$

5. Automorphismes de $(\mathbb{Z}/22\mathbb{Z})^* \stackrel{G}{=}$

$f \in \text{Aut}(G)$: f est complètement déterminé par $f(\bar{7})$

En effet, soit $g \in G$, il existe $s \in \mathbb{Z}$ tel que $g = \bar{7}^s$ et donc $f(g) = f(\bar{7}^s) = f(\bar{7})^s$

et ainsi $f(\bar{7})$ est forcément un générateur

Car un isomorphisme conserve l'ordre.

Donc on a 4 éléments dans $\text{Aut}(G)$

$$f_1(\bar{7}) = \bar{7}, \quad f_3(\bar{7}) = \bar{7}^3$$

$$f_7(\bar{7}) = \bar{7}^7 \quad \text{et} \quad f_9(\bar{7}) = \bar{7}^9$$

done $|Aut(G)| = 4.$

6.

	$f_1 \bar{0}$	$f_3 \bar{1}$	$f_7 \bar{3}$	$f_5 \bar{2}$
$f_1 \bar{0}$	$f_1 \bar{0}$	$f_3 \bar{1}$	$f_7 \bar{3}$	$f_5 \bar{2}$
$f_3 \bar{1}$	$f_3 \bar{1}$	$f_5 \bar{2}$	$f_1 \bar{0}$	$f_7 \bar{3}$
$f_7 \bar{3}$	$f_7 \bar{3}$	$f_1 \bar{0}$	$f_5 \bar{2}$	$f_3 \bar{1}$
$f_5 \bar{2}$	$f_5 \bar{2}$	$f_7 \bar{3}$	$f_3 \bar{1}$	$f_1 \bar{0}$

$$f_1(f_1(\bar{7})) = f_1(\bar{7}) = \bar{7}$$

$$\begin{aligned} f_3(f_3(\bar{7})) &= f_3(\bar{7})^3 \\ &= (\bar{7}^3) = \bar{7}^9 \end{aligned}$$

$$f_5(f_5(\bar{7})) = \bar{7}^{ab}$$

done $Aut(G) \cong \mathbb{Z}/4\mathbb{Z}$