Calculer $\mathrm{Aut}\left((\mathbb{Z}/22\mathbb{Z})^*\right)$
$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \shortparallel$ G

1. $|G| = \varphi(22)$

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

2. Montrer que $G = \langle \bar{7} \rangle$

$G = \langle \bar{7} \rangle \iff$ ordre $\bar{7} = 10$

$\iff$ ordre $\bar{7} \neq 1, 2$ ou 5

ordre $\bar{7} \neq 1$ car $\bar{7} \neq \bar{1}$

ordre $\bar{7} \neq 2$ car $\bar{7}^2 = \bar{5} \neq \bar{1}$ $\quad (7^2 = 49 \equiv 5\ (22))$

ordre $\bar{7} \neq 5$ car $\bar{7}^5 = (\bar{7}^2)^2 \times \bar{7} = \bar{3}\times\bar{7} = \overline{21} \neq \bar{1}$
$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \shortparallel$
$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \overline{-1}$

donc ordre $\bar{7}$ est 10.

3. Les sous-groupes de $(\mathbb{Z}/22\mathbb{Z})^*$?

Rq : Si G est monogène et H sous-groupe de G, alors H est monogène

Les sous-groupes de $(\mathbb{Z}/22\mathbb{Z})^*$ sont cycliques.

Soit $d \mid 10$. Puisqu'il existe $\bar{a} \in G$ d'ordre d, il existe (au moins) un sous-groupe (cyclique) d'ordre d, celui engendré par $\bar{a}$. Ce sous-groupe est unique.

Th : G cyclique d'ordre n. Pour tout $d \mid n$, il existe un unique sous-groupe de G d'ordre d.

Sous-groupes de $(\mathbb{Z}/22\mathbb{Z})^*$

ordre 1 $\{\bar{1}\}$

ordre 2 $\{\bar{1}, -\bar{1}\}$

ordre 5 $\langle \bar{7}^2 \rangle$

ordre 10 : G

$\langle g^{n/d} \rangle$ avec g générateur de G.

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

$G = \{ \bar{7}^a : 0 \le a \le 9 \}$

$$\text{ordre } \bar{7}^a = \frac{10}{PGCD(10,a)} = 10 \text{ si } PGCD(10,a) = 1$$

$\rightsquigarrow a = 1, 3, 7, 9$ générateurs $\bar{7}, \bar{7}^3, \bar{7}^7, \bar{7}^9$

Remarque : $\bar{7}^{10} = \bar{1}$ or donc $\forall a \in \mathbb{Z}$,

$$\bar{7}^a = \bar{7}^r \text{ avec } a \equiv r \pmod{10}$$

5. Déterminer $Aut(G)$?

$\varphi : G \to G$ morphisme

$\varphi(\bar{7}) = \bar{7}^a$ pour $0 \le a \le 9$

[Remarque : cela détermine totalement φ puisque

$$\varphi(\bar{7}^c) = (\bar{7}^a)^c = \bar{7}^{ac}$$
]

φ est un automorphisme $\begin{cases} \text{ssi } \varphi \text{ est injectif} \\ \text{ssi } \varphi \text{ est surjectif} \\ \text{ssi } \varphi(\bar{7}) \text{ est générateur} \end{cases}$

donc $a = 1, 3, 7, 9$

On pose $\varphi_a(\bar{7}) = \bar{7}^a$

On a $\mathrm{Aut}\left(\mathbb{Z}/22\mathbb{Z}\right)^* = \{ \varphi_1^{\,1d}, \varphi_3, \varphi_7, \varphi_9 \}$

6. Multiplication $\mathrm{Aut}(G)$

$\circ$ ← composition

$\circ$	φ_1 0	φ_3 1	φ_7 3	φ_9 2
φ_1 0	φ_1^0	φ_3^1	φ_7^3	φ_9^2
φ_3 1	φ_3^1	φ_9^2	φ_1^0	φ_7^3
φ_7 3	φ_7^3	φ_1^0	φ_9^2	φ_3^1
φ_9 2	φ_9^2	φ_7^3	φ_3^1	φ_1^0

$\mathbb{Z}/4\mathbb{Z}$

mêmes tables !

$$(\varphi_3 \circ \varphi_3)(\bar{7}) = \varphi_3(\bar{7}^3) = (\bar{7}^3)^3 = \bar{7}^9$$

$$(\varphi_3 \circ \varphi_7)(\mathbb{F}) = \varphi_3(\mathbb{F}^7) = \mathbb{F}^{21} = \mathbb{F}$$

$$\rightsquigarrow \quad \mathrm{Aut}\left((\mathbb{Z}/22\mathbb{Z})^*\right) \simeq \mathbb{Z}/4\mathbb{Z}$$