G cyclique = monogène + fini

monogène : $\exists g \in G$ tel que $G = \langle g \rangle$

$$\begin{aligned} \phi : \mathbb{Z} &\to G \quad \text{morphisme surj} \\ a &\mapsto g^a \end{aligned}$$

cyclique : $|G|$ fini, disons $n = |G|$

On a $|G| = |\langle g \rangle| = \mathrm{ord}(g)$

$a \in \operatorname{Ker} \phi \iff \phi(a) = e \iff g^a = e$

$g^a = g^b \iff a \equiv b \pmod n$ $\qquad \iff n \mid a$

$\iff a \in n\mathbb{Z}$

d'où $\operatorname{Ker} \phi = n\mathbb{Z}$

et par factorisation $\mathbb{Z}/n\mathbb{Z} \simeq G$

À iso. près, il existe un unique groupe

cyclique d'ordre n.

$\mathbb{Z}/10\mathbb{Z}$ groupe cyclique d'ordre 10

$$(\mathbb{Z}/10\mathbb{Z})^* = \{\cancel{\bar{0}}, \bar{1}, \cancel{\bar{2}}, \bar{3}, \cancel{\bar{4}}, \cancel{\bar{5}}, \cancel{\bar{6}}, \bar{7}, \cancel{\bar{8}}, \bar{9}\}$$
$$= \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$$

$\bar{3}$ est un générateur de $\mathbb{Z}/10\mathbb{Z}$

$0 \times \bar{3} = \bar{0}$, $1 \times \bar{3} = \bar{3}$, $2 \times \bar{3} = \bar{6}$, $3 \times \bar{3} = \bar{9}$
$4 \times \bar{3} = \bar{2}, \ldots$

Nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$

$= |(\mathbb{Z}/n\mathbb{Z})^*| = \underline{\varphi(n) \text{ Fonction d'Euler}}$

<u>Théorème</u> :

- p premier $\varphi(p) = p-1$
- —, $e \geq 1$: $\varphi(p^e) = p^{e-1}(p-1)$
- a et $b \geq 1$ premiers entre eux : $\varphi(ab) = \varphi(a) \times \varphi(b)$
- $n = p_1^{e_1} \dots p_t^{e_t}$ factorisation

$$\varphi(n) = p_1^{e_1-1} \dots p_t^{e_t-1} (p_1-1) \dots (p_t-1)$$

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

premiers divisant n

$$\varphi(10) = 10 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right)$$

$$= \cancel{10} \times \frac{1}{\cancel{2}} \times \frac{4}{\cancel{5}} = 4$$