$g \in G$ d'<u>ordre</u> n

1) $\langle g \rangle = \{ g^m : m \in \mathbb{Z} \}$

- c'est un sous-groupe
- il contient $\langle g \rangle$

2) $m = qn + r$ div. euclidienne $0 \leq r < n$

$m \in \mathbb{Z}$

$$g^m = \underbrace{(\underbrace{g^n}_{e})^q}_{e} \cdot g^r \text{ d'où } g^m = g^r$$

$$\langle g \rangle \subseteq \{ g^r : 0 \leq r < n \}$$

3) il reste à montrer que les g^r $0 \leq r < n$, sont tous distincts.

Sinon $g^i = g^j$ $\quad 0 \leq i < j < n$

d'où $g^{j-i} = e$ avec $\underline{0} \leq j-i < n$

donc $j = i$ #

par minimalité de l'ordre