Déf. p premier p-groupe ~~est~~ un groupe fini d'ordre p^e $e \geq 1$

1. G p-groupe : $Z(G) \neq \{e\}$

!! G agit sur X, $X^G = \{x \in X \mid \forall g \in G, g \cdot x = x\}$

Montrer
$$\mathrm{card}(X) \equiv \mathrm{card}(X^G) \pmod p$$

On a
$$\mathrm{card}(X) = \sum_{\Omega \in X/G} \mathrm{card}(\Omega)$$

$$= \sum_{\substack{\Omega \in X/G \\ \mathrm{card}(\Omega)=1}} \mathrm{card}(\Omega) + \underbrace{\sum_{\substack{\Omega \in X/G \\ \mathrm{card}(\Omega)\neq 1}} \mathrm{card}(\Omega)}$$

Soit $\Omega \in X/G$ avec $\mathrm{card}(\Omega) \neq 1$, on a

$\mathrm{card}(\Omega) \mid |G|$ d'où $\mathrm{card}(\Omega) \equiv 0 \pmod p$

puissance de p

Si $\mathrm{card}(\Omega) = 1$ alors $\Omega = \{x\}$ et $\forall g \in G,\ g \cdot x = x$

ou encore $x \in X^G$

d'où
$$\mathrm{card}\, X \equiv \sum_{x \in X^G} 1 \pmod p$$
$$\equiv \mathrm{card}(X^G) \pmod p$$

1.2 $Z(G) = \{ c \in G \mid \forall g \in G \ \ cg = gc \}$

$$cg = gc \Leftrightarrow cgc^{-1} = g$$

conjugaison par c

On fait agir G sur lui-même par conjugaison :

$g \in G$, $x \in \boxed{G = X}$

$$g \cdot x = gxg^{-1}$$
$$g \cdot (g' \cdot x) = (gg') \cdot x \quad \text{(à faire)}$$

$$X^G = \{ x \in G \text{ tel que } \forall g \in G,\ g \cdot x = x \}$$

$= \{x \in G \text{ tel que } \forall g \in G,\ gxg^{-1} = x\}$

$gx = xg$

$= Z(G)$

D'où par la question 1.1,

$$|G| \equiv |Z(G)| \pmod p$$

donc $|Z(G)| \equiv 0 \pmod p$

mais $|Z(G)| \geq 1$ d'où $|Z(G)| \geq p \geq 2$

et donc $Z(G) \neq \{e\}$

---

2. G fini avec $G/Z(G)$ cyclique

Montrer G abélien

d'ordre n

$$G/Z(G) = \langle \bar{g} \rangle = \{\bar{e}, \bar{g}, \dots, \bar{g}^{n-1}\}$$

$\bar{e} = Z(G)$ $\qquad \bar{g}^i = g^i Z(G)$

Soient $a, b \in G$, alors il existe $i \in \{0, \dots, n-1\}$ et $c \in Z(G)$ tel que $a = g^i c$

De même, il existe j et $d \in Z(G)$ tel que $b = g^j d$.

$g^{i+j} = g^j g^i$

On calcule $ab = g^i c g^j d = g^i g^j c d$ $\quad c \in Z(G)$

$= g^j g^i c d = g^j d g^i c = ba$.

car $d \in Z(G)$

Donc G est abélien.

Application : p premier G d'ordre p^2

Résultat : G est abélien :

On considère $Z(G)$. On a $Z(G) \neq \{e\}$

d'où $|Z(G)| = p$ ou p^2 (divise $|G| = p^2$)

Si $|Z(G)| = p^2$ alors $Z(G) = G$ et G abélien

Si $|Z(G)| = p$ alors $G/Z(G)$ groupe d'ordre $\frac{p^2}{p} = p$

Th : Un groupe d'ordre p (premier) est cyclique

Preuve : Soit g avec $g \neq e$ alors l'ordre de g est p

donc g est un générateur. $\square$

Donc $G/Z(G)$ cyclique donc G abélien

Un groupe d'ordre p^2 est abélien et on a

$G \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$