p premier, G p-groupe : $\exists t \geq 1$, $|G| = p^t$

(1) Montrer que $Z(G) \neq \{e\}$

$\left\| \begin{array}{l} e.x = x \ \forall x \\ g.g'.x = gg'.x \end{array} \right.$

1.1 $G \circlearrowright X$ fini $\quad X^G = \{x \in X \text{ tq } \forall g \in G,\ g.x = x\}$

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

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

mais on sait $\forall \Omega \in X/G$, $\operatorname{card}(\Omega) \mid |G| = p^t$

donc : $\operatorname{card}(\Omega) = 1$ ou $p \mid \operatorname{card}(\Omega)$

($\operatorname{card}(\Omega) = p^s$ avec $s \geq 1$)

donc $\operatorname{card}(X) \equiv \sum_{\Omega \in X/G} \operatorname{card}(\Omega) \pmod p$

$\operatorname{card}|\Omega| = 1$: $\operatorname{card}(\Omega) = 1$

$\equiv \operatorname{card}\{\Omega \in X/G \text{ avec } \operatorname{card}(\Omega) = 1\} \pmod p$

On a, pour $x \in X$, $\operatorname{card}(\Omega_x) = 1$ ssi $\forall g \in G\ g.x = x$

($\Leftrightarrow \Omega_x = \{x\}$) ssi $x \in X^G$

d'où $\text{card}\{\Omega \in X/G,\ \text{card}(\Omega)=1\} = \text{card}\, X^G$.

donc $\text{card}(X) \equiv \text{card}(X^G) \pmod p$.

1.2. On prend $X = G$ par $g \in G, x \in G$

on pose $g \cdot x = gxg^{-1} \in X = G$

On a $X^G = \{x \in G \text{ tq } \forall g \in G,\ g \cdot x = x\}$

$= \{\text{---------},\ gxg^{-1} = x\}$

$gx = xg$

$= Z(G)$

Donc par la question précédente :

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

mais $|G| \equiv 0 \pmod p$ d'où $p \mid |Z(G)| \geq 1$

d'où $|Z(G)| \geq p$ et donc $Z(G) \neq \{e\}$

2. Soit G groupe fini tel que $G/Z(G)$ cyclique.

Alors G est abélien :

Il existe $\gamma \in G$ tel que $G/Z(G) = \langle \bar{\gamma} \rangle$ (n)

$\bar{\gamma} = \gamma Z(G)$

On montre que G est abélien : $\forall x, y \in G$,

$\bar{x} = \bar{\gamma}^s$ pour $s \in \mathbb{Z}$

$x = z\gamma^s$ $z \in Z(G)$

$\bar{y} = \bar{\gamma}^t$ pour $t \in \mathbb{Z}$

$y = z'\gamma^t$ $z' \in Z(G)$

On a $xy = yx$.

On calcule $xy = z\gamma^s z'\gamma^t$ ($z' \in Z(G)$)

$= zz'\gamma^{s+t} = z'z\gamma^{s+t}$ ($zz' = z'z$, $s+t = t+s$)

$= z'z\gamma^t\gamma^s = z'\gamma^t z\gamma^s = yx$ ($z \in Z(G)$)

Donc G est abélien.

Application : G d'ordre p^2. On montre que G est abélien : Supposons le contraire

alors $|Z(G)| = p$ et donc $|G/Z(G)| = p$

d'où $\boxed{G/Z(G) \text{ cyclique}}$ donc G est abélien #

par ce qui précède

Théorème : G groupe abélien fini d'ordre $n \geq 2$

Alors il existe $s \geq 1$, des entiers $a_1, \dots, a_s \geq 2$ vérifiant $a_{i+1} | a_i$ pour $1 \leq i \leq s-1$ tels que

$$G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \dots \times \mathbb{Z}/a_s\mathbb{Z}$$

De plus, $a_1 \cdots a_s = n$

et les $a_1, \dots, a_s$ sont uniques

Ici $n = p^2$: $a_1 = p^2$

$a_1 = a_2 = p$

G d'ordre $p^2 \Rightarrow G \simeq \mathbb{Z}/p^2\mathbb{Z}$

$G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$