p premier

p-Groupe = groupe d'ordre p^e avec $e \geq 1$

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

1.1. X ensemble fini

$G \circlearrowleft X$

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

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

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

et pour $\Omega \in X/G$ (orbite), on sait que

$\mathrm{card}(\Omega) \mid |G|$ d'où $\mathrm{card}(\Omega) = 1$

ou $\mathrm{card}(\Omega) = p^f$ (avec $f \leq 1$) et dans ce

cas $\mathrm{card}(\Omega) \equiv 0 \ (p)$ d'où

$$\mathrm{card}(X) \equiv \sum_{\substack{\Omega \in X/G \\ \mathrm{card}(\Omega) = 1}} 1 \pmod p$$

$$\equiv \mathrm{card}\{\Omega \in X/G \mid \mathrm{card}(\Omega) = 1\} \pmod p$$

Soit $\Omega \in X/G$, et soit $x \in \Omega$,

on a $\mathrm{card}(\Omega) = 1 \Leftrightarrow \Omega = \{x\}$

$\Leftrightarrow \forall g \in G,\ g \cdot x = x$

$\Leftrightarrow x \in X^G$

d'où $\mathrm{card}\{\Omega \text{ avec } \mathrm{card}(\Omega) = 1\} = \mathrm{card}\, X^G$

et on a bien $\mathrm{card}(X) \equiv \mathrm{card}(X^G) \pmod p$.

1.2 On fait agir G sur lui-même $X = G$

généralement $x \in Z(G) \Leftrightarrow \forall g \in G,\ gxg^{-1} = x$
$\Updownarrow$
$gx = xg$

Donc on fait agir G sur lui-même
par conjugaison : $g \cdot x = gxg^{-1}$ pour $g \in G, x \in G$
Alors $Z(G) = X^G$ avec $X = G$
et donc $|Z(G)| \equiv |G| \pmod p$ par 1.1
mais $|G| \equiv 0\ (p)$ car G p-groupe
donc $|Z(G)| \equiv 0\ (p)$

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

2. G groupe fini avec $G/Z(G)$ est cyclique.
(Remarque : $Z(G) \triangleleft G$)
Montrer G est abélien

On pose $G/Z(G) = \langle \bar{a} \rangle$ avec $a \in G$
$\bar{a} = aZ(G)$

Soient $g, h \in G$, on a $\bar{g} = \bar{a}^s$ pour $s \in \mathbb{Z}$
donc $g = a^s z$ avec $z \in Z(G)$
De même, $h = a^t w$ avec $t \in \mathbb{Z}, w \in Z(G)$
On calcule $gh = a^s z a^t w = a^s a^t z w$
car $z \in Z(G)$
$= a^t a^s z w$ car $a^s a^t = a^{s+t} = a^t a^s$
$= a^t w a^s z$ car $w \in Z(G)$
$= hg$
d'où G est abélien

p premier, $|G| = p^2$

- G est abélien : sinon $|Z(G)| = p$ d'où

$$\left|G/Z(G)\right| = p^2/p = p \quad \text{donc est cyclique}$$

or G est abélien #

- Deux cas possibles:
  - G possède un elt d'ordre p^2 donc G cyclique alors $G \simeq \mathbb{Z}/p^2\mathbb{Z}$
  - tous les elts $\neq e$ de G sont d'ordre p alors $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

G groupe fini, H sous groupe

indice de H dans $G = (G:H) = [G:H]$

$$= |G|/|H| \in \mathbb{N}$$

1. H d'indice 2 dans G.

Montrer $H \triangleleft G$

On a $H \triangleleft G \iff \forall g \in G, gHg^{-1} = H \iff \forall g, gH = Hg$

$(\iff \forall g \in G, gHg^{-1} \subset H)$

Soit $g \in G$: • $g \in H$: $gH = H$ et $Hg = H$

d'où $gH = Hg$

- $g \notin H$ alors $G = H \cup gH$ car $|G/H| = 2$

$= H \cup Hg$ (unions disjointes)

d'où $gH = G \setminus H = Hg$

et $H \triangleleft G$.

2. Supposons que H est d'indice p avec p plus petit premier diviseur $|G|$. On montre $H \trianglelefteq G$

On fait agir G sur G/H par multi. à gauche :

$g \in G$, $aH \in G/H$ $\quad g \cdot aH = gaH$

2.1 Montrer que cette action est transitive :

$\forall aH, bH \in G/H$, il existe $g \in G$ tel que

$$g \cdot aH = bH$$

On prend $g = ba^{-1}$

2.2 Soit K noyau de l'action. Montrer $K \subseteq H$

Soit $g \in K$, on a $\forall aH \in G/H$, $g \cdot aH = aH$

par exemple pour la classe triviale $H \in G/H$, on trouve $g \cdot H = gH = H$ d'où $g \in H$ et $K \subseteq H$

2.3 Montrer G/K iso. à un sous-groupe de S_p

On numérote les elts de $G/H = \{C_1, \dots, C_p\}$

et on définit $\pi : G \to S_p$

$$g \mapsto \pi_g \quad \text{où } \forall i \quad g \cdot C_i = C_{\pi_g(i)}$$

Alors π est un morphisme de groupe dont le noyau est K (noyau de l'action)

Donc on a $G/K \simeq \mathrm{Im}(\pi) \subseteq S_p$

2.4. En déduire $H = K$

On sait que $K \subseteq H$, G/H de cardinal p

et $G/K \simeq$ sous-groupe de S_p

On écrit $\frac{|G|}{|H|} = p \quad \frac{|G|}{|K|} \mid p!$ et $|K| \mid |H|$

Notons $h = |H|$, $|G| = ph$ et $k = |K|$ et $h = kt$

d'où $\frac{|G|}{|K|} = \frac{ph}{k} = pt$ multiple de p

mais $\frac{|G|}{|K|} \mid p! = 1 \times 2 \times \dots \times (p-1) \times p$.

d'où $t \mid (p-1)!$ mais $t \mid |G|$ et

p est le plus petit premier diviseur $|G|$

donc $t = 1$ et $H = K$

et comme $K \trianglelefteq G$ (noyau), on a bien $H \trianglelefteq G$.