

Théorème de Cauchy et premier Théorème de Sylow

Recapitulés: 109, 190, 107, 103, 121

Théorème (de Cauchy) [VLM] p72

Soit G un groupe fini d'ordre divisible par p premier.
Alors il existe un élément d'ordre p dans G .

Preuve:

On va poser multiples objets puis en déduire le résultat.

On pose $G^p = \{(g_1, \dots, g_p) : g_1, \dots, g_p \in G\}$ les p -uplets d'éléments de G .

On considère l'action de G_p sur G^p .

On pose $H = \langle (1, 2, \dots, p) \rangle$ et on considère l'action de H sur G^p comme restriction de l'action de G_p sur G^p . (On considère $H \hookrightarrow G_p \rightarrow G(G^p)$.)

On pose $X = \{(g_1, \dots, g_p) \in G^p \mid g_1 \dots g_p = e\}$ et on remarque que pour $g_1, \dots, g_p \in G$, si $g_1 \dots g_p = e$ alors $g_p = (g_1 \dots g_{p-1})^{-1}$ puis $g_p g_1 \dots g_{p-1} = e$, ce qui nous donne que $|X| = |G|^{p-1}$ (On a $|G|$ choix pour g_1 , $|G|$ choix pour $g_2, \dots, |G|$ choix pour g_{p-1} , puis $g_p = (g_1 \dots g_{p-1})^{-1}$).

On considère X^H et on remarque que ses éléments sont de la forme $(g, \dots, g)$ avec $g \in G$.

On invoque la formule $|X^H| = |X| [p] = |G|^{p-1} [p] = 0 [p]$.

On remarque que $e \in X^H$, donc $|X^H| \geq 2$, donc il existe un élément d'ordre p dans X^H . Notons le $(g, \dots, g) \in X^H$, $g \in G \setminus \{e\}$.

On conclut avec $g^p = e$ et $o(g) \mid p$ et $o(g) \neq 1$, donc $o(g) = p$.

Théorème (Premier Théorème de Sylow) [GOU] p44

Soit G un groupe fini d'ordre n .

Si p est premier, $\alpha \in \mathbb{N}$ tq $p^\alpha \mid n$, alors il existe un n -groupe de G d'ordre p^α .

Preuve:

On raisonne par récurrence sur $n = \text{Card}(G)$.

S: $n=1$, c'est trivial.

Supposons le théorème vrai pour tous groupes d'ordre $< n$ ($n > 1$).

Si $\alpha = 0$, il n'y a rien à faire.

Supp. $\alpha \geq 1$.

On considère l'action de G_p sur G_p par permutation des coordonnées.

On note Ω' l'ensemble des classes de conjugaison non réduites à un élément.
On a alors $(\Omega \cup \Omega')$ une famille de sous-groupes de G telle que

$$\text{Card}(G) = n = \text{Card}(\Omega(G)) + \sum_{\omega \in \Omega'} \frac{n}{\text{Card}(\omega)}$$

(En fait pour $w \in \Omega'$, $S_w = \text{stab}(x)$ pour un $x \in w$.)

On a alors deux cas:

→ S'il existe $w \in \Omega'$ tel que $p^x \nmid \text{card}(S_w)$

en si $\Rightarrow$
 $\text{card}(S_w) = h$,
 $S_w = Z(G)$.
et on arrive
au cas 2.

Puisque $\text{card}(S_w) < h$, il existe par HR $H < S_w$ d'ordre p^x .

On a alors $H < G$ d'ordre p^x .

→ Si pour tout $w \in \Omega'$, $p^x \nmid \text{card}(S_w)$

Tout d'abord, $\forall w \in \Omega'$, $p \mid \frac{h}{\text{card}(S_w)}$.

On a $p \mid h$ par hypothèse.

Donc $p \mid \text{card}(Z(G))$

Par le théorème de Cauchy, il existe $C < Z(G)$ d'ordre p et puisque $C \leq Z(G)$,
 $C \trianglelefteq G$.

Cela nous permet de poser $\pi: G \xrightarrow[\text{surjectif}]{\text{homomorphisme}} G/C$

On a alors $\text{card}(G/C) = \frac{h}{p} < h$ et $p^{x-1} \nmid \text{card}(G/C)$ donc par HR, il existe $H' < G/C$ d'ordre p^{x-1} .

On pose alors $H = \pi^{-1}(H')$.

Alors $H < G$ et $\text{card}(H) = \text{card}(C) \cdot \text{card}(H') = p^x$.

□