Théorèmes de Sylow

On considère un nombre premier p et un groupe fini G. On note $\alpha = \nu_p(|G|)$ et on appelle alors *p-sylow* de G un sous-groupe de G, H tel que:

$$|H| = p^\alpha$$

On a alors les trois théorèmes suivants:

Théorème 1:

G admet un p-sylow.

Théorème 2:

Les p-sylow de G sont conjugués et si H est un p-sous-groupe de G, on dipose de S un p-sylow de G tel que $H \subseteq S$.

Théorème 3:

Si on note $|G| = p^\alpha s$ et n_p le nombre de p-sylow de G alors:

$$n_p \mid s \qquad n_p \equiv 1[p]$$

Lemme :

Soit $n \in \mathbb{N}^*$ et $p \in \mathcal{P}$, alors $\mathrm{GL}_n(\mathbb{F}_p)$ admet un p-sylow.

Preuve :

On remarque que $\left|\mathrm{GL}_n(\mathbb{F}_p)\right| = (p^n - 1)(p^n - p)...(p^n - p^{n-1}) = sp^{\frac{n(n-1)}{2}}$ avec $s \wedge p = 1$ (on compte les bases de $\mathbb{F}_p^n$).

Si l'on note G l'ensemble des matrices triangulaire supérieur avec des 1 sur la diagonale alors:

$$\begin{aligned} (i) &\quad G \text{ est un sous-groupe de } \mathrm{GL}_n(\mathbb{F}_p) \\ (ii) &\quad |G| = p^{\frac{n(n-1)}{2}} \end{aligned}$$

Soit :

$$G \text{ est un } p \text{-sylow de } \mathrm{GL}_n(\mathbb{F}_p)$$

□

Lemme :

Soit G un groupe fini, p un nombre premier et supposons que $S \subseteq G$ est un p-sylow. Alors si H est un sous-groupe de G, on dipose de $a \in G$ tel que:

$$H \cap aSa^{-1} \text{ est un } p \text{ -sylow de } H$$

Preuve :

On note maintenant S un p-sylow de G.

G agit par translation à gauche sur G/S: pour $g \in G$ et $aS \in G/S$,

$$g \cdot aS := gaS$$

On remarque alors que, pour $aS \in G/S$, $\mathrm{Stab}_G(aS) = aSa^{-1}$:

Soit $g \in \mathrm{Stab}_G(aS)$, on a donc $gaS = aS$, ainsi $gae = ah$ avec $h \in S$. Par suite, $g = aha^{-1} \in aSa^{-1}$. Finalement, $\mathrm{Stab}_G(aS) \subseteq aSa^{-1}$. L'inclusion réciproque est évidente. ■

On remarque que l'action de G sur G/S se traduit en une action de H sur G/S par restriction. Le stabilisateur de aS sous l'action de H est donc

$$H_a := \mathrm{Stab}_H(aS) = H \cap aSa^{-1}$$

Pour $aS \in G/S$, H_a est un sous-groupe de aSa^{-1}, par le theorème de Lagrange, car aSa^{-1} est un p-groupe, H_a aussi.

Si l'on note maintenant pour $aS \in G/S$, $\omega(aS)$ l'orbite de aS sous l'action de H, alors $|\omega(aS)| = |H/H_a|$.

Si l'on note $E \subseteq G$ un ensemble tel que :

$$G/S = \bigsqcup_{a \in E} \omega(aS)$$

Alors:

$$|G/S| = \sum_{a \in E} |H/H_a|$$

Ainsi, comme S est un p-sylow de G, $p \nmid |G/S|$, par suite on dipose d'un $a \in E$ tel que $p \nmid |H/H_a|$ et alors:

$$H_a = H \cap aSa^{-1} \text{ est un } p\text{-sylow de } H$$

□

Preuve :*(Du théorème 1)*

Soit G un groupe fini et $p \in \mathcal{P}$ tel que $n := |G| = p^\alpha s$ avec $p \wedge s = 1$

En remarquant que l'action de G sur lui même par translation à gauche (i.e. $g \cdot a = ga$) est simplement transitive, on a que G s'injecte dans $\mathfrak{S}_n$ (c'est le *théorème de Cayley*).

Aussi, en considérant:

$$\begin{aligned} \phi : \mathfrak{S}_n &\hookrightarrow \mathrm{GL}_n(\mathbb{F}_p) \\ \sigma &\longmapsto \left(\delta_{i,\sigma(j)}\right)_{i,j\in[\![1,n]\!]} \end{aligned}$$

$\mathfrak{S}_n$ s'injecte dans $\mathrm{GL}_n(\mathbb{F}_p)$, par suite, comme $\mathrm{GL}_n(\mathbb{F}_p)$ admet un p-sylow il en va de même pour $\mathfrak{S}_n$ puis G.

$\square$

Preuve :*(Du thèorème 2)*

Soit H un p-sous-groupe de G, on note S un p-sylow de G. On dispose donc de $a \in G$ tel que $H \cap aSa^{-1}$ est un p-sylow de H mais comme H est un p-groupe,

$$H \cap aSa^{-1} = H$$

Soit:

$$H \subseteq aSa^{-1}$$

Si de plus H est un p-sylow, alors, par égalité des cardinaux,

$$H = aSa^{-1}$$

$\square$

Corrolaire :

Si $S \lhd G$ est un p-sylow de G alors il est l'unique p-sylow de G.

Preuve :

Soit H un p-sylow de G. On dipose donc de $a \in G$ tel que $H = aSa^{-1}$, or $S \lhd G$ donc $aSa^{-1} = S$ soit finalement:

$$H = S$$

$\square$

Corrolaire :

Si l'on note n_p le nombre de p-sylow de G, alors:

$$n_p \mid |G|$$

Preuve :

On note X l'ensemble des sous groupe de G, on fait agir G sur X par conjugaison, si l'on note alors S un p-sylow de G, par le théorème 2, $\omega(S)$ est exactement l'ensemble des p-sylow de G, soit $|\omega(S)| = n_p$ puis:

$$n_p \mid |G|$$

□

Lemme :

Soit $p \in \mathcal{P}$ et G un p-groupe agissant sur un ensemble fini X. Alors si l'on note:

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

on a:

$$|X| \equiv \left|X^G\right| [p]$$

Preuve :

On note $|G| =: p^\alpha$.

Pour $x \in X$, on note $\omega(x)$ son orbite sous l'action de G. Alors, $\omega(x) = \{x\}$ ssi $x \in X^G$. Pour $x \in X \setminus X^G$, on a:

$$(i) \quad |\omega(x)| > 1 \qquad (ii) \quad |\omega(x)| \mid p^\alpha$$

Ainsi,

$$p \mid |\omega(x)|$$

Par suite, si l'on écrit X comme réunion disjointe des ses orbites sous l'action de G avec un ensemble représenant E:

$$X = \bigsqcup_{x \in E} \omega(x) = \bigsqcup_{x \in X^G} \{x\} \sqcup \bigsqcup_{x \in E \setminus X^G} \omega(x)$$

Soit:

$$|X| = \left|X^G\right| + \sum_{x \in E \setminus X^G} |\omega(x)| \equiv \left|X^G\right| [p]$$

$\square$

Preuve :(Du théorème 3)

On rappelle que $|G| = p^\alpha s$ avec $s \wedge p = 1$ et que l'on note n_p le nombre de p-sylow de G.

Soit $S \subseteq G$ un p-sylow et X l'ensemble des p-sylow de G. En considérant l'action de S sur X par conjugaison, on a:

$$|X| \equiv \left|X^S\right| [p]$$

Montrons que $\left|X^S\right| = 1$

On a déjà $S \in X^S$, soit maintenant $P \in X^S$.

Considérons $N := \langle P \cup S \rangle$. C'est un sous-groupe de G dont P et S sont des p-sylows. On remarque que, par ce que $P \in X^S$, P est distingué dans N, mais alors le lemme précédent nous dit que P est l'unique p-sylow de N soit:

$$P = S$$

Finalement $X^S = \{S\}$ et donc:

$$n_p \equiv 1[p]$$

mais comme $n_p \mid |G|$, par le lemme de Gauss,

$$n_p \mid s$$

$\square$