Conséquences du Théorème de Sylow

Soit $(G,\cdot)$ un groupe fini de cardinal $|G| = p^r m$ avec $p \in \mathbb{P}$ et $p \wedge m = 1$. Un p-Sylow S est un p-sous-groupe maximal, c'est à dire de cardinal $|S| = p^r$. On note $p\mathrm{Syl}(G)$ l'ensemble des p-Sylow de G.

Théorème de Sylow.

i. Il existe un p-Sylow de G.

ii. Tous les p-Sylow de G sont conjugués entre eux :

$$\forall S_1, S_2 \in p\mathrm{Syl}(G), \quad \exists g \in G : \quad S_2 = g S_1 g^{-1}$$

Soit $S \in p\mathrm{Syl}(G)$ un p-Sylow de G. Alors S est normal si et seulement si c'est l'**unique** p-Sylow de G :

$$\boxed{S \trianglelefteq G \iff p\mathrm{Syl}(G) = \{S\}}$$

En effet, par le théorème de Sylow, tous les p-Sylow sont conjugués à S, c'est à dire que $\forall S' \in p\mathrm{Syl}(G)$, $\exists g \in G : gSg^{-1} = S'$. Or S est normal, donc $\forall g \in G,\ gSg^{-1} = S$. Donc $S' = S$ nécessairement.

Réciproquement, $\forall g \in G$, puisque gSg^{-1} est encore un p-Sylow par cardinalité ($gSg^{-1} \cong S$), nécessairement $gSg^{-1} = S$ car S est l'unique p-Sylow de G. Donc S est distingué dans G.

Soit S_0 un p-Sylow de G, qui **existe** par le théorème de Sylow. On considère l'action de S_0 sur l'ensemble $p\mathrm{Syl}(G)$ des p-Sylow de G par conjugaison :

$$\begin{array}{rccc} \star : & S_0 \times p\mathrm{Syl}(G) & \longrightarrow & p\mathrm{Syl}(G) \\ & (g, S) & \longmapsto & gSg^{-1} \end{array}$$

bien définie dans $p\mathrm{Syl}(G)$ car la conjugaison conserve le cardinal (p^r ici). Puisque le groupe S_0 agissant sur $p\mathrm{Syl}(G)$ est un ***p*-groupe**, la formule des classes indique que

$$|p\mathrm{Syl}(G)| \equiv |\mathrm{Fix}_\star| \mod p$$

Montrons donc que l'action $\star$ possède un **unique point fixe**. Puisque S_0 est un groupe, on a $\forall g \in S_0$, $gS_0g^{-1} = S_0$ donc S_0 est un point fixe. Soit $S \in \mathrm{Fix}_\star$ un autre p-Sylow fixe, et montrons que $S = S_0$.

Considérons $H := \langle S_0, S\rangle$ le sous-groupe engendré par S_0 et S. Puisque $S \subset H \subset G$, par le théorème de Lagrange, $p^r = |S| \operatorname{div} |H| \operatorname{div} |G| = p^r m$ donc $|H| = p^r m'$ avec $m' \wedge p = 1$, donc

$$S_0 \text{ et } S \text{ sont des } p\text{-Sylow de } H = \langle S_0, S\rangle$$

Or par définition, puisque S est stable par conjugaison par S_0 et par S lui même, il est stable par H :

$$\forall h \in H,\ hSh^{-1} = S \qquad \text{ou dit autrement} \qquad S \trianglelefteq H$$

C'est un p-Sylow normal de H, donc par le **théorème de Sylow** (p-Sylow tous conjugués entre eux),

$$S \text{ est l'unique } p\text{-Sylow de } H \qquad \text{donc} \qquad \{S, S_0\} \subset p\mathrm{Syl}(H) = \{S\} \qquad \text{donc} \qquad S = S_0$$

Ainsi,

$$\mathrm{Fix}_\star = \{S_0\} \qquad \text{donc} \qquad \boxed{|p\mathrm{Syl}(G)| \equiv 1 \mod p}$$

Considérons maintenant l'action de G entier sur l'ensemble $p\mathrm{Syl}(G)$ de ses p-Sylow par conjugaison :

$$\begin{array}{rcl} \star' : G \times p\mathrm{Syl}(G) & \longrightarrow & p\mathrm{Syl}(G) \\ (g, S) & \longmapsto & gSg^{-1} \end{array}$$

bien définie dans $p\mathrm{Syl}(G)$ car la conjugaison conserve le cardinal. De plus, le **théorème de Sylow** indique que les p-Sylow sont tous conjugués entre eux, c'est à dire que si l'on fixe un quelconque $S \in p\mathrm{Syl}(G)$,

$$p\mathrm{Syl}(G) \;=\; \left\{ gSg^{-1} \,:\, g \in G \right\} \;=\; \mathrm{Orb}_{\star'}(S)$$

Or $|p\mathrm{Syl}(G)| \not\equiv 1 \bmod p$. De plus, le théorème orbite-stabilisateur impose que $|\mathrm{Orb}_{\star'}(S)| \operatorname{div} |G|$. Donc

$$\left\{ \begin{array}{l} |p\mathrm{Syl}(G)| \operatorname{div} |G| = p^r m \\ |p\mathrm{Syl}(G)| \wedge p = 1 \end{array} \right. \qquad \text{donc (Gauss)} \qquad \boxed{|p\mathrm{Syl}(G)| \operatorname{div} m}$$

Supposons que $p^2 \not\operatorname{div} |G|$, c'est à dire que $|G| = p\,m$. Soient $S_1, S_2 \in p\mathrm{Syl}(G)$ deux p-Sylow de G.

Alors $S_1 \cap S_2 \leq S_1$, donc par le théorème de Lagrange, $|S_1 \cap S_2| \operatorname{div} |S_1| = p$ puisque S_1 est un p-Sylow. $p \in \mathbb{P}$ donc $|S_1 \cap S_2| = 1$ (et alors $S_1 \cap S_2 = \{e\}$) ou $|S_1 \cap S_2| = p = |S_1|$ (et alors $S_1 = S_1 \cap S_2$). Ainsi,

$$\boxed{p^2 \not\operatorname{div} |G| \quad \Longrightarrow \quad \forall (S_1, S_2) \in p\mathrm{Syl}(G)^2_{\neq},\; S_1 \cap S_2 = \{e\}}$$

En conséquence, on peut déterminer le nombre d'éléments d'ordre p de G à partir du nombre de p-Sylow. En effet, par définition et puisque seul l'élément neutre n'est pas d'ordre p dans un p-Sylow, c'est à dire un groupe d'ordre p (théorème de Lagrange), $\forall g \in G$,

$$\mathrm{ord}(g) = p \quad \Longleftrightarrow \quad \langle g \rangle \in p\mathrm{Syl}(G) \quad \Longleftrightarrow \quad g \in \bigcup p\mathrm{Syl}(G) \setminus \{e\} \quad \Longleftrightarrow \quad g \in \bigsqcup_{S \in p\mathrm{Syl}(G)} S \setminus \{e\}$$

car avec le résultat précédent, l'union des p-Sylow est disjointe après élimination l'élément neutre près. Donc

$$\left| \mathrm{ord}^{\leftarrow}(p) \right| = \left| \bigsqcup_{S \in p\mathrm{Syl}(G)} S \setminus \{e\} \right| = \sum_{S \in p\mathrm{Syl}(G)} \overbrace{|S \setminus \{e\}|}^{=p-1} = |p\mathrm{Syl}(G)| \times (p-1)$$

Ainsi,

$$\boxed{p^2 \not\operatorname{div} |G| \quad \Longrightarrow \quad |\mathrm{ord}^{\leftarrow}(p)| = |p\mathrm{Syl}(G)| \times (p-1)}$$

Posons le morphisme de $(G, \cdot)$ dans $(\mathfrak{S}(p\mathrm{Syl}(G)), \circ)$ associé à l'action de G par conjugaison sur $p\mathrm{Syl}(G)$:

$$\begin{array}{rcl} \Phi : G & \longrightarrow & \mathfrak{S}(p\mathrm{Syl}(G)) \\ g & \longmapsto & (S \mapsto gSg^{-1}) \end{array}$$

($\forall g \in G$, $\Phi(g)$ est bien dans $p\mathrm{Syl}(G)$ car $|S| = |gSg^{-1}|$ et est bijective d'inverse $\Phi(g^{-1})$. De plus, Φ est un morphisme : $\forall g, g' \in G$, $\Phi(gg') = S \mapsto gg'S(gg')^{-1} = (S \mapsto gSg^{-1}) \circ (S \mapsto g'Sg'^{-1}) = \Phi(g) \circ \Phi(g')$)

Calculons son noyau : $\forall g \in G$,

$$\begin{aligned} g \in \mathrm{Ker}(\Phi) &\iff \Phi(g) = S \mapsto gSg^{-1} = e_{(\mathfrak{S},\circ)} = S \mapsto S \\ &\iff \forall S \in p\mathrm{Syl}(G),\ gSg^{-1} = S \\ &\iff g \in \bigcap_{S \in p\mathrm{Syl}(G)} \{g \in G : gSg^{-1} = S\} = \bigcap_{S \in p\mathrm{Syl}(G)} \mathrm{N}_G(S) \end{aligned}$$

avec $\mathrm{N}_G(S)$ le **normalisateur** de S dans G. De plus, $\forall S \in p\mathrm{Syl}(G)$, $\mathrm{N}_G(S) \trianglelefteq G$ est distinguée dans G donc l'intersection est encore distinguée dans G. Ainsi

$$\boxed{\mathrm{Ker}(\Phi) = \bigcap_{S \in p\mathrm{Syl}(G)} \mathrm{N}_G(S) \trianglelefteq G}$$

Si $\mathrm{Ker}(\Phi) = G$, alors nécessairement $\exists S \in p\mathrm{Syl}(G) : \mathrm{N}_G(S) = G$, c'est à dire $S \trianglelefteq G$. Donc par un corollaire du théorème de Sylow, S est l'unique p-Sylow.

Réciproquement, si $|p\mathrm{Syl}(G)| = 1$, alors $\mathfrak{S}(p\mathrm{Syl}(G))$ est trivial, donc Φ aussi. Donc

$$\boxed{\Phi \text{ trivial} \overset{\text{def}}{\iff} \mathrm{Ker}(\Phi) = G \iff |p\mathrm{Syl}(G)| = 1}$$

Si G est **simple**, alors $\mathrm{Ker}(\Phi) = G$ ou $\{e\}$. Et si $|p\mathrm{Syl}(G)| \neq 1$, alors nécessairement $\mathrm{Ker}(\Phi) = \{e\}$, donc le morphisme Φ est injectif, donc par factorisation canonique $G \cong \mathrm{Im}(\Phi) \leq \mathfrak{S}(p\mathrm{Syl}(G))$, donc par le théorème de Lagrange, $|G| \operatorname{div} |\mathfrak{S}(p\mathrm{Syl}(G))| = |p\mathrm{Syl}(G)|!$, d'où

$$\boxed{G \text{ simple et } |p\mathrm{Syl}(G)| \neq 1 \implies |G| \operatorname{div} |p\mathrm{Syl}(G)|!}$$