Théorèmes de Sylow

Lemme 1. *Soit G un groupe fini d'ordre $p^\alpha m$, où $p \nmid m$. Soit H un groupe, et soit S un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ est un p-Sylow de H.*

Démonstration.

On considère l'action de G sur G/S définie par :

$$\varphi : \left| \begin{array}{ccc} G \times G/S & \longrightarrow & G/S \\ (g, aS) & \longmapsto & g \cdot (aS) = (ga)S \end{array} \right.$$

En effet, φ est une action de groupe, puisque, pour tous $g, g' \in G$ et tout $a \in G$, on a :

$$\varphi(e, aS) = e \cdot (aS) = (ea)S = aS$$

$$\varphi(g, \varphi(g', aS)) = \varphi(g, g' \cdot (aS)) = \varphi(g, (g'a)S) = g \cdot (g'a)S = (gg'a)S = (gg') \cdot (aS) = \varphi(gg', aS)$$

On note S_{aS} le stabilisateur de aS sous l'action de G sur G/S. Alors
- Soit $g \in S_{aS}$, alors $gaS = aS$, c'est-à-dire qu'il existe $s_1, s_2 \in S$ tels que $gas_1 = as_2$.
  Ainsi $g = as_2 s_1^{-1} a^{-1} \in aSa^{-1}$, donc $S_{aS} \subseteq aSa^{-1}$.
- Soit $h \in aSa^{-1}$. Il existe $s \in S$ tel que $h = asa^{-1}$. Ainsi $h \cdot aS = (asa^{-1}a)S = aS$, et $aSa^{-1} \subseteq S_{aS}$.

On a donc finalement que $S_{aS} = aSa^{-1}$.

En restreignant φ à H, on a que H agit sur G/S.
En notant S'_{aS} le stabilisateur de aS sous l'action de H, on obtient que $S'_{aS} = aSa^{-1} \cap H$.
En choisissant $a_1, \dots, a_m$ un système de représentants des orbites, l'équation aux classes donne :

$$m = |G/S| = \sum_{i=1}^{m} \frac{|H|}{|a_i S a_i^{-1} \cap H|}$$

Or, si pour tout $i \in [\![1, m]\!]$, on a $p \mid [H : S'_{aS}]$, alors $p \mid |G/S| = m$, ce qui contredit le fait que S soit un p-Sylow.
Il existe donc $i \in [\![1, m]\!]$ tel que $p \wedge [H : S'_{aS}] = 1$.

De plus, $a_i S a_i^{-1} \cap H$ est un sous-groupe de $a_i S a_i^{-1}$, donc $a_i S a_i^{-1} \cap H$ est un p-groupe, donc $|a_i S a_i^{-1} \cap H| = p^k$ et $|H| = p^j n$, où $k \leqslant j \leqslant \alpha$ et $n \mid m$. Cependant, $[H : S'_{aS}] = p^{j-k} n \wedge p = 1$, donc $j = k$.
Finalement, $a_i S a_i^{-1} \cap H$ est un p-Sylow de H.

□

Lemme 2. *Soit G un p-groupe agissant sur X. On note X^G l'ensemble des points fixes de X par G. Alors $|X| \equiv |X^G| \mod p$.*

Démonstration.

On écrit X comme réunion disjointe de ses orbites sous G. Si $x \notin X^G$, alors son orbite $\omega(x)$ est de cardinal strictement supérieur à 1, mais comme ce cardinal divise $|G| = p^n$, on a que $p \mid |\omega(x)|$. Si θ est un système de représentants, alors l'équation aux classe donne :

$$|X| \equiv |X^G| + \sum_{x \in \theta \setminus X^G} |\omega(x)| \equiv |X^G| \mod p$$

□

Théorème 3 (Sylow). *On suppose G fini d'ordre $n = p^\alpha m$, où $p \nmid m$.*

(i) L'ensemble $Syl_p(G)$ des p-Sylow de G est non vide.

(ii) Tous les p-Sylow sont conjugués.

(iii) $|Syl_p(G)| \equiv 1 \mod p$ et $|Syl_p(G)| \mid m$.

Démonstration.

(i) Par le théorème de Cayley, on sait qu'il existe un isomorphisme $g : G \to A$, où $A \subseteq \mathfrak{S}_n$.
Soit $(e_1, \dots, e_n)$ une base de $\mathbb{F}_q^n$. On considère l'application :

$$\psi : \left| \begin{array}{ccc} \mathfrak{S}_n & \longrightarrow & GL_n(\mathbb{F}_p) \\ \sigma & \longmapsto & u_\sigma : \left| \begin{array}{ccc} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ e_i & \longmapsto & e_{\sigma(i)} \end{array} \right. \end{array} \right.$$

De plus, ψ est un morphisme de groupes. En effet, pour tous $\sigma, \sigma' \in \mathfrak{S}_n$, et tout $i \in [\![1, n]\!]$, on a :

$$\psi(\sigma \circ \sigma')(e_i) = e_{\sigma(\sigma(i))} = \psi(\sigma)(\psi(\sigma')(e_i)) = (\psi(\sigma) \circ \psi(\sigma'))(e_i)$$

Donc $\psi(\sigma \circ \sigma') = (\psi(\sigma) \circ \psi(\sigma'))$, et ψ est un morphisme de groupes.
On a également l'injectivité de ψ, puisque :

$$\mathrm{Ker}(\psi) = \left\{\sigma \in \mathfrak{S}_n \;\middle|\; u_\sigma = Id\right\} = \left\{\sigma \in \mathfrak{S}_n \;\middle|\; \forall\, i \in [\![1, n]\!],\ e_{\sigma(i)} = e_i\right\} = \{Id\}$$

En posant $\theta = \psi|_A \circ g$, θ est un morphisme de groupe de G dans $GL_n(\mathbb{F}_p)$.
De plus, θ est injectif, donc, par le premier théorème d'isomorphie, on a $G \cong \mathrm{Im}(\theta)$.
Or, $\mathrm{Im}(\theta)$ est un sous-groupe de $GL_n(\mathbb{F}_p)$, qui possède un p-Sylow.
Par le Lemme 1, $\mathrm{Im}(\theta)$ contient également un p-Sylow, et donc G aussi par isomorphie.

(ii) Soit H un p-sous-groupe de G, et soit S un p-Sylow de G.
Par le Lemme 1, il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.
On a donc $|H| = p^k$ et $aSa^{-1} \cap H \subseteq H$, et $|aSa^{-1} \cap H| = p^k$, donc $aSa^{-1} \cap H = H$, et $H \subseteq aSa^{-1}$.
Si de plus H est un p-Sylow, alors $H = aSa^{-1}$.

(iii) Soit S un p-Sylow de G. On considère l'action par conjugaison de S sur $Syl_p(G)$.
Pour tout $s \in S$, on a $sSs^{-1} = S$, donc $S \in (Syl_p(G))^S$. Montrons que c'est le seul point fixe.
Soit $T \in (Syl_p(G))^S$, donc tel que, pour tout $s \in S$, on a $sTs^{-1} = T$.
On pose $N = \langle S, T\rangle$ le sous-groupe de G engendré par S et T. On a $T \leqslant N \leqslant G$.
Comme T est un p-Sylow de G, c'est aussi un p-Sylow de N. De même pour S.
T et S sont donc deux p-Sylow de N, donc il existe $a \in N$ tel que $S = aTa^{-1}$.
Or, comme S normalise T, on a que $T \trianglelefteq N$, d'où $aTa^{-1} = T$.
Le Lemme 2 donne que $|Syl_p(G)| \equiv 1 \mod p$.

Enfin, on considère l'action par conjugaison de G sur l'ensemble de ses sous-groupes.
$Syl_p(G)$ forme une orbite sous cette action par le point précédent.
On a alors $|Syl_p(G)| \mid |G| = p^\alpha m$ et $|Syl_p(G)| \wedge p = 1$, donc, par le lemme de Gauss, on a $|Syl_p(G)| \mid m$.

□

Conclusion. Les théorèmes de Sylow donnent l'existence de p-Sylow pour n'importe quel groupe, et permettent de les dénombrer plus facilement. ◁

Références

[Per] Daniel Perrin. *Cours d'Algèbre*. Ellipses