Titre : **Théorèmes de Sylow**
Recasages : 101,103,104,105
Thème : Théorie des groupes, actions de groupes.
Références : Perrin, Cours d'algèbre (page 18)

Théorème 1. *(Sylow)*
Soit p un nombre premier, G un groupe fini d'ordre $n = p^\alpha m$ avec $p \nmid m$. Alors

(a) L'ensemble $\mathrm{Syl}_p(G)$ des p-Sylow de G est non vide.

(b) Pour $H \leqslant G$ un p-sous-groupe de G, et $S \in \mathrm{Syl}_p(G)$, il existe $a \in G$ tel que $H \subset aSa^{-1}$. En particulier, tous les p-sous-groupes de Sylow de G sont conjugués.

(c) Le cardinal de $\mathrm{Syl}_p(G)$ est congru à 1 modulo p et divise m.

La preuve va essentiellement reposer sur la proposition suivante :

Proposition 2. *Soit H un sous-groupe de G, et $S \in \mathrm{Syl}_p(G)$, il existe $a \in G$ tel que $aSa^{-1} \cap H$ est un p-Sylow de H.*

Démonstration. On fait agir G sur l'ensemble quotient G/S par translation à gauche. Pour $aS \in G/S$ et $g \in G$, on a

$$g.(aS) = aS \Leftrightarrow a^{-1}gaS = S \Leftrightarrow a^{-1}ga \in S$$

D'où $G_{aS} = aSa^{-1}$. Par restriction, le groupe H agit également sur G/S, et $H_{aS} = H \cap G_{aS} = H \cap aSa^{-1}$. En choisissant $a_1, \cdots, a_m$ un système de représentants des orbites de G/S, on obtient par la formule des orbites

$$|G/S| = \sum_{i=1}^{m} [H : H_{a_i S}]$$

S est un p-Sylow si et seulement si son indice dans G est premier avec p. Par hypothèse, $|G/S| = [G : S]$ est premier avec p. Or $[H : H_{a_i S}]$ est soit premier avec p, soit divisible par p, s'il ils sont tous divisible par p, alors $\sum_{i=1}^{m} [H : H_{a_i S}]$ l'est également, ce qui contredit le fait que S soit un p-Sylow. Donc il existe a_i tel que $[H : H_{a_i S}]$ soit premier avec p, donc $H_{a_i S} = H \cap a_i S a_i^{-1}$ est un p-Sylow de H. □

Une fois ce premier résultat montré, nous allons l'appliquer en plongeant G dans un groupe connu : $Gl_n(\mathbb{F}_p)$. Par le théorème de Cayley, il existe un morphisme injectif $G \to \mathfrak{S}_n$, et en faisant agir $\mathfrak{S}_n$ sur $[\![1, n]\!]$, on obtient une représentation fidèle $\mathfrak{S}_n \to Gl_n(\mathbb{F}_p)$. On peut donc voir G comme un sous-groupe de $Gl_n(\mathbb{F}_p)$. Or on sait (en comptant les bases) que

$$|Gl_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) = p^{\frac{n(n-1)}{2}} (p^n - 1)(p^{n-1} - 1) \cdots (p - 1)$$

Avec p ne divisant pas $m = (p^n - 1)(p^{n-1} - 1) \cdots (p - 1)$. On cherche donc un sous-groupe de $Gl_n(\mathbb{F}_p)$ d'ordre $p^{\frac{n(n-1)}{2}}$, un tel groupe est donné par les matrices triangulaires supérieures strictes :

$$\{A = (a_{i,j})_{i,j} \in [\![1, n]\!] \mid a_{i,j} = 0 \text{ si } i > j \text{ et } a_{i,i} = 1 \text{ pour } i \in [\![1, n]\!]\}$$

Il s'agit bien d'un sous-groupe de $Gl_n(\mathbb{F}_p)$, dont l'ordre est bien $p^{\frac{n(n-1)}{2}}$ (il faut choisir les coefficients strictement supérieurs, et ce choix est libre).
La proposition 2 donne le premier théorème de Sylow pour G.

Le deuxième théorème est conséquence directe de la proposition : si $H \subset G$ est un p-groupe et $S \leqslant G$ un p-Sylow. La proposition 2 nous donne un $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de G, mais comme H est un p-groupe, il est son seul p-Sylow, d'où $aSa^{-1} \cap H = H$ et $H \subset aSa^{-1}$.

Pour le troisième théorème, on choisit $S \in \mathrm{Syl}_p(G)$ et on fait agir S sur $\mathrm{Syl}_p(G)$ par conjugaison (on pose $s.T = sTs^{-1}$ pour $s \in S$ et T un p-Sylow de G). On va utiliser le résultat suivant

Proposition 3. *Si G est un p-groupe opérant sur un ensemble X et soit X^G l'ensemble des points fixes de X sous l'action de G. Alors $|X| \equiv |X^G|[p]$.*

Nous voulons montrer que l'action de S sur $\mathrm{Syl}_p(G)$ admet un unique point fixe : Comme S est un sous-groupe de G, S est un point fixe (en effet, $sSs^{-1} = S$ pour $s \in S$). Soit maintenant $T \in \mathrm{Syl}_p(G)$ un point fixe sous l'action de S, par hypothèse, S normalise T. On pose $N = \langle S, T \rangle$ le sous-groupe de G engendré par T et S. On a par construction $T \leqslant N \leqslant G$, comme T est un p-Sylow de G, il s'agit aussi d'un p-Sylow de N, de même que S.
Enfin, comme S normalise T, T est distingué dans N (en effet S et T sont inclus dans le normalisateur de T, ce qui est donc aussi le cas du sous-groupe qu'ils engendrent). Par le deuxième théorème, on déduit que $T = S$, d'où le résultat.
Enfin, pour montrer que $|\mathrm{Syl}_p(G)|$ divise m, on fait agir G par conjugaison sur l'ensemble de ses sous-groupes, par le deuxième théorème, $\mathrm{Syl}_p(G)$ forme une orbite sous cette action, donc son cardinal (égal à l'indice de son stabilisateur) divise n. Comme $|\mathrm{Syl}_p(G)|$ est (par le troisième théorème) premier avec p, c'est qu'il divise m.