1 Théorèmes de Sylow

1.1 Première version

Théorème. *Soit G un groupe fini avec $|G| = np^\alpha$ avec $\alpha \in \mathbb{N}$, $p \nmid n$ et p premier. Alors il existe un sous-groupe de G d'ordre p^α.*

Lemme. *Soit G un groupe abélien fini et p un nombre premier tel que $p \mid |G|$, alors il existe un sous-groupe de G d'ordre p.*

Démonstration. G est fini donc engendré par un nombre fini de générateurs $x_1, \dots, x_n$, notons $r_1, \dots, r_n$ leurs ordres respectifs. Posons $\varphi : \begin{array}{ccc} \langle x_1 \rangle \times \cdots \times \langle x_n \rangle & \longrightarrow & G \\ (y_1, \dots, y_n) & \longmapsto & y_1 \dots y_n \end{array}$.
Alors φ est un homomorphisme de groupe car G est abélien et est surjectif car $x_1, \dots, x_n$ sont des générateur de G. Alors par le premier théorème d'isomorphisme φ induit un isomorphisme $\langle x_1 \rangle \times \cdots \times \langle x_n \rangle / \mathrm{Ker}(\varphi) \cong G$. En particulier $|G| \times |\mathrm{Ker}(\varphi)| = |\langle x_1 \rangle \times \cdots \times \langle x_n \rangle| = r_1 \dots r_n$.
Or $p \mid |G|$ donc $p \mid r_1 \dots r_n$ et il existe donc $i \in [|1, n|]$ tel que $p \mid r_i \Rightarrow r_i = ap$. Alors l'élément x_i^a est d'ordre p et engendre un sous groupe d'ordre p. $\square$

Démonstration du théorème. Soit G un groupe fini tel que $|G| = np^\alpha$. On montre le théorème par récurrence sur l'ordre de G.
Initialisation : Si $|G| = 1$ alors c'est trivial.
Hérédité : Supposons le résultat démontré pour tout les groupes d'ordre inférieur à $|G|$.
Si $\alpha = 0$ c'est évident, supposons donc que $\alpha \geq 1$. On fait agir G sur lui même par conjugaison : $G \times G \longrightarrow G : (g, x) \longmapsto gxg^{-1}$. On note $G_x = \{gxg^{-1} \mid g \in G\}$ l'orbite de x et $\mathrm{Stab}(x) = \{g \in G \mid gxg^{-1} = x\}$ le stabilisateur de x. Soit X un système de représentants des orbites, on a :

$$|G| = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|\mathrm{Stab}(x)|}$$

or $\mathrm{Stab}(x) = G \iff \forall g \in G,\ gxg^{-1} = x \iff x \in Z(G)$ d'où :

$$|G| = \sum_{x \in X} \frac{|G|}{|\mathrm{Stab}(x)|} = \sum_{x \in Z(G)} \frac{|G|}{|\mathrm{Stab}(x)|} + \sum_{x \in X \setminus Z(G)} \frac{|G|}{|\mathrm{Stab}(x)|} = |Z(G)| + \sum_{x \in X \setminus Z(G)} \frac{|G|}{|\mathrm{Stab}(x)|}.$$

On distingue deux cas :
Si il existe $x \in X$ tel que $p^\alpha \mid |\mathrm{Stab}(x)|$ alors par hypothèse de récurrence comme $|\mathrm{Stab}(x)| < |G|$ il existe un sous groupe d'ordre p^α de $\mathrm{Stab}(x)$ donc de G.
Si pour tout $x \in X$ tel que $p^\alpha \nmid |\mathrm{Stab}(x)|$ alors $\forall x \in X$, $p \mid \frac{|G|}{|\mathrm{Stab}(x)|}$ et donc $p \mid |Z(G)|$ qui est abélien. Par le lemme, il existe H un sous groupe de $Z(G)$ tel que $|H| = p$ or H est normal car $H \in Z(G)$. Alors $|G/H| = \frac{|G|}{|H|} = np^{\alpha-1}$ et par hypothèse de récurrence il existe K un sous groupe de G/H d'ordre $p^{\alpha-1}$, soit alors $\pi : G \twoheadrightarrow G/H$ la projection quotient, alors $\pi^{-1}(K)$ est un sous groupe de G d'ordre $|H||K| = p^\alpha$. $\square$

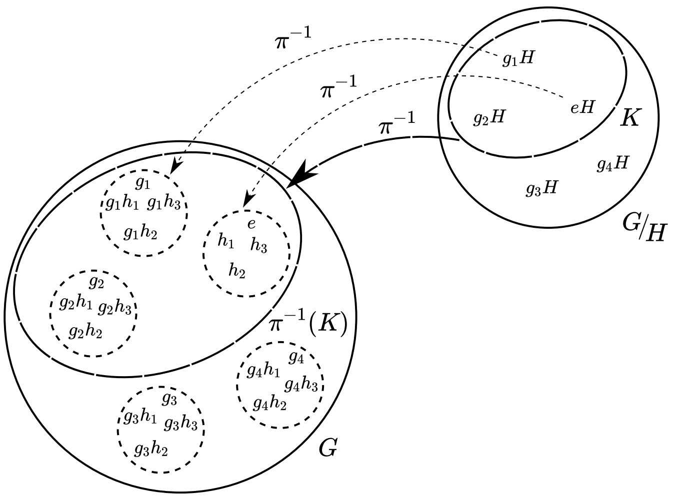

FIGURE 1 – Calcul du cardinal de $\pi^{-1}(K)$

Théorème. *Si H est un p-sous-groupe de G, alors pour tout p-Sylow S de G il existe $g \in G$ tel que $H \subseteq gSg^{-1}$. En particulier les p-Sylow de G sont conjugués entre eux.*

Démonstration. Soit S un p-Sylow de G avec $|G| = np^{\alpha}$ et $p \nmid n$, soit H un p-sous-groupe de G alors H agit sur ${G}/{S}$ (pas un groupe !) par $\begin{array}{ccc} H \times {G}/{S} & \longrightarrow & {G}/{S} \\ (h, gS) & \longmapsto & (hg)S \end{array}$. Soit $(g_iS)_{i\in I}$ un système de représentant des orbites, la formule des classes donne : $|{G}/{S}| = \displaystyle\sum_{i\in I} \frac{|H|}{|\mathrm{Stab}(g_iS)|}$.
Or $n = |{G}/{S}|$, $p \nmid n$ et $p \mid |H|$ donc il existe g_iS tel que $|H| = |\mathrm{Stab}(g_iS)|$ donc $H = \mathrm{Stab}(g_iS)$ ainsi $\forall h \in H$, $hg_iS = g_iS$ donc $hg_i \in g_iS$ et $h \in g_iSg_i^{-1}$ d'où $H \subseteq g_iSg_i^{-1}$. En particulier si H est un p-Sylow l'égalité des cardinaux donne $H = g_iSg_i$. □

Remarque. Je pense qu'il est bon d'avoir une vague idée de comment montrer le deuxième théorème sans pour autant l'inclure obligatoirement dans le développement. La figure est juste là pour donner un argument visuel rapide au fait que l'ordre de $\pi^{-1}(K)$ est $|H||K|$.

Références.
Lemme et théorème : GOURDON, *Les maths en tête. Algèbre et probabilités* prb 7 p40 + thm 8 p22.
Second théorème : Trouvable dans pas mal de livre.