Théorèmes de Sylow

Perrin, *Cours d'algèbre*, page 16

Théorème : Soit G un groupe fini, p un facteur premier de l'ordre n de G, et soit $n = p^k p_2^{k_2} \dots p_s^{k_s} = p^k q$ la décomposition en facteurs premiers de n.

1. Il existe dans G un p-sous-groupe de Sylow.
2. Tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow de G.
3. Les p-sous-groupes de Sylow de G sont conjugués.
4. Le nombre n_p de p-sous-groupes de Sylow de G vérifie

$$n_p | q \qquad \text{et} \qquad n_p \equiv 1 \pmod p$$

Rappels :

- un groupe d'ordre p^k, p premier, est appelé un p-groupe.
- Si G est un groupe tel que $|G| = p^k p_2^{k_2} \dots p_s^{k_s}$ et si H est un sous-groupe de cardinal p^k, on dit que H est un p-sous-groupe de Sylow de G.

Lemme : *Soit G un groupe avec $|G| = n = p^\alpha m$ avec $p \not| m$ et soit H un sous-groupe de G. Soit S un p-Sylow de G. Alors, il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.*

Demontrons le lemme : le groupe G opère sur G/S par translation à gauche et le stabilisateur de aS est aSa^{-1}. Mais H opère lui aussi sur G/S par restriction, avec comme stabilisateur de aS, $aSa^{-1} \cap H$. Il reste à voir que l'un de ces groupes est un Sylow de H. Ce sont déjà des p-groupes et il suffit donc que, pour un $a \in G$, $|H/(aSa^{-1} \cap H)|$ soit premier à p. Mais on a $|H/(aSa^{-1} \cap H)| = |\omega(aS)|$, cardinal de l'orbite de aS dans G/S sous l'action de H. Si tous ces nombres étaient divisibles par p, il en serait de même de $|G/S|$ car G/S est réunion des orbites $\omega(aS)$. Mais ceci contredit le fait que S est un p-Sylow de G.

A présent, démontrons le théorème en lui-même :

1. Soit G un groupe et p un diviseur de $|G| = n$. On plonge d'abord G dans $\mathcal{S}_n$ (par Cayley), puis on plonge $\mathcal{S}_n$ dans $GL_n(\mathbb{F}_p)$ de la manière classique, à savoir que $\sigma \in \mathcal{S}_n$ s'envoie sur l'endomorphisme u_σ défini dans la base canonique par $u_\sigma(e_i) = e_{\sigma(i)}$.

   Finalement, on a donc réalisé G comme un sous-groupe de $GL_n(\mathbb{F}_p)$ qui possède un p-Sylow, donc G aussi par le lemme.

2. Si H est un p-sous-groupe et S un p-SYlow de G, il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H. Mais comme H est un p-groupe, on a $aSa^{-1} \cap H = H$, donc H est inclus dans aSa^{-1} qui est un Sylow. Si de plus H est un Sylow, on a exactement $H = aSa^{-1}$.
3. Fait dans le (2).
4. On fait opérer G par conjugaison sur l'ensemble X de ses p-Sylow. Soit S un p-Sylow, S opère lui-aussi sur X et on a encore la congruence

   $$|X| = |X^S| \pmod p$$

   Il reste à voir que l'on a $|X^S| = 1$. Bien sûr, si $s \in S$, on a $sSs^{-1} = S$, autrement dit $S \in X^S$, on doit donc montrer que c'est le seul. Pour cela, soit T un p-Sylow, et supposons que T soit normalisé par S :

   $$\forall s \in S, sTs^{-1} = T$$

   On considère alors le sous-groupe N de G engendré par S et T. On a $S \subset N$, $T \subset N$ et ce sont, *a fortiori*, des p-Sylow de N. Mais comme S normalise T, on a $T \lhd N$ et donc T est l'unique Sylow de N, donc $S = T$.