1.2 Deuxième version (Wielandt) ♡

Théorème (De Sylow)**.**
Soit p un nombre premier et G un groupe fini, alors $\left|\mathrm{Syl}_p(G)\right| \equiv 1 \mod (p)$.

Démonstration. Soit G un groupe tel que $|G| = np^a$ avec p premier tel que $p \nmid n$.
On pose $\Omega = \{S \subseteq G \mid |S| = p^a\}$ l'ensemble des parties à p^a éléments, alors G agit sur Ω par translation à gauche $* : \begin{array}{ccc} G \times \Omega & \longrightarrow & \Omega \\ (g, S) & \longmapsto & g * S = gS = \{gs,\ s \in S\} \end{array}$

On s'intéresse aux orbites des p-Sylow : si $S \in \mathrm{Syl}_p(G)$ alors $\mathrm{Stab}(S) = S$, en effet, $S \subseteq \mathrm{Stab}(S)$ car S est un groupe et si $g \in \mathrm{Stab}(S)$, $gS = S$ et alors $g \in S$. Dans ce cas, $|\mathrm{Stab}(S)| = |S| = p^a$. De plus, S est le seul p-Sylow dans son orbite, car si S' est un autre groupe dans l'orbite de S, il existe $g \in G$ tel que $S = gS'$ donc $S = S'$. On voit ainsi que à un p-Sylow correspond une orbite de cardinal $|G * S| = \frac{|G|}{|\mathrm{Stab}(S)|} = \frac{np^a}{p^a} = n$.

Réciproquement, regardons ce que l'on peut dire de $|G * S|$ pour $S \in \Omega$ quelconque. Remarquons que $\mathrm{Stab}(S)$ agit sur S par translation à gauche : $\begin{array}{ccc} \mathrm{Stab}(G) \times S & \longrightarrow & S \\ (g, s) & \longmapsto & gs \end{array}$.
On prend $s_1, \ldots, s_r$ un système de représentants des orbites. Les orbites sous cette action sont de la forme $\mathrm{Stab}(S)s_i = \{gs_i, g \in \mathrm{Stab}(S)\}$, par la formule des classes on obtient que $p^a = |S| = \sum_{i=1}^r |\mathrm{Stab}(S)s_i| = r|\mathrm{Stab}(S)|$. On a en particulier que $|\mathrm{Stab}(S)| \mid p^a$.
Si $|\mathrm{Stab}(S)| = p^b < p^a$ alors $|G * S| = \frac{np^a}{p^b} = np^{a-b}$.
Si $|\mathrm{Stab}(S)| = p^a$ alors $|G * S| = n$ et $p^a = |S| = r|\mathrm{Stab}(S)| = rp^a$ donc $r = 1$ et l'action de $\mathrm{Stab}(S)$ sur S est alors transitive, il existe $s \in S$ tel que $S = \mathrm{Stab}(S)s$. Alors $s^{-1} * S = s^{-1}S$ est dans l'orbite de S et $s^{-1}S = s^{-1}\mathrm{Stab}(S)s$ est un p-Sylow de G car $|s^{-1}\mathrm{Stab}(S)s| = p^a$.

Il apparaît alors qu'il y a autant d'orbite de cardinal n que de p-Sylow de G, et que les orbites ne contenant pas de p-Sylow sont de cardinal divisible par np. Soit $(S_i)_{i \in I}$ un système de représentants des orbites de Ω, on a par la formule des classes :

$$|\Omega| = \sum_{i \in I} |G * S_i| = \sum_{i / |G * S_i| = n} |G * S_i| + \sum_{i / |G * S_i| \neq n} |G * S_i| \equiv n|\mathrm{Syl}_p(G)| + np \times A,\ A \in \mathbb{N},$$

d'où : $|\Omega| \equiv n|\,\mathrm{Syl}_p(G)| \mod (np)$. Or $|\Omega| = \binom{|G|}{p^a} = \binom{np^a}{p^a}$ ne dépend pas du groupe choisit et vaut la même quantité pour tout groupe G, en particulier si $G = \mathbb{Z}/np^a\mathbb{Z}$, G possède un unique sous-groupe d'ordre p^a donc un seul p-Sylow et l'égalité trouvée devient : $|\Omega| \equiv n \mod (np)$.
Finalement $n \equiv |\Omega| \equiv n|\,\mathrm{Syl}_p(G)| \mod (pn)$ donc $1 \equiv |\,\mathrm{Syl}_p(G)| \mod (p)$. □

Théorème.

1. *Si H est un p-sous-groupe de G, alors pour tout p-Sylow S de G il existe $g \in G$ tel que $H \subseteq gSg^{-1}$.*
2. *Les p-Sylow de G sont conjugués entre eux.*
3. *Pour $G = np^a$ avec $p \nmid n$ on a $|\,\mathrm{Syl}_p(G)| \mid n$.*

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 $H = g_iSg_i$, on obtient bien que les p-Sylow sont conjugué entre eux.

Le groupe G agit donc par conjugaison sur ses p-Sylow, et ce de façon transitive, par l'équation aux classes on a donc pour S un p-Sylow : $|\mathrm{Syl}_p(G)| = \frac{|G|}{|\mathrm{Stab}(S)|}$. Donc $|\mathrm{Syl}_p(G)| \mid np^a$ mais on sait que $|\mathrm{Syl}_p(G)|$ est premier avec p donc $|\mathrm{Syl}_p(G)|$ divise n. □

Remarque. Cette version est plus personnelle, basée sur la démonstration donnée par Wielandt. Cette version est très intéressante pour plusieurs raisons : en plus de donner l'existence de p-Sylow on donne une congruence (ce qui rend le développement plus utilisable dans la leçon sur le dénombrement) et on utilise uniquement des résultats provenant des actions de groupes.

Références. C'est classique mais pas dans les références classique de l'agrégation...