Les théorèmes de Sylow

Perrin

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

$G \curvearrowright G/S$ par $g \cdot aS = (ga)S$. On a $\mathrm{Stab}(aS) = aSa^{-1}$.
Par restriction, $H \curvearrowright G/S$ et $\mathrm{Stab}_H(aS) = aSa^{-1} \cap H$. Or, $\forall a \in G$, $|aSa^{-1}| = |S| = p^\alpha$. i.e. $|aSa^{-1} \cap H| = p^\beta$
D'où $|aSa^{-1} \cap H| = p^\gamma$ car $aSa^{-1} \cap H < aSa^{-1}$. On écrit $H = p^\beta n$. Mq $\exists a \in G$ tq $\left|\frac{H}{aSa^{-1} \cap H}\right|$ soit premier avec p.
On a $\left|\frac{H}{aSa^{-1} \cap H}\right| = |O_{aS}|$ et $m = |G/S| = \sum_{aS \in \Omega} |O_{aS}|$. Si $p \mid |O_{aS}|$, $\forall aS$, alors $p \mid m \Rightarrow \in$.

Ω système de représentant des orbites + Équation aux classes

Théorème : Soit G groupe d'ordre $n = p^\alpha m$ avec $p \nmid m$.
1) Il existe un p-Sylow
2) Les p-Sylow sont tous conjugués
3) Soit n_p le nombre de p-Sylow. On $n_p \equiv 1 \ (p)$ et $n_p \mid m$.

1) Par le théorème de Cayley, G est isomorphe à un sous-groupe de $GL_n(\mathbb{F}_p)$. $G \hookrightarrow S_n \hookrightarrow GL_n(\mathbb{F}_p)$
On a $|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) = p^{\frac{n(n-1)}{2}} m$ avec $p \nmid m$.
L'ensemble des matrices de la forme $\begin{pmatrix} 1 & & * \\ & \ddots & \\ (0) & & 1 \end{pmatrix}$ est un p-Sylow de $GL_n(\mathbb{F}_p)$.
Par le lemme, G admet un p-Sylow.

2) Soit H, S deux p-Sylow de G. Par le lemme, il existe $a \in G$ tq $aSa^{-1} \cap H$ soit un p-Sylow de H.
D'où $aSa^{-1} \cap H = H$ et $H \subset aSa^{-1}$. Par égalité des cardinaux, $H = aSa^{-1}$.

3) G agit par conjugaison sur $X = \{p\text{-Sylow de } G\}$.
Soit S un p-Sylow de G. Par restriction, S agit sur X.
Par les équations aux classes, $n_p = |X| \equiv |X^S| \ (p)$, où $X^S = \{T \in X ;\ \forall s \in S,\ sTs^{-1} = T\}$
car S est un p-groupe
Mq $|X^S| = 1$:
X^S est non vide car contient S. Soit $T \in X^S$. Soit $N = \langle T, S \rangle$. Alors $|N| = p^\alpha r$ où $r \mid m$
et, T et S sont des p-Sylow de N.
Mais $T \lhd N$. En effet, si $x \in T$, $xTx^{-1} = T$
si $x \in S$, $xTx^{-1} = T$ car $T \in X^S$
Ainsi T est l'unique p-Sylow de N i.e. $T = S$ et $|X^S| = 1$.
D'où $n_p \equiv 1 \ (p)$.
De plus, $n_p \mid n$. En effet, pour S p-Sylow de G, on a $n = |G| = |\mathrm{Stab}(S)| \times \underbrace{|O_S|}_{= n_p}$
Puisque $n_p \wedge p$, $n_p \mid m$.