Théorèmes de Sylow

Théo Jaudon

Théorème 1. *Soit p un nombre premier et G un groupe d'ordre $n = p^\alpha m$ où p ne divise pas m. Alors*

1. *G possède un p-Sylow.*
2. *Tous les p-Sylow de G sont conjugués.*
3. *Le nombre n_p de p-Sylow de G vérifie $n_p \mid m$ et $n_p = 1 \pmod p$*

Remarque 2. *Un sous-groupe H de G est un p-Sylow de G si et seulement si c'est un p-groupe et si $[G : H]$ n'est pas divisible par p.*

On commence par prouver le lemme suivant.

Lemme 3. *Soit G un groupe comme ci-dessus, S un p-Sylow de G et H un sous-groupe de G. Il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.*

Preuve. Le groupe H agit sur l'ensemble des classes à gauche G/S via $h \cdot aS = haS$. On se donne $\mathcal{R} \subset G$ un système de représentants pour la partition en orbites et la formule des classes donne

$$[G : S] = |G/S| = \sum_{a \in \mathcal{R}} [H : Stab(aS)].$$

Reste à décrire les stabilisateurs, ce qu'on peut faire par équivalences successives. En effet $h \in Stab(aS) \iff haS = aS \iff ha \in aS \iff h \in aSa^{-1}$.
Remarquons que pour $a \in \mathcal{R}$, $H \cap aSa^{-1}$ est d'une part un sous groupe de H et d'autre part un p-groupe en tant que sous groupe du p-groupe aSa^{-1}. Ainsi $H \cap aSa^{-1}$ est un p-Sylow de H si et seulement si $[H : H \cap aSa^{-1}]$ n'est pas divisible par p.
Mais comme S est un p-Sylow de G, $[G : S]$ n'est pas divisible par p donc il existe $a \in \mathcal{R}$ tel que $[H : H \cap aSa^{-1}]$ ne soit pas divisible par p et donc $H \cap aSa^{-1}$ est un p-Sylow de H.

On peut maintenant passer à la preuve des théorèmes de Sylow.

Preuve.
D'après le théorème de Cayley on a un morphisme injectif $G \hookrightarrow \mathcal{S}(G) \simeq \mathcal{S}_n$ et via les matrices de permutations on a un morphisme injectif $\begin{array}{ccc} \mathcal{S}_n & \hookrightarrow & GL_n(\mathbb{F}_p) \\ \sigma & \mapsto & P_\sigma = (\delta_{i,\sigma(j)})_{1 \leq i,j \leq n} \end{array}$
de sorte que G s'identifie à un sous groupe de $GL_n(\mathbb{F}_p)$. Or

$$\begin{aligned} |GL_n(\mathbb{F}_p)| &= (p^n - 1)(p^n - p) \dots (p^n - p^{n-1}) \\ &= \prod_{1 \leq k \leq n-1} p^k \times (p^n - 1)(p^{n-1} - 1) \dots (p - 1) \\ &= p^{\frac{n(n-1)}{2}} (p^n - 1)(p^{n-1} - 1) \dots (p - 1) \end{aligned}$$

où le terme $(p^n - 1)(p^{n-1} - 1) \dots (p - 1)$ est congru à ± 1 modulo p. On vérifie ensuite sans difficulté que l'ensemble des matrices triangulaires supérieures avec des 1 sur la

diagonale est un p-Sylow de $GL_n(\mathbb{F}_p)$. D'après le lemme précédent, G possède un p-Sylow, ce qui prouve le point *1.*
Soient S et K deux p-Sylow de G. D'après le lemme, il existe $a \in G$ tel que $K \cap aSa^{-1}$ soit un p-Sylow de K c'est-à-dire $K = K \cap aSa^{-1}$. On en déduit que $K \subset aSa^{-1}$ et comme ces deux sous-groupes ont le même cardinal on a $K = aSa^{-1}$ ce qui prouve le point *2.*
Avec ce qui précède on sait que G agit par conjugaison et de façon transitive sur l'ensemble X de ses p-Sylow. On se donne S un p-Sylow de G. Le stabilisateur de S pour cette action est le sous-groupe $N_G(S) = \{\ g \in G \quad | \quad gSg^{-1} = S\ \}$, appelé le normalisateur de S dans G et qui vérifie toujours $S \lhd N_G(S)$. La relation orbite-stabilisateur fournit $n_p = |X| = [G : N_G(S)]$ et par multiplicativité de l'indice on trouve $n_p[N_G(S) : S] = [G : N_G(S)] \times [N_G(S) : S] = [G : S] = m$ i.e n_p divise m.
Par restriction, le p-Sylow S agit aussi sur X par conjugaison. D'après la relation orbite-stabilisateur, le cardinal des orbites non ponctuelles est divisible par p de sorte que

$$n_p = |X| = |X^S| \pmod{p}.$$

Reste à voir que S est la seule orbite non ponctuelle. Soit K un p-Sylow de G tel que pour tout $g \in S$ on ait $gKg^{-1} = K$. Alors $K \lhd N_G(K) < G$ et $S < N_G(K) < G$ donc S et K sont des p-Sylow de $N_G(K)$. Ils sont donc conjugués dans $N_G(K)$ d'après le point *2.* mais comme $K \lhd N_G(K)$ on trouve $S = K$ et $n_p = 1 \pmod{p}$.

Quelques remarques et compléments sur ce développement :

Ce développement est un bon moyen de pratiquer les actions de groupe.
Les trois points du théorème montrent en particulier qu'un p-Sylow de G est distingué dans G si et seulement si c'est le seul p-Sylow de G i.e si $n_p = 1$. Ainsi les théorèmes de Sylow sont des résultats accessibles permettant déjà de faire quelques petits progrès dans la classification des groupes finis simples. Citons par exemple.

Proposition 4. *Soient p, q deux nombres premiers distincts. Alors tout groupe d'ordre pq n'est pas simple.*

Preuve. On se donne G un groupe d'ordre pq. Par symétrie des rôles joués par p et q on peut supposer $q < p$. Le nombre n_p de p-Sylow de G divise q, il est donc égal à 1 ou q. Et comme $n_p = 1 \pmod{p}$ et $1 \leq q - 1 < p$ on trouve que $n_p = 1$. Ainsi G possède un unique p-Sylow qui est donc distingué dans G et G n'est pas simple.

Avec un peu plus de subtilité on montre aussi le résultat suivant.

Proposition 5. *Soient p, q, r des nombres premiers distincts. Alors tout groupe d'ordre pqr n'est pas simple.*

Recasages : 101, 103, 104 etc ?
Références : Perrin, Algèbre.