18 Théorèmes de Sylow

Théorème. *Soit G un groupe fini et p un nombre premier divisant $n = \#G$. On écrit $n = p^\alpha m$, où m est premier avec p.*
1. *G a au moins un p-Sylow. De plus, tout p-sous-groupe de G est contenu dans un p-Sylow.*
2. *Tous les p-Sylow sont conjugués (en particulier ils sont isomorphes).*
3. *Le nombre de p-Sylow divise m et il est congru à 1 modulo p.*

On peut rajouter que G a des sous-groupes d'ordre p^k pour tout $1 \leqslant k \leqslant \alpha$. C'est une conséquence immédiate du premier théorème de Sylow et de la proposition plus précise qui suit :

4. Si G est un p-groupe non trivial, il existe une suite de sous-groupes $\{e\} \subset G_1 \subset ... \subset G_{r-1} \subset G$ avec $G_i \triangleleft G_{i+1}$ et G_{i+1}/G_i cyclique d'ordre p (en particulier, un p-groupe est résoluble).

G a au moins un p-Sylow

Preuve.
On montre d'abord le lemme suivant : si H est un sous-groupe d'un groupe G et S un p-Sylow de G, alors il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H.

H agit par translations à gauche sur l'ensemble G/S, on vérifie que le stabilisateur d'une orbite gS sous cette action est $H_{gS} = gSg^{-1} \cap H$. Supposons que ce sous-groupe de H ne soit jamais un p-Sylow de H. En vertu de l'égalité $H.gS = (H : H_{gS})$, p divise le cardinal de toutes les orbites. En sommant, on obtient que p divise le cardinal de G/S, ce qui est une contradiction.

Passons maintenant à l'existence d'un p-Sylow de G, avec les notations du théorème. On plonge G canoniquement dans $\mathfrak{S}_n$ puis dans $\mathrm{GL}_n(\mathbb{F}_p)$. En vertu du lemme, il nous suffit de montrer l'existence d'un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$. En comptant le nombre de bases de $\mathbb{F}_p^n$, on voit que $\#\mathrm{GL}_n(\mathbb{F}_p) = (p^n - 1)(p^n - p)...(p^n - p^{n-1})$ soit encore $\#\mathrm{GL}_n(\mathbb{F}_p) = p^{n(n-1)/2}m$ où $m = (p^n - 1)(p^{n-1} - 1)...(p - 1)$ est premier avec p. Soit $B \subset \mathrm{GL}_n(\mathbb{F}_p)$ l'ensemble des matrices de la forme $I_n + T$, où T est une matrice triangulaire supérieure stricte. Alors B est un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$ de cardinal $p^{n(n-1)/2}$, c'est donc un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$.

□

Les points 1. 2. et 3.

Preuve.
Nous utiliserons le lemme suivant : Si H est un p-groupe agissant sur un ensemble X, alors

le nombre de points fixes de X sous l'action de H est égal à $\#X$ modulo p. C'est une conséquence directe de la formule des classes $\#X = \sum_i (H : H_{x_i})$.

Soient H un p-sous-groupe de G et S un p-Sylow de G. G agit sur l'ensemble de ses sous-groupes par conjugaison, notons X l'orbite de S. On a $\#X = (G : G_S)$, et comme G_S contient S, on en déduit que $\#X$ divise m (au fait, G_S est exactement le normalisateur de S dans G). H agit aussi sur X par restriction, comme p ne divise pas $\#X$ cette action a au moins un point fixe T (qui est un p-Sylow de G) d'après le lemme. On en déduit que H est contenu dans le normalisateur de T (par définition). Cela entraîne que $H \subset T$, admettons-le un instant, et le point **1.** est montré.

En prenant pour H un p-Sylow S' de G, on a nécessairement $S' = T$ (ils ont le même cardinal), si bien que S et S' sont conjugués et le point **2.** est montré. On voit en particulier que l'action de S' sur X a exactement un point fixe (à savoir S'), on a donc $\#X = 1 \mod p$ toujours grâce au lemme et aussi $\#X$ divise m (cf. plus haut), mais X est exactement l'ensemble des p-Sylow d'après **2.**, d'où le point **3.**

Enfin, reste à montrer ce que nous avions temporairement admis, à savoir que si un p-sous-groupe H est contenu dans le normalisateur $\mathrm{Nor}(S)$ d'un p-Sylow S, alors $H \subset S$. On voit facilement que HS est un sous-groupe de $\mathrm{Nor}(S)$ et que S est distingué dans HS. Ensuite, on remarque que l'application $h \mapsto h \mod S$ de H dans HS/S est surjective (en utilisant que $H \subset \mathrm{Nor}(S)$), et son noyau est exactement $H \cap S$. On en déduit que $(HS : S) = (H : H \cap S)$. Comme H est un p-groupe, si $H \cap S \neq H$, alors p divise $(H : H \cap S)$ donc $(HS : S)$, ce qui est exclu car S est un p-Sylow. On a donc $H \cap S = H$ *i.e.* $H \subset S$.

□

Le point 4.

Preuve.
Un p-groupe non trivial a un centre non trivial. En effet, G agit sur lui-même par conjugaison et la formule des classes donne $\#G = \#Z_G + \sum_i (G : G_{x_i})$, où la somme porte sur les orbites non réduites à un point. On en déduit que $0 = \#Z_G + 0 \mod p$, si bien que $\#Z_G$ n'est pas réduit à $\{e\}$.

Ensuite, on raisonne par récurrence sur α, où $\#G = p^\alpha$. Si $\alpha = 0$, il n'y a rien à faire. Si $\alpha \geqslant 1$, comme on sait que le centre de G est non trivial, on peut trouver un élément h d'ordre p dans le centre de G. Soit H le groupe cyclique engendré par h, H est d'ordre p et distingué dans G. G/H est donc un p-groupe d'ordre $p^{\alpha-1}$, et on peut appliquer l'hypothèse de récurrence : il existe $\{\overline{e}\}(= H) \subset \overline{G_1} \subset ... \subset \overline{G_{r-1}} \subset \overline{G}(= G/H)$ vérifiant les conditions voulues. On vérifie que la suite $\{e\} \subset H \subset G_1 \subset ... \subset G_{r-1} \subset G$ convient. □

Leçons possibles
101 Groupe opérant sur un ensemble. Exemples et applications.
103 Exemples de sous-groupes distingués et de groupes quotients. Applications.
104 Groupes finis. Exemples et applications.
105 Groupe des permutations d'un ensemble fini. Applications.

Références
[Lan04] pp35 et suivantes.
Un cours d'agrégation sur les-mathematiques.net.