4 Théorèmes de Sylow

ref : Perrin

THÉORÈME 4.1 (SYLOW) *Soit G un groupe de cardinal $n = p^\alpha m$ avec p premier, $\alpha \geq 1$ et m premier à p. On appelle p-sylow de G un sous-groupe de G de cardinal p^α.*

1. *G admet un p-sylow.*
2. *Les p-sylows de G sont tous conjugués.*
3. *Si n_p désigne le nombre de p-sylows de G. Ce nombre est contraint aux congruences suivantes :*
   (a) *$n_p = [G : N_G(S)]$, indice du normalisateur de n'importe quel p-sylow S, en particulier n_p divise n.*
   (b) *$n_p = 1 \pmod p$*
   (c) *n_p divise m*

PREUVE.

1. Le groupe $GL(n, \mathbb{F}_p)$ est de cardinal :

$$(p^n - 1)(p^n - p)...(p^n - p^{n-1}) = p^{\frac{n(n-1)}{2}}(p^n - 1)(p^{n-1} - 1)...(p - 1)$$

   Le sous-groupe des matrices triangulaires supérieures avec des 1 sur la diagonale est de cardinal $p^{\frac{n(n-1)}{2}}$ (le nombre de coefficient dans le triangle supérieur strict). C'est donc un p-sylow de $GL(n, \mathbb{F}_p)$.
   On sait par ailleurs que tout groupe de cardinal n se réalise comme sous-groupe de $\mathfrak{S}_n$, lui même sous-groupe de $GL(n, K)$ pour n'importe quel corps K (via les matrices de permutations). Donc il suffit maintenant de voir qu'un sous-groupe d'un groupe admettant un p-sylow en admet un aussi. Pour cela, on va le chercher sous-forme de conjugué de ce p-sylow.
   Soit H un sous-groupe de G et S un p-sylow de G. Le groupe G agit naturellement sur G/S par translation. Le stabilisateur de la classe de 1 est S, et les autres stabilisateurs lui sont conjugués. Restreignons cette action à une action de H sur G/S. Celle-ci n'est a priori plus transitive. Les stabilisateurs sont les $H \cap gSg^{-1}$ pour $g \in G$. L'un de ces stabilisateurs est nécessairement un p-sylow de G. En effet, H agit sur G/S qui est un ensemble de cardinal premier à p car S est un p-sylow de G. L'ensemble G/S est partitionné en ses orbites sous l'action de H qui ne peuvent donc pas être toutes de cardinal divisibles par p. Cela signifie justement qu'un des stabilisateurs est de cardinal p^α, à savoir la puissance de p maximale pour un sous-groupe de H.
2. C'est une conséquence de la version forte de l'existence que l'on vient de montrer. Si S et S' sont deux p-sylows, il existe une conjugaison par $g \in G$ qui envoie S sur un p-sylow de S', c'est à dire S' tout entier.
3. D'après 2., G agit transitivement par conjugaison sur l'ensemble de ses p-sylows. Le stabilisateur d'un p-sylow pour cette action est exactement le normalisateur de ce p-sylow. En effet, c'est l'ensemble $Stab(S) = \{g \in G | gSg^{-1} = S\}$, c'est la définition du normalisateur de S dans G noté $N_G(S)$. En particulier, n_p divise n, l'ordre de G. Les autres congruences s'obtiennent en restreignant cette action par conjugaison sur l'ensemble des sylows à une action d'un sylow particulier. Cette fois, c'est une action d'un p-groupe, donc l'ensemble de ces points fixes à même cardinal modulo p que l'ensemble entier. C'est-à-dire, $n_p = \#\{S' | sS's^{-1} = S', \forall s \in S\} \pmod p$. On utilise l'argument de Frattini : Soit S'

différent de S, stable par conjugaison par les éléments de S. Le groupe P engendré par S et S' normalise S'. Mais ce groupe P a deux p-sylows distincts S et S' qui sont conjugués dans P par le point 2., ce qui est contradictoire. Donc S est le seul sylow dans l'ensemble ci-dessus, d'où $n_p = 1 \pmod p$. Le dernier point est conséquence du lemme de Gauss.

□

Applications

1. Un groupe d'ordre 63 n'est jamais simple. En effet, $63 = 9 \times 7$, il n'y a qu'un 7-sylow car n_7 divise 9 et $n_7 = 1 \pmod 7$ implique $n_7 = 1$. S'il existe un unique p-sylow dans un groupe il est distingué (même caractéristique), donc ce 7-sylow est distingué.
2. Un groupe d'ordre 255 n'est jamais simple. On a : $255 = 5 \times 51$. Le 51-sylow est unique donc distingué.
3. Construction d'un automorphisme non intérieur de $\mathfrak{S}_6$. Le groupe $\mathfrak{S}_5$ a six 5-sylows. Il faut compter les sous-groupes d'ordre 5 de $\mathfrak{S}_5$, ils sont engendrés par des 5-cycles qui figurent au nombre de 24. Chaque 5-sylow en contient 4 (+ l'identité), donc il y a $\frac{24}{4} = 6$, 5-sylows. Autre méthode, d'après le théorème de Sylow n_5 divise 24 et est congru à 1 modulo 5, donc $n_5 = 1$ ou 6. Mais 1 n'est pas possible le 5-sylow serait distingué

   L'action par conjugaison de $\mathfrak{S}_5$ sur ses 5-sylows est transitive d'après le théorème de Sylow. L'action est alors fidèle car le noyau de l'action est un sous-groupe distingué de $\mathfrak{S}_5$ qui est au moins d'indice 6 car l'action est transitive (donc l'image de l'action a au moins 6 permutations), et $\mathfrak{S}_5$ n'a que $\mathfrak{A}_5$ comme sous-groupe distingué qui lui est d'indice 2. On a donc trouvé un sous-groupe d'indice 6 de $\mathfrak{S}_6$ qui n'est conjugué à aucun des stabilisateurs des $i \in [|1, n|]$ puisqu'il agit transitivement. Ces deux actions inéquivalentes fournissent un automorphisme non intérieur de $\mathfrak{S}_6$. A revoir, ce n'est pas clair..

Leçons concernées : action de groupe,groupes finis, sous-groupe distingué, (groupe linéaire).