Théorèmes de Sylow

Chen Thomas
t.chen.thomas1[at]gmail.com

16 mai 2024

Attention

1. Ce document contient certainement des coquilles. N'hésitez pas à me le signaler. De même si vous avez une question.
2. Pour les recasages, ce sont les miens mais ce développement se case peut-être ailleurs et je n'y ai pas réfléchi.
3. Il se peut que ce développement dure plus de 15 minutes. J'ai essayé de le découper pour faire des recollements personnalisés.

Leçons

- 101 : Groupe opérant sur un ensemble. Exemples et applications.
- 103 : Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.
- 104 : Groupes finis. Exemples et applications.
- 190 : Méthodes combinatoires, problèmes de dénombrement. Applications.

Références

[1] D. Perrin. *Cours d'algèbre.* Ellipses, 1996.

Tout est dans [1].

Lemme 1. Soit $G = \mathrm{GL}_n(\mathbb{F}_p)$. Alors S, le sous-groupe de G constitué de matrices triangulaires supérieures de diagonale égale à 1, est un p-Sylow de G.

Démonstration. Pour obtenir le cardinal de G, il suffit de regarder le nombre de choix par colonne. Pour la première colonne, il y a $p^n - 1$ choix, pour la deuxième, $p^n - p$ choix, etc. Au final,

$$|G| = \prod_{i=0}^{n-1} (p^n - p^i) = \prod_{i=1}^{n-1} p^i \prod_{i=1}^{n} (p^i - 1) = p^{n(n-1)/2} m$$

avec $m = \prod_{i=1}^{n} (p^i - 1)$ et $p \nmid m$. Cela coïncide avec le cardinal de S donc S est bien un p-Sylow de G. $\square$

Lemme 2. Soit G un groupe fini et H un sous-groupe de G. Soit S un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.

Démonstration. On considère l'action de H sur G/S par translation à gauche. Le stabilisateur pour cette action de aS est alors $aSa^{-1} \cap H$. En effet, si $h \in aSa^{-1} \cap H$, alors $haS = aS$ et réciproquement, si $h \in H$ vérifie $haS = aS$, alors pour tout $s \in S$, il existe $s' \in S$ tel que $h = ass'a^{-1}$ donc $h \in aSa^{-1} \cap H$.

On a alors $|\omega(aS)| = \dfrac{|H|}{|aSa^{-1} \cap H|}$. Puisque $|G/S|$ est la somme des cardinaux des différents orbites, tous les cardinaux des orbites ne peut être divisible par p : il existe donc $a \in G$ tel que $p \nmid |\omega(aS)|$ ce qui signifie que $|aSa^{-1} \cap H|$ est un p-Sylow de H. □

Théorème 3 (Premier théorème de Sylow). *Si G est un groupe fini de cardinal n et p un diviseur premier de $|G|$, alors G admet un p-Sylow.*

Démonstration. G s'injecte dans $\mathfrak{S}_n$: en effet, G agit sur lui-même par translation à gauche ce qui induit une injection de G dans $\mathfrak{S}_G \simeq \mathfrak{S}_n$ par l'action. Enfin, $\mathfrak{S}_n$ s'injecte dans $\mathrm{GL}_n(\mathbb{F}_p)$ via les matrices de permutations. Autrement dit, G est un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$ qui admet un p-Sylow par le premier lemme. Par le deuxième lemme, G admet un p-Sylow. □

Théorème 4 (Deuxième théorème de Sylow). *Soit G un groupe fini de cardinal $n = p^\alpha m$ avec $p \nmid m$, $p \in \mathcal{P}, \alpha \in \mathbb{N}^*$.*

1. *Si H est un p-groupe de G, alors il existe S p-Sylow de G tel que $H \subset G$.*
2. *Les p-Sylow de G sont conjugués : en particulier, leur nombre n_p divise n.*
3. *$n_p \equiv 1[p]$ donc $n_p | m$.*

Démonstration.

1. Soit S un p-Sylow de G (existe par le premier théorème de Sylow). Alors par le lemme 2, il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H. Un p-Sylow d'un p-groupe, c'est le p-groupe donc $aSa^{-1} \cap H = H$ *i.e.* $H \subset S$.
2. Si H est un p-Sylow de G, par le point précédent, $H \subset aSa^{-1}$ et par cardinalité, $H = aSa^{-1}$: les p-Sylow sont conjugués. En notant X l'ensemble des p-Sylow de G, G agit sur X par conjugaison et cette action n'a qu'une seule orbite : son cardinal, qui est $|X| = n_p$, divise donc $|G|$.
3. On fait agir S sur X et on note $X^S := \{Y \in X : \forall s \in S, sYs^{-1} = Y\}$ avec toujours X l'ensemble des p-Sylow de G. Alors $|X| \equiv |X^S| \quad [p]$. En effet, X^S est l'ensemble des points fixes pour l'action donc en rangeant les orbites par leurs cardinaux, $|X| = |X^S| + \sum_{|\omega|>1} |\omega|$. Or, $|\omega|$ divise $|S|$ donc si le cardinal n'est pas 1, il est divisible par p. En plongeant modulo p, on obtient le résultat.

   Il suffit donc de montrer que $X^S = 1$. Soit $T \in X^S$ ce qui signifie que $\forall s \in S, sTs^{-1} = T$. Soit $N = \langle T, S \rangle$. Alors $\forall n \in N, nTn^{-1} = T$ donc T est un p-Sylow de G donc de N et est distingué dans N : par le point précédent, il est donc unique et puisque S vérifie la même assertion, $S = T$.

□