Théorème de Sylow

Leçons : 101, 103, 104

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

Définition 1

Un p-Sylow de G est un sous-groupe de G d'ordre p^α, ou bien de manière équivalente un p-sous-groupe maximal de G.

Théorème 2

Soit p premier et G un groupe d'ordre $p^\alpha m$ où $p \not| m$. Alors

1. *G admet au moins un p-Sylow.*
2. *Si H est un sous-groupe de G qui est un p-groupe, il existe un p-Sylow S de G contenant H.*
3. *Les p-Sylow sont tous conjugués et leur nombre k divise n.*
4. *$k \equiv 1[p]$ donc k divise m.*

Lemme 3

Si G admet un p-Sylow S et H est un sous-groupe de G d'ordre divisible par p, alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de G.

Démonstration. Le groupe G agit sur l'ensemble des classes à gauche modulo S, G/S, via $g \cdot (aS) = (ga)S$ (action par translation) et on vérifie sans mal que le stabilisateur de aS est aSa^{-1}. Donc H agit par restriction sur G/S et le stabilisateur de aS est $aSa^{-1} \cap H$. Fixons $a_1, \dots, a_r$ des représentants des orbites de cette action. Selon la formule des classes,

$$m = \frac{|G|}{|S|} = \sum_{i=1}^{r} \frac{|H|}{|a_i S a_i^{-1} \cap H|}$$

donc comme p ne divise pas m, il existe $i \in [\![1, r]\!]$ tel que p ne divise pas $\dfrac{|H|}{|a_i S a_i^{-1} \cap H|}$. Par conséquent, $a_i S a_i^{-1} \cap H$ est un p-Sylow de H. □

Démonstration. **1** Tout d'abord, remarquons qu'on peut supposer que G est un sous-groupe de $G' = \mathrm{GL}_n(\mathbb{F}_p)$. En effet,

$$\begin{array}{rccc} \varphi : & G & \longrightarrow & \mathfrak{S}_n \\ & g & \longmapsto & (x \mapsto gx) \end{array} \quad \text{et} \quad \begin{array}{rccc} \psi : & \mathfrak{S}_n & \longrightarrow & \mathrm{GL}(\mathbb{F}_p^n) \\ & \sigma & \longmapsto & (e_i \mapsto e_{\sigma(i)}) \end{array}$$

(avec $(e_1, \dots, e_n)$ la base canonique de $\mathbb{F}_p^n$) sont des morphismes injectifs.

Or, l'ensemble T des matrices triangulaires supérieures de la forme $\begin{pmatrix} 1 & & \star \\ & \ddots & \\ (0) & & 1 \end{pmatrix}$ est de cardinal $p \times p^2 \times \cdots \times p^{n-1} = p^{n(n-1)/2}$, alors que $\mathrm{GL}_n(\mathbb{F}_p)$ est d'ordre

$$(p^n - 1) \times (p^n - p) \times \cdots \times (p^n - p^{n-1}) = p^{n(n-1)/2} \prod_{i=0}^{n-1} (p^{n-i} - 1)$$

donc T est un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$. Selon le lemme, G admet un p-Sylow.

2 Soit H sous-groupe de G d'ordre p^i, soit S p-Sylow de G. Selon le lemme, il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H. Mais H étant un p-groupe, on a $aSa^{-1} \cap H = H$. Par ailleurs, $aSa^{-1} \cap H \subset aSa^{-1}$, ce dernier groupe étant un p-Sylow de G puisqu'il est de même ordre que S. Donc H est bien contenu dans un p-Sylow de G.

3 Soit S' p-Sylow de G. Appliquons le raisonnement du **2** avec $H = S'$: on trouve que $S' = aSa^{-1} \cap S' \subset aSa^{-1}$; ainsi, grâce à l'égalité des cardinaux de part et d'autre, $S' = aSa^{-1}$: les p-Sylow sont tous conjugués. Par conséquent, si X est l'ensemble des p-Sylow de G, G agit transitivement par conjugaison sur X, de sorte que selon la relation orbite-stabilisateur, k divise n.

4 Si S est un p-Sylow de G, il agit sur X par restriction de l'action précédente. S étant un p-groupe, selon un résultat bien connu, si $X^S = \left\{S' \in X : \forall s \in S, sSs^{-1} = S'\right\}$, $|X| \equiv \left|X^S\right| [p]$.

Or, soit $T \in X^S$. Introduisons (c'est l'« argument de Frattini ») le sous-groupe N de G engendré par T et S. Le groupe T est distingué dans N par hypothèse, et de plus c'est un p-Sylow de N (puisque $N \subset G$). Donc T est l'unique p-Sylow de N selon le point **3**. Comme S est un p-Sylow de N, l'égalité $T = S$ s'ensuit, si bien que X^S est de cardinal 1. Donc $k = |X| \equiv 1[p]$.

Enfin, k divise m car $pk + 1$ et p sont premiers entre eux pour $k \in \mathbb{Z}$.

□

Corollaire 4

Il n'y a pas de groupe simple d'ordre 255.

Démonstration. Soit G d'ordre $255 = 3 \times 5 \times 17$. G admet $k_5 \equiv 1[5]$ p-Sylow d'ordre 5 et k_5 divise $3 \times 17 = 51$. Cela est impossible si $k_5 \neq 1$ (il suffit d'énumérer les premières valeurs possibles de k_5 pour s'en convaincre). Donc G admet un unique p-Sylow d'ordre 5 qui est donc un sous-groupe distingué.

□

Référence : Daniel PERRIN (1996). *Cours d'algèbre*. Ellipses, pp. 18-20