26. Théorème de Sylow [Per96, §I.5, p18–19] [Szp09, §3.VIII.2, p273–274]

Énoncé

Théorème. [Théorème de Sylow 1] *Il existe au moins un p-Sylow dans G.*

Corollaire. *Il existe au moins un sous-groupe de G d'ordre p^i pour tout $i \in [\![1, a]\!]$.*

Développement

Pour montrer le premier théorème de Sylow, on va d'abord étudier l'exemple de $\mathcal{GL}_n(\mathbb{F}_p)$ puis se ramener dans le cas général à l'étude de notre exemple.

1. Le cas de $G = \mathcal{GL}_n(\mathbb{F}_p)$. On a :

$$\begin{aligned}\operatorname{card}(\mathcal{GL}_n(\mathbb{F}_p)) &= \operatorname{card}(\text{bases de } \mathbb{F}_p) = (p^n - 1) \times (p^n - p) \times \cdots \times (p^n - p^{n-1}) \\ &= p^{n(n-1)/2} m\end{aligned}$$

   où $m \wedge p = 1$. Un p-Sylow de G a donc $p^{n(n-1)/2}$ éléments.

   Soit T l'ensemble des matrices triangulaires supérieures de coefficients diagonaux 1.
   On vérifie que c'est un sous-groupe de G de cardinal p puissance le nombre de coefficients strictement supérieurs, c'est-à-dire $p^{n(n-1)/2}$.
   Ainsi, T est un p-Sylow de $\mathcal{GL}_n(\mathbb{F}_p)$.

2. Soit maintenant G un groupe quelconque d'ordre n.
   On va montrer que G est isomorphe à un sous-groupe de $\mathcal{GL}_n(\mathbb{F}_p)$.

   Par le théorème de Cayley[1], on a que G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.
   De plus, l'application $\sigma \longmapsto P_\sigma$ est un morphisme injectif de $\mathfrak{S}_n$ dans $\mathcal{GL}_n(\mathbb{F}_p)$.
   On obtient donc que G est isomorphe à un sous-groupe de $\mathcal{GL}_n(\mathbb{F}_p)$.

3. Terminons en montrant que si G est un sous-groupe d'un groupe H possédant un p-Sylow S, alors G possède un p-Sylow.

   Faisons agir H sur H/S par translation à gauche. On a $\operatorname{Stab}_H(aS) = aSa^{-1}$ et en restreignant l'action à G, on a $\operatorname{Stab}_G(aS) = aSa^{-1} \cap G$.
   Les $(aSa^{-1} \cap G)_{a \in H}$ sont des p-groupes. Montrons que l'un d'entre eux est un p-Sylow de G, c'est-à-dire que $|G| \,/\, \left|aSa^{-1} \cap G\right| \wedge p = 1$ pour un $a \in H$.

   Supposons que ce n'est pas le cas. Alors p divise $|G| \,/\, |\operatorname{Stab}_G(aS)|$ pour tout $a \in H$ et donc par l'équation aux classes

$$p \mid |H/S| = \sum_{O \in \mathcal{O}_G} |O| = \sum_{O \in \mathcal{O}_G} |G| \,/\, |\operatorname{Stab}_G(a_O S)|$$

   où $a_O \in H$ est tel que $a_O S$ est un élément de l'orbite O.
   Ceci est absurde puisque S est un p-Sylow de H.

   Donc G admet un p-Sylow.

Montrons désormais le corollaire. Par le théorème, on peut supposer que G est un p-groupe d'ordre p^a. On procède par récurrence sur $a \in \mathbb{N}$:

- Si $a = 0$ ou $a = 1$, il n'y a rien à montrer.
- Si $a \geq 2$, supposons le résultat vrai pour $a - 1$.

  Le centre $Z(G)$ est un p-groupe non trivial de G, soit $x \neq e \in Z(G)$. On a $o(x) = p^b$ pour un $b < a$. Posant $y = x^{p^{b-1}}$, on a que y est d'ordre p et donc $H = G/\langle y \rangle$ est d'ordre p^{a-1}.

  Soit $i \leq a - 1$. Par hypothèse de récurrence, H possède un sous-groupe H_i d'ordre p^i.
  Posons $G_{i+1} = \pi^{-1}(H_i)$ où $\pi : G \longrightarrow G/H$ est la surjection canonique.
  Alors $G_{i+1} / \ker(\pi) \simeq H_i$ donc $|G_{i+1}| = p\,|H_i| = p^{i+1}$.
  On a donc trouvé un groupe d'ordre p^i pour $1 \leq i \leq a$. Bien sur, G possède un groupe d'ordre p^0.

  L'hypothèse de récurrence est donc vraie au rang a.

D'où le résultat par récurrence.

[1] on utilise l'action par translation à gauche pour le montrer