Premier théorème de Sylow

En procédant par récurrence sur le cardinal du groupe, on montre l'existence d'un sous-groupe de Sylow.

Théorème 1 (Cauchy "faible")**.** Soit G un groupe abélien fini et soit p un diviseur premier de l'ordre de G. Alors, il existe un sous-groupe de G d'ordre p. [GOU21] p. 44

Démonstration. G est fini, on peut donc l'écrire

$$G = \langle x_1, \dots, x_n \rangle$$

où $(x_1, \dots, x_n)$ est un système de générateurs de G. On définit

$$\varphi : \begin{array}{ccc} \langle x_1 \rangle \times \dots \times \langle x_n \rangle & \rightarrow & G \\ (y_1, \dots, y_n) & \mapsto & y_1 \dots y_n \end{array}$$

Comme G est abélien, φ est clairement un morphisme de groupes. Et comme $(x_1, \dots, x_n)$ est un système de générateurs de G, φ est surjectif. On peut appliquer le premier théorème d'isomorphisme pour obtenir

$$G \cong (\langle x_1 \rangle \times \dots \times \langle x_n \rangle)/\mathrm{Ker}(\varphi)$$

En particulier, $|G| \times |\mathrm{Ker}(\varphi)| = |\langle x_1 \rangle| \times \dots \times |\langle x_n \rangle|$. On note, pour tout $i \in [\![1, n]\!]$, $r_i = |\langle x_i \rangle|$. On a ainsi,

$$G \mid r_1 \dots r_n \implies p \mid r_1 \dots r_n$$

par transitivité de $\mid$. Par le lemme d'Euclide, il existe $i \in [\![1, n]\!]$ tel que $p \mid r_i$. On écrit $r_i = pq$ avec $q \in \mathbb{N}^*$, et on pose $x = x_i^q$. Alors, x est d'ordre p et $H = \langle x \rangle$ est un sous-groupe de G d'ordre p. □

Théorème 2 (Premier théorème de Sylow)**.** Soit G un groupe fini d'ordre np^α avec $n, \alpha \in \mathbb{N}$ et p premier tel que $p \nmid n$. Alors, il existe un sous-groupe de G d'ordre p^α.

Démonstration. Posons $h = |G|$. On va procéder par récurrence forte sur h.

— Si $h = 1$: Alors, $n = 1$ et $\alpha = 0$. La propriété est donc triviale.

— On suppose la propriété vraie pour les groupes d'ordre strictement inférieur à h. Si $\alpha = 0$, c'est encore une fois trivial, pour les mêmes raisons qu'à l'initialisation de la propriété. Supposons donc $\alpha \geq 1$. On fait agir G sur lui-même par conjugaison, via l'action :

$$(g, h) \mapsto ghg^{-1}$$

Soit Ω un système de représentants associé à la relation "être dans la même orbite". La formule des classes donne

$$|G| = \sum_{\omega \in \Omega} |G \cdot \omega| = \sum_{\omega \in \Omega} (G : \mathrm{Stab}_G(\omega)) = \sum_{\omega \in \Omega} \frac{|G|}{|\mathrm{Stab}_G(\omega)|} \qquad (*)$$

Mais,

$$\mathrm{Stab}_G(\omega) = G \iff \forall g \in G, g\omega g^{-1} = \omega \iff \omega \in Z(G)$$

donc, en regroupant, on peut réécrire $(*)$:

$$\begin{aligned} |G| &= \sum_{\omega\in\Omega} \frac{|G|}{|\mathrm{Stab}_G(\omega)|} \\ &= \sum_{\omega\in Z(G)} \frac{|G|}{|\mathrm{Stab}_G(\omega)|} + \sum_{\omega\notin Z(G)} \frac{|G|}{|\mathrm{Stab}_G(\omega)|} \\ &= |Z(G)| + \sum_{\omega\notin Z(G)} \frac{|G|}{|\mathrm{Stab}_G(\omega)|} \end{aligned} \tag{$**$}$$

On a maintenant deux cas :

— Il existe ω tel que $p^\alpha \mid |\mathrm{Stab}_G(\omega)|$: Alors, comme $\mathrm{Stab}_G(\omega)$ est un sous-groupe de G d'ordre divisant strictement celui de G, on peut y appliquer l'hypothèse de récurrence pour obtenir un sous-groupe d'ordre p^α. Ce sous-groupe est donc également un sous-groupe de G.

— Pour tout ω, $p^\alpha \nmid |\mathrm{Stab}_G(\omega)|$: Alors, en factorisant par p dans les termes de la somme de $(**)$, on constate que $p \mid \frac{|G|}{|\mathrm{Stab}_G(\omega)|}$ pour tout $\omega \notin Z(G)$. Comme $p \mid h$, toujours d'après $(**)$, on a

$$p \mid |Z(G)|$$

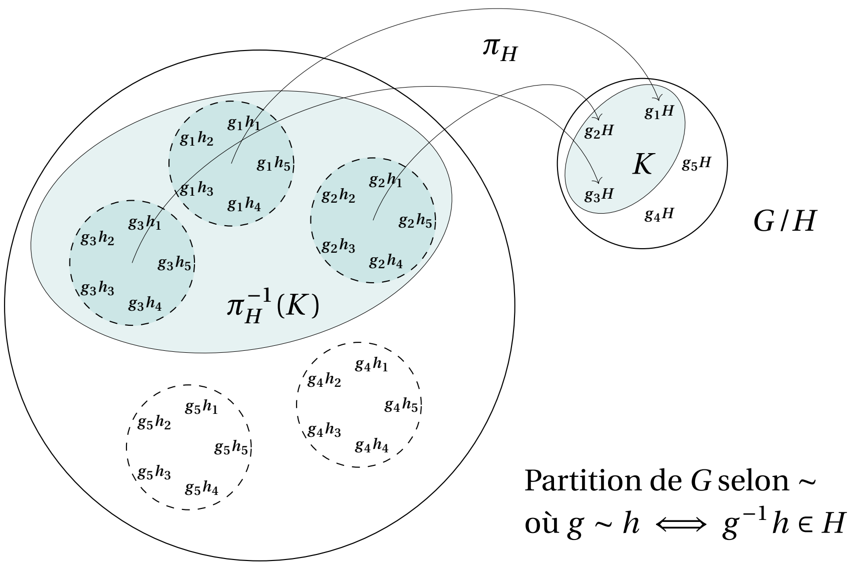
$Z(G)$ étant commutatif, on peut appliquer le Théorème 1. On obtient l'existence d'un sous-groupe H de $Z(G)$ d'ordre p, qui est de plus distingué dans G car inclus dans $Z(G)$. Alors,

$$|G/H| = \frac{|G|}{|H|} = np^{\alpha-1}$$

Il suffit maintenant d'appliquer l'hypothèse de récurrence à G/H, qui donne l'existence d'un sous-groupe K de G/H d'ordre $p^{\alpha-1}$. On considère la surjection canonique

$$\pi_H : G \to G/H$$

Alors, $\pi_H^{-1}(K) = \{g \in G \mid gH \in K\}$ est un sous-groupe de G d'ordre $|K| \times |H| = p^\alpha$:



ce qu'on voulait.

$\square$

Bibliographie

Les maths en tête **[GOU21]**

Xavier GOURDON. *Les maths en tête. Algèbre et probabilités.* 3e éd. Ellipses, 13 juill. 2021. https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html.