2.6 Théorèmes de Sylow et les groupes d'ordre pq (101, 103, 104) [11], [4]

Un théorème central de la théorie des groupes, utilisé pour classifier les groupes finis, et qui donne une réciproque partielle au théorème de Lagrange en plus d'être utile pour exhiber un automorphisme de $\mathfrak{S}_6$ qui ne soit pas intérieur (cf le développement juste après !). Utilise toute l'artillerie des actions de groupes, bref un des théorèmes les plus pédagogiquement efficaces que j'ai vus !

Théorème 2.16 (Sylow)**.** Soit G un groupe fini, de cardinal $p^\alpha m$ avec $\alpha \in \mathbb{N}^*$, p un nombre premier et $m \in \mathbb{N}^*$ tel que $p \nmid m$. Alors :

1. Il existe un sous-groupe de G de cardinal p^α. Un tel sous-groupe est appelé p-Sylow.
2. Si H est un p-sous-groupe de G (i.e. un sous-groupe de G de cardinal une puissance de p), alors H est contenu dans un p-Sylow de G.
3. Les p-Sylow de G sont tous conjugués. En particulier, G a un unique p-Sylow si et seulement s'il est distingué dans G.
4. Si n_p désigne le nombre de p-Sylow de G, on a :

$$\begin{cases} n_p \mid m \\ n_p \equiv 1 \ [p]. \end{cases}$$

Démonstration. 1. À peu près tous les résultats énoncés vont découler du lemme suivant :

Lemme 2.17. Soient G un groupe fini, p un nombre premier divisant $|G|$ et H un sous-groupe de G. Si S est un p-Sylow de G alors, il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H.

Démonstration du lemme. On considère l'action de G sur le quotient $\dfrac{G}{S}$ par translation à gauche, c'est-à-dire :

$$\forall h \in G, \ \forall h \in G, \quad h \cdot (gS) = (hg)S.$$

Si $g \in G$, on a alors que le stabilisateur de la classe gS est :

$$\mathrm{Stab}_G(gS) := \{h \in G \mid (hg)S = gS\} = gSg^{-1}.$$

On a alors que les groupes $gSg^{-1} \cap H$ sont en fait les stabilisateurs de gS pour l'action précédente, restreinte à H. Montrons que l'un de ces stabilisateurs est un p-Sylow de H. Pour cela, il suffit de montrer qu'il existe $g \in G$ tel que l'indice $[H : gSg^{-1} \cap H]$ soit premier avec p. Si tel n'était pas le cas, on aurait, par la formule des classes :

$$\left|\frac{G}{S}\right| = \sum_{gS \in \mathscr{R}} |H \cdot (gS)|$$

où $\mathscr{R}$ désigne un système de représentants pour l'action de H sur $\frac{G}{S}$. Or, par la relation orbites-stabilisateurs :

$$|H \cdot (gS)| = [H : gSg^{-1} \cap H].$$

Ainsi, si pour tout $g \in G$, $[H : gSg^{-1} \cap H]$ était divisible par p, il en serait de même pour $\left|\frac{G}{S}\right| = m$, premier avec p par hypothèse ! **ABSURDE !** Cela conclut donc la preuve de ce lemme. □

À partir de là, on peut, grâce au théorème de Cayley, plonger G dans le groupe symétrique $\mathfrak{S}_{p^\alpha m}$. En

effet, l'action de G sur lui-même par translation à gauche donne un morphisme injectif (car l'action est libre) :

$$\begin{array}{rccl} \rho & : & G & \longrightarrow & \mathfrak{S}_G \\ & & g & \longmapsto & \rho(g) : h \mapsto gh \end{array}$$

et le groupe $\mathfrak{S}_G$ est évidemment isomorphe à $\mathfrak{S}_{|G|} = \mathfrak{S}_{p^\alpha m}$. On a également le morphisme injectif suivant :

$$\begin{array}{rccl} \Psi & : & \mathfrak{S}_{p^\alpha m} & \longrightarrow & GL_{p^\alpha m}(\mathbb{F}_p) \\ & & \sigma & \longmapsto & P_\sigma = \left(\delta_{i,\sigma(j)}\right)_{1\leq i,j\leq p^\alpha m}. \end{array}$$

Ainsi, G est isomorphe à un sous-groupe de $GL_n(\mathbb{F}_p)$ avec $n = p^\alpha m$, dont on connaît le cardinal et un p-Sylow ! En effet :

$$|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)\dots(p^n - p^{n-1}) = p^{\frac{n(n-1)}{2}} \prod_{i=1}^{n}(p^i - 1),$$

et le sous-groupe :

$$U = \{I_n + T \mid T \in \mathscr{T}_n^{*\sup}(\mathbb{F}_p)\}$$

des matrices unipotentes triangulaires supérieures (ici $\mathscr{T}_n^{*\sup}(\mathbb{F}_p)$ désigne les matrices triangulaires supérieures strictes à coefficients dans $\mathbb{F}_p$) est exactement d'ordre $p^{\frac{n(n-1)}{2}}$, c'est donc un p-Sylow de $GL_n(\mathbb{F}_p)$. Ainsi, par le lemme, G possède un p-Sylow !

2. Prenons donc S un p-Sylow de G. En reprenant la démonstration du lemme avec H un p-sous-groupe, on a donc qu'il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H, mais comme H est un p-groupe, on a donc :

$$H = gSg^{-1} \cap H$$

et donc :

$$H \subset gSg^{-1}$$

qui est un p-Sylow de G.

3. Si H est cette fois un p-Sylow, alors par égalité des cardinaux, on a :

$$H = gSg^{-1}.$$

Les p-Sylows sont donc tous conjugués. Ainsi, si G a un unique p-Sylow S, on a :

$$\forall g \in G, \quad gSg^{-1} = S$$

car gSg^{-1} est également un p-Sylow. Donc S est normal dans G. Réciproquement, si S est normal dans G, alors, si H est un p-Sylow de G, il est conjugué à S. Étant donné que S est normal, on a donc $H = S$.

4. Le poiont 3 permet alors de justifier l'action suivante, en notant $\mathscr{S}$ l'ensemble des p-Sylows de G :

$$\begin{array}{rcl} G \times \mathscr{S} & \longrightarrow & \mathscr{S} \\ (g, H) & \longmapsto & gHg^{-1}. \end{array}$$

Les p-Sylows de G étant tous conjugués, on a que cette action est transitive, et donc :

$$|\mathscr{S}| := n_p = |G \cdot S| = [G : \mathrm{Stab}_G(S)].$$

Ainsi :

$$n_p \mid p^\alpha m.$$

Considérons cette fois l'action restreinte à S. Si $H \in \mathscr{S}$, quel est son stabilisateur pour cette action ?

$$\mathrm{Stab}_S(H) = \left\{ g \in S \;\middle|\; gHg^{-1} = H \right\} = N_G(H) \cap S$$

où $N_G(H)$ désigne le *normalisateur* de H dans G. Par la formule des classes, on a :

$$|\mathscr{S}| := n_p = \left|\mathscr{S}^S\right| + \sum_{i=1}^{r} [S : N_G(H_i) \cap S],$$

où $(H_1, \ldots, H_r)$ désigne un système de représentants des orbites sous l'action de S dont les stabilisateurs ne sont pas S tout entier, et $\mathscr{S}^S$ désigne l'ensemble des points fixes pour cette action. Montrons :

$$\mathscr{S}^S = \{S\}.$$

On a déjà que S est un point fixe : pour tout $g \in S$, $gSg^{-1} = S$. Si cette fois H est un p-Sylow tel que pour tout $g \in S$, $gHg^{-1} = H$, on a :

$$S \subset N_G(H)$$

donc S est un p-Sylow de $N_G(H)$. Or, H est aussi un p-Sylow de $N_G(H)$ et on a en plus qu'il est distingué dans $N_G(H)$. Donc, par le point 3, $H = S$. Ainsi, on a :

$$n_p = 1 + \sum_{i=1}^{r} \underbrace{[S : N_G(H_i) \cap S]}_{=p^\beta \text{ avec } \beta \in [\![1,\alpha]\!]} \equiv 1 \ [p].$$

On a donc en particulier que $n_p \wedge p = 1$ et donc, puisque $n_p \mid p^\alpha m$:

$$n_p \mid m.$$

Cela conclut donc la démonstration ! □

S'il vous reste du temps, vous pouvez en profiter pour faire une application pas très dure de classification, par exemple :

Proposition 2.18 (Les groupes d'ordre pq)**.** Soient p et q deux nombres premiers avec $p < q$ et G un groupe d'ordre pq. Alors :

1. G n'est pas simple,
2. Si $p \nmid q - 1$, alors :
$$G \simeq \frac{\mathbb{Z}}{q\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}},$$
3. Si $p \mid q - 1$, alors il y a deux classes d'isomorphismes :
$$\frac{\mathbb{Z}}{q\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}$$
ou un produit semi-direct
$$\frac{\mathbb{Z}}{q\mathbb{Z}} \rtimes \frac{\mathbb{Z}}{p\mathbb{Z}}$$

Démonstration. 1. Si n_q désigne le nombre de q-Sylows de G, on a :

$$n_q \in \{1, p\},$$

car p est un nombre premier. Si $n_q = p$, on aurait :

$$q \mid p-1, \quad \textbf{ABSURDE !!}$$

car $p < q$! Donc $n_q = 1$. En particulier, si S_1 désigne cet unique q-Sylow, il est distingué dans G. Donc G n'est pas simple.

2. Si $p \nmid q-1$, on a alors $n_p = 1$ également. En effet, $n_p \in \{1, q\}$ puisque q est premier et $n_p \neq q$ car $q \not\equiv 1\ [p]$. Ainsi, si S_2 désigne l'unique p-Sylow de G, on a que S_2 est distingué dans G. Les conditions suivantes sont donc réunies :

$$S_1 \triangleleft G, \quad S_2 \triangleleft G, \quad S_1 \cap S_2 = \{e\} \quad \text{et} \quad S_1 S_2 = G$$

.

En effet, si $g \in S_1 \cap S_2$, alors son ordre divise $|S_1| = q$ et $|S_2| = p$. Étant donné que p et q sont premiers distincts, on a donc que g est d'ordre 1, donc $g = e$. Enfin, puisque $S_1 \cap S_2 = \{e\}$, on a $|S_1 S_2| = pq = |G|$, donc $S_1 S_2 = G$. Ainsi, on a l'isomorphisme :

$$G \simeq S_1 \times S_2.$$

Or S_1 est de cardinal q premier, donc $S_1 \simeq \dfrac{\mathbb{Z}}{q\mathbb{Z}}$. Idem, $S_2 \simeq \dfrac{\mathbb{Z}}{p\mathbb{Z}}$. D'où :

$$G \simeq \frac{\mathbb{Z}}{q\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}.$$

3. Dans cette situation, on est autorisé à avoir $n_p = q$. Dans ce cas, si S_2 est un p-Sylow de G, il n'est plus distingué. Cependant, les propriétés suivantes restent vérifiées :

$$S_1 \triangleleft G, \quad S_1 \cap S_2 = \{e\} \quad \text{et} \quad S_1 S_2 = G$$

.

pour les mêmes raisons que plus haut. On a donc :

$$G \simeq S_1 \rtimes_{\text{Int}} S_2$$

où Int désigne le morphisme :

$$\begin{array}{ccc} S_2 & \longrightarrow & \text{Aut}(S_1) \\ g & \longmapsto & \text{Int}_g : h \mapsto ghg^{-1}. \end{array}$$

Ainsi, on a donc l'isomorphisme avec un produit semi-direct :

$$G \simeq \frac{\mathbb{Z}}{q\mathbb{Z}} \rtimes \frac{\mathbb{Z}}{p\mathbb{Z}}.$$

□