Théorèmes de Sylow

Réf: Perrin, Cours d'algèbre p. 18 + Cours à l'ENS. «théorème de Cayley
Algèbre le grand combat p. 313.

Le théorème de Lagrange nous dit que si H est un ss-groupe de G alors $\#H \mid \#G$. On peut se demander si dans groupe de cardinal n, pour tout diviseur d de n il existe un sous-groupe de cardinal d. La réponse est non dans $\mathcal{A}_4$ on a $|\mathcal{A}_4| = 12$ et ne possède pas de sous-groupe de cardinal 6.
Les théorèmes de Sylow nous donnent une réciproque partielle à Lagrange.

Définition : p-Sylow.
Soit G un groupe fini de cardinal n et p un diviseurs premiers de n. Si $n = p^\alpha m$ avec $p \nmid m$, on appelle p-Sylow de G un sous-groupe de cardinal p^α.

Rmq: Dire que H est un p-Sylow de G signifie que:
1) H est un p-groupe
2) On a $[G:H] \wedge p = 1$.

Exemple très important: Vidéo dénombrement (léger).
Soit n un entier, p premier et $G = GL_n(\mathbb{F}_p)$.
G est un groupe fini de cardinal :

$$\#G = (p^n - 1)(p^n - p)\dots(p^n - p^{n-1}) = p^{1+(1+\dots+n-1)} \prod_{i=0}^{n-1} (p^{n-i} - 1) = p^{n(n+1)/2}\, q.$$

Avec $p \wedge q = 1$ car $p \nmid q$.
Un p-Sylow de G est donc un sous-groupe de G de cardinal $p^{n(n+1)/2}$ Or on a :

$$H = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right\} \subset GL_n(\mathbb{F}_p) = G$$

Il est facile de vérifier que H est un sous-groupe, de plus il est de cardinal:

$$\#H = p^{1+2+\dots+(n-1)} = p^{n(n+1)/2}$$

Donc H est un p-Sylow de G.

La clé pour prouver l'existence d'un p-Sylow va être le lemme suivant qui nous permet, à partir d'un p-Sylow de G trouver un p-Sylow si il est un sous-groupe de G.

Lemme: *Ici opération de groupe*

Soit G un groupe fini avec $\#G = n = p^\alpha m$, avec $p \nmid m$ et soit H un sous-groupe de G. Soit S un p-Sylow de G alors il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H.

Preuve:

On pose $X = G/S$. Alors G opère par translation à gauche par translation :

$$\begin{aligned} G \times G/S &\longrightarrow G/S \\ (g, \overline{g'}) &\longmapsto \overline{gg'} \end{aligned}$$

Par restriction cela induit une action de H sur G/S, et on pose $\overline{g} \in G/S$ que:

$$\mathrm{Stab}_H(\overline{g}) = \{h \in H \mid \overline{g} = \overline{hg}\} = \{h \in H \mid g^{-1}(hg) \in S\} = gSg^{-1} \cap H.$$

Il reste à voir que un de ses sous-groupes. Pour $\overline{g} \in G/S$, on pose $d = \#\mathrm{Stab}_H(\overline{g})$. Comme

$$\#gSg^{-1} = \#S.$$

On sait que gSg^{-1} est un p-Sylow de G, donc $\#gSg^{-1} = p^\alpha$ et

$$d \mid gSg^{-1} = p^\alpha$$

car ss-groupe

Ainsi pour tout $\overline{g} \in G/S$, $\mathrm{Stab}_H(\overline{g})$ est un p-groupe.

Il suffit donc de montrer qu'il existe $\overline{g} \in G/S$ tel que $[H : \mathrm{Stab}_H(\overline{g})] \wedge p = 1$.

Or on sait par la relation orbite stabilisateur que:

$$[H : \mathrm{Stab}_H(\overline{g})] = \#O_g.$$

Par l'absurde si toutes les orbites de G/S sous l'action de H étaient divisibles par p alors $\#G/S$ aussi, car G/S est la réunion des orbites disjointes. Mais ceci est absurde car S est un p-Sylow donc $p \nmid [G : S]$.

Ainsi il existe $g \in G$ tq $[H : \mathrm{Stab}_H(\overline{g})] \wedge p = 1$ i.e $\mathrm{Stab}_H(\overline{g}) = gSg^{-1} \cap H$ est un p-Sylow de H.

On peut maintenant montrer les théorèmes de Sylow.

Théorèmes : de Sylow.

Soit G un groupe fini, et soit p un nombre premier. Écrivons $\#G = p^\alpha m$ avec $\alpha \geq 0$ et $p \nmid q$.
Alors :

1) Il existe des p-Sylow de G et tout p-sous-groupe de G est contenu dans un p-Sylow.
2) Les conjugués d'un p-Sylow de G et un p-Sylow de G et tous les p-Sylow de G sont conjugués.
   En particulier, si S est un p-Sylow de G alors S est distingué dans G, si et seulement si, S est l'unique p-Sylow de G.
3) Si N_p est le nombre de p-Sylow de G, on a $N_p \equiv 1 [p]$ et $N_p \mid m$.

Preuve :

1 et 2) Par le théorème de Cayley, le groupe G s'identifie à un sous-groupe de $\mathfrak{S}_n$, où $n = |G|$.
Maintenant on identifie $\mathfrak{S}_n$ à un sous-groupe de $GL_n(\mathbb{F}_q)$.
Si $\sigma \in \mathfrak{S}_n$, on pose $M_\sigma = (m_{ij})$ où

$$m_{\sigma(j)j} = 1, m_{ij} = 0 \text{ si } i \neq \sigma(j)$$

On vérifie aisément que l'application

$$\begin{aligned} \mathfrak{S}_n &\longrightarrow GL_n(\mathbb{F}_p) \\ \sigma &\longmapsto M_\sigma \end{aligned}$$

est un morphisme de groupes injectif.
Ainsi G est isomorphe à un sous-groupe G' de $GL_n(\mathbb{F}_p)$. Or d'après l'exemple $GL_n(\mathbb{F}_p)$ possède un p-Sylow donc par le lemme G' aussi. Ainsi G possède un p-Sylow.

Soit maintenant H un p-sous-groupe de G et soit S un p-Sylow de G. Par le lemme on sait qu'il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H.
Mais H est un p-groupe donc par égalité du cardinal on a :

$$gSg^{-1} \cap H = H \text{ donc } H \subset gSg^{-1}.$$

Or on a déjà vu que gSg^{-1} est aussi un p-Sylow (égalité des cardinaux avec S) donc H inclus dans un p-Sylow.
De plus si H est un p-Sylow de G alors par égalité des cardinaux $H = gSg^{-1}$ donc les p-Sylow sont conjugués.

Si de plus S est le seul p-Sylow alors pour tout $g \in G$, $gSg^{-1} = S$ donc S est distingué.
Réciproquement, si S est un p-Sylow de G qui est distingué dans G alors pour $g \in G$ on a:

$$gSg^{-1} = S$$

Or tout les p-Sylow sont conjugués, on obtient que S est l'unique p-Sylow de G.

3). On note $\mathcal{E}$ l'ensemble des p-Sylow de G. D'après le point 2 on peut faire agir G sur $\mathcal{E}$ par conjugaison :

$$\begin{aligned} G \times \mathcal{E} &\longrightarrow \mathcal{E} \\ (g, S) &\longmapsto gSg^{-1} \end{aligned}$$

De plus on sait que cette action est transitive donc pour $S \in \mathcal{E}$, $\mathcal{O}_S = \mathcal{E}$ or le cardinal d'une orbite divise le cardinal de G donc $N_p \mid n = p^d m$.

Remarquons que pour S un p-Sylow de G, S opère par restriction sur $\mathcal{E}$ donc comme S est un p-groupe on a:

$$N_p \equiv |\mathcal{E}^S| \ [p] \qquad \leftarrow \text{point fixe sous l'action de } S.$$

Nous allons montrer que $\mathcal{E}^S = \{S\}$.
Il est clair que $\forall s \in S$, $sSs^{-1} = S$ donc $S \in \mathcal{E}^S$.
Soit T un p-Sylow tel que $T \in \mathcal{E}^S$, on a donc :

$$\forall s \in S, \ sTs^{-1} = T.$$

Soit G' le sous-groupe G engendré par S et T. On a $S \subset G'$ et $T \subset G'$ et ce sont donc p-Sylows de G'.
En effet puisque G' est un sous-groupe de G son ordre est de la forme :

$$\#G' = p^l m' \text{ avec } \alpha \geq l \geq 0 \text{ et } p \nmid m'.$$

Or $S \subset G'$ et $\#S = p^\alpha$ donc $l = \alpha$. Ainsi les p-Sylow de G' sont d'ordres p^α, donc S et T sont des p-Sylow de G'.
Or pour tout $g \in S \cup T$, on a: $gTg^{-1} \subset T$ donc $\forall g \in G'$, $gTg^{-1} \subset T$.
Donc T est distingué dans G', c'est donc l'unique p-Sylow, d'où $T = S$.
On a donc bien $\mathcal{E}^S = \{S\}$ ce qui donne:

$$N_p \equiv 1 \ [p]$$

Puisque $N_p \mid p^d m$ et $N_p \wedge p = 1$ on a: $N_p \mid m$, d'où le résultat. ∎

Corollaire: voir p18, Gourdon, Algèbre.

Si $|G| = p^\alpha m$, $p \nmid m$ alors pour tout $i \in [\![0, \alpha]\!]$, G contient un sous-groupe d'ordre p^i.

Preuve: Il suffit de montrer le résultat dans un p-Sylow de G qui est de cardinal p^α.

Ainsi on se place dans S qui est un p-sous-groupe de G de cardinal p^α.

On raisonne par récurrence sur α.

- Si $\alpha = 1$, le résultat est évident.
- On suppose le résultat vraie pour $\alpha \geq 1$ et on le montre pour $\alpha+1$.

Soit m tq $1 \leq m \leq \alpha+1$ (si $m=0$, $\{e\}$ convient)

Comme S est un p-groupe $Z(S) \neq \{e\}$ (son centre), soit $x \in Z(S) \setminus \{e\}$ alors x est d'ordre p^β avec $1 \leq \beta \leq \alpha+1$.

Ainsi $y = x^{p^{\beta-1}}$ est d'ordre p i.e $\langle y \rangle = H$ est d'ordre p, par ailleurs $H \subset Z(S)$ donc H est distingué dans S.

On considère donc le groupe quotient S/H qui est d'ordre $p^{\alpha-1}$. Par hypothèse de récurrence, S/H possède un sous-groupe d'ordre p^{m-1} noté K

On note $\pi : S \to S/H$ la surjection canonique et $F = \pi^{-1}(K)$. Ainsi F est un sous-groupe de S et par ailleurs :

$$K = \pi(F) = F/H$$

Ce qui donne :

$$p^{m-1} = \frac{\#F}{p} \quad \text{donc} \quad \#F = p^m$$

Donc F est un sous-groupe de S de cardinal p^m.

Application:

Exemple: Un groupe d'ordre 63 n'est pas simple.

En effet soit G un tel groupe, $\#G = 63 = 3^2 \cdot 7$.

On a $N_7 \mid 9$ donc $N_7 = 1, 3$ ou 9 or $N_7 \equiv 1 [7]$ donc $N_7 = 1$. Ainsi le 7-Sylow est d'ordre 7 est distingué dans G.

Le même type d'argument par $856 = 3 \times 5 \times 7$. ☑

Exemple: Un groupe d'ordre 33 est cyclique

Soit G d'ordre $33 = 3 \times 11$ alors $N_3 \mid 11$ donc $N_3 = 1$ ou 11 or $N_3 \equiv 1[3]$ donc $N_3 = 1$. Ainsi le 3-Sylow de G, H_1, est distingué dans G.

De même, $N_{11} \mid 3$ donc $N_{11} = 1$ ou 3 or $N_{11} \equiv 1[11]$ donc $N_{11} = 1$. Ainsi le 11-Sylow, H_2, est distingué dans G.

Or comme 3 et 11 sont premier entre eux $H_1 \cap H_2 = \{1_G\}$. Et comme 3 et 11 sont premiers, H_1 et H_2 sont cycliques, engendrés par h_1 et h_2 qui sont d'ordre 3 et 11.

Montrons que h_1 et h_2 commutes en effet: $h_1 h_2 = h_2 h_1$

$$\underbrace{h_1 h_2 h_1^{-1} h_2^{-1}}_{\in H_2 \text{ car distingué}} \in H_2 \quad \text{et} \quad \underbrace{h_1 h_2 h_1^{-1} h_2^{-1}}_{\in H_1 \text{ car distingué}} \in H_1$$

donc $h_1 h_2 h_1^{-1} h_2^{-1} \in H_1 \cap H_2 = \{1\}$ donc $h_1 h_2 = h_2 h_1$.

Donc $o(h_1 h_2) = \text{ppcm}(3, 11) = 33$ i.e G est cyclique engendré par $h_1 h_2$. ☑

Rmq:

Théorème de Cayley:

Soit G un groupe fini d'ordre n. Alors, G est isomorphe à un sous-groupe de $\mathfrak{S}_n$

Preuve:

On fait opérer G sur lui même par translation à gauche i.e

$$G \times G \longrightarrow G$$
$$(g, h) \longmapsto gh$$

Cette action est fidèle en effet soit $g \in G$ tel que:

$$\forall h \in G,\ gh = h \quad \text{avec } h = 1,\ g = 1.$$

Ainsi le morphisme associé à l'action: $\varphi: G \hookrightarrow \mathfrak{S}(G)$ est injectif.

Or G étant d'ordre n on a $\mathfrak{S}(G) \simeq \mathfrak{S}_n$ ainsi on obtient un morphisme injectif.

$$G \hookrightarrow \mathfrak{S}_n.$$

Donc G s'identifie à son image dans $\mathfrak{S}_n$ qui est un sous-groupe. ☑