Théorème de Sylow

Référence : [Per96] p.18-20.

Théorème 0.1 *Soit G un groupe de cardinal $|G| = n = p^\alpha m$ avec p premier et m ne divisant pas p. Alors :*

1. *Si H est un sous-groupe de G qui est un p-groupe alors il existe un p-Sylow S tel que $H \subset S$;*
2. *Les p-Sylow sont tous conjugués dans G (et donc leur nombre k divise n) ;*
3. *On a $k \equiv 1[p]$ (donc k divise m).*

Rappels :

Définition 0.1 *On appelle p-sous-groupe de G (où $|G| = p^\alpha m$ avec p premier et m ne divisant pas p) un sous-groupe de cardinal p^a (avec $a \leq \alpha$).*

Définition 0.2 *On appelle p-sous-groupe de Sylow de G (où $|G| = p^\alpha m$, p premier et m ne divisant pas p) un sous-groupe de cardinal p^α.*

Remarque : S est un p-sous-groupe de Sylow de G signifie :
– S est un p-groupe ;
– l'indice $(G : S)$ est premier avec p.

Démonstration

Étape 1 On montre l'existence d'un p-Sylow dans G.
On plonge tout d'abord G dans $\mathfrak{S}_n$ d'après le théorème de Cayley. Puis on plonge $\mathfrak{S}_n$ dans $GL_n(\mathbb{F}_p)$ de la manière suivante :

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

où u_σ est défini sur la base canonique par $u_\sigma(e_i) = e_{\sigma(i)}$.
Finalement, on a réalisé G comme sous-groupe de $GL_n(\mathbb{F}_p)$ qui possède un p-Sylow, donc G aussi d'après le lemme (0.1).

Étape 2 On démontre (1) et (2) ensemble.
Soit H un p-sous-groupe. Soit S un p-Sylow de G.
D'après un lemme ci-dessous, on sait qu'il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de G.
Mais comme H est un p-groupe, ie $|H| = p^\beta$, ainsi on a :
– $aSa^{-1} \cap H \subset H$ (par définition de l'intersection) ;
– $|H| = p^\beta$ et $|aSa^{-1} \cap H| = p^\alpha$ car c'est un p-Sylow.
Or p^α est le plus grand cardinal possible pour un p-sous-groupe d'où $H = aSa^{-1} \cap H$. En particulier $H \subset aSa^{-1}$ qui est un p-Sylow (car $aSa^{-1} \cap H \subset aSa^{-1}$). D'où le (1).
Si de plus H est un p-Sylow, alors on a exactement $H = aSa^{-1}$ car on peut faire la même preuve et aboutir à $H \subset aSa^{-1}$ et $|H| = |aSa^{-1}|$, d'où $H = aSa^{-1}$ dans ce cas. D'où le (2).

Étape 3 Montrons (3).
Soit X l'ensemble des p-Sylow de G. On considère l'action par conjugaison de G sur X, ie :

$$\begin{aligned}\rho : G &\longrightarrow \mathfrak{S}(X)\\ g &\longmapsto \rho_g : h \longmapsto ghg^{-1}\end{aligned}$$

Soit S un p-Sylow. S opère sur X (par restriction de l'action à S) et on a via un lemme qui suit :

$$|X| \equiv |X^S|[p]$$

Il reste à voir que $|X^S| = 1$. Bien sûr si $s \in S$, on a $sSs^{-1} = S$, autrement dit $S \in X^S$ et on doit donc montrer que c'est le seul.
Pour cela, soit T un p-Sylow et supposons T normalisé par S, ie

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

On considère le sous-groupe N de G engendré par S et T, ie $N =< S, T >$.
On a $S \subset N$ et $T \subset N$ et ce sont, a fortiori, des p-Sylow de N. Mais comme S normalise T, on a T distingué dans S et donc T est l'unique p-Sylow de N donc $S = T$.

Lemmes utilisés

Lemme 0.1 *Soit G un groupe avec $|G| = n = p^\alpha m$ avec p premier et m ne divisant pas p.*
Soit H un sous-groupe de G. Soit S un p-Sylow de G.
Alors $\exists a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de G.

Démonstration Le groupe G opère sur G/S ($= \{aS, a \in G\}$) par translation à gauche :

$$\begin{aligned}\sigma : G &\longrightarrow \mathfrak{S}(G/S)\\ g &\longmapsto \sigma_g : (aS) \longmapsto g.(aS) = (ga)S\end{aligned}$$

Montrons tout d'abord que le stabilisateur de aS dans G est aSa^{-1}.
- Soit $g \in Stab_G(aS)$, ie $g.(aS) = aS$, ie $\exists s, s' \in S$ tels que : $gas = as'$, ie $ga = as's^{-1}$, ie $g = as's^{-1}a^{-1}$, d'où $g \in aSa^{-1}$ (car S est un groupe).
- Soit $g \in aSa^{-1}$, alors $\exists s \in S$ tel que $g = asa^{-1}$. On considère $g.(aS) = (ga)S$, ie $g.(aS) = (asa^{-1}a)S = aS$ (car S est un groupe).

De plus H opère aussi sur G/S par restriction de l'action avec pour stabilisateur de aS : $aSa^{-1} \cap H$.
Il reste donc à voir que l'un de ces sous-groupes (les $aSa^{-1} \cap H$) est un Sylow de H. Ce sont déjà des p-groupes et il suffit donc que pour un $a \in G$, $|H/(aSa^{-1} \cap H)|$ soit premier avec p.
Mais on a d'après un lemme ci-dessous que $|H/(aSa^{-1} \cap H)| = |\omega(aS)|$ le cardinal de l'orbite de aS dans G/S sous l'action de H. Si tous ces nombres étaient divisibles par p, il en serait de même de $|G/S|$ car G/S est réunion des orbites $|\omega(aS)|$; ce qui contredit que S est un p-Sylow de G.

Lemme 0.2 *Soit G un p-groupe opérant sur un ensemble X. Soit X^G l'ensemble des points fixes sous G, ie*

$$X^G = \{x \in X, \forall g \in G, g.x = x\}$$

Alors $|X| \equiv |X^G|[p]$.

Démonstration On écrit X comme réunion disjointe de ses orbites sous G en remarquant que :

$$x \in X^G \Leftrightarrow \omega(x) = \{x\}$$

En effet :
- Si $x \in X^G$, alors par définition $\forall g \in G$, $g.x = x$. Or par définition :

$$\omega(x) = \{y \in X, \exists g \in G, y = g.x\} = \{g.x, g \in G\}$$

  D'où $\omega(x) = \{x\}$.
- Si $\omega(x) = \{x\}$ alors $\forall g \in G$, $g.x = x$ d'où $x \in X^G$.

Si $x \notin X^G$, on a donc $|\omega(x)| > 1$ et comme $|\omega(x)|$ divise $|G| = p^n$ (d'après le théorème de Lagrange), alors p divise $|\omega(x)|$.
Le résultat provient alors de l'égalité :

$$|X| = |X^G| + \sum_{x \notin X^G} |\omega(x)|$$

Lemme 0.3 *L'application :*

$$\begin{aligned} G/Hx &\longrightarrow \omega(x) \\ \overline{g} &\longmapsto g.x \end{aligned}$$

est une bijection (Hx est l'ensemble des classes à gauche).

Lemme 0.4 *$GL_n(\mathbb{F}_p)$ possède un p-Sylow.*

Démonstration Soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ avec p premier le corps fini à p éléments et on considère $GL_n(\mathbb{F}_p)$ pour $n \in \mathbb{N}^*$.
Alors on sait que $GL_n(\mathbb{F}_p)$ est un groupe fini de cardinal : $(p^n - 1)(p^n - p)\dots(p^n - p^{n-1})$, ie $|GL_n(\mathbb{F}_p)| = mp^{n\frac{n-1}{2}}$ avec m ne divisant pas p.
Soit $P = \{A = (a_{ij}), a_{ij} = 0, \text{si } i > j \text{ et } a_{ii} = 0\}$ l'ensemble des matrices triangulaires supérieures avec des 1 sur la diagonale. Alors P est un p-Sylow, en effet, les a_{ij} pour $i < j$ sont choisis quelconques et il reste $n^2/2 - n/2$ coefficients à choisir, sachant qu'on a p possibilités pour chaque coefficients car ils sont dans $\mathbb{F}_p$, d'où $|P| = p \times p \times \dots \times p = p^{n\frac{n-1}{2}}$.
Montrons que $|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)\dots(p^n - p^{n-1})$.
On sait que les colonnes d'une matrice $A \in GL_n(\mathbb{K})$ forment une base de $\mathbb{K}^n$, donc $|GL_n(\mathbb{F}_p)|$ correspond au cardinal de l'ensemble des bases de $\mathbb{F}_p^n$. Déterminons alors le cardinal de cet ensemble.
On choisit tout d'abord un premier vecteur a_1 pour former notre base de $\mathbb{F}_p^n$ et on le choisit non nul, donc on a $p^n - 1$ possibilités pour choisir ce vecteur (car $|\mathbb{F}_p^n| = p^n$). Ensuite on choisit notre deuxième vecteur a_2 de tel sorte que $a_2 \notin < a_1 >$, ce qui nous laisse $p^n - p$ possibilités pour a_2 (car $< a_1 >= \{\lambda a_1, \lambda \in \mathbb{F}_p\}$, ie $| < a_1 > | = p$). Ainsi de suite on construit notre base, si on a déjà choisi $a_1, \dots, a_i$ éléments pour choisir a_{i+1}, on le prend $\notin < a_1, \dots, a_i >$, donc on a $p^n - p^i$ possibilités pour a_{i+1}. Enfin on choisit en dernier a_n pour lequel il reste $p^n - p^{n-1}$ possibilités, d'où le résultat.

Lemme 0.5 (Théorème de Cayley) *Un groupe fini de cardinal n est isomorphe à un sous-groupe de $\mathfrak{S}_n$ (autrement dit se plonge dans $\mathfrak{S}_n$).*

Démonstration On sait que le groupe G agit sur lui-même par translation à gauche, ie :

$$\begin{aligned} \sigma : G &\longrightarrow \mathfrak{S}(G) \\ g &\longmapsto \sigma_g : x \longmapsto g.x \end{aligned}$$

Comme G est de cardinal n alors on sait que $\mathfrak{S}(G)$ est isomorphe à $\mathfrak{S}_n$.
Montrons maintenant que le morphisme σ est injectif.
Soit $g \in \ker(\sigma)$, alors $\sigma_g = id$, ie $\forall x \in G$, $g.x = x$ donc en multipliant par x^{-1} on obtient que $g = e$. Donc σ est bien injective.
De plus d'après la propriété universelle du quotient, on sait qu'il existe un isomorphisme entre $G/\ker(\sigma)$ et $\Im(\sigma)$ qui est un sous-groupe de $\mathfrak{S}_n$. D'où le résultat.

Références

[Per96] Daniel Perrin. *Cours d'algèbre.* Ellipses, 1996.