Théorème de Sylow

Laura Gay

Référence : Perrin : Cours d'algèbre p. 18

Contexte : Soit G un groupe d'ordre $n = p^\alpha m$, où p est un nombre premier, $n \in \mathbb{N}$ et $p \nmid m$.
On se servira souvent du fait que S est un p-Sylow de $G \Leftrightarrow S$ est un p-groupe et $[G : S]$ est premier à p.

Lemme 1

$GL_n(\mathbb{F}_p)$ a un p-Sylow.

Preuve du Lemme 1 :

Déjà, $|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)\cdots(p^n - p^{n-1}) =$ [1] $\underbrace{(p^n - 1)(p^{n-1} - 1)\cdots(p - 1)}_{m}\, p^{\frac{n(n-1)}{2}}$ où $p \nmid m$.

Soit P l'ensemble des matrices triangulaires supérieures strictes :

$$P := \{A = (a_{ij}) \ / \ a_{ij} = 0 \text{ si } i > j \text{ et } a_{ii} = 1\}$$

Pour $i < j$, les a_{ij} sont quelconques [2] donc $|P| = p.p^2.\cdots.p^{n-1} = p^{\frac{n(n-1)}{2}}$.
Ainsi, P est un p- Sylow de $GL_n(\mathbb{F}_p)$. ■

Lemme 2

Soient $H < G$, S p-Sylow de G, alors $\exists a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.

Preuve du Lemme 2 :

G agit par translation à gauche sur ${}^{G}\!/_{S}$ [3] (on multiplie à gauche).
Le stabilisateur de aS est aSa^{-1} (se montre par double inclusion). Mais comme H opère lui aussi sur ${}^{G}\!/_{S}$ par restriction, pour cette action restreinte, le stabilisateur de aS est $aSa^{-1} \cap H$.
Il reste à voir que l'un de ces sous-groupes est un Sylow de H. $aSa^{-1} \cap H$ est un sous-groupe de aSa^{-1} car cette intersection est non vide (neutre). Donc $\left|Sa^{-1} \cap H\right|$ divise $\left|aSa^{-1}\right| = |S| = p^\alpha$ donc $Sa^{-1} \cap H$ est un p-groupes.
On veut donc montrer que, pour un $a \in G$, $\left|{}^{H}\!/_{(aSa^{-1} \cap H)}\right|$ est premier à p.
La formule des classes donne $\left|{}^{H}\!/_{(aSa^{-1} \cap H)}\right| = \dfrac{|H|}{|aSa^{-1} \cap H|} = |$orbite de aS pour l'action de $H|$. Or :

$${}^{G}\!/_{S} = \bigcup (\text{orbite de } aS \text{ pour l'action de } H)$$

Supposons par l'absurde que $\forall a \in G,\ p \mid \left|{}^{H}\!/_{(aSa^{-1} \cap H)}\right|$. Alors $p \mid \left|{}^{G}\!/_{S}\right|$. Absurde car S est un p-Sylow de G. Donc $\exists a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H. ■

Lemme 3

Soit S un p-groupe opérant sur un ensemble X. Alors $|X| \equiv \left|X^S\right| \ [p]$.

Preuve du Lemme 3 :
On note ω pour l'orbite.

1. On a $\displaystyle\prod_{i=0}^{n-1}(p^n - p^i) = \prod_{i=0}^{n-1} p^i(p^{n-i} - 1) = (p^n - 1)\cdots(p-1)\prod_{i=0}^{n-1} p^i = (p^n-1)\cdots(p-1)p^{\sum_{i=0}^{n-1} i} = (p^n-1)\cdots(p-1)p^{\frac{n(n-1)}{2}}$
2. Première ligne : 0 case, Deuxième ligne : 1 case, ...,n-ième ligne : $n-1$ cases
3. Attention, S n'est pas forcément distingué, donc ${}^{G}\!/_{S}$ n'est pas nécessairement un groupe. Cela désigne simplement l'ensemble des classes à gauche modulo S.

Si $x \in X^S$, $\omega(x) = \{x\}$ car c'est un point fixe.
Si $x \notin X^S$, $|\omega(x)| > 1$ et comme $|\omega(x)| \mid |S|$, $p \mid |\omega(x)|$.
On a, comme X peut s'écrire comme partition disjointe de ses classes (orbites) :

$$|X| = \underbrace{\sum_{x \in X^G} |\omega(x)|}_{|X^G|} + \underbrace{\sum_{x \notin X^G} |\omega(x)|}_{\text{divisible par } p}$$

D'où le résultat. ■

Théorème (*Sylow-1872*)

1. Il existe un p-Sylow dans G.
2. Si H est un p-sous-groupe de G, il est contenu dans un p-Sylow S.
3. Les p-Sylow de G sont tous conjugués entre eux. (i.e. si H et K sont deux p-Sylow de G, alors il existe un élément g dans G vérifiant $gHg^{-1} = K$)
4. Si S est un p-Sylow de G, on a, $S \lhd G \Leftrightarrow n_p = 1$.
5. Soit n_p le nombre de p-Sylow de G. Alors $n_p \equiv 1\ [p]$ et donc $n_p | m$.

Preuve du Théorème :

1. Comme $|G| = n$, on plonge G dans $\mathcal{S}_n$. Puis on plonge $\mathcal{S}_n$ dans $GL_n(\mathbb{F}_p)$ par

$$u : \begin{array}{ccc} \mathcal{S}_n & \longrightarrow & GL_n(\mathbb{F}_p) \\ \sigma & \longmapsto & u_\sigma \end{array} \quad \text{où } u_\sigma(e_i) = e_{\sigma(i)}\ ,\ (e_i)_i \text{ base canonique}$$

   Ainsi, on réalise G comme sous-groupe de $GL_n(\mathbb{F}_p)$. Ce dernier a un p-Sylow (**Lemme 1**) donc G aussi (**Lemme 2**).
2. Soit H un p-sous-groupe de G et S un p-Sylow de G (possible car on a montré en 1. l'existence). Il existe, par le **Lemme 2**, $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H. Or, comme H est un p-groupe (son cardinal est un p^β) donc un p-Sylow c'est forcément tout H ie $aSa^{-1} \cap H = H$ ie $H \subset aSa^{-1}$, ce dernier étant un p-Sylow.
3. Si de plus H est un Sylow, on a exactement $H = aSa^{-1}$ ie les Sylow sont tous conjugués.
4. Comme ils sont tous conjugués et que S est distingué Ok...
5. On fait opérer G par conjugaison sur l'ensemble X de ses p-Sylow. Soit S un p-Sylow, S opère lui aussi sur X et le **Lemme 3** donne $|X| = n_p \equiv \left|X^S\right|\ [p]$.
   Il reste à voir que $\left|X^S\right| = 1$.
   Déjà, si $s \in S$, on a clairement $sSs^{-1} = S$ donc $S \in X^S$. Il faut montrer que c'est le seul.
   Soit T un autre p-Sylow. On suppose que $T \in X^S$ ie $\forall s \in S$, $sTs^-1 = T$.
   Soit N le sous-groupe de G engendré par S et T. S et T sont a fortiori des p-Sylow de N (s'écrit facilement). Mais par construction de N et de $T \in X^S$ on a $T \lhd N$ et le 3. donne que T est l'unique p-Sylow de N ie $T = S$. Donc $n_p \equiv 1\ [p]$.
   Comme $n_p \mid |G|$ et $n_p \wedge p = 1$ on a (théorème de Gauss) $n_p | m$.

■

Application

[Ulmer p.88] Un groupe d'ordre 15 est toujours cyclique et isomorphe à $\mathbb{Z}/15\mathbb{Z}$. En effet, par le théorème on a $n_5 | 3$ et $n_5 \equiv 1\ [5]$. Donc $n_5 = 1$. De même, on a $n_3 = 1$. Notons P_i le i-Sylow qui est distingué dans G. On a $|P_i| = i$ premier donc les P_i sont cycliques. et $G \cong$ [4] $P_3 \times P_5 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$ par le théorème chinois.

4. C'est un théorème car ils sont distingués et G est fini.

Notes :

✓ **A l'oral**, bla
✓ Rappel (définition d'un p-groupe) : Soit p un nombre premier. On appelle p-groupe un groupe dont tout élément a pour ordre une puissance de p.
✓ Rappel (définition d'un p-Sylow) : Soit p un nombre premier et G un groupe fini ; on définit un p-sous-groupe de Sylow (ou p-Sylow) de G comme un élément maximal de l'ensemble des p-sous-groupes de G, au sens de l'inclusion. Autrement dit, c'est un p-sous-groupe de G qui n'est contenu dans aucun autre p-sous-groupe de G. Tout p-sous-groupe de G est inclus dans un p-sous-groupe maximal, ce qui garantit l'existence de p-Sylow. L'ensemble (non vide, donc) de tous les p-Sylow pour un entier premier p donné est parfois noté $\mathrm{Syl}_p G$.
♣ Ludwig Sylow (1832- 1918) est un mathématicien norvégien. Il étudia la théorie des groupes. Conjointement avec Lie, il travailla sur les travaux d'Abel entre 1873 et 1881.