Théorème de Sylow

Arnaud Girand

11 décembre 2011

Référence :
- [Per96] ; p. 18–20

Leçons :
- 101 - Groupe opérant sur un ensemble. Exemples et applications.
- 104 - Groupes finis. Exemples et applications.
- 110 - Nombres premiers. Applications.

Prérequis :
- formule des classes.

Soit G un groupe fini de cardinal $n \geq 1$. On suppose qu'il existe un nombre premier p et deux entiers $\alpha, m \geq 1$ tels que $n = p^\alpha m$, avec $p \nmid m$.

Lemme 1
Soit $H \leq G$.
Soit S un p–Sylow de G.
Alors il existe $a \in G$ tel que $H_a := aSa^{-1} \cap H$ soit un p–Sylow de H.

Démonstration : G agit sur G/S par translation à gauche et :

$$\begin{aligned} \forall a, g \in G,\ g.(aS) = as &\Leftrightarrow \forall s \in S,\ \exists s' \in S,\ gas = as' \\ &\Leftrightarrow \forall s \in S,\ \exists s' \in S,\ g = as's^{-1}a^{-1} \\ &\Leftrightarrow g \in aSa^{-1} \end{aligned}$$

On a donc $\forall a, g \in G$, $\mathrm{Stab}_G(aS) = aSa^{-1}$. Or H agit sur G/S par restriction et $\mathrm{Stab}_H(aS) = \mathrm{Stab}_G(aS) \cap H = H_a$ est un sous–groupe de $\mathrm{Stab}_G(aS)$, d'où $|H_a| \,|\, |aSa^{-1}| = |S| = p^\alpha$. De fait, par primalité, $p \,|\, |H_a|$.
Or $|H_a| = \dfrac{|H|}{(H : H_a)}$ donc il nous suffit de trouver $a \in G$ tel que $(H : H_a) \wedge p = 1$.

Si on note $\omega(aS)$ l'orbite d'un élément aS de G/S sous l'action de H, l'application $g \mapsto g.aS$ et la propriété universelle du quotient nous indiquent que $(H : H_a) = |H/H_a| = |\omega(aS)|$. De fait, si p divisait tous les indices $(H : H_a)$, on aurait par la formule des classes que p divise $m = |G/S|$, ce qui est impossible, d'où le résultat.

Proposition 1 (Sylow)
On note $c_p \geq 0$ le nombre de p–Sylow de G.
Alors :

(i) pour tout p–groupe $H \leq G$, il existe un p–Sylow de G contenant H (et donc $c_p \geq 1$) ;

(ii) les p–Sylow de G sont tous conjugués (et donc $c_p | n$), en particulier si S est un p–Sylow de G et si $S \lhd G$ alors S est l'unique p–Sylow de G ;

(iii) $c_p \equiv 1[p]$ (et donc $c_p | m$).

Démonstration :

(*i*) On a l'injection suivante (où $(e_1, \ldots, e_n)$ désigne la base canonique de $\mathbb{F}_p^n$) :

$$\begin{aligned} \mathfrak{S}_n &\hookrightarrow GL_n(\mathbb{F}_p) \\ \sigma &\mapsto (u_\sigma : e_i \mapsto e_{\sigma(i)}) \end{aligned}$$

Ainsi, d'après le théorème de Cayley (proposition 2) et la propriété universelle du quotient, on peut identifier G à un sous groupe de $GL_n(\mathbb{F}_p)$. Or $GL_n(\mathbb{F}_p)$ possède un p–Sylow (les

matrices triangulaires supérieures "strictes", cf. infra) donc d'après le lemme 1, G aussi : notons le S.

Toujours d'après le lemme 1, comme H est un sous–groupe de G, il existe $a \in G$ tel que H_a soit un p–Sylow de H. Or H est également un p–groupe et donc son unique p–Sylow est lui–même, ergo $H_a = H$, ce qui implique que $H \subset aSa^{-1}$, qui est un p–Sylow [1].

(ii) On procède comme pour le point (i) en imposant à H d'être un p–Sylow. On obtient bien alors que pour tout p–Sylow S de G, il existe $a \in G$ tel que $H \subset aSa^{-1}$. Or $|H| = p^\alpha = |S| = |aSa^{-1}|$ donc $H = aSa^{-1}$ est conjugué à S.

(iii) Notons X l'ensemble des p–Sylow de G. On sait que G agit sur X par conjugaison et si $S \in X$, cette action en induit une de S sur X. D'après le lemme 2 on a donc $|X| \equiv |X^S|[p]$. Il est de plus clair que $S \in X^S$.

Soit $T \in X^S$, i.e $\forall s \in S$, $sTs^{-1} = T$. On considère le sous–groupe N de G engendré par S et T ; alors $S \leq N$ et $T \leq N$ sont deux p–Sylow de N. Cependant il est clair que $T \lhd N$ et donc par le point (ii) $T = S$. In fine $X^S = \{S\}$ et donc $c_p = |X| \equiv 1[p]$.

Détails supplémentaires :

– *$GL_n(\mathbb{F}_p)$ admet un p–Sylow* (cf. [Per96], p.15). Commençons par remarquer que :

$$\forall A \in \mathcal{M}_n(\mathbb{F}_p), \quad A \in GL_n(\mathbb{F}_p) \Leftrightarrow (Ae_1, \dots, Ae_n) \text{ est une base de } \mathbb{F}_p^n$$

$GL_n(\mathbb{F}_p)$ est de facto équipotent à l'ensemble des bases de $\mathbb{F}_p^n$. Or pour se donner une telle base $(a_1, \dots, a_n)$, on dispose de $p^n - 1$ choix pour a_1 (on choisit $a_1 \in \mathbb{F}_p^n \setminus \{0\}$, de $p^n - p$ choix pour a_2 (on choisit $a_2 \notin \langle a_1 \rangle$) et de manière générale de $p^n - p^{i-1}$ choix pour a_i, $i \in [n]$ (on choisit $a_i \notin \langle a_1, \dots, a_{i-1} \rangle$). In fine :

$$|GL_n(\mathbb{F}_p)| = \prod_{k=0}^{n-1} (p^n - p^k)$$

On a donc $|GL_n(\mathbb{F}_p)| = p^{n(n-1)/2} m$, avec $p \nmid m$. On considère alors le sous–groupe de $GL_n(\mathbb{F}_p)$ constitué des matrices triangulaires supérieures "strictes" :

$$P := \{A \in GL_n(\mathbb{F}_p) \,|\, \forall i, j \in [n],\ a_{i,j} = 0 \text{ si } i > j,\ a_{i,i} = n\} \leq GL_n(\mathbb{F}_p)$$

Alors $|P| = p^{n(n-1)/2}$ (on "choisit" exactement $\frac{n(n-1)}{2}$ coefficients de chaque matrice) donc P est un p–Sylow de $GL_n(\mathbb{F}_p)$.

– On trouve le résultat suivant dans [Per96], p.15 :

Proposition 2 (Cayley)
Soit G un groupe fini de cardinal $n \geq 1$.
Alors G est isomorphe à un sous–groupe de $\mathfrak{S}_n$.
Démonstration : G agit sur lui–même par translation à gauche donc il existe un morphisme de groupes de G dans $\mathfrak{S}(G) \cong \mathfrak{S}_n$. Ce morphisme est de plus injectif car si $g, h \in G$ $(\forall x \in G,\ g.x = h.x) \Rightarrow (g = h)$. On conclut par propriété universelle du quotient.

– Le lemme suivant est démontré dans [Per96], p.17 :

Lemme 2
Soit G un p–groupe.
Soit X un G–ensemble fini.
Alors :

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

Démonstration : D'après la formule des classes :

$$|X| = |X^G| + \sum |\omega(x)|$$

Où la somme compte une fois chaque orbite non triviale. De fait, chacun de ces $|\omega(x)|$ est strictement supérieur à 1 et divise $|G|$ donc $p||\omega(x)|$, d'où le résultat.

– *Une application classique : il n'existe pas de groupe simple d'ordre 63.* Soit G un groupe d'ordre $63 = 3^2 \times 7$. Alors $c_7 \equiv 1[7]$ et $c_7|9$ donc $c_7 = 1$: G admet un unique 7–Sylow qui est donc distingué.

1. La conjugaison conservant les cardinaux, le conjugué d'un p–Sylow est un p–Sylow de G.

Références

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