UE2 Groupes et Géométrie — Université de Nice
2019-2020

LES THÉORÈMES DE SYLOW

Référence : Perrin, Cours d'Algèbre, pages 18-20

Leçons possibles :
101 : Groupe opérant sur un ensemble. Exemples et applications.
104 : Groupes finis. Exemples et applications.
103 : Exemples de sous-groupes distingués et de groupes quotients. Applications.

D'après le théorème de Lagrange si G est un groupe fini et H un sous-groupe de G, alors $|H|$ divise $|G|$. Réciproquement on peut se demander si dans un groupe de cardinal n il existe pour tout diviseur d de n un (ou plusieurs) sous-groupe d'ordre d. La réponse est non en général ; par exemple $\mathcal{A}_4$ est un sous-groupe de cardinal 12 qui ne contient pas de sous-groupe d'ordre 6. Néanmoins il y a toute une classe de groupes où cette propriété est vraie, ce sont les sous-groupes de Sylow.

Soit p un nombre premier.

Définition. Soit G un groupe fini de cardinal n. Soit p un diviseur premier de n. Si $n = p^\alpha m$ et si p ne divise pas m, on appelle un p-sous-groupe de Sylow de G un sous-groupe de cardinal p^α.

Exemple. Soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments (p premier). Soit $G = \mathrm{GL}(n, \mathbb{F}_p)$, $n \in \mathbb{N}^*$. Le groupe G est un fini de cardinal

$$|G| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$$

(il suffit de compter les bases de $\mathbb{F}_p^n$) ; en particulier $|G| = mp^{n(n-1)/2}$ avec p ne divise pas m.

L'ensemble des matrices triangulaires supérieures strictes

$$\left\{A = (a_{ij}) \,|\, a_{ij} = 0 \text{ si } i > j \text{ et } a_{ii} = 1\right\}$$

est un p-sous-groupe de Sylow de G. En effet comme les a_{ij}, pour $i < j$, sont quelconques on a

$$|P| = p \times p^2 \times \ldots \times p^{n-1} = p^{n(n-1)/2}.$$

L'énoncé suivant atteste l'existence des sous-groupes de Sylow :

Théorème 1. *Soit G un groupe fini. Soit p un diviseur premier de $|G|$. Alors G contient au moins un p-sous-groupe de Sylow.*

Avant de démontrer ce résultat donnons un lemme qui permet, connaissant un Sylow d'un groupe G d'en trouver un pour un sous-groupe H :

Lemme 2. *Soit G un groupe tel que $|G| = n = p^\alpha m$ avec $p \nmid m$. Soit H un sous-groupe de G. Soit S un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.*

Démonstration. Notons G/S l'ensemble des classes à gauche modulo S (*i.e.* l'ensemble des parties aS pour $a \in G$). Le groupe G opère sur G/S par translation à gauche (en posant $g \cdot (aS) = (ga)S$). Le stabilisateur

$$\mathrm{Stab}(aS) = \{g \in G \,|\, g \cdot aS = aS\}$$

de aS est aSa^{-1}. Mais H opère lui aussi sur G/S par restriction avec $aSa^{-1} \cap H$ comme stabilisateur de aS.

Montrons qu'un de ces groupes est un Sylow de H. Ce sont déjà des p-groupes. Il suffit donc que pour un $a \in G$, $|H/(aSa^{-1} \cap H)|$ soit premier à p.

Rappelons le :

Lemme 3. *L'application*

$$G/\mathrm{Stab}(x) \to \mathcal{O}(x) \qquad\qquad \overline{g} \mapsto g \cdot x$$

de l'ensemble des classes à gauche dans l'orbite de x est bien définie et est une bijection.

Ainsi $|H/(aSa^{-1} \cap H)| = |\mathcal{O}(aS)|$ où $|\mathcal{O}(aS)|$ désigne 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 $\mathcal{O}(aS)$: contradiction avec le fait que S est un p-Sylow de G. □

Démonstration du Théorème 1, basée sur [Serre, Groupes finis, https ://arxiv.org/abs/math/0503154.] Soit G un groupe. Soit p un diviseur de $|G| = n$. On plonge G dans $\mathcal{S}_n$ (théorème de Cayley). Puis on plonge $\mathcal{S}_n$ dans $\mathrm{GL}(n, \mathbb{F}_p)$: l'élément σ de $\mathcal{S}_n$ s'envoie sur l'endomorphisme u_σ défini dans la base canonique par : $u_\sigma(e_i) = e_{\sigma(i)}$.

On a donc réalisé G comme un sous-groupe de $\mathrm{GL}(n, \mathbb{F}_p)$ qui possède un p-Sylow (Exemple), donc G aussi par le Lemme 2. □

Corollaire 4. *Si G est un groupe tel que $|G| = p^\alpha m$ avec $p \nmid m$, alors G contient des sous-groupes d'ordre p^i pour tout $i \leq \alpha$.*

Démonstration. D'après le Théorème 1 on est ramené au cas des p-groupes qui se traite par récurrence étant l'existence d'un centre non trivial. □

Le deuxième théorème de Sylow étudie la conjugaison des p-sous-groupes de Sylow.

Théorème 5. *Soit G un groupe de cardinal $|G| = p^\alpha m$ avec $p \nmid m$.*

(1) Si H est un sous-groupe de G qui est un p-groupe, il existe un p-Sylow S tel que $H \subset S$.

(2) Les p-Sylow sont tous conjugués et leur nombre n_p divise n.

(3) On a $n_p \equiv 1$ mod p, donc n_p divise m.

L'assertion n_p divise n résulte du fait que les p-Sylow forment une orbite sous G.

Corollaire 6. *Si S est un p-Sylow de G, alors*

$$S \triangleleft G \Leftrightarrow S \text{ est l'unique } p\text{-Sylow de } G \Leftrightarrow n_p = 1$$

Lemme 7. *Soit G un p-groupe opérant sur un ensemble X. Soit*

$$X^G = \left\{x \in X \,|\, \forall\, g \in G \quad g \cdot x = x\right\}$$

l'ensemble des points fixes sous G, alors $|X| \equiv |X^S| \mod p$.

Démonstration. Écrivons X comme réunion disjointe de ses orbites sous G en remarquant que $x \in X^G$ si et seulement si $\mathcal{O}(x) = \{x\}$. Si x n'appartient pas à X^G, alors $|\mathcal{O}(x)| > 1$ et comme $|\mathcal{O}(x)|$ divise $|G| = p^n$, p divise $|\mathcal{O}(x)|$. Le résultat provient alors de l'égalité

$$|X| = |X^G| + \sum_{x \notin X^G} |\mathcal{O}(x)|.$$

□

Démonstration du Théorème 5. Si H est un p-sous-groupe de G et si S est un p-Sylow de G, alors d'après le Lemme 2 il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H. Mais comme H est un p-groupe, $aSa^{-1} \cap H = H$. Par suite H est inclus dans aSa^{-1} qui est un Sylow. Si de plus H est un Sylow on a $H = aSa^{-1}$. On a donc montré les deux premi‘eres assertions.

Faisons opérer G par conjugaison sur l'ensemble X de ses p-Sylow [1] Soit S un p-Sylow, S opère lui aussi sur X et on a (Lemme 7)

$$|X| \equiv |X^S| \mod p$$

Montrons que $|X^S| = 1$. Bien sûr si $s \in S$, on a $sSs^{-1} = S$, autrement dit $S \in X^S$. Montrer que $|X^S| = 1$ revient donc à montrer que S est l'unique élément de X^S. Soit T un p-Sylow. Supposons que T soit normalisé par S :

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

Considérons le sous-groupe N de G engendré par S et T. On a $S \subset N$, $T \subset N$ et ce sont a fortiori des p-Sylow de N. Mais comme S normalise T on a $T \triangleleft N$. Le Corollaire 6 assure que T est l'unique Sylow de N. Ainsi $S = T$. □

1. Si G est un groupe et X l'ensemble de ses sous-groupes, alors G opère sur X par automorphisme intérieur : $g \cdot H = gHg^{-1}$.