AMS Autour des p-sous-groupes de Sylow

Samy Amara, Gabriel Pitino, et Guillaume Salloum

Résumé

Le but de cette AMS est d'étudier les théorèmes de Sylow, qui forment une réciproque partielle au théorème de Lagrange. Nous introduirons quelques notions utiles pour enonçer les théorèmes, puis nous en donnerons deux preuves : la première utilise les actions de groupes, tandis que la deuxième se base sur ???? . Enfin nous en donnerons quelques applications, notemment pour la classification des groupes simples finis.

Table des matières

Dans tout ce qui suit, nous utiliserons les notations suivantes :

Notations

G	Groupe quelconque.
$Card(X)$, $Card(G)$	Cardinal de l'ensemble X, ordre d'un groupe G.
$H \lhd G$	H est un sous-groupe distingué de G.
x^g	Conjugué à gauche de x par g.
$Stab_G(x)$	Stabilisateur de x dans G.
$N_G(H)$	Normalisateur de H dans G.
$Syl_p(G)$	Ensemble des p-sous-groupes de Sylow de G.
$n_p(G)$	Nombre de p-sous-groupes de Sylow de G.
$A \cong B$, $A \overset{\varphi}{\cong} B$	A est isomorphe à B, φ est un isomorphisme de A vers B.

1 Théorèmes de Sylow

1.1 Notions préliminaires

Définition 1.1.1 (Action de groupe, chapitre 1 du cours)**.** Soit G un groupe et A un ensemble quelconque. Une *action à gauche* de G sur A est une application $f : G \times A \to A$ qui satisfait :

(i) $g1.(g2.a) = (g1g2).a$ pour tout $g1, g2 \in G$, $a \in A$,

(ii) $1.a = a$ pour tout $a \in A$

On peut définir de manière équivalente d'après le chapitre 1 du cours une action comme un morphisme $\varphi : G \to S_A$ de G dans le groupe des permutations de A satisfaisant :

$$g.a = \varphi(g)(a) \quad \forall g \in G, \forall a \in A \tag{1}$$

Un exemple important d'action de G sur un ensemble A que nous allons utiliser par la suite est la *conjugaison à gauche*.

$$\begin{aligned} f : G \times A &\to A \\ (g, a) &\mapsto a^g := gag^{-1} \end{aligned}$$

Définition 1.1.2 (Normalisateur de H dans G)**.** [Che24, p. 217]. Le normalisateur de H dans G est l'ensemble $N_G(H) := \{g \in G \mid gPg^{-1} = P\}$. De manière équivalente, c'est le stabilisateur de H sous l'action de conjugaison de G sur l'ensemble de ses sous-groupes.

Définition 1.1.3 (Sous-ensembles conjugués)**.** [DF03, p. 123] Soit G un groupe, A et B deux sous-ensembles de G. A et B sont dit *conjugués dans* G s'il existe $g \in G$ tel que $B = gAg^{-1}$. En d'autres termes, A et B sont dans le même orbite pour l'action de conjugaison. Si A et B sont des sous-groupes de G, ce sont des *sous-groupes conjugués* de G.

1.2 Enoncé

Nous enonçons en premier lieu quelques définitions issues de l'énoncé du sujet (ou de manière équivalente de [DF03, p. 123 et 139]) utiles pour poser le théorème.

Définition 1.2.1 (p-groupe)**.** Soit G un groupe et p un nombre premier.

(i) Si $Card(G) = p^n$ pour un $n > 0$, G est un p*-groupe*. Un sous groupe H de G est appelé p*-sous groupe*.

(ii) Si $Card(G) = p^n m$ où m n'est pas un multiple de p, alors un sous groupe d'ordre p^n est appelé p*-sous groupe de Sylow de* G.

(iii) L'ensemble des p-sous groupes de Sylow de G est noté $Syl_p(G)$, et le nombre de p-sous groupes de Sylow de G est noté $n_p(G)$.

Plusieurs formulations sont possibles pour les théorèmes, nous avons décidé d'adapter celle de l'énoncé du sujet directement en ajoutant un dernier point issu de [Che24, p. 215].

Théorème 1.2.2 (Théorèmes de Sylow)**.** *Soit G un groupe d'ordre $p^n m$ où p est un nombre premier, m et p sont premiers entre eux. Alors on a :*

(i) *(Existence) Au moins un p-sous-groupe de Sylow existe, c'est-à-dire que $n_p(G) \geq 1$ et $Syl_p(G) \neq \emptyset$.*

(ii) *Tout sous-groupe de G d'ordre p^r avec $0 \leq r \leq n$ est inclus dans un p-sous-groupe de Sylow.*

(iii) *Deux p-sous-groupes de Sylow H et H' de G sont conjugués entre eux, c'est-à-dire il existe $g \in G$ tel que $H' = gHg^{-1} = \{ghg^{-1} \mid h \in H, g \in G\}$. Par conséquent $H \cong H'$.*

(iv) *Le nombre de p-sous-groupes de Sylow de G est congru à 1 modulo p, i.e. $n_p \equiv 1[p]$ ou $Card(Syl_p(G)) = n_p(G) = 1 + kp$. On a de plus, pour tout $P \in Syl_p(G)$, $n_p(G) = [G : N_G(P)]$, donc m est un diviseur de $n_p(G)$.*

1.3 Première démonstration

La première preuve est due à [Che24, p. 216-218], nous l'avons reformulée et avons explicité certains détails supplémentaires pour plus de clarté dans la présentation.

Démonstration. (i) Soit

$$\begin{aligned} \varphi : G \times X &\to X \\ (g, x) &\mapsto \varphi(g, x) \coloneqq g.x \end{aligned}$$

une action de G sur X, où X est l'ensemble des parties de G de cardinal p^n. En utilisant un résultat de théorie des nombres (théorème de Lucas) que l'on admet, on a :

$$Card(X) = \binom{p^n m}{p^n} \not\equiv 0 \mod p$$

En d'autres termes $Card(X)$ n'est pas un multiple de p. Soit O une orbite de X sous l'action φ telle que p ne divise pas $Card(O)$. Soit $S \in O$ et $H = Stab_G(S) = \{g \in G \mid g.S = S\}$.
Montrons que $Card(H) = p^n$ en montrant qu'on a à la fois $Card(H) \mid p^n$ et $p^n \mid Card(H)$.

Montrons d'abord que $Card(H) \mid p^n$. G est fini et on a une bijection entre O_x et G/H, alors $Card(O_x) = [G : H] = \frac{Card(G)}{Card(H)}$. On en déduit que $p^n \mid Card(H)$, car sinon $Card(X)$ pourrait être un multiple de p.

Réciproquement, montrons que $p^n \mid Card(H)$. Soit une nouvelle action :

$$\begin{aligned} \psi : H \times S &\to S \\ (h, s) &\mapsto h.s \end{aligned}$$

Or pour $s \in S$ fixé, on a :

$$\begin{aligned} Stab_H(s) &= \{h \in H \mid h.s = s\} \\ &= \{h \in \{g \in G \mid g.s = s\} \mid h.s = s\} \text{ par définition de } H \\ &= \{e_G\} \end{aligned}$$

S est partitionné en orbites que l'on note O_y. On a alors $S = \bigsqcup O_y$ et $Card(S) = \sum Card(O_y)$. Par bijection entre O_y et $S/Stab_H(s)$, une orbite O_y de S sous ψ est de cardinal $Card(O_y) = [H : Stab_H(s)] = Card(H)$ car $Card(Stab_H(s)) = Card(e_G) = 1$.
D'où $Card(S) = \sum Card(O_y) = \sum Card(H)$.
Ainsi $Card(H) \mid Card(S) = p^n$.

(ii) Soit $r \in [[0, n]]$, Q un sous-groupe de G d'ordre p^r. D'après (i) au moins un $P \in Syl_p(G)$ existe, où $Card(P) = p^n \geq p^r = Card(Q)$. Donc $Q \subseteq P$.

(iii) Soit $P \in Syl_p(G)$. Montrons que pour tout p-sous-groupe Q de G il existe $g \in G$ tel que $Q \subseteq gPg^{-1}$, c'est-à-dire que Q est un sous-groupe conjugué de P. On procède par disjonction de cas sur Q.

Supposons que Q est un p-sous-groupe de Sylow de G :
$Card(Q) = p^m$ pour $1 \leq m \leq n$. Puique $Card(P) = p^l$ pour $1 \leq l \leq n$ aussi, on a soit $l \geq m$, soit $l \leq m$. Dans les deux cas il existe bien un $g \in G$ tel que $gPg^{-1} = Q$ donc à fortiori $Q \subseteq gPg^{-1}$.

Supposons que Q n'est pas un p-sous-groupe de Sylow de G :
On considère l'action φ de Q sur les classes à gauche de P pour la relation $\sim_P$ de congruence à gauche modulo P définie comme dans le cours.

$$\begin{aligned} \varphi : Q \times gP &\to gP \\ (q, gp) &\mapsto q.gp \end{aligned}$$

Soit O_p un orbite de gP. Puisque gP est partitionné en orbites et que Q et un p-groupe, alors $Card(O_p)$ est un diviseur de p. Or le nombre de classes à gauche de P est $[G : P] = \frac{p^n m}{p^n} = m$, qui n'est pas un diviseur de p.
Alors une classe gP est un point fixe pour tout $q \in Q$, c'est-à-dire que $\forall q \in Q, \exists g \in G, qgP = gP$.
Donc $\forall q \in Q, qg \in gP$. D'où $\forall q \in Q, q \in gPg^{-1}$ pour un $g \in G$ soit $\exists g \in G, Q \subseteq gPg^{-1}$.
Ainsi dans les deux cas Q est un sous-groupe conjugué de G.

(iv) Soit $P \in Syl_p(G)$, et χ l'action de conjugaison de G sur $Syl_p(G)$:

$$\begin{aligned} \chi : G \times Syl_p(G) &\to Syl_p(G) \\ (g, P) &\mapsto g.P = gPg^{-1} \end{aligned}$$

Puisque P est en particulier un p-groupe, $n_p(G) \mod p$ est le nombre de points fixes de χ. Montrons que P est le seul point fixe de χ, cela est équivalent à montrer que $Stab_P(G) = \{g \in G \mid g.P = gPg^{-1} = P\} = P$ donc que $N_G(P) = P$ et $P \lhd G$. Soit Q un autre point fixe de χ, c'est-à-dire $Q \in Stab_Q(G) = \{g.Q \mid g.Q = gQg^{-1} = Q\}$.
Alors $N_G(Q) = \{g \in G \mid gQg^{-1} = Q\}$ avec $P \subset N_G(Q)$ et $Q \subset N_G(Q)$.
On applique (iii) sur $N_G(Q)$: P et Q sont des p-sous-groupes de Sylow de $N_G(Q)$, donc ce sont des sous-groupes conjugués. D'où $P = Q$ et P est le seul point fixe de χ. On en déduit que $n_p(G) \equiv 1 \mod p$.
Montrons ensuite que m est un diviseur de $n_p(G)$: d'après ce qui précède, χ ne possède qu'un seul orbite O_P qui est $Syl_p(G)$ entier. Puisqu'on a une bijection entre O_P et $G/Stab_G(P)$, on en déduit que :

$$\begin{aligned} Card(O_P) = Card(Syl_p(G)) = n_p(G) &= [G : Stab_G(P)] \\ &= \frac{Card(G)}{Card(Stab_G(P))} \end{aligned}$$

D'où $n_p(G) \mid Card(G)$, et puisque $n_p(G) \equiv 1 \mod p$, on a $n_p(G) \mid m$.

□

1.4 Deuxième démonstration

2 Applications

2.1 Corollaires

Il est possible de prouver le théorème de Cauchy sans passer par le théorème de Sylow, mais ce dernier a l'avantage que l'on peut en déduire l'autre directement. Nous donnons ici une preuve rapide dûe à [Ser79].

Théorème 2.1.1 (Cauchy)**.** *Soit G un groupe tel que $p \mid Card(G)$. Alors il existe $g \in G$ tel que g est d'ordre p.*

Démonstration. Soit $H \in Syl_p(G)$. Pusique $p \mid Card(G)$ alors $H \neq \{e_G\}$. En prenant un $h \in H, h \neq e_G$ on a h est d'ordre p^a où $a \geq 1$. D'où $h^{p(a-1)}$ est d'ordre p. $\square$

2.2 Prouver l'existence d'un sous-groupe normal de G

Pour des groupe d'ordre assez petit, d'après Théorème (iv) on peut "forcer" l'existence d'un sous-groupe normal. Dans les autres cas, certaines conditions supplémentaires que l'on énonce ci-dessous permettent de pallier à ce problème. [DF03, p. 142]

2.3 Classifing all groups of a given order n up to isomorphism

In the following part, we will use Sylow's theorem to prove whether a group G is simple or not. Given the order n of G and the simplicity (or not) of G, one can then classify all groups of order n up to isomorphism. We first define these notions using mainly [DF03, p. 103].

Definition 2.3.1 (Simple group)**.** A group G is simple if and only it it has two normal subgroups : $\{e_G\}$ and itself.

Simple group arise in a similar way to prime numbers in the unique factorization of integers : we can break a group G into smaller pieces, namely the simple groups, to unravel the structure of G. This is precisely the notion of a *composition series*.

Definition 2.3.2 (Composition series)**.** A composition series of a group G is a sequence of subgroups $H_0, \dots, H_n$ such that :

(i) the subgroups are pairwise normal : $\forall i \in [\![0, n-1]\!], H_i \lhd H_{i+1}$

(ii) And the pairwise quotient groups, called the *composition factors*, are all simple : $\forall i \in [\![0, n-1]\!], H_{i+1}/H_i$ is a simple group

In practice, n is chosen to be as large as possible so that we have a maximal number of distinct composition factors. The following theorem which we admit asserts that up to a permutation of the composition factors, a finite group G has a unique composition series.

Theorem 2.3.3 (Jordan-Hölder)**.** *Every finite group G has a unique composition series up to a permutation of the composition factors.*

Références

[Che24] E. Chen. *An Infinitely Large Napkin*. Revision 1.6.20240911. Sept. 2024.

[DF03] D.S. Dummit et R.M. Foote. *Abstract Algebra*. Wiley, 2003. isbn : 9780471433347.

[Ser79] J.-P. Serre. *Groupes finis*. Cours à l'École Normale Supérieure de Jeunes Filles. 1978–1979.