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

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

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 lui-même que nous allons utiliser par la suite est la *conjugaison*.

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

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

Définition 1.1.3 (Sous-ensembles conjugués)**.** [DF03, p. ? ?] 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.

1.2 Enoncé

Nous enonçons en premier lieu quelques définitions issues de l'énoncé du sujet (ou de manièr 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 $H' = gHg^{-1} = \{ghg^{-1} \mid h \in H, g \in G\}$.*

(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 $Card(Syl_p(G)) = n_p = 1 + kp$. 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

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_x une orbite de X sous l'action de φ telle que p ne divise pas $Card(O_x)$. Soit $S \in O_x$ et $H = Stab_G(S)$ où $H = \{g.s = s \mid g \in G, s \in S\}$.
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 $Card(H) \mid p^n$.
Comme G est fini, 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 :

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

Or

$$\begin{aligned} Stab_H(s) &= \{h \in H, s \in S \mid h.s = s\} \\ &= \{h \in \{g \in G \mid g.s = s\} \mid h.s = s\} \\ &= \{e_G\} \end{aligned}$$

S est partitionné en orbites que l'on note O_y. On a alors $S = \bigsqcup O_y$ et $Card(S) = \sum Card(O_y)$. Donc les orbites de S sous l'action de ψ sont de cardinal $Card(O_y) = [H : Stab_H(s)] = \frac{Card(H)}{Card(Stab_H(s))} = Card(H)$ car $Card(Stab_H(s)) = Card(e_G) = 1$.
D'où $Card(S) = Card(H) = \sum Card(O_y)$.
Ainsi $Card(H) \mid Card(S) = p^n$.

(ii) Soit $P \in Syl_p(G)$. P existe d'après (i). Montrons que pour tout p-sous-groupe Q de G on a $Q \subseteq gPg^{-1}$, c'est-à-dire que Q est dans 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 $gPg^{-1} = Q$.
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.

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

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 gacuhe de P est $[G : P] = \frac{p^n m}{p^n} = m$, qui n'est pas un diviseur de p.
Alors une classe $\overline{g}P$ est un point fixe pour tout $q \in Q$, c'est-à-dire que $\forall q \in Q, \exists \overline{g} \in G, q\overline{g}P = \overline{g}P$.
Donc $\forall q \in Q, qg \in gP$. D'où $\forall q \in Q, q \in gPg^{-1}$ soit $Q \subseteq gPg^{-1}$.

(iii)

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

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

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 $Stab_P(G) = \{g \in G \mid gPg^{-1} = P\} = N_G(P) = P$ donc que $P \triangleleft G$. 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 $N_G(Q) = \{g \in Q \mid gQg^{-1} = Q\}$ est tel que $P \subset N_G(Q)$ 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 $n_p(G)$:

□

1.4 Deuxième démonstration

2 Applications

2.1 Application à la classification des groupes simples finis

[DF03]

2.2 Example : classifing all groups of order 60 up to isomorphism

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.