

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 énoncer les théorèmes, puis nous en donnerons une preuve utilisant en grande partie les actions de groupes. Enfin nous en donnerons quelques applications, notamment pour la classification des groupes simples finis.

Table des matières

Notations	2
1 Théorèmes de Sylow	3
1.1 Notions préliminaires	3
1.2 Énoncé	4
1.3 Démonstration	5
2 Applications	9
2.1 Some corollaries	9
2.2 Proving that there exists a normal subgroup of G	9
2.3 Classifying all groups of a given order n up to isomorphism	9

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 .
$H \triangleleft G$	H est un sous-groupe distingué de G .
x^g	Conjugué à gauche de x par g .
O_x	Orbite de x pour l'action de G .
$N_G(H)$	Normalisateur de H dans G .
$Stab_G(x)$	Stabilisateur de x 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 .
$A \cong B, A \stackrel{\varphi}{\cong} B$	A est isomorphe à B , φ est un isomorphisme de A vers B .
Z_n	Groupe cyclique d'ordre n .

1 Théorèmes de Sylow

1.1 Notions préliminaires

Définition 1.1.1 (Action de groupe). Soit G un groupe et A un ensemble non vide. Une *action à gauche* de G sur A est une application $f : G \times A \rightarrow A$ qui satisfait :

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

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

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

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

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

Le résultat suivant a été démontré en cours.

Proposition 1.1.2 (Bijection entre $G/Stab_G(x)$ et O_x). Soit G un groupe, $\varphi : G \times A \rightarrow A$ une action à gauche de G sur A et $x \in A$. Alors $G/Stab_G(x)$ et O_x sont en bijection.

Définition 1.1.3 (Normalisateur de H dans G). [Che24, p. 217]. Le normalisateur de H dans G est l'ensemble $N_G(H) := \{g \in G \mid gHg^{-1} = H\}$. De manière équivalente, c'est le stabilisateur de H sous l'action de conjugaison de G sur l'ensemble de ses sous-groupes.

Définition 1.1.4 (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 .

On utilise le résultat suivant issu de [Fin47] dans la preuve du point (i) du théorème de Sylow.

Lemme 1.1.5 (Théorème de Lucas). Soit p un nombre premier, $n, k \in \mathbb{N}$ tels que :

$$\begin{aligned} m &= \sum_{i=0}^r M_i p^i & (0 \leq M_i < p) \\ n &= \sum_{i=0}^r N_i p^i & (0 \leq N_i < p) \end{aligned}$$

On a la relation de congruence suivante :

$$\binom{n}{m} = \prod_{i=0}^r \binom{n_i}{k_i} \pmod{p}$$

Démonstration. Si p est un nombre premier et $n \in \mathbb{N}$ tel que $1 \leq n \leq p-1$, alors le numérateur du coefficient binomial

$$\binom{p}{n} = \frac{p \cdot (p-1) \cdot \dots \cdot (p-n+1)}{n \cdot (n-1) \cdot \dots \cdot 1}$$

est divisible par p , mais le dénominateur ne l'est pas. D'où p divise $\binom{p}{n}$. On en déduit :

$$(1+X)^p \equiv 1 + X^p \pmod{p}$$

Par récurrence, on a alors pour tout $i \in \mathbb{N}$

$$(1+X)^{p^i} \equiv 1 + X^{p^i} \pmod{p}$$

Soit $m \in \mathbb{N}$ et p un nombre premier. En écrivant m en base p

$$m = \sum_{i=0}^k m_i p^i$$

avec $k \in \mathbb{N}$ et $m_i \in \mathbb{N}$ tels que $0 \leq m_i \leq p-1$, on a :

$$\begin{aligned} \sum_{n=0}^m \binom{m}{n} X^n &= (1+X)^m = \prod_{i=0}^k ((1+X)^{p^i})^{m_i} \\ &\equiv \prod_{i=0}^k (1+X^{p^i})^{m_i} = \prod_{i=0}^k \left(\sum_{j_i=0}^{m_i} \binom{m_i}{j_i} X^{j_i p^i} \right) \\ &= \prod_{i=0}^k \left(\sum_{j_i=0}^{p-1} \binom{m_i}{j_i} X^{j_i p^i} \right) \\ &= \sum_{n=0}^m \left(\prod_{i=0}^k \binom{m_i}{n_i} \right) X^n \pmod{p}, \end{aligned}$$

□

1.2 Énoncé

Nous énonçons en premier lieu une définition issue de l'énoncé du sujet (ou de manière équivalente de [DF03, p. 123 et 139]) utile pour poser le théorème.

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

- (i) Si $\text{Card}(G) = p^n$ pour un $n > 0$, G est un p -groupe. Un sous groupe H de G est appelé p -sous groupe.
- (ii) Si $\text{Card}(G) = p^n m$ 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 $\text{Syl}_p(G)$, et le nombre de p -sous groupes de Sylow de G est noté $n_p(G)$.

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

Théorème 1.2.2 (Théorèmes de Sylow). *Soit G un groupe d'ordre $p^n m$, p un nombre premier tel que 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 $n_p(G) \geq 1$ et $\text{Syl}_p(G) \neq \emptyset$.*
- (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 P et Q de G sont conjugués entre eux : il existe $g \in G$ tel que $Q = gPg^{-1} = \{gxg^{-1} \mid x \in P, g \in G\}$. Par conséquent $P \cong Q$.*
- (iv) *Le nombre de p -sous-groupes de Sylow de G est donné par $n_p \equiv 1[p]$. De plus, pour tout $P \in \text{Syl}_p(G)$, $n_p(G) = [G : N_G(P)]$, donc m est un diviseur de $n_p(G)$.*

1.3 Démonstration

Cette preuve est due à [Che24, p. 216-218]. Nous avons explicité certains détails supplémentaires pour plus de clarté dans la présentation.

Démonstration. (i) Soit

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

une action de G sur X , où X désigne l'ensemble des parties de G de cardinal p^n . En utilisant le théorème 1.1.5 avec

$$\binom{p^n m}{p^n} = \prod_{i=0}^n \binom{n_i}{k_i} = \prod_{i=0}^n \binom{m}{1} = m \not\equiv 0 \pmod{p}$$

où $0 \leq m \leq p-1$, on en déduit que

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

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

Montrons d'abord que $\text{Card}(H)$ divise p^n . G est fini et on a une bijection entre O et G/H par le résultat 1.1.2 du cours. On a donc $\text{Card}(O) = [G : H] = \frac{\text{Card}(G)}{\text{Card}(H)}$. On en déduit que p^n divise $\text{Card}(H)$.

Réciproquement, montrons que p^n divise $\text{Card}(H)$. Soit une nouvelle action :

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

Or pour $s \in S$ fixé, on a :

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

S est partitionné en orbites que l'on note O_s où $s \in S$. On a alors $S = \bigsqcup_{s \in S} O_s$ et $\text{Card}(S) = \sum_{s \in S} \text{Card}(O_s)$. D'après le résultat 1.1.2 du cours, une orbite O_s de S sous ψ est de cardinal $\text{Card}(O_s) = [H : \text{Stab}_H(s)] = \text{Card}(H)$ car $\text{Card}(\text{Stab}_H(s)) = \text{Card}(e_G) = 1$.
D'où $\text{Card}(S) = \sum_{s \in S} \text{Card}(O_s) = \sum \text{Card}(H)$.
Ainsi $\text{Card}(H)$ divise $\text{Card}(S) = p^n$. D'où on a $\text{Card}(H) = p^n$.

- (ii) Soit Q un sous-groupe de G d'ordre p^r avec $0 \leq r \leq n$. D'après (i) au moins un $P \in \text{Syl}_p(G)$ existe, où $\text{Card}(P) = p^n \geq p^r = \text{Card}(Q)$. Donc $Q \subseteq P$.
- (iii) Soit $P \in \text{Syl}_p(G)$. 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 .

Premier cas : supposons que Q est un p -sous-groupe de Sylow de G :

$\text{Card}(Q) = p^k$ pour $1 \leq k \leq n$. Puisque $\text{Card}(P) = p^l$ pour $1 \leq l \leq n$ aussi, on a soit $l \geq k$, soit $l \leq k$. Dans les deux cas il existe bien un $g \in G$ tel que $gPg^{-1} = Q$ donc à fortiori $Q \subseteq gPg^{-1}$.

Deuxième cas : 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.

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

Soit O_p un orbite de gP . Puisque gP est partitionné en orbites et que Q est un p -groupe, alors $\text{Card}(O_p)$ 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 pour tout $q \in Q$, il existe $g \in G$ tel que $qgP = gP$. Donc pour tout $q \in Q$, $qg \in gP$. D'où pour tout $q \in Q$, $q \in gPg^{-1}$. Il existe donc $g \in G$, $Q \subseteq gPg^{-1}$.

Ainsi dans les deux cas Q est un sous-groupe conjugué de G . De plus, dans le premier cas où $Q \in \text{Syl}_p(G)$, on vérifie que $\Psi : P \rightarrow gPg^{-1}$ est un isomorphisme de groupes.

Pour tout $x_1, x_2 \in P$, on a :

$$\begin{aligned}\Psi(x_1x_2) &= gx_1x_2g^{-1} \\ &= gx_1e_Gg^{-1} \\ &= gx_1g^{-1}gx_2g^{-1} \\ &= \Psi(x_1)\Psi(x_2)\end{aligned}$$

Donc Ψ est un morphisme de groupes. Vérifions que Ψ est une bijection.

$$\begin{aligned}x \in \ker(\Psi) &\iff \Psi(x) = e_G \\ &\iff gxg^{-1} = e_G \\ &\iff x = e_G\end{aligned}$$

Donc $\ker(\Psi) = e_G$ et Ψ est injectif. Soit $y \in gPg^{-1}$, alors il existe $x \in P$ tel que $y = gxg^{-1}$. On a donc $\varphi(x) = gxg^{-1} = y$. Donc Ψ est surjectif. Par conséquent, Ψ est un isomorphisme et on a $P \stackrel{\Psi}{\cong} Q$.

(iv) Soit $P \in \text{Syl}_p(G)$, et χ l'action de conjugaison de G sur $\text{Syl}_p(G)$:

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

Puisque P est en particulier un p -groupe, $n_p(G) \bmod p$ est le nombre de points fixes de χ . Montrons que P est le seul point fixe de χ , cela est équivalent à montrer que $\text{Stab}_P(G) = \{g \in G \mid g.P = gPg^{-1} = P\} = P$ donc que $N_G(P) = P$ et $P \triangleleft G$. Soit Q un autre point fixe de χ , c'est-à-dire $Q \in \text{Stab}_Q(G) = \{g.Q \mid g.Q = gQg^{-1} = Q\}$.

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 $n_p(G) \equiv 1 \bmod p$.

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 $\text{Syl}_p(G)$ entier. Puisqu'on a une bijection entre O_P et $G/\text{Stab}_G(P)$, on en déduit que :

$$\begin{aligned}\text{Card}(O_P) &= \text{Card}(\text{Syl}_p(G)) = n_p(G) = [G : \text{Stab}_G(P)] \\ &= \frac{\text{Card}(G)}{\text{Card}(\text{Stab}_G(P))}\end{aligned}$$

D'où $n_p(G) \mid \text{Card}(G)$, et puisque $n_p(G) \equiv 1 \bmod p$, on a $n_p(G) \mid m$. □

Remarque 1.3.1. Il existe d'autres preuves utilisant des arguments similaires à ceux que nous avons exposés, comme par exemple celle de [DF03, p. 140-141].

Mentionnons aussi les théorèmes de Hall qui généralisent ceux de Sylow (nous avons choisi de ne pas les exposer car cela dépasse le cadre du sujet) dont on peut trouver une présentation dans [Ser79, p. 40-44].

2 Applications

2.1 Some corollaries

One can prove Cauchy's theorem without using Sylow's theorem, however the latter has an advantage in the sense that it can be used to prove the former. We give a quick proof here due to [Ser79].

Theorem 2.1.1 (Cauchy). *Let G be a group such that p divides $\text{Card}(G)$. Then there exists some $g \in G$ such that g has order p .*

Proof. Let $H \in \text{Syl}_p(G)$. Since $p \mid \text{Card}(G)$ then $H \neq \{e_G\}$. Picking $h \in H, h \neq e_G$ then h has order p^a with $a \geq 1$. Hence $h^{p^{a-1}}$ has order p . \square

2.2 Proving that there exists a normal subgroup of G

Given groups of small order one can force the existence of a normal subgroup in certain cases. We give one of the following :

Proposition 2.2.1. *Let G be a group such that $\text{Card}(G) = pq$ with p, q primes such that $p < q$. Given two Sylow subgroups P and Q with $\text{Card}(P) = p^n$ and $\text{Card}(Q) = q^m$ ($n, m \geq 0$) then $Q \triangleleft G$. Moreover if $P \triangleleft G$, G is cyclic.*

Proof. Since $n_q(G) = 1 + kq, k > 0$ and Q is a subgroup of G , then P and Q are conjugate subgroups of G by theorem 1.2.2. Moreover $n_q(G)$ divides p , that is to say $p = n_q(G) \times a$ for some $a \in \mathbb{N}$. But $p < q$ so $p = (1 + kq) \times a$.

If $k \geq 1, p = (a + kqa) > q$ which is impossible. Hence $k = 0$. Thus $n_q(G) = 1$ i.e. $[G : N_G(Q)] = 1$ so $N_G(Q) = Q$. Hence $Q \triangleleft G$.

Now suppose P is normal in G , let $P = \langle x \rangle$ and $Q = \langle y \rangle$.

We have $C_G(P) = \{g \in G \mid gpg^{-1} = p, \forall p \in P\}$ i.e. the centraliser of P in G . There exists a subgroup H of $\text{Aut}(\mathbb{Z}_q)$ the set of bijections of \mathbb{Z}_q onto \mathbb{Z}_q of order $q - 1$ such that $G/C_G(P)$ is isomorphic to H .

Since q does not divide $p - 1$ and q does not divide $p - 1$, then by Lagrange's theorem we have $G = C_G(P)$. So P is a subgroup of the center of G , hence $xy = yx$. The order of xy is equal to pq . Thus G is isomorphic to \mathbb{Z}_{pq} and G is cyclic. \square

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

One can use Sylow's theorem to prove whether a group G is simple or not. Given the order n and the simplicity 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 if it has two normal subgroups : $\{e_G\}$ and itself.

Simple groups arise in a similar way to prime numbers in the unique factorization of integers : we can break down 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 : $H_i \triangleleft H_{i+1}$ for $0 \leq i \leq n-1$
- (ii) the pairwise quotient groups, called the *composition factors*, are all simple : H_{i+1}/H_i is a simple group for $0 \leq i \leq n-1$

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.*

We study the case $\text{Card}(G) = 10$. We will prove that up to isomorphism there are only two groups of order 10 : \mathbb{Z}_{10} and D_5 the dihedral group of order 10, which is defined as follows :

Définition 2.3.4 (Dihedral group). The dihedral group D_{2n} is the group generated by rotations and symmetries in a regular n -gon, that is to say

$$D_{2n} = \langle r, s \mid r^n = s^2 = e, rs = sr^{-1} \rangle$$

Proof. Let G be of order 10. We break down in two cases : either G is simple or not. We will prove that if G is simple then $G \cong D_{10}$ and otherwise $G \cong \mathbb{Z}_{10}$.

Observe that $\text{Card}(G) = 10 = 2 \times 5$ with primes $2 < 5$, so by Proposition 2.2.1 given $Q \in \text{Syl}_5(G)$ then $Q \triangleleft G$ (or we can say that since $[G : Q] = 2$ then $Q \triangleleft G$). Moreover by Sylow's Theorem (iv) there are one or five subgroups in $\text{Syl}_2(G)$. In the first case, this subgroup is normal in G so G is not simple. G is generated by elements of order 2 and 5 which commute so it is abelian, hence $G \cong \mathbb{Z}_{10}$. Now in the second case, since $n_2(G) = 5$ then G has 5 elements of order 2 and similarly has 5 elements of order 5. Identifying those with rotations (order 5) and symmetries (order 2) in D_{10} , we get $G \cong D_{10}$ as desired. \square

Proposition 2.3.5 (Groups of order 15). *Let G be a group of order 15. Then $G \cong \mathbb{Z}_{15}$.*

Proof. \square

Remarque 2.3.6. *Using these notions, we can state and prove the following result for $n = 60$:*

Proposition 2.3.7 (Groups of order 60). *There are only two groups of order 60 up to isomorphism: A_5 and \mathbb{Z}_{60} .*

Références

- [Che24] E. CHEN. *An Infinitely Large Napkin*. Revision 1.6.20240911. Sept. 2024 (cité pp. 3, 5).
- [DF03] D.S. DUMMIT et R.M. FOOTE. *Abstract Algebra*. Wiley, 2003 (cité pp. 3, 4, 7, 9).
- [Fin47] Nathan J FINE. “Binomial coefficients modulo a prime”. In : *The American Mathematical Monthly* 54.10 (1947), p. 589-592 (cité p. 3).
- [Ser79] J.-P. SERRE. *Groupes finis*. Cours à l’École Normale Supérieure de Jeunes Filles. 1978–1979 (cité pp. 8, 9).