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

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.
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.
$A \cong B, A \overset{\varphi}{\cong} B$	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 $f : G \times A \to A$ 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 de groupe 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*.

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

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, $\varphi : G \times A \to A$ 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 $N_G(H) := \{g \in G \mid gHg^{-1} = H\}$. En particulier c'est un sous-groupe de G. 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. De plus 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 :

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

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

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

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

$$(1+X)^p \equiv 1 + X^p \mod p$$

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

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

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 :

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

□

1.2 Enoncé

Nous enonçons 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 $Card(G) = p^n$ 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 pour les théorèmes sont possibles, nous avons décidé d'adapter celle de l'énoncé du sujet en ajoutant quelques résultats issus 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 $Syl_p(G) \neq \emptyset$.*

(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 $P \in Syl_p(G)$, $n_p(G) = [G : N_G(P)]$, 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

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

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

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

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

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

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

Montrons d'abord que $Card(H)$ 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 $Card(O) = [G : H] = \frac{Card(G)}{Card(H)}$. On en déduit que p^n divise $Card(H)$.

Réciproquement, montrons que p^n divise $Card(H)$. 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 :

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

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 $Card(S) = \sum_{s\in S} Card(O_s)$. D'après le résultat 1.1.2 du cours, une orbite O_s de S sous ψ est de cardinal $Card(O_s) = [H : Stab_H(s)] = Card(H)$ car $Card(Stab_H(s)) = Card(e_G) = 1$.
D'où $Card(S) = \sum_{s\in S} Card(O_s) = \sum Card(H)$.
Ainsi $Card(H)$ divise $Card(S) = p^n$. D'où on a $Card(H) = p^n$.

(ii) Soit Q un sous-groupe de G d'ordre p^r avec $0 \leq r \leq n$. D'après (i) au moins un $P \in Syl_p(G)$ 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.

Premier cas : supposons que Q est un p-sous-groupe de Sylow de G :
$Card(Q) = p^k$ pour $1 \leq k \leq n$. Puique $Card(P) = p^l$ 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.

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

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 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 $g \in G$ tel que $Q \subseteq gPg^{-1}$.
Ainsi dans les deux cas Q est un sous-groupe conjugué de G. De plus, dans le premier cas où $Q \in Syl_p(G)$, montrons que $\Psi : P \to gPg^{-1}$ 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 bijectif.

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

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 $\varphi(x) = gxg^{-1} = y$. Donc Ψ est surjectif. D'où Ψ est un isomorphisme et on a $P \overset{\Psi}{\cong} Q$.

(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, on a $Q \in Stab_Q(G) = \{g.Q \mid g.Q = gQg^{-1} = Q\}$. 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 $G/Stab_G(P)$ par 1.1.2, 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 $n_p(G)$ divise $Card(G)$. Or $Card(G) = p^n m$ et $n_p(G) \equiv 1 \mod p$, on en déduit que $n_p(G)$ divise m.

□

Remarque 1.3.1. *Il existe d'autres preuves utilisant des arguments similaires à ceux que nous avons exposés avec des actions de groupes, comme par exemple celle de [DF03, p. 140-141] où l'on retrouve aussi l'équation aux classes.*

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

2 Applications

2.1 Deducing Cauchy's theorem

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, p. 12].

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

Proof. Let $H \in Syl_p(G)$. Since p divides $Card(G)$ then $H \neq \{e_G\}$. Pick $h \in H$ such that $h \neq e_G$, then h has order p^a with $a \geq 1$. Hence $h^{p^{(a-1)}}$ has order p. □

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 due to [DF03, p. 143].

Proposition 2.2.1. *Let G be a group such that $Card(G) = pq$ for p, q prime numbers with $p < q$. Given $P \in Syl_p(G)$ and $Q \in Syl_q(G)$ then $Q \lhd G$. If we also have $P \lhd G$, then G is cyclic.*

Proof. By Sylow's theorem (iv), $n_q(G) = 1 + kq$ for $k \in \mathbb{N}$. Moreover $n_q(G)$ divides p, that is to say $p = n_q(G).a = (1 + kq).a$ for some $a \in \mathbb{N}$. If $k \geq 1$ then $p = (a + kqa) > q$ which is impossible since $p < q$. Hence $k = 0$. Thus $n_q(G) = 1$ and $[G : N_G(Q)] = 1$, so $N_G(Q) = G$. Hence $Q \lhd G$.

Now suppose $P \lhd G$. Let $P = \langle x \rangle$ and $Q = \langle y \rangle$.

Define the *centralizer of P in G* as the set $C_G(P) = \{g \in G \mid gpg^{-1} = p, \forall p \in P\}$. In particular it is a subgroup of G. Recall that $\mathrm{Aut}(\mathbb{Z}_p)$ is the group of automorphisms of $\mathbb{Z}_p$ of order $p - 1$. Since $P \lhd G$ there exists a subgroup H of $\mathrm{Aut}(\mathbb{Z}_p)$ such that $G/C_G(P)$ is isomorphic to H. Since p does not divide $p - 1$ and q does not divide $p - 1$, then by Lagrange's theorem we have $G = C_G(P)$. In this case P is a subgroup of $Z(G)$ the center of G, hence $xy = yx$.

The order of xy is equal to pq. Thus G is cyclic and $G \cong \mathbb{Z}_{pq}$. □

2.3 Classifing 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 group 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 : $H_i \lhd H_{i+1}$ 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 first study the case $Card(G) = 10$, for which we need the following definition.

Definition 2.3.4 (Dihedral group)**.** The dihedral group D_{2n} of order $2n$ is the group generated by rotations and symmetries in a regular n-gon, which has the presentation

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

We can now prove the following :

Proposition 2.3.5 (Groups of order 10)**.** *There are only two groups of order 10 up to isomorphism : $\mathbb{Z}_{10}$ the cylic group of order 10 and D_{10} the dihedral group of order 10.*

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 $Card(G) = 10 = 2 \times 5$ with primes $2 < 5$. By Proposition 2.2.1, given $Q \in Syl_5(G)$ then $Q \lhd G$ (or we can say that since $[G : Q] = 2$ then $Q \lhd G$). Moreover by Sylow's Theorem (iv) there are one or five subgroups in $Syl_2(G)$. 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. □

Proposition 2.3.6 (Groups of order 15)**.** *Let G be a group of order 15. Then* $G \cong \mathbb{Z}_{15}$.

Proof. As in the proof of the previous proposition, observe that $Card(G) = 15 = 3 \times 5$ with primes $3 < 5$. □

Proposition 2.3.7 (Groups of order 60)**.** *There are only two groups of order 60 up to isomorphism:* A_5 *and* 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, 8, 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 p. 8).