SOUS-GROUPES DE SYLOW

Chapitre 4

Table des matières

1. Théorèmes de Sylow

Nous avons vu que le théorème de Cauchy donne une réciproque partielle au théorème de Lagrange : pour tout p entier premier tel que p divise $|G|$, il existe un sous-groupe d'ordre p de G. Nous allons montrer plus généralement que G contient des sous-groupes d'ordre p^i, pour tout i tel que p^i divise $|G|$.

Notation 1.1. — *Soit G un groupe et p un nombre premier divisant $|G|$. On note α et m les entiers tels que $|G| = p^\alpha m$ avec $p \nmid m$.*

Définition 1.2. — *Un sous-groupe S de G est appelé p-sous-groupe de Sylow (ou p-Sylow) si S est de cardinal p^α.*

On peut remarquer que, de manière équivalente, cela signifie que l'ordre de G/S est premier à p.

Exemple 1.3. — *Soit G un groupe d'ordre p^α. Alors G lui-même est l'unique p-sous-groupe de Sylow de G. En effet, par définition, un p-Sylow doit être un sous-groupe de G d'ordre p^α.*

Exemple 1.4. — *Soit $G = \mathrm{GL}_n(\mathbb{F}_p)$ le groupe linéaire sur le corps $\mathbb{Z}/p\mathbb{Z}$. Soit $S \leq G$ le sous-groupe des matrices triangulaires supérieures avec des coefficients 1 sur la diagonale. Alors S est un p-sous-groupe de Sylow de G.*

Démonstration. — Tout d'abord, pour produire une base de $\mathbb{F}_p^n$, on peut choisir un vecteur non nul. Il y a $p^n - 1$ choix pour cela. On peut ensuite choisir un vecteur non colinéaire à celui-là : il y a $p^n - p$ choix pour cela. On choisit encore un vecteur qui n'est pas dans le plan engendré par les deux

vecteurs déjà choisis ($p^n - p^2$ choix), et ainsi de suite. Le groupe G est donc d'ordre

$$(p^n-1)(p^n-p)\dots(p^n-p^{n-1}) = p^{n(n-1)/2}(p^n-1)(p^{n-1}-1)\dots(p-1).$$

Puisque p ne divise aucun facteur $p^t - 1$ pour $1 \leq t \leq n$, on a $\alpha = n(n-1)/2$ et $m = (p^n-1)(p^{n-1}-1)\dots(p-1)$.

D'un autre côté, pour se donner un élément de S, on doit se donner les valeurs des $n(n-1)/2$ coefficients au-dessus de la diagonale, et ces coefficients sont des éléments quelconques de $\mathbb{F}_p$. Donc

$$|H| = p^{n(n-1)/2} = p^\alpha.$$

S est donc bien un p-sous-groupe de Sylow. □

Pour montrer l'existence de p-sous-groupes de Sylow, on montre d'abord que ce résultat d'existence passe aux sous-groupes :

Lemme 1.5. — *Soit G un groupe d'ordre $p^\alpha m$ comme précédemment. Soit H un sous-groupe de G et S un p-Sylow de G. Alors il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H.*

Démonstration. — Le groupe G opère sur G/S par translations à gauche et le stabilisateur de gS est gSg^{-1}. Donc, par restriction, H opère aussi sur G/S, avec comme stabilisateur de gS le sous-groupe $gSg^{-1} \cap H$.

Il reste à montrer qu'un des groupes $gSg^{-1} \cap H$ est un p-Sylow de H, c'est-à-dire qu'il existe g tel que $|H/(gSg^{-1} \cap H)|$ soit premier à p. Dans l'hypothèse contraire, toutes les H-orbites de gS dans G/S seraient de cardinal divisible par p. Ceci impliquerait que p divise G/S, une contradiction avec l'hypothèse que S est un p-Sylow de G. □

On peut maintenant montrer l'existence de p-Sylows :

Théorème 1.1. — *Soit G un groupe fini et p un nombre premier divisant $|G|$. Alors G admet des p-sous-groupes de Sylow.*

Démonstration. — D'après l'Exemple 1.4 et le Lemme 1.5, il suffit de savoir que tout groupe s'injecte dans un groupe $\mathrm{GL}_n(\mathbb{F}_p)$. Or, c'est le contenu du Corollaire 1.7 dans le chapitre 2 (Corollaire au Théorème de Cayley). □

On peut maintenant généraliser le théorème de Cauchy :

Corollaire 1.6. — *Avec la Notation 1.1, soit i un entier tel que $0 \leq i \leq \alpha$. Il existe un sous-groupe de G d'ordre p^i.*

Démonstration. — Tout d'abord, il existe un p-sylow, c'est-à-dire un sous-groupe S de cardinal p^α. En remplaçant G par S, il suffit donc de montrer le résultat lorsque G est un p-groupe. On suppose donc $|G| = p^\alpha$.

D'après le Théorème 3.7 du chapitre 2, le centre $Z(G)$ de G est non trivial : il est donc d'ordre p^β avec $1 \leq \beta \leq \alpha$. Si $i \leq \beta$, comme $Z(G)$ est abélien, d'après le Théorème 5.6 dans le chapitre 3, $Z(G)$ admet un sous-groupe d'ordre p^i, qui est donc un sous-groupe de G d'ordre p^i.

Si $i > \beta$, on peut supposer par récurrence qu'il existe un sous-groupe K d'ordre $p^{i-\beta}$ dans le quotient $G/Z(G)$, d'ordre $p^{\alpha-\beta}$. Soit $\pi : G \to G/Z(G)$ le morphisme quotient. D'après la Proposition 9.6 dans le chapitre 1, $\pi^{-1}(K)$ est un sous-groupe de G contenant $Z(G)$, et il est de cardinal

$$|K| \cdot |\operatorname{Ker}(\pi)| = |K| \cdot |Z(G)| = p^{i-\beta} \cdot p^{\beta} = p^i.$$

L'existence est donc aussi montrée dans le cas $i > \beta$. □

Le deuxième théorème de Sylow étudie qualitativement la famille de tous les p-sous-groupes de Sylow :

Théorème 1.2. — *Soit G un groupe de cardinal $p^\alpha m$ avec $p \nmid m$.*

1. *Si H est un sous-groupe de G et un p-groupe, alors il existe un p-Sylow de G contenant H.*
2. *Les p-Sylow sont tous conjugués.*

Démonstration. — Soit H un p-sous-groupe de G et S un p-Sylow de G. D'après le Lemme 1.5, il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H. Or, comme H est un p-groupe, H lui-même est l'unique p-Sylow de H (cf Exemple 1.3) : ainsi on obtient $gSg^{-1} \cap H = H$, soit $H \subset gSg^{-1}$. Ceci montre le premier point. Si de plus H est un p-Sylow de G, l'inclusion $H \subset gSg^{-1}$ devient une égalité puisque $|H| = |gSg^{-1}| = p^\alpha$: on a donc montré le deuxième point. □

Le troisièmé théorème de Sylow porte sur le nombre de p-Sylow :

Théorème 1.3. — *Soit G un groupe de cardinal $p^\alpha m$ avec $p \nmid m$. Soit n_p le nombre de p-Sylow. On a $n_p | m$ et $n_p \equiv 1\ [p]$.*

Démonstration. — On fait d'abord agir S par conjugaison sur l'ensemble X des p-Sylow de G. Le Corollaire 3.4 dans le chapitre 2 donne $|X| \equiv |\operatorname{Fix}(S)|\ [p]$. Pour montrer que $n_p \equiv 1\ [p]$, il suffit donc de montrer que $\operatorname{Fix}(S) = \{S\}$. Clairement, $sSs^{-1} = S$ pour tout $s \in S$, donc $S \in \operatorname{Fix}(S)$. Soit maintenant $T \in \operatorname{Fix}(S)$: ceci signifie que T est un p-Sylow et que pour tout $s \in S$, on a $sTs^{-1} = T$. Soit alors $N \leq G$ le sous-groupe engendré par S et T. On a $S, T \subset N \subset G$, donc S et T sont tous deux des p-Sylow de N. Or, pour $n \in S$, ainsi que pour $n \in T$, on a $nTn^{-1} = T$. On a donc cette relation pour tout $n \in N$. D'après le point 2) du Théorème 1.2 appliqué au groupe N, S et T sont conjugués dans N : soit donc $n \in N$ tel que $S = nTn^{-1}$. Comme $nTn^{-1} = T$, ceci montre $S = T$.

On fait maintenant agir G par conjugaison sur l'ensemble X des p-Sylow de G. D'après le point 2), il n'y a qu'une seule orbite, donc $|X| = \frac{|G|}{|G_S|}$, où S est un p-Sylow fixé. Donc $n_p | p^\alpha m$. Comme on a déjà montré que n_p est premier à p, on en déduit que $n_p | m$. □

Remarque 1.7. — *En particulier, Le Théorème 1.3 implique que p divise $n_p - 1$, donc que si $n_p > 1$, alors $p < n_p$.*

2. Application : groupes simples de cardinal au plus 60

Pour étudier les groupes de manière très générale, une stratégie consiste à les "dévisser" : si un groupe G contient un sous-groupe distingué N, alors on a une suite exacte de groupes

$$\{e\} \to N \to G \to Q \to \{e\} \tag{1}$$

avec $Q = G/N$. Un certain nombre de questions (comme la classification) portant sur G se ramènent aux mêmes questions pour N et G/N, plus la détermination de toutes les suites exactes (1), N et Q étant fixés.

A ce titre, les groupes n'admettant pas de sous-groupes distingués non triviaux sont les briques élémentaires de la théorie des groupes, c'est pourquoi il est naturel d'introduire la définition suivante :

Définition 2.1. — *Un groupe G est dit simple lorsque ses sous-groupes distingués sont tous triviaux, à savoir égaux à G ou $\{e\}$.*

La théorie exposée au chapitre 3, des groupes abéliens finis, montre que parmi les groupes abéliens finis, seuls les groupes Z/pZ avec p premier sont simples.

On se propose à titre d'application des théorèmes de Sylow de montrer que le plus petit ordre d'un groupe simple non abélien est 60.

Théorème 2.1. — *Tout groupe simple d'ordre au plus 59 est abélien.*

On verra dans le chapitre suivant que le groupe alterné $\mathcal{A}_5$ est simple, non abélien, et de cardinal 60. Ceci et le théorème montrent l'affirmation ci-dessus.

Ce théorème sera la conséquence d'une série de lemmes qu'on établira après les remarques qui suivent.

Remarque 2.2. — *Soit G un groupe et H un sous-groupe de G d'indice $k > 1$, tels que $|G|$ ne divise pas $k!$. Alors G est simple.*

Démonstration. — Soit $\gamma : G \to \mathfrak{S}(G/H)$ le morphisme donné par l'action à gauche de G sur G/H. Le noyau de γ ne peut pas être réduit à $\{e\}$ car alors $\mathrm{Im}(\gamma)$ serait d'ordre $|G|$, et un sous-groupe du groupe $\mathfrak{S}(G/H)$, identifié à $\mathfrak{S}_k$, et donc d'ordre $k!$. L'hypothèse de non divisibilité contredirait alors le Théorème de Lagrange.

Pour $x \in \mathrm{Ker}(\gamma)$, $x \cdot eH = xH = eH$, donc $x \in H$: le noyau de γ est inclus dans H, donc ne peut pas être égal à G. Ainsi, $\mathrm{Ker}(\gamma)$ est un sous-groupe distingué non trivial de G, qui n'est donc pas simple. □

Remarque 2.3. — *Soit G un groupe d'ordre $p^\alpha q$. Si $n_q = p^\alpha$, alors G est simple.*

Démonstration. — Supposons $n_q = p^\alpha$. Notons $S_1, \ldots, S_{p^\alpha}$ les q-Sylow. Pour i, j distincts, on doit avoir $|S_i \cap S_j| = 1$ par le Théorème de Lagrange, donc $S_i \cap S_j = \{e\}$. La réunion $\bigcup_i (S_i \setminus \{e\})$ contient donc $p^\alpha(q-1)$ éléments et ils sont tous d'ordre q. Le complémentaire $C := G \setminus \bigcup_i (S_i \setminus \{e\})$ est de cardinal

$|G| - p^\alpha(q-1) = p^\alpha$. Soit S un p-Sylow, les éléments de S ont un ordre qui divise p^α, donc différent de q. Ainsi $S \subset C$. Comme $|S| = p^\alpha = |C|$, on en déduit que $S = C$. Ainsi, C est l'unique p-Sylow, et G n'est pas simple. □

Lemme 2.4. — *Soit G un groupe d'ordre p^α avec p premier. Alors G est simple si et seulement si $\alpha = 1$.*
Démonstration. — On sait que le seul groupe d'ordre p est $\mathbb{Z}/p\mathbb{Z}$, et il est simple. Si $\alpha > 1$, il y a deux cas de figure : soit G est abélien, et d'après le chapitre 3 on sait qu'il n'est pas simple, soit G n'est pas abélien, et son centre est donc un sous-groupe strict de G. Par ailleurs, $Z(G)$ n'est pas réduit à $\{e\}$, par le Théorème 3.7 du chapitre 2. Ainsi, $Z(G)$ est un sous-groupe non trivial, et distingué, donc G n'est pas simple. □

Lemme 2.5. — *Soit G un groupe de cardinal pq avec p et q des entiers premiers distincts. Alors G n'est pas simple.*
Démonstration. — On peut supposer $p > q$. D'après le Théorème 1.3, on a $n_p | q$, donc $n_p = 1$ ou $n_p = q$. Si $n_p > 1$, la Remarque 1.7 donne $p < q$, contredisant notre hypothèse. Ainsi $n_p = 1$, donc l'unique p-Sylow de G est distingué, montrant que G n'est pas simple. □

Lemme 2.6. — *Soit G un groupe de cardinal p^2q avec p et q des entiers premiers distincts. Alors G n'est pas simple.*
Démonstration. — On a $n_q \in \{1, p, p^2\}$.

Si $n_q = 1$, alors l'unique q-Sylow est distingué, donc G n'est pas simple.

Supposons $n_q = p$. La Remarque 1.7 donne $q < p$. Si $n_p = q$, alors de même $p < q$, ce qui est une contradiction. On a donc $n_p = 1$, et le lemme est montré car l'unique p-Sylow est distingué.

Finalement, si $n_q = p^2$, alors G n'est pas simple par la Remarque 2.3. □

Lemme 2.7. — *Soit G un groupe d'ordre pqr avec p, q, r trois nombres premiers distincts. Alors G n'est pas simple.*
Démonstration. — On peut supposer $p > q > r$. On montre d'abord

$$pqr > n_p(p-1) + n_q(q-1) + n_r(r-1). \tag{2}$$

En effet, un p-Sylow est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, donc il contient l'élément neutre et $p-1$ éléments d'ordre p. De plus, deux p-Sylow ne se rencontrent qu'en l'élément neutre. Donc les n_p p-Sylow contiennent $n_p(p-1)$ éléments d'ordre p. De même, G contient $n_q(q-1)$ éléments d'ordre q et $n_r(r-1)$ éléments d'ordre r. Puisque G contient en outre l'élément neutre, (2) est montré.

Montrons que l'un des trois entiers n_p, n_q, n_r est égal à 1 (et que donc G n'est pas simple). Sous l'hypothèse inverse, on a

$$n_p = qr \ , \ n_q \geq p \ , \ n_r \geq q \, . \tag{3}$$

En effet, on sait que n_p divise qr et que p divise $n_p - 1$. Si $n_p = q$, alors $p \leq q - 1$, contrairement à ce que nous avons supposé. De même, l'hypothèse $n_p = r$ est absurde. On a donc bien $n_p = qr$.

De la même manière, n_q divise pr et q divise $p_q - 1$. Comme ci-dessus, n_q ne peut pas être égal à r. Il est donc égal à p ou pr, donc $n_q \geq p$.

L'inégalité $n_r \geq q$ résulte du simple fait que n_r divise pq et n'est pas égal à 1 : (3) est montré.

En utilisant (3), on obtient

$$\begin{aligned} n_p(p-1) + n_q(q-1) + n_r(r-1) &\geq qr(p-1) + p(q-1) + q(r-1) \\ &= pqr + pq - p - q \\ &= pqr + (p-1)(q-1) - 1 \geq pqr \end{aligned}$$

Ceci contredit (2), donc un des trois entiers n_p, n_q, n_r doit être égal à 1. □

Lemme 2.8. — *Soit G un groupe d'ordre $p^\alpha q$ avec p et q premiers distincts et $\alpha \geq 2$. Si $p > q$ ou $p^\alpha \not| (q-1)!$, alors G n'est pas simple.*

Démonstration. — Supposons d'abord $p > q$. On a $n_p = 1$ ou $n_p = q$, et si $n_p = q$ conduit à $p < q$. Donc dans ce cas $n_p = 1$ et G n'est pas simple.

Supposons que p^α ne divise pas $(q-1)!$. Alors $|G| = p^\alpha q$ ne divise pas $q!$. Soit S un p-Sylow de G. Il est d'ordre p^α, donc la Remarque 2.2 s'applique. □

On peut observer que les Lemmes 2.4 à 2.8 traitent tous les groupes d'ordre 2 à 59 sauf ceux d'ordre $36, 40$ ou 56. On traite maintenant séparément ces trois cas de figure.

Lemme 2.9. — *Un groupe d'ordre $36 = 2^2 3^2$ n'est pas simple.*

Démonstration. — Un 3-Sylow est d'indice 4, donc la Remarque 2.2 s'applique, puisque $36 \not| 4!$. □

Lemme 2.10. — *Un groupe d'ordre $40 = 2^3 5$ n'est pas simple.*

Démonstration. — On a $n_5 | 8$ et $n_5 \equiv 1$ [5], donc $n_5 = 1$ et l'unique 5-Sylow est distingué. □

Lemme 2.11. — *Un groupe G d'ordre $56 = 2^3 7$ n'est pas simple.*

Démonstration. — On a $n_7 | 8$ et $n_7 \equiv 1$ [7], donc $n_7 = 1$ ou $n_7 = 8$. Si $n_7 = 1$, G n'est pas simple. Si $n_7 = 8$, G n'est pas simple par la Remarque 2.3. □

3. Classification

Dans certains cas favorables, l'étude des sous-groupes de Sylow permet de classifier tous les groupes d'un ordre fixé.

Lemme 3.1. — *Soit G un groupe. Si pour tout premier p, G n'admet qu'un p-Sylow, alors G est produit direct de ses sous-groupes de Sylow.*

Pour rappel, les produits directs de sous-groupes sont définis dans la Proposition 9.3 du chapitre 1.

Démonstration. — Soit $p_1, \dots, p_k$ les diviseurs premiers de $|G|$, et écrivons $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Utilisant l'hypothèse, pour tout i, soit S_i l'unique p_i-Sylow de G. Pour $g \in G$, gS_ig^{-1} est un p_i-Sylow, donc par unicité $gS_ig^{-1} = S_i$, autrement dit S_i est distingué. De plus, pour $h_i \in S_i$ et $h_j \in S_j$, on a comme dans la preuve de la Proposition 9.3 du chapitre 1, $x := h_j^{-1}h_ih_jh_i^{-1} \in H_i \cap H_j$. L'ordre de x divise donc à la fois $p_i^{\alpha_i}$ et $p_j^{\alpha_j}$, de sorte qu'il est égal à 1. Ainsi $x = e$ et $h_ih_j = h_jh_i$.

Par ailleurs, rappelons les notations de la Proposition 9.3 du chapitre 1. Nous avions introduit l'application

$$\begin{array}{rccc} \varphi & : & S_1 \times \cdots \times S_k & \to & G \\ & & (h_1, \dots, h_k) & \mapsto & h_1 \cdots h_k \, . \end{array}$$

Montrons que φ est une bijection. Les deux ensembles ayant cardinal $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, il suffit de montrer que φ est injective. Or, si on a $\varphi(h_1, \dots, h_k) = \varphi(h'_1, \dots, h'_k)$, on en déduit par commutativité

$$h_1(h'_1)^{-1} = h'_2h_2^{-1} \cdots h'_kh_k^{-1}.$$

En posant $m = p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, on a $(h'_2h_2^{-1} \cdots h'_kh_k^{-1})^m = (h'_2h_2^{-1})^m \cdots (h'_kh_k^{-1})^m = e$. Ainsi l'ordre de $h'_2h_2^{-1} \cdots h'_kh_k^{-1}$ divise m. En outre, l'ordre de $h_1(h'_1)^{-1}$ divise $p_1^{\alpha_1}$. On en déduit que cet ordre commun est 1, et que $h_1(h'_1)^{-1} = e$, d'où $h_1 = h'_1$. Par symétrie, on obtient $h_i = h'_i$ pour tout i. L'injectivité de φ est donc établie. On a donc montré toutes les conditions de la Proposition 9.3 du chapitre 1. □

Proposition 3.2. — *Soit G un groupe d'ordre pq avec p et q premiers tels que $p \not\equiv 1$ $[q]$ et $q \not\equiv 1$ $[p]$. Alors G est cyclique.*

Démonstration. — On sait que $n_q | p$ et $n_q \equiv 1$ $[q]$, doncc $n_q = 1$. De même, $n_p = 1$. Le Lemme 3.1 et le Théorème des restes chinois permet de conclure. □

Proposition 3.3. — *Soit G un groupe d'ordre $2p$ avec p premier impair. Alors G est soit cyclique, soit diédral.*

Démonstration. — Par le Théorème de Cauchy, soit r d'ordre p et s d'ordre 2. Les éléments r^i pour $0 \leq i \leq n-1$ sont tous distincts, ainsi donc que les éléments r^is pour $0 \leq i \leq n-1$. Par ailleurs, on ne peut pas avoir $r^i = r^js$ pour des entiers i, j, car cela conduirait à l'égalité $s = r^{i-j}$ qui implique que l'ordre de s divise p. On a donc $G = \{e, r, \dots, r^{n-1}, s, rs, \dots, r^{n-1}s\}$.

Comme $n_p \in \{1, 2\}$ et $n_p \equiv 1$ $[p]$, $n_p = 1$: il n'y a qu'un p-Sylow, c'est $\{e, r, \dots, r^{p-1}\}$. Pour conclure, raisonnons sur l'ordre de rs, qui doit diviser $2p$:

– S'il est égal à 1, alors $rs = e$, donc $r = s$, contradiction.

– S'il est égal à p, alors rs engendre un groupe d'ordre p, donc l'unique p-Sylow, donc $rs \in \{e, r, \ldots, r^{p-1}\}$, contradiction à nouveau.
– S'il est égal à $2p$, alors G est cyclique et la Proposition est vraie.
– S'il est égal à 2, alors $rsrs = e$ donc $rs = sr^{-1}$, et on retrouve la présentation du groupe diédral donnée dans l'Exemple 7.9 du chapitre 1.

□

CHAPITRE 4