il existe 14 groupes d'ordre 16, 51 d'ordre 32, 267 d'ordre 64, ..., 49487365422 d'ordre 1024, et on ne connaît pas leur nombre d'ordre 2048.

COROLLAIRE 1.9. *Les p-groupes sont résolubles.*

DÉMONSTRATION — On montre par récurrence sur $n \geqslant 0$ qu'un p-groupe P d'ordre p^n est résoluble. C'est clair pour $n = 0$. Pour $n > 0$ on sait que le centre $\mathrm{Z}(P)$ de P est non trivial. Si on a $\mathrm{Z}(P) = P$ alors P est abélien, donc résoluble. Sinon, $\mathrm{Z}(P)$ et $P/\mathrm{Z}(P)$ sont deux p-groupes d'ordre $< p^n$, résolubles par récurrence, et donc P est résoluble par la Proposition 6.11 Chap. 4. □

En fait, les p-groupes vérifient une condition beaucoup plus forte que la résolubilité, appelée *nilpotence*. Nous renvoyons au Complément 6 pour une discussion de cette notion importante, et aux exercices pour des compléments sur les p-groupes.

2. Les théorèmes de Sylow

Soient G un groupe fini et p un nombre premier divisant $|G|$. On peut donc écrire $|G| = p^\alpha m$ avec $p \wedge m = 1$ et $\alpha \geqslant 1$. On rappelle qu'un p-Sylow de G est un sous groupe de G de cardinal exactement p^α. On a déjà démontré le premier théorème de Sylow (Théorème 4 Chap. 1.14), qui affirme que G possède au moins un p-Sylow. Si P est un p-Sylow de G, il en va de même de chaque conjugué gPg^{-1} pour $g \in G$ (un sous-groupe isomorphe à P via l'automorphisme $x \mapsto gxg^{-1}$). On a en fait les énoncés plus précis suivants.

THÉORÈME 2.1. (Sylow) *Soient G un groupe fini et p premier divisant $|G|$.*

(i) G possède des p-Sylow,

(ii) Tout p-sous-groupe[1] *de G est inclus dans un p-Sylow de G,*

(iii) Deux p-Sylow de G sont conjugués (en particulier, isomorphes).

EXEMPLE 2.2. Le groupe S_4 est d'ordre $24 = 3 \cdot 8$. Les 3-Sylow de S_4 sont donc ses sous-groupes d'ordre 3, nécessairement engendrés par un 3-cycle. Ils sont bien conjugués car les 3-cycles sont conjugués dans S_n pour $n \geqslant 3$. Les 2-Sylow de S_4 sont ses sous-groupes d'ordre 8. Un exemple est $\mathrm{D}_8 \subset \mathrm{S}_4$, et tout 2-Sylow est donc conjugué à D_8 par le théorème. Observons cependant que $A := \mathrm{K}_4$, $B := \langle (1\,2\,3\,4) \rangle$ et $C := \langle (1\,3), (2\,4) \rangle$ sont 3 sous-groupes d'ordre 4 de S_4 (en fait, ce sont les 3 sous-groupes d'ordre 4 de D_8), et qu'ils sont deux-à-deux non conjugués dans S_4 ! Ainsi, il n'est pas vrai que deux p-sous groupes de G de même ordre sont conjugués, ni même isomorphes (cas de A et B), et il n'est pas vrai non plus que deux p-sous groupes isomorphes sont conjugués (cas de A et C).

Ce théorème va découler entièrement du lemme suivant, qui peut-être vu comme une version abstraite de la Proposition 1.4.

LEMME 2.3. (Alignement des p-Sylow) *Soient G un groupe fini, H un sous-groupe de G et p premier divisant $|H|$. Si P est un p-Sylow de G, il existe $g \in G$ tel que $gPg^{-1} \cap H$ est un p-Sylow de H.*

1. Un p-sous-groupe d'un groupe G est un sous-groupe de G qui est un p-groupe.

Démonstration — On considère la restriction à H de l'action par translations de G sur G/P. Comme $|G/P| = |G|/|P|$ est premier à p, au moins une des orbites $O \subset G/P$ sous l'action de H est de cardinal premièr à p, par l'équation aux classes. Disons que O est l'orbite de gP, pour un certain $g \in G$. Le stabilisateur de gP dans H est $gPg^{-1} \cap H$. Il est d'indice $|O|$ dans H (Formule orbite-stabilisateur), qui est premier à p par hypothèse. C'est aussi un p-sous groupe de H car il est inclus dans le p-groupe gPg^{-1} : c'est un p-Sylow de H. □

Démonstration — (Du Théorème 2.1). Re-démontrons le (i). On sait que tout groupe fini G est isomorphe à un sous-groupe de S_n. Mais S_n est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ (matrices de permutations). On peut donc supposer que G est inclus dans $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. Mais ce dernier possède $P = \mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})$ pour p-Sylow. Il existe donc $g \in \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ tel que $gPg^{-1} \cap G$ est un p-Sylow de G.

Le (ii) est une conséquence directe du lemme. En effet, si H est un p-sous groupe de G, et si P est un p-Sylow de G (on sait qu'il en existe par le (i)), il existe $g \in G$ tel que $gPg^{-1} \cap H$ est un p-Sylow de H. Mais comme H est un p-groupe, cela veut dire $gPg^{-1} \cap H = H$, et donc $H \subset gPg^{-1}$. Ainsi, gPg^{-1} est le p-Sylow de G cherché. Dans le cas particulier où H est un p-Sylow, l'inclusion $H \subset gPg^{-1}$ est une égalité pour une raison de cardinal, on a donc $H = gPg^{-1}$: on a montré le (iii). □

Définition 2.4. *On notera* $\mathrm{Syl}_p(G)$ *l'ensemble des p-Sylow de G et* $\mathrm{n}_p(G)$ *le nombre de p-Sylow de G. Autrement dit, on a* $\mathrm{n}_p(G) = |\mathrm{Syl}_p(G)|$.

Corollaire 2.5. *On a* $\mathrm{n}_p(G) = 1 \iff$ *G possède un p-Sylow distingué.*

Démonstration — Si on a $\mathrm{n}_p(G) = 1$ alors G possède un unique p-Sylow P, nécessairement distingué car on a alors $gPg^{-1} = P$ pour tout $g \in G$. Réciproquement, si P est un p-Sylow de G, alors tout autre p-Sylow est un conjugué de P par le théorème (iii), et donc égal à P si ce dernier est distingué. □

Théorème 2.6. (Sylow) *Soit G un groupe fini de cardinal $p^\alpha m$ avec $\alpha \geqslant 1$ et $p \wedge m = 1$. On a* $\mathrm{n}_p(G) \mid m$ *et* $\mathrm{n}_p(G) \equiv 1 \bmod p$.

Démonstration — Soit $S := \mathrm{Syl}_p(G)$. On a $S \neq \varnothing$ par le Théorème 2.1 (i). Le groupe G agit par conjugaison sur S, $(g, P) \mapsto gPg^{-1}$, transitivement par le (iii) du même théorème. Le stabilisateur de $P \in S$ est son normalisateur $\mathrm{N}_G(P)$ par définitions. Par la formule orbite-stabilisateur on a donc

$$\mathrm{n}_p(G) = |S| = |G|/|\mathrm{N}_G(P)|, \text{ puis } \mathrm{n}_p(G) \mid |G|.$$

Fixons $P \in S$ et considérons son action sur S (donc par $(g, Q) \mapsto gQg^{-1}$). Montrons que son unique point fixe est P lui-même. On aura alors bien $|S| \equiv 1 \bmod p$ par la Proposition 1.6. Soit Q un p-Sylow de G qui est fixe, *i.e.* avec $gQg^{-1} = Q$ pour tout $g \in P$. Autrement dit, on a $P \subset \mathrm{N}_G(Q)$ et donc P est un p-Sylow de $\mathrm{N}_G(Q)$. Mais Q est manifestement un p-Sylow distingué de $\mathrm{N}_G(Q)$, et donc l'unique p-Sylow de ce dernier par le Corollaire 2.5 appliqué à $\mathrm{N}_G(Q)$, donc on a $P = Q$. □

EXEMPLE 2.7. Les p-Sylow de S_p sont ses sous-groupes d'ordre p. Chaque tel sous-groupe est engendré par un unique p-cycle de la forme $(1\,2\,\cdots)$. Il y en a donc $(p-2)! \equiv 1 \bmod p$ (Wilson), conformément à $\mathrm{n}_p(G) \equiv 1 \bmod p$, et ils sont bien tous conjugués car les p-cycles le sont dans S_p.

Comme nous le verrons dans les exercices, ce théorème permet typiquement de montrer que G possède un p-Sylow distingué. Donnons une autre application.

EXEMPLE 2.8. *Un groupe simple d'ordre* 60 *est isomorphe à* A_5. En effet, soit G un tel groupe. On a $60 = 12 \cdot 5$, donc $\mathrm{n}_5(G) \mid 12$ et $\mathrm{n}_5(G) \equiv 1 \bmod 5$, puis $\mathrm{n}_5(G) = 6$ (1 est interdit car G est simple). Ainsi, l'action naturelle de G par conjugaison sur l'ensemble des six 5-Sylow de G définit un morphisme $f : G \to \mathrm{S}_6$ d'image transitive par Sylow. Comme G est simple, ce morphisme est injectif, et pour la même raison on a aussi $\varepsilon \circ f = 1$, donc $f(G) \subset \mathrm{A}_6$. La même démonstration que pour S_n montre qu'un sous-groupe d'indice n de A_n est isomorphe à A_{n-1}. On en déduit $G \simeq \mathrm{A}_5$ (et que f est l'action exotique !).

Une conséquence technique utile de la conjugaison des p-Sylow est le lemme suivant, dont la démonstration est souvent appelée *argument de Frattini*.

LEMME 2.9. (Frattini) *Soient G un groupe fini, N un sous-groupe distingué de G, P un p-Sylow de N et $\mathrm{N}_G(P)$ le normalisateur de P dans G. On a $G = N\,\mathrm{N}_G(P)$.*

DÉMONSTRATION — Soit g dans G. Le p-groupe gPg^{-1} est inclus dans N, car N est distingué dans G. C'est donc encore un p-Sylow de N. Par conjugaison des p-Sylow de N dans N, il existe $n \in N$ tel que $gPg^{-1} = nPn^{-1}$. On en déduit $n^{-1}g \in \mathrm{N}_G(P)$, et donc $g \in n\mathrm{N}_G(P)$. □

3. Le théorème de Schur-Zassenhaus

THÉORÈME 3.1. (Schur-Zassenhaus) *Soient G un groupe fini d'ordre mn avec $m \wedge n = 1$ et possédant un sous-groupe distingué d'ordre n. Alors G possède un sous-groupe d'ordre m.*

Remarquer que si on a $|G| = mn$ comme ci-dessus, avec $N \lhd G$ d'ordre n et $M \leqslant G$ d'ordre m, alors on a $M \cap N = \{1\}$ par Lagrange, et $|G| = |M||N|$. Ainsi, M est un complément de N dans G et on a $G = N \rtimes M$ (produit semi-direct interne). Cela démontre que l'intérêt du théorème de Schur-Zassenhaus dans des questions de dévissage.

EXEMPLE 3.2.
(i) Supposons qu'un groupe fini G possède un p-Sylow P distingué. Le théorème de Schur-Zassenhaus implique que P possède un complément K, puis $G \simeq P \rtimes K$ avec $|K|$ premier à p.
(ii) Soient H un groupe fini et P un p-Sylow de H. Le (i) s'applique à $G = \mathrm{N}_H(P)$ car P est un p-Sylow de G. Ainsi, un p-Sylow admet toujours un complément dans son normalisateur.
(iii) Soient $H = \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ et $P = \mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})$. On peut montrer que le normalisateur de P dans H est le sous-groupe $\mathrm{T}_n(\mathbb{Z}/p\mathbb{Z})$ des matrices triangulaires supérieures dans $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ (Exercice 6.3). On constate que le sous-groupe P admet bien un complément dans G, par exemple le sous-groupe des matrices diagonales, d'ordre $(p-1)^n$, illustrant le (ii).

La démonstration du Théorème 3.1 est assez difficile, et sera découpée en plusieurs étapes. En particulier, il conviendra de traiter à part le cas particulier du théorème dans lequel on suppose en plus que N est abélien, ce que nous ferons au § 5. Nous allons montrer ici que ce cas abélien entraîne le cas général :

LEMME 3.3. *Le cas particulier N abélien du théorème de Schur-Zassenhaus implique le cas général.*

DÉMONSTRATION — Soient G un groupe fini d'ordre mn avec $m \wedge n = 1$, et N un sous-groupe distingué de G d'ordre n. On raisonne par récurrence sur $|G|$. On peut supposer $1 < n$, sans quoi $M = G$ convient.

Soient p un diviseur premier de n et P un p-Sylow de N. On pose $G' = \mathrm{N}_G(P)$ et $N' = N \cap G'$. On a $N' \lhd G'$ et le Lemme de Frattini s'écrit $G = G'N$. Le morphisme de groupes $G' \to G/N, g \mapsto gN$, est donc surjectif. Son noyau est $N \cap G' = N'$, donc on a un isomorphisme naturel

$$G'/N' \xrightarrow{\sim} G/N.$$

Ainsi, N' est d'indice $m = |G'/N'| = |G/N|$ dans G', et d'ordre divisant n (car $N' \subset N$). Ainsi, si on a $G' \neq G$, alors par récurrence sur $|G|$ le groupe G' possède un sous-groupe d'ordre m, ainsi donc que G car on a $G' \leqslant G$.

On peut donc supposer $G' = G$, *i.e.* P distingué dans N. Soit Z le centre du p-groupe P. On a $Z \neq \{1\}$ par la Proposition 1.6. On a Z caractéristique dans P, et P distingué dans G, donc Z est distingué dans G (Exercice 4 Chap. 4.11 (ii)). On considère alors le groupe quotient G/Z. Son sous-groupe N/Z est d'ordre $n/|Z|$ (noter $Z \subset N$) et d'indice $(mn/|Z|)/(n/|Z|) = m$. Par récurrence, G/Z possède un sous-groupe d'ordre m, nécessairement de la forme G''/Z avec G'' un sous-groupe de G contenant Z. Ainsi, on a $|G''| = |Z|m$ avec Z abélien distingué dans G'' et $|Z| \,|\, n$. Par le cas abélien du théorème de Schur-Zassenhaus, G'' possède un sous-groupe d'ordre m, ainsi donc que G. (Noter que l'on peut très bien avoir $Z = P = N$, et donc $G'' = G$, auquel cas on ne peut appliquer l'hypothèse de récurrence.) □

REMARQUE 3.4. On peut raffiner l'énoncé du théorème de Schur-Zassenhaus : Si N est abélien (voire même résoluble), alors les sous-groupes d'ordre m de G sont conjugués dans G : voir l'Exercice 6.36.

4. Les théorèmes de P. Hall

C'est le théorème suivant : [2]

THÉORÈME 4.1. (P. Hall) *Soit G un groupe fini résoluble. On suppose $|G| = mn$ avec $m \wedge n = 1$. Alors G possède un sous-groupe d'ordre m.*

Un sous-groupe H d'un groupe G tel que $|H|$ et $|G|/|H|$ sont premiers entre eux est appelé *sous-groupe de Hall*.

2. P. Hall, *A note on soluble groups*, Journal London Math. Soc. 3 (1928).

REMARQUE 4.2. Le groupe A_5 n'est pas résoluble, et il est d'ordre $60 = 3 \cdot 4 \cdot 5$. Il possède bien des sous-groupes d'ordre 3, 4 et 5 (ses Sylow), ainsi qu'un sous-groupe d'ordre $3 \cdot 4 = 12$ (à savoir A_4). Par contre, il n'a pas de sous-groupe d'ordre 15 ou 20. En effet si H était un tel sous-groupe, l'action par translations de A_5 sur A_5/H (un ensemble à $n \leqslant 4$ éléments) fournirait un morphisme $\mathrm{A}_5 \to \mathrm{S}_n$ d'image transitive (donc non triviale). Un tel morphisme serait injectif car A_5 est simple : absurde car $|\mathrm{S}_n| < 60$ pour $n = 3$ ou 4.

REMARQUE 4.3. Le groupe A_4 est résoluble d'ordre 12. Il possède des sous-groupes cycliques d'ordre $1, 2, 3$, et un sous-groupe d'ordre 4 (à savoir K_4). En revanche, il ne possède pas de sous-groupe d'ordre 6. En fait, A_n n'a jamais de sous-groupe d'indice 2, car il contiendrait le carré (et donc l'inverse) de tout 3 cycle, et donc tous les 3-cycles, alors qu'on a vu que ces derniers engendrent A_n. Cela montre que l'hypothèse $m \wedge n = 1$ est nécessaire, même pour les groupes résolubles.

DÉMONSTRATION — On procède par récurrence sur $|G|$, et on peut supposer $|G| \neq 1$. Comme G est résoluble, il possède un sous-groupe abélien distingué A non trivial. En effet, si r le plus petit entier $\geqslant 1$ tel que $\mathrm{D}^r(G) = 1$, alors $A = \mathrm{D}^{r-1}(G)$ convient (il est même caractéristique). Soit p premier divisant $|A|$. Quitte à remplacer A par son sous-groupe caractéristique

$$A[p] = \{a \in A \mid pa = 0\}$$

(non trivial par Cauchy car p divise $|A|$), on peut supposer que A est un p-groupe abélien distingué non trivial de G. Il y a deux cas :

Cas (a) : p divise m. Dans ce cas, on a $|A|$ divise m. Par récurrence, le groupe (résoluble !) G/A possède donc un sous-groupe d'ordre $m/|A|$. Il est donc de la forme H/A avec $A \subset H$, et on a donc $|H| = |H/A||A| = m$, ce que l'on voulait démontrer.

Cas (b) : p divise n. Dans ce cas, on a $|A|$ premier à m. Par récurrence, le groupe G/A possède un sous-groupe d'ordre m. Il est donc de la forme H/A avec A inclus dans H, et on a donc $|H| = |A|m$. Comme A est distingué dans H, on peut appliquer le théorème de Schur-Zassenhaus (dans le cas "abélien"), qui assure alors que H contient un sous-groupe d'ordre m. □

P. Hall démontre aussi que, sous les hypothèses du théorème ci-dessus, *tous les sous-groupes d'ordre m sont conjugués*. De manière tout aussi intéressante, Hall montre aussi une réciproque au théorème ci-dessus :

THÉORÈME 4.4. (P. Hall) *Soit G un groupe fini d'ordre d. On suppose que pour toute factorisation $d = mn$ avec $m \wedge n = 1$, le groupe G possède un sous-groupe d'ordre m. Alors G est résoluble.*

Par exemple, supposons que l'on a $|G| = p^a q^b$ avec p, q premiers distincts. On sait que G a des sous-groupes d'ordre p^a et q^b, d'après Sylow ! On doit donc pouvoir en déduire que G est résoluble. C'est effectivement le cas, et c'est un théorème dû à Burnside. Sa démonstration utilise la théorie des caractères, et sera reportée à la toute fin du cours. Ce résultat de Burnside est un ingrédient essentiel dans la démonstration du théorème ci-dessus de Hall, dont nous reportons donc aussi la démonstration à plus tard.