

LES GROUPES FINIS SIMPLES D'ORDRE INFÉRIEUR À 660

La théorie des groupes est un domaine complexe dès qu'on s'y frotte franchement, mais la relative facilité des résultats qu'on en présente en Licence ne le laisse pas vraiment entrevoir. Le sommet d'un cours de théorie des groupes en Licence, c'est souvent ce moment où l'on détermine tous les groupes d'ordre inférieur à 12, ou bien ce moment où l'on applique les théorèmes de Sylow pour montrer qu'aucun groupe d'ordre 40, par exemple, n'est simple.

Cette recherche des groupes finis simples est justifiée par un théorème important, le *théorème de Jordan-Hölder* selon lequel tout groupe fini est un empilement de groupes simples. Les outils de théorie des groupes présentés en Licence ne permettent malheureusement de démontrer, à de rares exceptions près, que des propositions de la forme : « Il n'existe pas de groupe simple d'ordre n ». Le malheur est ici double. D'une part, ces propositions ne sont que négatives. D'autre part, elles manquent de généralité, on ne va pas tester un à un tous les entiers.

Il faut pourtant savoir que la classification des groupes finis simples est aujourd'hui achevée. Elle a occupé les théoriciens des groupes finis pendant quelques décennies au 20^{ème} siècle, et il faut bien dire que c'est un monstre — plus de 10 000 pages, plus de 500 articles et plus de 100 auteurs. La « vraie » théorie des groupes finis, c'est ce fossé énorme qui s'est creusé entre les outils simples qu'on présente en Licence et qui remontent tous au 19^{ème} siècle, et les outils d'une complexité inouïe que les mathématiciens ont forgés au 20^{ème} siècle, notamment à partir des années 50. Deux théorèmes au moins méritent qu'on les connaisse si l'on veut comprendre la faiblesse des outils développés dans ce texte.

■ **Théorème (Théorème de Feit-Thompson)** L'ordre d'un groupe fini simple non abélien est pair.

■ **Théorème (Théorème de Burnside)** L'ordre d'un groupe fini simple non abélien est divisible par au moins trois nombres premiers.

Le théorème de Feit-Thompson date de 1963 et faisait suite à un travail inaugural de Suzuki qui prolongeait lui-même une preuve de Frobenius. Sa démonstration initiale, qui ne faisait pas moins de 255 pages, a été l'un des moments les plus marquants de la théorie des groupes finis. Le théorème de Burnside est plus ancien, il date de 1905. On le démontre assez commodément dans le cadre de la théorie des caractères, mais c'est une théorie que nous n'aborderons pas. Au début des années 70, Goldschmidt, Bender et Matsuyama en ont trouvé des preuves indépendantes de la théorie des caractères, mais beaucoup plus difficiles. Quant au théorème de Feit-Thompson, il repose lui aussi en partie sur la théorie des caractères, mais à un niveau de difficulté plutôt décourageant.

Ce texte ne se propose surtout pas de vous présenter l'inouï, je vais tâcher plutôt d'y pousser les techniques de Licence à leur apogée. Il sera donc beaucoup question d'actions de groupes et des théorèmes de Sylow. Nous découvrirons tout de même en cours de route un outil très puissant pas tout à fait élémentaire de la théorie des groupes finis — le *transfert*. À la fin, nous aurons démontré le résultat suivant :

■ **Théorème (Groupes finis simples d'ordre inférieur à 660)** S'il existe un groupe fini simple non abélien d'ordre inférieur à 660, il ne peut avoir pour ordre que l'un des entiers suivants :

60, 168, 360, 504 et 660.

Nous ne le démontrerons pas dans ce texte, mais chacun des 5 entiers retenus dans ce théorème se trouve être réellement l'ordre d'un groupe fini simple non abélien avec unicité à isomorphisme près. On peut montrer en effet que le groupe alterné A_n est simple pour tout $n \geq 5$, et que pour tout $n \geq 2$ et pour toute puissance non triviale q d'un nombre premier avec $(n, q) \neq (2, 2)$ et $(n, q) \neq (2, 3)$, le groupe spécial linéaire $\text{PSL}_n(\mathbb{F}_q)$ est simple. Or il se trouve que :

$$|A_5| = |\text{PSL}_2(\mathbb{F}_4)| = |\text{PSL}_2(\mathbb{F}_5)| = 60, \quad |\text{PSL}_2(\mathbb{F}_7)| = |\text{PSL}_3(\mathbb{F}_2)| = 168, \quad |A_6| = |\text{PSL}_2(\mathbb{F}_9)| = 360, \\ |\text{PSL}_2(\mathbb{F}_8)| = 504 \quad \text{et} \quad |\text{PSL}_2(\mathbb{F}_{11})| = 660.$$

Nous terminerons cette introduction par le rappel de quelques notations.

$ X $	Cardinal de l'ensemble X
$H \leq G$	« H est un sous-groupe du groupe G »
$v_p(n)$	Valuation p -adique de l'entier naturel non nul n pour un nombre premier p
$\text{Syl}_p(G)$	Ensemble des p -Sylow du groupe fini G pour un nombre premier p
$n_p(G)$	Nombre de p -Sylow du groupe fini G pour un nombre premier p
$N_G(H)$	Normalisateur dans le groupe G du sous-groupe H
$C_G(H)$	Centralisateur dans le groupe G du sous-groupe H
$\langle X \rangle$	Sous-groupe engendré par l'ensemble X dans un groupe donné
G/H	Ensemble des classes à droite de G modulo H
$ G : H $	Indice du sous-groupe H dans le groupe G
S_n	Groupe symétrique de $[[1, n]]$
S_X	Groupe symétrique de l'ensemble non vide X
ε	Morphisme signature dans un groupe symétrique
A_n	Groupe alterné de $[[1, n]]$
A_X	Groupe alterné de l'ensemble non vide X
\mathbb{Z}_n	Quotient du groupe \mathbb{Z} par son sous-groupe $n\mathbb{Z}$ pour un entier naturel non nul n
\mathbb{F}_q	Corps fini de cardinal q où q est une puissance non triviale d'un nombre premier
$\text{GL}_n(\mathbb{F}_p)$	Groupe général linéaire de degré n sur \mathbb{F}_p
$\text{Aut}(G)$	Groupe des automorphismes du groupe G
$[x, y]$	Commutateur $x^{-1}y^{-1}xy$ de x et y
$D(G)$	Sous-groupe dérivé du groupe G

Pour quelles valeurs de n entre 1 et 660 peut-il exister un groupe simple d'ordre n ? Nous dirons que l'entier n peut être *éliminé* s'il n'existe pas de groupe simple d'ordre n . Nous avons en tout 654 entiers à tester après exclusion des groupes d'ordre 1, 60, 168, 360, 504 et 660. Le cas des p -groupes est par ailleurs vite traité grâce au théorème suivant, très classique.

■ **Théorème 1 (p -groupes finis simples)** Soit p un nombre premier. Tout p -groupe fini possède un centre non trivial. En particulier, un p -groupe fini est simple si et seulement s'il est d'ordre p .

Ce théorème 1 élimine 142 entiers, dont 120 sont premiers. Nous avons donc en tout 512 entiers en ligne de mire.

■ 1 THÉORÈMES DE SYLOW ET PRINCIPE FACTORIEL

■ 1.1 NON-SIMPLICITÉ PAR APPLICATION DIRECTE DES THÉORÈMES DE SYLOW

À défaut de les démontrer, rappelons au moins l'énoncé des théorèmes de Sylow.

■ **Théorème 2 (Théorèmes de Sylow)** Soient G un groupe fini et p un diviseur premier de $|G|$.

- Le groupe G possède des p -Sylow. Plus précisément : $n_p(G) \equiv 1 [p]$.
- Les p -Sylow de G sont conjugués dans G et pour tout p -Sylow P de G : $n_p(G) = |G : N_G(P)|$. En particulier, $n_p(G)$ divise $|G|$.

Il arrive souvent que 1 soit le seul entier $k \in \mathbb{N}^*$ pour lequel à la fois k divise $|G|$ et $k \equiv 1 [p]$. Dans ce cas, forcément $n_p(G) = 1$, donc G ne possède qu'un seul p -Sylow, forcément distingué. Si G n'est pas un p -groupe, cela montre que G n'est pas simple.

En d'autres termes, un entier non premier n peut être éliminé s'il possède un diviseur premier p pour lequel :

$$\forall k \in \mathbb{N}^*, \quad (k \text{ divise } n \text{ et } k \equiv 1 [p]) \implies k = 1.$$

Ce critère de non-simplicité élimine à lui seul 451 entiers, dont le lecteur intéressé trouvera le détail en annexe. C'est vraiment énorme, mais il nous reste quand même 61 entiers sur les bras : 12, 24, 30, 36, 48, 56, 72, 80, 90, 96, 105, 108, 112, 120, 132, 144, 150, 160, 180, 192, 210, 216, 224, 240, 252, 264, 270, 280, 288, 300, 306, 315, 320, 324, 336, 351, 380, 384, 392, 396, 400, 420, 432, 448, 450, 480, 495, 520, 525, 528, 540, 546, 552, 560, 576, 600, 612, 616, 630, 640 et 648. Ils ne sont déjà plus que 5 à être impairs.

Nous venons d'éliminer en particulier tous les entiers de la forme pq où p et q sont deux nombres premiers distincts. En effet, si $p < q$ par exemple, 1 est le seul diviseur k de n pour lequel $k \equiv 1 [q]$.

1.2 LE PRINCIPE FACTORIEL

Le théorème qui suit montre que les sous-groupes propres d'un groupe fini simple non abélien ne peuvent pas être trop gros. Les anglo-saxons l'appellent parfois le *théorème de l'indice*, nous l'appellerons quant à nous le *principe factoriel* — il s'agit là d'une dénomination personnelle.

Théorème 3 (Principe factoriel) Soient G un groupe fini simple non abélien et H un sous-groupe propre de G . Le groupe G est alors isomorphe à un sous-groupe du groupe alterné $A_{G/H}$. En particulier, $|G|$ divise $|G : H|!$.

Comme H est distinct de G , on peut même dire que $|G|$ divise $\frac{1}{2} |G : H|!$.

Démonstration Notons φ le morphisme de G dans $S_{G/H}$ que nous fournit l'action de G sur l'ensemble G/H des classes à droite de G modulo H . Le noyau de cette action est exactement l'intersection des conjugués de H dans G . C'est un sous-groupe propre de G car H l'est par hypothèse. Il en découle par simplicité de G que $\text{Ker } \varphi = \{1\}$, donc φ est injectif.

Intéressons-nous alors au morphisme $\varepsilon \circ \varphi$ de G dans $\{-1, 1\}$ obtenu à partir de φ par composition par la signature de $S_{G/H}$. Si $\varepsilon \circ \varphi$ pouvait prendre la valeur -1 , G posséderait un sous-groupe distingué d'indice 2 et ne serait pas simple non abélien. Conclusion : le morphisme $\varepsilon \circ \varphi$ est trivial. Comme voulu, φ plonge donc G dans $A_{G/H}$. En particulier, $|G|$ divise $|S_{G/H}| = |G : H|!$. ■

En termes d'action de groupe, le principe factoriel signifie qu'un groupe fini simple non abélien ne peut pas agir sur des ensembles de trop petite taille, si ce n'est trivialement. Pour un tel groupe G opérant non trivialement sur un ensemble X , toute orbite non ponctuelle d'un élément x de X de stabilisateur G_x a en effet pour cardinal $|G : G_x|$. D'après le principe factoriel, $|G|$ divise donc $|G : G_x|!$, donc aussi $|X|!$, ce qui empêche X d'être trop petit.

Le cas particulier suivant du principe factoriel complète utilement les théorèmes de Sylow.

Théorème 4 (Principe factoriel et p -Sylow) Soient G un groupe fini simple non abélien et p diviseur premier de $|G|$.

- L'entier $|G|$ divise alors $n_p(G)!$.
- L'action par conjugaison de G sur l'ensemble $\text{Syl}_p(G)$ de ses p -Sylow induit par ailleurs un morphisme injectif de G dans $A_{\text{Syl}_p(G)}$.

De nouveau, on peut préciser en fait que $|G|$ divise $\frac{1}{2} n_p(G)!$.

Démonstration Soit P un p -Sylow de G . Comme G est simple non abélien, $N_G(P)$ est un sous-groupe propre de G , donc $|G|$ divise $|G : N_G(P)|!$ d'après le principe factoriel, lequel coïncide avec $n_p(G)!$ d'après les théorèmes de Sylow.

Le deuxième point du théorème n'est qu'une adaptation de la preuve du principe factoriel à l'action par conjugaison de G sur $\text{Syl}_p(G)$. ■

Au paragraphe précédent, nous pouvions éliminer un entier non premier n quand il possédait un diviseur premier p pour lequel : $\forall k \in \mathbb{N}^*, (k \text{ divise } n \text{ et } k \equiv 1 [p]) \implies k = 1$. Ce critère efficace n'en était pas moins exigeant. Il échoue pour $n = 12$ par exemple. Pour un groupe G d'ordre 12, en effet, les théorèmes de Sylow permettent à $n_2(G)$ de valoir 1 ou 3 et à $n_3(G)$ de valoir 1 ou 4. En revanche, $|G| = 12$ ne divise pas $3! = 6$, donc d'après le théorème précédent, G n'est pas simple. En d'autres termes, nous venons d'affaiblir la condition suffisante de non-simplicité du paragraphe précédent. Un entier non premier n peut être éliminé s'il possède un diviseur premier p pour lequel :

$$\forall k \in \mathbb{N}^*, (k \text{ divise } n \text{ et } k \equiv 1 [p]) \implies n \text{ ne divise pas } k!$$

Sur les 61 entiers que nous avons encore à étudier, ce nouveau critère en élimine 24. De nouveau, le lecteur intéressé trouvera plus de détails sur cette élimination en annexe. Il nous reste 37 entiers à étudier : 30, 56, 90, 105, 112, 120, 132, 144, 180, 210, 240, 252, 264, 280, 288, 306, 315, 336, 351, 380, 396, 400, 420, 432, 480, 495, 520, 525, 528, 540, 546, 552, 560, 576, 612, 616 et 630.

On peut en réalité éliminer aussi 112 grâce au principe factoriel. Pour un groupe G d'ordre $112 = 2^4 \cdot 7$, les théorèmes de Sylow n'autorisent en effet $n_7(G)$ qu'à valoir 1 ou 7, or il se trouve que 112 ne divise pas $\frac{1}{2} \times 7! = 2^3 \cdot 3^2 \cdot 5 \cdot 7$ — alors qu'il divise $7!$. L'amélioration d'un facteur $\frac{1}{2}$ du principe factoriel dont nous venons de tirer profit n'élimine malheureusement aucun autre entier.

1.3 UN RAFFINEMENT PAR DÉNOMBREMENT

Pour un groupe G d'ordre 30, les théorèmes de Sylow permettent à $n_2(G)$ de valoir 1, 3, 5 ou 15, à $n_3(G)$ de valoir 1 ou 10 et à $n_5(G)$ de valoir 1 ou 6. Si on suppose de plus que G est simple, le principe factoriel autorise $n_2(G)$ à valoir seulement 5 ou 15 et impose les égalités $n_3(G) = 10$ et $n_5(G) = 6$. Ce n'est pas suffisant pour conclure.

Pour aller plus loin, remarquons à présent que les 5-Sylow de G sont d'ordre premier, donc deux à deux d'intersection triviale. Comme chacun d'entre eux contient $5 - 1 = 4$ éléments d'ordre 5, G contient exactement $(5 - 1)n_5(G) = 4 \times 6 = 24$ éléments d'ordre 5. Un raisonnement analogue montre que G contient $(3 - 1)n_3(G) = 2 \times 10 = 20$ éléments d'ordre 3 et au moins $(2 - 1) \times 5 = 5$ involutions. En comptant l'élément neutre, nous venons de dénicher $1 + 5 + 20 + 24 = 50$ éléments dans G — c'est beaucoup trop ! La simplicité de G nous a conduit à une contradiction et l'entier 30 se trouve éliminé.

Donnons-nous à présent un entier naturel non nul n et faisons l'hypothèse qu'il existe un groupe simple G d'ordre n . L'entier n a deux sortes de diviseurs premiers p , ceux pour lesquels $v_p(n) = 1$ et ceux pour lesquels $v_p(n) \geq 2$.

- Commençons par un diviseur premier p de n pour lequel $v_p(n) = 1$. Les p -Sylow de G sont d'ordre p , donc deux à deux d'intersection triviale. Le groupe G contient ainsi $(p - 1)n_p(G)$ éléments d'ordre p . Or les théorèmes de Sylow et le principe factoriel ne permettent pas à $n_p(G)$ d'avoir n'importe quelle valeur. Si nous notons $\min_p(n)$ la plus petite valeur de $n_p(G)$ qu'ils autorisent, le groupe G contient au moins $(p - 1) \min_p(n)$ éléments d'ordre p .
- Donnons-nous à présent un diviseur premier p de n pour lequel $v_p(n) \geq 2$. Il est plus difficile d'évaluer le nombre de p -éléments de G car ses p -Sylow peuvent avoir des intersections diverses. Chacun d'entre eux contient en tout cas $p^{v_p(n)} - 1$ éléments non triviaux, et comme ils sont plusieurs par simplicité de G , G contient au moins $p^{v_p(n)}$ p -éléments non triviaux. On pourrait améliorer cette estimation, mais cela n'éliminerait pas davantage d'entiers entre 1 et 660.

Au total, nous avons déniché avec l'élément neutre : $1 + \sum_{v_p(n)=1} (p - 1) \min_p(n) + \sum_{v_p(n) \geq 2} p^{v_p(n)}$ éléments dans G . La simplicité de G conduit dès lors à une contradiction si cette quantité s'avère strictement supérieure à $|G| = n$.

En d'autres termes, un entier n peut être éliminé avec ce procédé de dénombrement si :

$$1 + \sum_{v_p(n)=1} (p - 1) \min_p(n) + \sum_{v_p(n) \geq 2} p^{v_p(n)} > n,$$

où pour tout diviseur premier p de n , $\min_p(n)$ est le plus petit diviseur k de n pour lequel $k \equiv 1 [p]$ et n divise $k!$.

Sur les 36 entiers qu'il nous reste à tester, ce nouveau critère en élimine 13, à savoir : 30, 56, 105, 132, 280, 306, 351, 380, 495, 520, 546, 552 et 616. Ils ne sont finalement plus que 23 à nous résister : 90, 120, 144, 180, 210, 240, 252, 264, 288, 315, 336, 396, 400, 420, 432, 480, 525, 528, 540, 560, 576, 612 et 630, dont seulement 2 à être impairs.

Nous venons d'éliminer en particulier tous les entiers de la forme p^2q ou pqr où p, q et r sont des nombres premiers distincts.

- Si $n = p^2q$ avec $p < q$, c'est facile, 1 est le seul diviseur k de n pour lequel $k \equiv 1 [p]$.

— Si $n = p^2q$ avec $p > q$, il se trouve que $\min_q(n) \geq p^2$. On peut ainsi éliminer n car :

$$1 + (q - 1) \min_q(n) + p^2 \geq 1 + (q - 1)p^2 + p^2 = p^2q + 1 > p^2q = n.$$

— Enfin, si $n = pqr$ avec $p < q < r$, alors : $\min_p(n) \geq q$, $\min_q(n) \geq r$ et $\min_r(n) \geq pq$. On peut ainsi éliminer n car :

$$1 + (p - 1) \min_p(n) + (q - 1) \min_q(n) + (r - 1) \min_r(n) \geq 1 + (p - 1)q + (q - 1)r + (r - 1)pq = pqr + (q - 1)(r - 1) > pqr = n.$$

1.4 ET SI UN GROUPE FINI CONTIENT EXACTEMENT $p + 1$ p -SYLOW ?

D'après les théorèmes de Sylow, $n_p(G) \equiv 1 [p]$ pour tout groupe fini G et pour tout diviseur premier p de $|G|$. Dans le cas où G est simple non abélien, à défaut de pouvoir prendre la valeur 1, $n_p(G)$ peut prendre les valeurs $p + 1, 2p + 1, 3p + 1$, etc. Ce paragraphe est entièrement dévolu au cas $p + 1$.

Théorème 5 (Normalisateurs d'un p -Sylow de A_{p+1}) Soit p un nombre premier impair. Les p -Sylow de A_{p+1} sont d'ordre p et leurs normalisateurs d'ordre $\frac{p(p-1)}{2}$.

Démonstration Les p -Sylow de S_{p+1} sont d'ordre p car p^2 ne divise pas $(p + 1)!$, et comme p est impair, c'est aussi le cas des p -Sylow de A_{p+1} . À l'élément neutre près, leur réunion est exactement l'ensemble des éléments d'ordre p de A_{p+1} , en l'occurrence ici des p -cycles, en nombre $(p - 1)n_p(A_{p+1})$.

Il n'est pas difficile de calculer indépendamment le nombre de p -cycles de A_{p+1} . Construire un tel p -cycle revient à choisir d'abord un p -arrangement de $\llbracket 1, p + 1 \rrbracket$, mais on compte ainsi p fois chaque p -cycle car un p -cycle est sans commencement. Le groupe A_{p+1} contient ainsi exactement $\frac{(p + 1)!}{p}$ p -cycles.

Ainsi, par double comptage : $(p - 1)n_p(A_{p+1}) = \frac{(p + 1)!}{p}$, donc les normalisateurs de p -Sylow de A_{p+1} sont d'ordre $\frac{|A_{p+1}|}{n_p(A_{p+1})} = \frac{\frac{(p + 1)!}{2}}{\frac{(p + 1)!}{p(p - 1)}} = \frac{p(p - 1)}{2}$.

Théorème 6 (Groupes simples pour lesquels $n_p(G) = p + 1$) Soient G un groupe fini simple non abélien et p un diviseur premier de $|G|$. Si $n_p(G) = p + 1$, $|G|$ divise $\frac{(p - 1)p(p + 1)}{2}$.

Démonstration D'après le principe factoriel, l'action par conjugaison de G sur l'ensemble $\text{Syl}_p(G)$ de ses p -Sylow identifie G à un sous-groupe de $A_{\text{Syl}_p(G)}$, et même par hypothèse à un sous-groupe de A_{p+1} , et comme G n'est pas abélien, p est impair. Donnons-nous alors un p -Sylow P de G . D'après le théorème 5, P est aussi un p -Sylow de A_{p+1} et $|N_{A_{p+1}}(P)| = \frac{p(p-1)}{2}$. L'entier $|N_G(P)|$ divise a fortiori $\frac{p(p-1)}{2}$, et comme $n_p(G) = |G : N_G(P)|$ d'après les théorèmes de Sylow, $|G|$ divise $\frac{p(p-1)}{2} \times n_p(G) = \frac{(p-1)p(p+1)}{2}$.

Donnons-nous à présent un entier naturel non nul n et faisons l'hypothèse qu'il existe un groupe simple d'ordre n . Faisons en outre l'hypothèse que pour un certain diviseur premier p de n , $p + 1$ soit la seule valeur de $n_p(G)$ permises par les théorèmes de Sylow et le principe factoriel. Le théorème 6 montre alors que n divise $\frac{(p - 1)p(p + 1)}{2}$. Si jamais ce n'est pas le cas, l'entier n peut être éliminé.

Sur les 23 entiers que nous avons encore à tester, ce raisonnement en élimine 7 : 90 et 120 pour $p = 5$, 336 et 560 pour $p = 7$ et 264, 396 et 528 pour $p = 11$. Les 16 entiers restants sont : 144, 180, 210, 240, 252, 288, 315, 400, 420, 432, 480, 525, 540, 576, 612 et 630.

2 NON SIMPLICITÉ DES GROUPES D'ORDRE $2^\alpha p^\beta$ POUR $\alpha \leq 5$

D'après le théorème de Burnside, l'ordre d'un groupe fini simple non abélien est divisible par au moins trois nombres premiers distincts, mais ce théorème ne fait pas partie de nos bagages. Nous allons éliminer 5 nouveaux entiers dans cette partie sur les 16 qui nous restent sur les bras, en l'occurrence ceux qui possèdent exactement deux diviseurs premiers : 144, 288, 400, 432 et 576, tous de la forme $2^\alpha p^\beta$ avec $\alpha \in \{4, 5, 6\}$ et $p \in \{3, 5, 7\}$. Nous éliminerons en passant un autre entier, l'entier 480. Si les techniques utilisées ne dépassent pas le cadre des actions de groupes et des théorèmes de Sylow, les raisonnements proposés sont plus délicats que ceux de la partie précédente.

2.1 QUELQUES OUTILS

Théorème 7 (À propos de l'indice $|\mathrm{N}_G(H) : \mathrm{C}_G(H)|$) Soient G un groupe fini et H un sous-groupe de G . L'indice $|\mathrm{N}_G(H) : \mathrm{C}_G(H)|$ divise $|\mathrm{Aut}(H)|$.

Démonstration L'action par conjugaison de $\mathrm{N}_G(H)$ sur H nous fournit, après quotient par son noyau $\mathrm{C}_G(H)$, un morphisme injectif de $\frac{\mathrm{N}_G(H)}{\mathrm{C}_G(H)}$ dans $\mathrm{Aut}(H)$. En particulier, $|\mathrm{N}_G(H) : \mathrm{C}_G(H)|$ divise $|\mathrm{Aut}(H)|$. ■

Théorème 8 (Normalisateurs dans un p -groupe fini) Soient p un nombre premier, G un p -groupe fini et H un sous-groupe propre de G . Alors $|\mathrm{N}_G(H)| > |H|$.

Démonstration On s'intéresse à l'action par translation de H sur G/H . Les orbites non ponctuelles de cette action sont nécessairement de cardinal divisible par p . D'après l'équation aux classes, le nombre d'orbites ponctuelles est dès lors congru à $|G : H|$ modulo p , donc est divisible par p puisque H est propre dans G .

Or que sont précisément les orbites ponctuelles ? Pour tout $x \in G$, l'orbite de Hx est ponctuelle si et seulement si $Hxh = Hx$ pour tout $h \in H$, i.e. $x^{-1}Hx = H$, ou encore $x \in \mathrm{N}_G(H)$. L'action étudiée possède ainsi $|\mathrm{N}_G(H) : H|$ orbites ponctuelles. Conclusion : $|\mathrm{N}_G(H) : H|$ est divisible par p , donc $|\mathrm{N}_G(H)| > |H|$. ■

Théorème 9 (Intersection maximale de deux p -Sylow) Soient G un groupe fini et p un diviseur premier de $|G|$.

- Si $n_p(G) \not\equiv 1 \pmod{p^2}$, G possède deux p -Sylow P et P' pour lesquels $|P : P \cap P'| = p$.
- Par ailleurs, si G possède deux p -Sylow P et P' pour lesquels $|P : P \cap P'| = p$, alors $|\mathrm{N}_G(P \cap P')| = m|P|$ avec $m > p$.

Démonstration

- Faisons l'hypothèse que $n_p(G) \not\equiv 1 \pmod{p^2}$ et donnons-nous un p -Sylow P de G . Ce sous-groupe P agit par conjugaison sur l'ensemble des p -Sylow de G distincts de P , de cardinal $n_p(G) - 1 \not\equiv 0 \pmod{p^2}$. Cette action possède forcément une orbite de cardinal non divisible par p^2 , dont nous considérons un membre P' . Comme $P' \neq P : \mathrm{N}_p(P') \neq P$. L'orbite de P' est ainsi non ponctuelle et son cardinal est forcément p . Ensuite : $P \cap P' \leq \mathrm{N}_p(P')$, donc $|P : P \cap P'|$ est divisible par p sans être égal à 1. Comme voulu : $|P : P \cap P'| = p$.
- Faisons désormais l'hypothèse que G possède deux p -Sylow P et P' pour lesquels $|P : P \cap P'| = p$. On a donc aussi $|P' : P \cap P'| = p$. D'après le théorème 8 : $\mathrm{N}_p(P \cap P') = P$ et $\mathrm{N}_{p'}(P \cap P') = P'$, donc $|\mathrm{N}_G(P \cap P')| = m|P|$ pour un certain $m \in \mathbb{N}^*$ premier à p . Mais cela montre aussi que $\mathrm{N}_G(P \cap P')$ contient l'ensemble $PP' = \{xx' \mid x \in P \text{ et } x' \in P'\}$. Or on montre aisément grâce au lemme des bergers, en étudiant l'application $(x, x') \mapsto xx'$ de $P \times P'$ dans PP' , que $|PP'| = \frac{|P| \cdot |P'|}{|P \cap P'|} = p|P|$. Il en découle que $m|P| = |\mathrm{N}_G(P \cap P')| \geq |PP'| = p|P|$, puis que $m \geq p$, et même $m > p$ puisque m et p sont premiers entre eux. ■

Voyons à présent de quelle manière le théorème 9 élimine l'entier $480 = 2^5 \cdot 3 \cdot 5$. Supposons par l'absurde qu'il existe un groupe simple G d'ordre 480. D'après les théorèmes de Sylow et le principe factoriel : $n_2(G) = 15$. En particulier : $n_2(G) \not\equiv 1 \pmod{4}$, donc d'après le théorème 9, G possède deux 2-Sylow S et S' pour lesquels, en notant I le sous-groupe

$S \cap S' : |I| = 16$ et $|N_G(I)| = 32m$ avec $m > 2$. Ainsi $|N_G(I)| \geq 3 \times 32 = 96$, donc $|G : N_G(I)| \leq 5$, ce que contredit le principe factoriel car $5! = 120$ n'est pas divisible par 480.

2.2 ÉLIMINATION DES ENTIERS 288 ET 576

Nous allons éliminer ensemble les entiers $288 = 2^5 \cdot 3^2$ et $576 = 2^6 \cdot 3^2$. Les entiers 144, 400 et 432 seront éliminés au paragraphe suivant.

Supposons donc par l'absurde qu'il existe un groupe simple G d'ordre 288 ou 576.

- Si $|G| = 288$, les théorèmes de Sylow et le principe factoriel montrent que $n_3(G) = 16 \not\equiv 1 [9]$. D'après le théorème 9, G possède donc deux 3-Sylow distincts d'intersection non triviale.
- Si $|G| = 576$, faisons l'hypothèse que les 3-Sylow de G sont deux à deux d'intersection triviale. Il en découle d'une part grâce au théorème 9 que $n_3(G) \equiv 1 [9]$, et d'autre part que le groupe G contient donc $(9 - 1)n_3(G)$ 3-éléments non triviaux. Or par simplicité, G contient plusieurs 2-Sylow pour un total d'au moins 65 éléments. Dans ces conditions : $8n_3(G) + 65 \leq 576$, donc $n_3(G) < 64$. Pourtant, les théorèmes de Sylow et le principe factoriel montrent que $n_3(G) \in \{16, 64\}$. Conclusion : $n_3(G) = 16 \not\equiv 1 [9]$ — contradiction.
- Dans les deux cas traités, nous pouvons finalement nous donner deux 3-Sylow T et T' pour lesquels $T \cap T' \neq \{1\}$. Si nous notons I le sous-groupe $T \cap T'$, le théorème 9 montre que $|I| = 3$ et $|N_G(I)| = 9m$ avec $m > 3$. L'entier m étant ici forcément une puissance de 2, $|N_G(I)|$ est divisible par 36. Or par ailleurs, $|N_G(I) : C_G(I)|$ divise $|\text{Aut}(I)|$ d'après le théorème 7, avec $|\text{Aut}(I)| = |\text{Aut}(\mathbb{Z}_3)| = 2$ car I est cyclique d'ordre 3. Il en découle que $|C_G(I)|$ est divisible par 18. En particulier, $C_G(I)$ contient un élément c d'ordre 6.

Intéressons-nous pour finir à l'action par conjugaison de G sur l'ensemble $\text{Syl}_2(G)$ de ses 2-Sylow. Cette action nous fournit d'après le principe factoriel un morphisme injectif φ de G dans $A_{\text{Syl}_2(G)}$, lequel est isomorphe à A_9 car $n_2(G) = 9$ d'après les théorèmes de Sylow et le principe factoriel. Que pouvons-nous dire alors de la permutation $\varphi(c)$?

- L'égalité $n_2(G) = 9$ montre que $N_G(S)$ est un 2-groupe pour tout 2-Sylow S de G . D'ordre 6, c ne normalise donc pas S , ce qu'on reformuler en disant que la permutation $\varphi(c)$ n'a pas de point fixe.
- Pour tout $k \in \{2, 3, 6\}$, notons c_k le nombre de k -cycles disjoints qui composent $\varphi(c)$. D'après le point précédent et sachant $\varphi(c)$ est d'ordre 6 : $2c_2 + 3c_3 + 6c_6 = 9$.
- Élément de $A_{\text{Syl}_2(G)}$, la permutation $\varphi(c)$ est paire, donc l'entier $c_2 + c_6$ est pair.

Il reste à vérifier qu'une telle décomposition de 9 est impossible. Or si $c_6 \geq 1$, alors $c_2 = 0$ et $c_3 = c_6 = 1$, donc $c_2 + c_6$ est impair. Conclusion : $c_6 = 0$, donc c_2 vaut 2 ou 4, ce que ne permet aucune valeur entière de c_3 .

2.3 NON-SIMPLICITÉ DES GROUPES D'ORDRE $2^\alpha p^\beta$ POUR $\alpha \leq 5$

Le théorème qui suit élimine les 3 entiers 144, 400 et 432, mais sa portée, de toute évidence, est plus générale.

■ **Théorème 10 (Non-simplicité des groupes d'ordre $2^\alpha p^\beta$ avec $\alpha \leq 5$)** Soient p un nombre premier impair et α et β deux entiers naturels non nuls avec $\alpha \leq 5$. Il n'existe pas de groupe simple d'ordre $2^\alpha p^\beta$.

Démonstration Supposons par l'absurde qu'il existe un groupe simple G d'ordre $2^\alpha p^\beta$.

- D'après le principe factoriel, sachant qu'il n'existe pas de groupe simple d'ordre inférieur à $24 = 4!$: $n_p(G) \geq 5$. Avec les théorèmes de Sylow, du coup $n_p(G) \in \{8, 16, 32\}$, avec $p = 7$ si $n_p(G) = 8$, $p \in \{3, 5\}$ si $n_p(G) = 16$, et enfin $p = 31$ si $n_p(G) = 32$.
- Dans tous les cas : $n_p(G) \not\equiv 1 [p^2]$. D'après le théorème 9, nous pouvons donc nous donner deux p -Sylow P et P' pour lesquels, en notant I le sous-groupe $P \cap P'$: $|I| = p^{\beta-1}$ et $|N_G(I)| = 2^\gamma p^\beta$ avec $2^\gamma \geq p$. Or $|G|$ divise $|G : N_G(I)|! = 2^{\alpha-\gamma}!$ d'après le principe factoriel, donc $2^{\alpha-\gamma} \geq 5$, puis $\alpha - \gamma \geq 3$. En retour : $p \leq 2^\gamma \leq 2^{\alpha-3} \leq 4$, donc $p = 3$. L'inégalité $2^\gamma \geq p = 3$ montre alors que $\gamma \geq 2$, et comme $\gamma + 3 \leq \alpha \leq 5$, finalement $\alpha = 5$ et $\gamma = 2$. Le fait que $|G|$ divise $|G : N_G(I)|! = 2^{\alpha-\gamma}! = 8! = 2^7 \cdot 3^2 \cdot 5 \cdot 7$ nous permet d'avancer : $\beta \leq 2$, et comme nous savons déjà qu'il n'existe pas de groupe simple d'ordre 96, forcément $\beta = 2$. Conclusion : $|G| = 2^5 \cdot 3^2 = 288$ — entier que nous avons déjà éliminé. ■

3 UNE INTRODUCTION AU TRANSFERT

Au point où nous en sommes, 10 entiers résistent encore, à savoir : 180, 210, 240, 252, 315, 420, 525, 540, 612 et 630.

3.1 DÉFINITION DU TRANSFERT

Nous partons dans ce paragraphe d'un groupe fini G et d'un sous-groupe H de G . Nous allons construire un morphisme de G dans le groupe abélien $\frac{H}{D(H)}$ qu'on appelle le *transfert de G dans H* . Ce morphisme est un outil fondamental de la théorie des groupes finis, mais nous n'en exploiterons pas toutes les possibilités. Rappelons simplement à ce stade que dans le cas où G est simple non abélien, un morphisme de G dans $\frac{H}{D(H)}$ est forcément trivial.

Le groupe G opère par translation sur l'ensemble G/H de ses classes à droite modulo H . Donnons-nous alors une transversale à droite quelconque θ de H dans G , autrement dit, pour toute classe $\alpha \in G/H$, un élément α^θ de α . L'ensemble $\{\alpha^\theta \mid \alpha \in G/H\}$ est aussi ce qu'on appelle souvent un ensemble de représentants des classes à droite de G modulo H . Pour tout $\alpha \in G/H$: $\alpha = H\alpha^\theta$.

Remarquons à présent que l'action de G sur G/H ne nous fournit aucune action de G sur l'ensemble des représentants $\{\alpha^\theta \mid \alpha \in G/H\}$. Pour tous $g \in G$ et $\alpha \in G/H$, en effet, alors que le produit $\alpha^\theta g$ appartient à la classe αg , rien ne nous dit qu'il coïncide avec le représentant $(\alpha g)^\theta$. Ce n'est pas le cas en général. Quoi qu'il en soit, l'égalité $H\alpha^\theta g = \alpha g = H(\alpha g)^\theta$ montre que le produit $\alpha^\theta g ((\alpha g)^\theta)^{-1}$ appartient à H . Si nous notons $h_\theta(\alpha, g)$ ce produit, alors :

$$\alpha^\theta g = h_\theta(\alpha, g)(\alpha g)^\theta,$$

relation que nous noterons ♠. On comprend sur cette relation le sens de la fonction h_θ . Cette fonction mesure l'écart qui sépare $\alpha^\theta g$ de $(\alpha g)^\theta$.

L'associativité du produit dans G donne à h_θ une propriété fonctionnelle bien particulière. Pour tous $g, g' \in G$ et $\alpha \in G/H$, en effet : $h_\theta(\alpha, gg')(\alpha gg')^\theta \stackrel{\spadesuit}{=} \alpha^\theta gg' \stackrel{\spadesuit}{=} h_\theta(\alpha, g)(\alpha g)^\theta g' \stackrel{\spadesuit}{=} h_\theta(\alpha, g)h_\theta(\alpha g, g')(\alpha gg')^\theta$. Finalement :

$$h_\theta(\alpha, gg') = h_\theta(\alpha, g)h_\theta(\alpha g, g'),$$

relation que nous noterons ♣. Cette identité n'est pas loin de faire de h_θ un morphisme de groupes par rapport à sa première variable, mais la deuxième variable fait obstacle. Pour la faire disparaître, l'idéal serait qu'on puisse écrire un produit de ce genre :

$$\prod_{\alpha \in G/H} h_\theta(\alpha, gg') = \prod_{\alpha \in G/H} h_\theta(\alpha, g) \prod_{\alpha \in G/H} h_\theta(\alpha g, g'),$$

qui deviendrait après changement d'indice : $\prod_{\alpha \in G/H} h_\theta(\alpha, gg') = \prod_{\alpha \in G/H} h_\theta(\alpha, g) \prod_{\alpha \in G/H} h_\theta(\alpha, g')$. La fonction $g \mapsto \prod_{\alpha \in G/H} h_\theta(\alpha, g)$ serait ainsi un morphisme de groupes de G dans H .

Le problème des calculs qui précèdent, c'est que le groupe H n'est pas commutatif. Or nous avons utilisé la commutativité du produit à deux endroits ci-dessus :

- une première fois avec la notation $\prod_{\alpha \in G/H}$ qui requiert un ordre d'énumération,
- une deuxième fois avec la règle implicite $\prod_{\alpha \in G/H} (x_\alpha y_\alpha) = \prod_{\alpha \in G/H} x_\alpha \prod_{\alpha \in G/H} y_\alpha$.

Finalement, il suffirait qu'on travaille dans le groupe abélien $\frac{H}{D(H)}$ et tout irait bien. Le *transfert de G dans H* est par définition l'application $g \mapsto \prod_{\alpha \in G/H} h_\theta(\alpha, g)$ de G dans $\frac{H}{D(H)}$, où le symbole \prod désigne un produit d'éléments de H calculé dans $\frac{H}{D(H)}$. Cette application $V_{G \rightarrow H}$ est comme annoncé un morphisme de groupes car pour tous $g, g' \in G$:

$$\begin{aligned} V_{G \rightarrow H}(gg') &= \prod_{\alpha \in G/H} h_\theta(\alpha, gg') \stackrel{\spadesuit}{=} \prod_{\alpha \in G/H} (h_\theta(\alpha, g)h_\theta(\alpha g, g')) = \prod_{\alpha \in G/H} h_\theta(\alpha, g) \prod_{\alpha \in G/H} h_\theta(\alpha g, g') \stackrel{\spadesuit}{=} \prod_{\alpha \in G/H} h_\theta(\alpha, g) \prod_{\alpha \in G/H} h_\theta(\alpha', g') \\ &= V_{G \rightarrow H}(g)V_{G \rightarrow H}(g'). \end{aligned}$$

Alors que $h_\theta(\alpha, g)$ mesure l'écart qui sépare $\alpha^\theta g$ de $(\alpha g)^\theta$, $V_{G \rightarrow H}(g)$ est en résumé la « somme » de ces écarts et mesure une sorte d'écart total qui sépare l'ensemble de représentants $\{\alpha^\theta \mid \alpha \in G/H\}$ de son produit $\{\alpha^\theta g \mid \alpha \in G/H\}$ par g .

Le transfert de G dans H semble d'ailleurs dépendre tout à fait de la transversale θ qu'on a choisie pour le définir. Ce n'est pourtant pas le cas. Donnons-nous en effet une transversale θ' de H dans G et notons $V'_{G \rightarrow H}$ le transfert de G dans H associé. Pour tout $\alpha \in G/H$: $H\alpha^{\theta'} = \alpha = H\alpha^\theta$, donc $\alpha^{\theta'} = \eta_\alpha \alpha^\theta$ pour un certain $\eta_\alpha \in H$. Les transferts $V_{G \rightarrow H}$ et $V'_{G \rightarrow H}$ coïncident car pour tout $g \in G$:

$$\begin{aligned} V'_{G \rightarrow H}(g) &= \prod_{\alpha \in G/H} h_{\theta'}(\alpha, g) = \prod_{\alpha \in G/H} \alpha^{\theta'} g ((\alpha g)^{\theta'})^{-1} = \prod_{\alpha \in G/H} \eta_\alpha \alpha^\theta g ((\alpha g)^\theta)^{-1} \eta_{\alpha g}^{-1} = \left(\prod_{\alpha \in G/H} \eta_\alpha \right) \prod_{\alpha \in G/H} h_\theta(g, \alpha) \left(\prod_{\alpha \in G/H} \eta_{\alpha g} \right)^{-1} \\ &\stackrel{\alpha' \equiv \alpha g}{=} \left(\prod_{\alpha \in G/H} \eta_\alpha \right) V_{G \rightarrow H}(g) \left(\prod_{\alpha' \in G/H} \eta_{\alpha'} \right)^{-1} = V_{G \rightarrow H}(g). \end{aligned}$$

L'énoncé suivant résume notre construction du transfert.

■ **Définition-théorème 11 (Transfert dans un sous-groupe)** Soient G un groupe fini et H un sous-groupe de G . Le symbole \prod désigne ci-dessous un produit d'éléments de H calculé dans $\frac{H}{D(H)}$.

- Pour tout $g \in G$ et pour toute transversale à droite θ de H dans G , l'élément $\prod_{\alpha \in G/H} \alpha^\theta g ((\alpha g)^\theta)^{-1}$ de $\frac{H}{D(H)}$ ne dépend pas de θ . On le note $V_{G \rightarrow H}(g)$.
- L'application $V_{G \rightarrow H}$ est un morphisme de groupes de G dans $\frac{H}{D(H)}$.

Cette définition ne brille pas par son évidence calculatoire. Nous venons de construire une foule de morphismes, mais est-il possible de les calculer concrètement? Le résultat qui suit montre que oui. S'il demeure obscur au premier abord, c'est vraiment grâce à lui que le transfert est toujours calculé.

■ **Théorème 12 (Calcul du transfert)** Soient G un groupe fini, H un sous-groupe de G et $g \in G$. L'action de $\langle g \rangle$ sur G/H possède un certain nombre r d'orbites dont on se donne des représentants $Hx_1^{-1}, \dots, Hx_r^{-1}$ avec $x_1, \dots, x_r \in G$. Pour tout $i \in \llbracket 1, r \rrbracket$, le cardinal de la $\langle g \rangle$ -orbite de Hx_i^{-1} est noté n_i . En particulier : $|G : H| = \sum_{1 \leq i \leq r} n_i$. Avec ces notations : $x_i^{-1} g^{n_i} x_i \in H$ pour tout $i \in \llbracket 1, r \rrbracket$ et $V_{G \rightarrow H}(g) = \prod_{1 \leq i \leq r} x_i^{-1} g^{n_i} x_i$.

Démonstration Les éléments de G/H sont exactement les ensembles $Hx_i^{-1} g^j$, i décrivant $\llbracket 1, r \rrbracket$ et j décrivant $\llbracket 0, n_i - 1 \rrbracket$. Le transfert ne dépendant pas de la transversale choisie pour le définir, nous allons calculer $V_{G \rightarrow H}(g)$ grâce à la transversale θ définie pour tous i et j par : $(Hx_i^{-1} g^j)^\theta = x_i^{-1} g^j$.

Remarquons tout d'abord que pour tout $i \in \llbracket 1, r \rrbracket$, par définition de n_i : $Hx_i^{-1} g^{n_i} = Hx_i^{-1}$, autrement dit $x_i^{-1} g^{n_i} x_i \in H$. À présent, pour tous $i \in \llbracket 1, r \rrbracket$ et $j \in \llbracket 0, n_i - 1 \rrbracket$, la contribution de $Hx_i^{-1} g^j$ au produit qui définit $V_{G \rightarrow H}(g)$ vaut dans H :

$$(Hx_i^{-1} g^j)^\theta g ((Hx_i^{-1} g^{j+1})^\theta)^{-1} = \begin{cases} (Hx_i^{-1} g^{n_i-1})^\theta g ((Hx_i^{-1} g^{n_i})^\theta)^{-1} = (x_i^{-1} g^{n_i-1}) g ((Hx_i^{-1})^\theta)^{-1} = x_i^{-1} g^{n_i} x_i & \text{si } j = n_i - 1 \\ (x_i^{-1} g^j) g (x_i^{-1} g^{j+1})^{-1} = 1 & \text{sinon.} \end{cases}$$

Par produit, comme voulu : $V_{G \rightarrow H}(g) = \prod_{1 \leq i \leq r} x_i^{-1} g^{n_i} x_i$. ■

■ 3.2 LE THÉORÈME DE p -NILPOTENCE DE BURNSIDE

Le transfert est utilisé le plus couramment dans le cas d'un p -Sylow. Le premier théorème dans cette direction est dû à Burnside et nécessite une définition préalable.

■ **Définition (p -nilpotence)** Soient G un groupe fini et p un nombre premier. On dit que G est p -nilpotent s'il est le produit semi-direct d'un p' -groupe distingué N par n'importe lequel de ses p -Sylow. Un tel sous-groupe N est appelé un p -complément distingué de G .

En particulier, un groupe p -nilpotent ne peut être simple que s'il est cyclique d'ordre p ou si c'est un p' -groupe.

■ **Théorème 13 (Lemme de Burnside)** Soient G un groupe fini, p un nombre premier, P un p -Sylow de G et $x, y \in P$. On suppose P abélien. Si x et y sont conjugués dans G , ils le sont aussi dans $N_G(P)$.

Démonstration Par hypothèse, $y = g^{-1}xg$ pour un certain $g \in G$. Les éléments x et y étant dans P et P étant abélien : $P \leq C_G(x)$ et $P \leq C_G(y)$. Par conjugaison : $g^{-1}Pg \leq C_G(g^{-1}xg) = C_G(y)$. En particulier, P et $g^{-1}Pg$ sont deux p -Sylow de $C_G(y)$, et sont donc conjugués dans $C_G(y)$ d'après les théorèmes de Sylow, $g^{-1}Pg = c^{-1}Pc$ pour un certain $c \in C_G(y)$. Posons $n = gc^{-1}$. Alors $n^{-1}Pn = P$, donc $n \in N_G(P)$, et comme voulu : $y = cy^{-1} = c g^{-1}x g c^{-1} = n^{-1}xn$. ■

■ **Théorème 14 (Théorème de p -nilpotence de Burnside)** Soient G un groupe fini, p un nombre premier et P un p -Sylow de G . Si $N_G(P) = C_G(P)$, G est p -nilpotent.

L'égalité $N_G(P) = C_G(P)$ implique en particulier que $P \leq C_G(P)$, autrement dit que P est abélien.

Démonstration Comme P est abélien, le transfert de G dans P est un morphisme de G dans P . Nous allons montrer que ce transfert est surjectif de G sur P . Son noyau sera un sous-groupe distingué de G de cardinal $|G : P|$, donc un p' -groupe. Les égalités $P \cap \text{Ker } V_{G \rightarrow P} = \{1\}$ et $|G| = |P| \cdot |\text{Ker } V_{G \rightarrow P}|$ montreront alors bien que G sera le produit semi-direct de $\text{Ker } V_{G \rightarrow P}$ par P , i.e. que G est p -nilpotent.

Nous allons montrer en fait que la restriction de $V_{G \rightarrow P}$ à P est surjective de P sur P . Soit $g \in P$. Avec les notations du théorème 12 : $V_{G \rightarrow P}(g) = \prod_{1 \leq i \leq r} x_i^{-1} g^{n_i} x_i$. Pour tout $i \in \llbracket 1, r \rrbracket$, le lemme de Burnside permet de choisir x_i^{-1} dans $N_G(P) = C_G(P)$, de sorte que x_i^{-1} et g^{n_i} commutent. Aussitôt : $V_{G \rightarrow P}(g) = \prod_{1 \leq i \leq r} g^{n_i} = g^{|G:P|}$.

La restriction de $V_{G \rightarrow P}$ à P coïncide finalement avec l'application $g \mapsto g^{|G:P|}$. Or comme $|P|$ et $|G : P|$ sont premiers entre eux, le théorème de Bézout donne deux entiers u et v pour lesquels $u|P| + v|G : P| = 1$. Les applications $g \mapsto g^{|G:P|}$ et $g \mapsto g^v$ sont alors réciproques l'une de l'autre d'après le théorème de Lagrange. En particulier, $g \mapsto g^{|G:P|}$ est surjective de P sur P . ■

Voyons à présent de quelle manière le théorème de p -nilpotence de Burnside élimine l'entier $252 = 2^2 \cdot 3^2 \cdot 7$. Supposons par l'absurde qu'il existe un groupe simple G d'ordre 252. D'après les théorèmes de Sylow : $|G : N_G(S)| = n_7(G) = 36$ pour tout 7-Sylow S de G , donc $|N_G(S)| = 7$, autrement dit $N_G(S) = S$. Comme S est abélien, il en découle que $N_G(S) = C_G(S)$, et donc que G est 7-nilpotent d'après le théorème de p -nilpotence de Burnside, ce qui contredit la simplicité de G .

Nous sommes aussi en mesure d'éliminer l'entier $180 = 2^2 \cdot 3^2 \cdot 5$. Supposons par l'absurde qu'il existe un groupe simple G d'ordre 180. D'après les théorèmes de Sylow : $n_5(G) = 6$ ou $n_5(G) = 36$. Le théorème 6 nous permet de rejeter le premier cas car 180 ne divise pas $\frac{4 \times 5 \times 6}{2} = 60$. Conclusion : $n_5(G) = 36$, donc pour tout 5-Sylow S de G : $|N_G(S)| = 5$, autrement dit $N_G(S) = S$. On conclut comme avec l'entier 252 un peu plus haut.

Nous allons tirer maintenant deux corollaires du théorème de p -nilpotence de Burnside, dont voici le premier.

■ **Théorème 15 (Corollaire cyclique du théorème de p -nilpotence de Burnside)** Soit G un groupe fini. On note p le plus petit diviseur premier de $|G|$. Si les p -Sylow de G sont cycliques, G est p -nilpotent.

Démonstration Soit P un p -Sylow de G . D'après le théorème de p -nilpotence de Burnside, il nous suffit de montrer l'égalité $N_G(P) = C_G(P)$, i.e. $|N_G(P) : C_G(P)| = 1$. Or n'oublions pas que, d'après le théorème 7, $|N_G(P) : C_G(P)|$ divise $|\text{Aut}(P)|$. Le résultat découle ainsi des trois remarques qui suivent.

- Pour commencer, P étant cyclique, disons d'ordre p^n : $|\text{Aut}(P)| = p^{n-1}(p-1)$.
- Ensuite, $C_G(P)$ contient P car P est abélien, donc $|N_G(P) : C_G(P)|$ est premier à p .
- Pour finir, p étant le plus petit diviseur premier de $|G|$, $|N_G(P) : C_G(P)|$ est premier à $p-1$. ■

Le petit résultat qui suit est classique et nous omettrons sa démonstration.

■ **Théorème 16 (Groupes d'ordre p^2)** Soit p un nombre premier. Tout groupe d'ordre p^2 est abélien, soit cyclique, soit isomorphe à \mathbb{Z}_p^2 .

Encore un lemme. Rappelons avant que si les notations \mathbb{Z}_p et \mathbb{F}_p désignent le même objet, \mathbb{Z}_p désigne plutôt un groupe additif et \mathbb{F}_p un corps.

■ **Théorème 17 (Automorphismes du groupe \mathbb{Z}_p^n)** Soient p un nombre premier et $n \in \mathbb{N}^*$. Tout automorphisme du groupe \mathbb{Z}_p^n est un automorphisme linéaire du \mathbb{F}_p -espace vectoriel \mathbb{Z}_p^n . En d'autres termes : $\text{Aut}(\mathbb{Z}_p^n) = \text{GL}_n(\mathbb{F}_p)$.

En particulier :
$$|\text{Aut}(\mathbb{Z}_p^n)| = \prod_{k=0}^{n-1} (p^n - p^k).$$

Démonstration Soient φ un automorphisme du groupe \mathbb{Z}_p^n , $\lambda \in \mathbb{F}_p$ et $(x_1, \dots, x_n) \in \mathbb{Z}_p^n$. Le scalaire λ est l'image dans \mathbb{F}_p d'un certain entier k . Aussitôt :

$$\begin{aligned} \varphi(\lambda \cdot (x_1, \dots, x_n)) &= \varphi(\underbrace{x_1 + \dots + x_1}_{k \text{ termes}}, \dots, \underbrace{x_n + \dots + x_n}_{k \text{ termes}}) = \varphi(\underbrace{(x_1, \dots, x_n) + \dots + (x_1, \dots, x_n)}_{k \text{ termes}}) \\ &= \underbrace{\varphi(x_1, \dots, x_n) + \dots + \varphi(x_1, \dots, x_n)}_{k \text{ termes}} = \lambda \cdot \varphi(x_1, \dots, x_n). \end{aligned}$$

Conclusion : l'automorphisme de groupe φ est en fait déjà un automorphisme linéaire de \mathbb{F}_p^n . Le calcul final du cardinal de $\text{GL}_n(\mathbb{F}_p)$ est classique. Une base de \mathbb{F}_p^n étant donnée, il y a autant d'automorphismes linéaires de \mathbb{F}_p^n que de bases de \mathbb{F}_p^n . Or pour construire une telle base, on a $p^n - 1$ choix pour le premier vecteur. Comme ce premier vecteur engendre une droite de cardinal p , le deuxième vecteur peut être choisi de $p^n - p$ façons. Ensuite, les deux premiers vecteurs engendrent un plan de cardinal p^2 , d'où un total de $p^n - p^2$ choix pour le troisième vecteur, etc. ■

Nous atteignons enfin notre deuxième corollaire du théorème de p -nilpotence de Burnside.

■ **Théorème 18 (Théorème 12-ou- p^3)** Soit G un groupe fini simple non abélien. On note p le plus diviseur premier de $|G|$. L'entier $|G|$ est alors divisible par 12 ou p^3 .

En particulier, si $|G|$ est pair, il est divisible par 8 ou 12.

En poussant plus loin les techniques de ce paragraphe, on pourrait remplacer « 8 ou 12 » par « 12, 16 ou 56 ».

Démonstration Le théorème 15 montre que $|G|$ ne peut pas être divisible par p sans l'être par p^2 , car un groupe d'ordre p est forcément cyclique. Il nous suffit dès lors de montrer, dans le cas où $|G|$ est divisible par p^2 sans l'être par p^3 , que $|G|$ est divisible par 12.

Plaçons-nous dans ce cas et fixons un p -Sylow P de G . D'après les théorèmes 15 et 16, P est isomorphe au groupe \mathbb{Z}_p^2 , et d'après le théorème 17 : $|\text{Aut}(P)| = (p^2 - 1)(p^2 - p) = (p - 1)^2 p(p + 1)$. Or :

- $|\text{N}_G(P) : \text{C}_G(P)|$ divise $|\text{Aut}(P)|$ d'après le théorème 7,
- $|\text{N}_G(P) : \text{C}_G(P)|$ est premier à p car P , abélien, est inclus dans $\text{C}_G(P)$,
- $|\text{N}_G(P) : \text{C}_G(P)|$ est premier à $p - 1$ car p est le plus petit diviseur premier de $|G|$.

Conclusion : $|\text{N}_G(P) : \text{C}_G(P)|$ divise $p + 1$. Le théorème de p -nilpotence de Burnside montre par ailleurs que $|\text{N}_G(P) : \text{C}_G(P)| \neq 1$. Les entiers $|G|$ et $p + 1$ ont ainsi un diviseur premier en commun, forcément $p + 1$ par hypothèse sur p . Or les entiers consécutifs p et $p + 1$ ne peuvent être premiers que si $p = 2$. Comme voulu, $|G|$ est divisible par $p^2 = 4$ et $p + 1 = 3$, donc par 12. ■

Sur les 8 entiers qu'il nous reste à tester, le théorème 12-ou- p^3 en élimine 4, dont les derniers impairs. Nos 4 irréductibles sont alors : 240, 420, 540 et 612.

Le théorème de p -nilpotence de Burnside n'a toutefois pas dit son dernier mot et va nous permettre d'éliminer encore quelques entiers. Nous commençons par un lemme.

■ **Théorème 19 (Groupes d'ordre pq avec $p < q$ et $q \not\equiv 1 [p]$)** Soient p et q deux nombres premiers pour lesquels $p < q$ et $q \not\equiv 1 [p]$. Tout groupe d'ordre pq est alors cyclique.

Démonstration Soit G un groupe d'ordre pq . D'après les théorèmes de Sylow : $n_q(G) = 1$, et comme $q \not\equiv 1 [p]$: $n_p(G) = 1$. Le groupe G possède ainsi un et un seul p -Sylow P et un et un seul q -Sylow Q , tous

deux distingués. Donnons-nous alors x un élément de P d'ordre p et y un élément de Q d'ordre q . Le commutateur $[x, y] = x^{-1}y^{-1}xy$ appartient à la fois à P et Q car $x^{-1}y^{-1}x \in Q$ et $y^{-1}xy \in P$. Or $P \cap Q = \{1\}$ car $|P|$ et $|Q|$ sont premiers entre eux, donc $[x, y] = 1$, ou encore $xy = yx$. Il en découle que : $(xy)^p = x^p y^p = y^p \neq 1$ et $(xy)^q = x^q y^q = x^q \neq 1$, autrement dit que l'ordre de xy n'est ni un diviseur de p , ni un diviseur de q . Conclusion : xy est d'ordre pq , donc $G = \langle xy \rangle$, ce qui montre bien que G est cyclique. ■

Donnons-nous à présent un entier naturel non nul n et supposons l'existence d'un groupe simple non abélien G d'ordre n . Fixons en outre un diviseur premier p de $|G|$ et un p -Sylow P de G . Les théorèmes de Sylow et le principe factoriel n'autorisent que quelques valeurs de $n_p(G) = |G : N_G(P)|$, et donc de $|N_G(P)|$. Faisons l'hypothèse que $|N_G(P)|$ ne puisse prendre qu'une seule valeur et que cette valeur soit pq avec $p < q$ et $q \not\equiv 1 [p]$. Le théorème 19 montre alors que $N_G(P)$ est cyclique. A fortiori $N_G(P) = C_G(P)$. Le théorème de p -nilpotence de Burnside contredit alors la simplicité de G . Ce raisonnement élimine l'entier 540 pour $p = 5$, et on va voir qu'il n'est pas loin d'éliminer aussi l'entier $240 = 2^4 \cdot 3 \cdot 5$.

Supposons en effet par l'absurde qu'il existe un groupe simple G d'ordre 240. D'après les théorèmes de Sylow : $n_5(G) = 6$ ou $n_5(G) = 16$, et il se trouve que ces deux possibilités conduisent à une contradiction. Si $n_5(G) = 16$, on peut conclure comme ci-dessus avec l'entier 540. Si au contraire $n_5(G) = 6$, le principe factoriel montre que G est isomorphe à un sous-groupe de A_6 alors que 240 ne divise pas $\frac{6!}{2} = 360$.

■ 4 LES RÉCALCITRANTS — 420 ET 612

En dépit de ces longs développements, il nous reste quand même encore deux entiers à éliminer, les entiers 420 et 612.

■ 4.1 GROUPES D'ORDRE 420

Supposons par l'absurde qu'il existe un groupe simple G d'ordre $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$. D'après les théorèmes de Sylow : $n_7(G) = 15$, donc pour tout 7-Sylow S de G : $|N_G(S)| = 28$. Le théorème 7 montre par ailleurs que $|N_G(S) : C_G(S)|$ divise $|\text{Aut}(S)| = |\text{Aut}(\mathbb{Z}_7)| = 6$, donc $C_G(S)$ est d'ordre 14 ou 28. Comme S est central dans $C_G(S)$, il en découle que $C_G(S)$ est cyclique, donc contient un élément c d'ordre 14.

Se peut-il que c normalise un 7-Sylow S' autre que S ? Si c'était le cas, c^2 serait un élément d'ordre 7 de $N_G(S')$, lequel admet S' pour unique 7-Sylow. Ainsi c^2 serait élément de S' , ce qui est impossible car $S \cap S' = \{1\}$. Conclusion : c ne normalise que S .

Intéressons-nous pour finir à l'action par conjugaison de G sur l'ensemble $\text{Syl}_7(G)$ de ses 7-Sylow. Cette action nous fournit un morphisme injectif φ de G dans $A_{\text{Syl}_7(G)}$, lequel est isomorphe à A_{15} , et nous venons de montrer que la permutation $\varphi(c)$ admet S pour seul point fixe. D'ordre 14, $\varphi(c)$ est un 14-cycle, donc une permutation impaire — contradiction.

■ 4.2 GROUPES D'ORDRE 612

Supposons par l'absurde qu'il existe un groupe simple G d'ordre $612 = 2^2 \cdot 3^2 \cdot 17$. D'après les théorèmes de Sylow et le principe factoriel : $n_3(G) = 34 \not\equiv 1 [9]$, donc d'après le théorème 9, il existe deux 3-Sylow T et T' de G pour lesquels, en notant I l'intersection de T et T' : $|I| = 3$ et $|N_G(I)| = 9m$ avec $m \geq 4$. Comme $|G : N_G(I)| \geq 17$ d'après le principe factoriel, forcément $m = 4$ et $N_G(I) = 36$. Le théorème 7 montre par ailleurs que $|N_G(I) : C_G(I)|$ divise $|\text{Aut}(I)| = |\text{Aut}(\mathbb{Z}_3)| = 2$, donc $C_G(I)$ est d'ordre 18 ou 36. Dans les deux cas, $C_G(I)$ contient un élément d'ordre 6, disons c .

Intéressons-nous à présent à l'action par conjugaison de G sur l'ensemble $\text{Syl}_{17}(G)$ de ses 17-Sylow. Cette action nous fournit un morphisme injectif φ de G dans $A_{\text{Syl}_{17}(G)}$, lequel est isomorphe à A_{18} car $n_{17}(G) = 18$ d'après les théorèmes de Sylow. Pour tout 17-Sylow S de G : $|N_G(S)| = 34$, donc ni c d'ordre 6 ni c^2 d'ordre 3 ne normalisent S . La permutation $\varphi(c)$ est ainsi sans point fixe et ne contient aucune transposition dans sa décomposition en produit de cycles disjoints. En résumé, $\varphi(c)$ est le produit de c_3 3-cycles et c_6 6-cycles avec $3c_3 + 6c_6 = 18$, ou encore $c_3 + 2c_6 = 6$. Il se trouve par ailleurs que $c_6 \geq 1$, sans quoi $\varphi(c)$ serait d'ordre 3, mais aussi que c_6 est pair, sans quoi $\varphi(c)$ serait une permutation impaire. Ces contraintes ne nous laissent guère le choix. Forcément $c_3 = c_6 = 2$. La permutation $\varphi(c)^3$ se présente en retour comme le produit de 6 transpositions. En d'autres termes, c^3 normalise exactement $18 - 2 \times 6 = 6$ 17-Sylow de G .

Donnons-nous pour finir un 17-Sylow fixé S de G . L'action par conjugaison de S sur $\text{Syl}_{17}(G) \setminus \{S\}$ est non triviale car un 17-Sylow ne peut jamais normaliser aucun autre 17-Sylow. Comme de plus $n_{17}(G) - 1 = 17$, cette action est nécessairement transitive. Sur les 6 17-Sylow de G que c^3 normalise, nous pouvons nous en donner deux qui ne sont pas S , disons S' et S'' . Nous venons de voir, par transitivité, que $S'' = s^{-1}S's$ pour un certain $s \in S$. Remarquons alors que :

$$[c^3, s]S''[c^3, s]^{-1} = c^{-3}s^{-1}c^3sS''s^{-1}c^{-3}sc^3 = c^{-3}s^{-1}c^3S'c^{-3}sc^3 = c^{-3}s^{-1}S'sc^3 = c^{-3}S''c^3 = S'',$$

autrement dit $[c^3, s] \in N_G(S'')$. Comme S est distingué dans $N_G(S)$, le commutateur $[c^3, s] = (c^{-3}s^{-1}c^3)s$ appartient par ailleurs à S , donc est d'ordre 1 ou 17, car $s \in S$ et $c^3 \in N_G(S)$. Or S'' , en tant qu'unique 17-Sylow de $N_G(S'')$, contient tous les éléments d'ordre 17 de $N_G(S'')$, donc $[c^3, s] \in S \cap S'' = \{1\}$. Conclusion : c^3 et s commutent, donc $c^3 \in C_G(S)$. Comme c^3 est d'ordre 2, ce résultat montre que $C_G(S)$ est d'ordre 34, et donc enfin que $N_G(S) = C_G(S)$, situation que le théorème de p -nilpotence de Burnside interdit.

5 ANNEXE – PRÉCISIONS SUR LES THÉORÈMES DE SYLOW ET LE PRINCIPE FACTORIEL

Les tableaux qui suivent explicitent les ressorts de l'élimination massive à laquelle les théorèmes de Sylow et le principe factoriel nous ont permis de procéder au début de ce texte.

- La première colonne de chaque tableau énumère les entiers n de 1 à 660.
- La deuxième colonne explicite la factorisation première de n .
- La troisième colonne fournit la liste des nombres premiers p , s'il en existe, pour lesquels :

$$\forall k \in \mathbb{N}^*, \quad (k \text{ divise } n \text{ et } k \equiv 1 [p]) \implies k = 1.$$

- La quatrième colonne fournit la liste des nombres premiers p , s'il en existe, qui ne figurent pas dans la colonne précédente et pour lesquels : $\forall k \in \mathbb{N}^*, \quad (k \text{ divise } n \text{ et } k \equiv 1 [p]) \implies n \text{ ne divise pas } k!$

1	1		
2	2		
3	3		
4	2 ²		
5	5		
6	2.3	3	
7	7		
8	2 ³		
9	3 ²		
10	2.5	5	
11	11		
12	2 ² .3		2
13	13		
14	2.7	7	
15	3.5	3,5	
16	2 ⁴		
17	17		
18	2.3 ²	3	
19	19		
20	2 ² .5	5	
21	3.7	7	
22	2.11	11	
23	23		
24	2 ³ .3		2
25	5 ²		
26	2.13	13	
27	3 ³		
28	2 ² .7	7	
29	29		
30	2.3.5		

31	31		
32	2 ⁵		
33	3.11	11,3	
34	2.17	17	
35	5.7	5,7	
36	2 ² .3 ²		3
37	37		
38	2.19	19	
39	3.13	13	
40	2 ³ .5	5	
41	41		
42	2.3.7	7	
43	43		
44	2 ² .11	11	
45	3 ² .5	3,5	
46	2.23	23	
47	47		
48	2 ⁴ .3		2
49	7 ²		
50	2.5 ²	5	
51	3.17	17,3	
52	2 ² .13	13	
53	53		
54	2.3 ³	3	
55	5.11	11	
56	2 ³ .7		
57	3.19	19	
58	2.29	29	
59	59		
60	2 ² .3.5		

61	61		
62	2.31	31	
63	3 ² .7	7	
64	2 ⁶		
65	5.13	13,5	
66	2.3.11	11	
67	67		
68	2 ² .17	17	
69	3.23	23,3	
70	2.5.7	5,7	
71	71		
72	2 ³ .3 ²		3
73	73		
74	2.37	37	
75	3.5 ²	5	
76	2 ² .19	19	
77	7.11	11,7	
78	2.3.13	13	
79	79		
80	2 ⁴ .5		2
81	3 ⁴		
82	2.41	41	
83	83		
84	2 ² .3.7	7	
85	5.17	17,5	
86	2.43	43	
87	3.29	29,3	
88	2 ³ .11	11	
89	89		
90	2.3 ² .5		
91	7.13	13,7	
92	2 ² .23	23	
93	3.31	31	
94	2.47	47	
95	5.19	5,19	
96	2 ⁵ .3		2
97	97		
98	2.7 ²	7	
99	3 ² .11	11,3	
100	2 ² .5 ²	5	
101	101		
102	2.3.17	17	
103	103		
104	2 ³ .13	13	
105	3.5.7		
106	2.53	53	
107	107		
108	2 ² .3 ³		3
109	109		
110	2.5.11	11	

111	3.37	37	
112	2 ⁴ .7		
113	113		
114	2.3.19	19	
115	5.23	23,5	
116	2 ² .29	29	
117	3 ² .13	13	
118	2.59	59	
119	7.17	17,7	
120	2 ³ .3.5		
121	11 ²		
122	2.61	61	
123	3.41	41,3	
124	2 ² .31	31	
125	5 ³		
126	2.3 ² .7	7	
127	127		
128	2 ⁷		
129	3.43	43	
130	2.5.13	13	
131	131		
132	2 ² .3.11		
133	7.19	7,19	
134	2.67	67	
135	3 ³ .5	3,5	
136	2 ³ .17	17	
137	137		
138	2.3.23	23	
139	139		
140	2 ² .5.7	5,7	
141	3.47	47,3	
142	2.71	71	
143	11.13	11,13	
144	2 ⁴ .3 ²		
145	5.29	29,5	
146	2.73	73	
147	3.7 ²	7	
148	2 ² .37	37	
149	149		
150	2.3.5 ²		5
151	151		
152	2 ³ .19	19	
153	3 ² .17	17,3	
154	2.7.11	11	
155	5.31	31	
156	2 ² .3.13	13	
157	157		
158	2.79	79	
159	3.53	53,3	
160	2 ⁵ .5		2

161	7.23	23,7	
162	$2 \cdot 3^4$	3	
163	163		
164	$2^2 \cdot 41$	41	
165	3.5.11	11	
166	2.83	83	
167	167		
168	$2^3 \cdot 3 \cdot 7$		
169	13^2		
170	2.5.17	17,5	
171	$3^2 \cdot 19$	19	
172	$2^2 \cdot 43$	43	
173	173		
174	2.3.29	29	
175	$5^2 \cdot 7$	5,7	
176	$2^4 \cdot 11$	11	
177	3.59	59,3	
178	2.89	89	
179	179		
180	$2^2 \cdot 3^2 \cdot 5$		
181	181		
182	2.7.13	7	
183	3.61	61	
184	$2^3 \cdot 23$	23	
185	5.37	5,37	
186	2.3.31	31	
187	11.17	11,17	
188	$2^2 \cdot 47$	47	
189	$3^3 \cdot 7$	7	
190	2.5.19	5,19	
191	191		
192	$2^6 \cdot 3$		2
193	193		
194	2.97	97	
195	3.5.13	13,5	
196	$2^2 \cdot 7^2$	7	
197	197		
198	$2 \cdot 3^2 \cdot 11$	11	
199	199		
200	$2^3 \cdot 5^2$	5	
201	3.67	67	
202	2.101	101	
203	7.29	29	
204	$2^2 \cdot 3 \cdot 17$	17	
205	5.41	41	
206	2.103	103	
207	$3^2 \cdot 23$	23,3	
208	$2^4 \cdot 13$	13	
209	11.19	11,19	
210	2.3.5.7		

211	211		
212	$2^2 \cdot 53$	53	
213	3.71	71,3	
214	2.107	107	
215	5.43	5,43	
216	$2^3 \cdot 3^3$		3
217	7.31	31,7	
218	2.109	109	
219	3.73	73	
220	$2^2 \cdot 5 \cdot 11$	11	
221	13.17	13,17	
222	2.3.37	37	
223	223		
224	$2^5 \cdot 7$		2
225	$3^2 \cdot 5^2$	5	
226	2.113	113	
227	227		
228	$2^2 \cdot 3 \cdot 19$	19	
229	229		
230	2.5.23	23	
231	3.7.11	11,7	
232	$2^3 \cdot 29$	29	
233	233		
234	$2 \cdot 3^2 \cdot 13$	13	
235	5.47	47,5	
236	$2^2 \cdot 59$	59	
237	3.79	79	
238	2.7.17	17,7	
239	239		
240	$2^4 \cdot 3 \cdot 5$		
241	241		
242	$2 \cdot 11^2$	11	
243	3^5		
244	$2^2 \cdot 61$	61	
245	$5 \cdot 7^2$	5,7	
246	2.3.41	41	
247	13.19	13,19	
248	$2^3 \cdot 31$	31	
249	3.83	3,83	
250	$2 \cdot 5^3$	5	
251	251		
252	$2^2 \cdot 3^2 \cdot 7$		
253	11.23	23	
254	2.127	127	
255	3.5.17	17	
256	2^8		
257	257		
258	2.3.43	43	
259	7.37	7,37	
260	$2^2 \cdot 5 \cdot 13$	13	

261	$3^2 \cdot 29$	29,3	
262	2.131	131	
263	263		
264	$2^3 \cdot 3 \cdot 11$		
265	5.53	53,5	
266	2.7.19	7,19	
267	3.89	89,3	
268	$2^2 \cdot 67$	67	
269	269		
270	$2 \cdot 3^3 \cdot 5$		5
271	271		
272	$2^4 \cdot 17$	17	
273	3.7.13	13,7	
274	2.137	137	
275	$5^2 \cdot 11$	11	
276	$2^2 \cdot 3 \cdot 23$	23	
277	277		
278	2.139	139	
279	$3^2 \cdot 31$	31	
280	$2^3 \cdot 5 \cdot 7$		
281	281		
282	2.3.47	47	
283	283		
284	$2^2 \cdot 71$	71	
285	3.5.19	5,19	
286	2.11.13	11,13	
287	7.41	41,7	
288	$2^5 \cdot 3^2$		
289	17^2		
290	2.5.29	29,5	
291	3.97	97	
292	$2^2 \cdot 73$	73	
293	293		
294	$2 \cdot 3 \cdot 7^2$	7	
295	5.59	59,5	
296	$2^3 \cdot 37$	37	
297	$3^3 \cdot 11$	11,3	
298	2.149	149	
299	13.23	23,13	
300	$2^2 \cdot 3 \cdot 5^2$		5
301	7.43	43	
302	2.151	151	
303	3.101	101,3	
304	$2^4 \cdot 19$	19	
305	5.61	61	
306	$2 \cdot 3^2 \cdot 17$		
307	307		
308	$2^2 \cdot 7 \cdot 11$	11	
309	3.103	103	
310	2.5.31	31	

311	311		
312	$2^3 \cdot 3 \cdot 13$	13	
313	313		
314	2.157	157	
315	$3^2 \cdot 5 \cdot 7$		
316	$2^2 \cdot 79$	79	
317	317		
318	2.3.53	53	
319	11.29	29,11	
320	$2^6 \cdot 5$		2
321	3.107	107,3	
322	2.7.23	23,7	
323	17.19	17,19	
324	$2^2 \cdot 3^4$		3
325	$5^2 \cdot 13$	13,5	
326	2.163	163	
327	3.109	109	
328	$2^3 \cdot 41$	41	
329	7.47	47,7	
330	2.3.5.11	11	
331	331		
332	$2^2 \cdot 83$	83	
333	$3^2 \cdot 37$	37	
334	2.167	167	
335	5.67	5,67	
336	$2^4 \cdot 3 \cdot 7$		
337	337		
338	$2 \cdot 13^2$	13	
339	3.113	113,3	
340	$2^2 \cdot 5 \cdot 17$	17,5	
341	11.31	31,11	
342	$2 \cdot 3^2 \cdot 19$	19	
343	7^3		
344	$2^3 \cdot 43$	43	
345	3.5.23	23,5	
346	2.173	173	
347	347		
348	$2^2 \cdot 3 \cdot 29$	29	
349	349		
350	$2 \cdot 5^2 \cdot 7$	5	
351	$3^3 \cdot 13$		
352	$2^5 \cdot 11$	11	
353	353		
354	2.3.59	59	
355	5.71	71	
356	$2^2 \cdot 89$	89	
357	3.7.17	17,7	
358	2.179	179	
359	359		
360	$2^3 \cdot 3^2 \cdot 5$		

361	19^2		
362	2.181	181	
363	3.11^2	11	
364	$2^2.7.13$	7	
365	5.73	73,5	
366	2.3.61	61	
367	367		
368	$2^4.23$	23	
369	$3^2.41$	41,3	
370	2.5.37	5,37	
371	7.53	53,7	
372	$2^2.3.31$	31	
373	373		
374	2.11.17	17	
375	3.5^3	5	
376	$2^3.47$	47	
377	13.29	29,13	
378	$2.3^3.7$	7	
379	379		
380	$2^2.5.19$		
381	3.127	127	
382	2.191	191	
383	383		
384	$2^7.3$		2
385	5.7.11	11,7	
386	2.193	193	
387	$3^2.43$	43	
388	$2^2.97$	97	
389	389		
390	2.3.5.13	13	
391	17.23	23,17	
392	$2^3.7^2$		7
393	3.131	131,3	
394	2.197	197	
395	5.79	5,79	
396	$2^2.3^2.11$		
397	397		
398	2.199	199	
399	3.7.19	19	
400	$2^4.5^2$		
401	401		
402	2.3.67	67	
403	13.31	31,13	
404	$2^2.101$	101	
405	$3^4.5$	3	
406	2.7.29	29	
407	11.37	11,37	
408	$2^3.3.17$	17	
409	409		
410	2.5.41	41	

411	3.137	3,137	
412	$2^2.103$	103	
413	7.59	59,7	
414	$2.3^2.23$	23	
415	5.83	5,83	
416	$2^5.13$	13	
417	3.139	139	
418	2.11.19	11,19	
419	419		
420	$2^2.3.5.7$		
421	421		
422	2.211	211	
423	$3^2.47$	47,3	
424	$2^3.53$	53	
425	$5^2.17$	17,5	
426	2.3.71	71	
427	7.61	7,61	
428	$2^2.107$	107	
429	3.11.13	11,13	
430	2.5.43	43	
431	431		
432	$2^4.3^3$		
433	433		
434	2.7.31	31,7	
435	3.5.29	29,5	
436	$2^2.109$	109	
437	19.23	23,19	
438	2.3.73	73	
439	439		
440	$2^3.5.11$	11	
441	$3^2.7^2$	7	
442	2.13.17	13,17	
443	443		
444	$2^2.3.37$	37	
445	5.89	89,5	
446	2.223	223	
447	3.149	3,149	
448	$2^6.7$		2
449	449		
450	$2.3^2.5^2$		5
451	11.41	41,11	
452	$2^2.113$	113	
453	3.151	151	
454	2.227	227	
455	5.7.13	13,7	
456	$2^3.3.19$	19	
457	457		
458	2.229	229	
459	$3^3.17$	17,3	
460	$2^2.5.23$	23	

461	461		
462	$2 \cdot 3 \cdot 7 \cdot 11$	11	
463	463		
464	$2^4 \cdot 29$	29	
465	$3 \cdot 5 \cdot 31$	31	
466	$2 \cdot 233$	233	
467	467		
468	$2^2 \cdot 3^2 \cdot 13$	13	
469	$7 \cdot 67$	7, 67	
470	$2 \cdot 5 \cdot 47$	47, 5	
471	$3 \cdot 157$	157	
472	$2^3 \cdot 59$	59	
473	$11 \cdot 43$	11, 43	
474	$2 \cdot 3 \cdot 79$	79	
475	$5^2 \cdot 19$	5, 19	
476	$2^2 \cdot 7 \cdot 17$	17, 7	
477	$3^2 \cdot 53$	53, 3	
478	$2 \cdot 239$	239	
479	479		
480	$2^5 \cdot 3 \cdot 5$		
481	$13 \cdot 37$	13, 37	
482	$2 \cdot 241$	241	
483	$3 \cdot 7 \cdot 23$	23, 7	
484	$2^2 \cdot 11^2$	11	
485	$5 \cdot 97$	97, 5	
486	$2 \cdot 3^5$	3	
487	487		
488	$2^3 \cdot 61$	61	
489	$3 \cdot 163$	163	
490	$2 \cdot 5 \cdot 7^2$	5, 7	
491	491		
492	$2^2 \cdot 3 \cdot 41$	41	
493	$17 \cdot 29$	29, 17	
494	$2 \cdot 13 \cdot 19$	13, 19	
495	$3^2 \cdot 5 \cdot 11$		
496	$2^4 \cdot 31$	31	
497	$7 \cdot 71$	71	
498	$2 \cdot 3 \cdot 83$	83	
499	499		
500	$2^2 \cdot 5^3$	5	
501	$3 \cdot 167$	3, 167	
502	$2 \cdot 251$	251	
503	503		
504	$2^3 \cdot 3^2 \cdot 7$		
505	$5 \cdot 101$	101	
506	$2 \cdot 11 \cdot 23$	23	
507	$3 \cdot 13^2$	13	
508	$2^2 \cdot 127$	127	
509	509		
510	$2 \cdot 3 \cdot 5 \cdot 17$	17	

511	$7 \cdot 73$	73, 7	
512	2^9		
513	$3^3 \cdot 19$	19	
514	$2 \cdot 257$	257	
515	$5 \cdot 103$	103, 5	
516	$2^2 \cdot 3 \cdot 43$	43	
517	$11 \cdot 47$	47, 11	
518	$2 \cdot 7 \cdot 37$	7, 37	
519	$3 \cdot 173$	3, 173	
520	$2^3 \cdot 5 \cdot 13$		
521	521		
522	$2 \cdot 3^2 \cdot 29$	29	
523	523		
524	$2^2 \cdot 131$	131	
525	$3 \cdot 5^2 \cdot 7$		
526	$2 \cdot 263$	263	
527	$17 \cdot 31$	31, 17	
528	$2^4 \cdot 3 \cdot 11$		
529	23^2		
530	$2 \cdot 5 \cdot 53$	53	
531	$3^2 \cdot 59$	59, 3	
532	$2^2 \cdot 7 \cdot 19$	7, 19	
533	$13 \cdot 41$	41, 13	
534	$2 \cdot 3 \cdot 89$	89	
535	$5 \cdot 107$	107, 5	
536	$2^3 \cdot 67$	67	
537	$3 \cdot 179$	3, 179	
538	$2 \cdot 269$	269	
539	$7^2 \cdot 11$	11, 7	
540	$2^2 \cdot 3^3 \cdot 5$		
541	541		
542	$2 \cdot 271$	271	
543	$3 \cdot 181$	181	
544	$2^5 \cdot 17$	17	
545	$5 \cdot 109$	109, 5	
546	$2 \cdot 3 \cdot 7 \cdot 13$		
547	547		
548	$2^2 \cdot 137$	137	
549	$3^2 \cdot 61$	61	
550	$2 \cdot 5^2 \cdot 11$	11	
551	$19 \cdot 29$	29, 19	
552	$2^3 \cdot 3 \cdot 23$		
553	$7 \cdot 79$	7, 79	
554	$2 \cdot 277$	277	
555	$3 \cdot 5 \cdot 37$	37	
556	$2^2 \cdot 139$	139	
557	557		
558	$2 \cdot 3^2 \cdot 31$	31	
559	$13 \cdot 43$	13, 43	
560	$2^4 \cdot 5 \cdot 7$		

561	3.11.17	11,17	
562	2.281	281	
563	563		
564	$2^2 \cdot 3 \cdot 47$	47	
565	5.113	113,5	
566	2.283	283	
567	$3^4 \cdot 7$	7	
568	$2^3 \cdot 71$	71	
569	569		
570	2.3.5.19	19	
571	571		
572	$2^2 \cdot 11 \cdot 13$	11,13	
573	3.191	191,3	
574	2.7.41	41,7	
575	$5^2 \cdot 23$	23,5	
576	$2^6 \cdot 3^2$		
577	577		
578	$2 \cdot 17^2$	17	
579	3.193	193	
580	$2^2 \cdot 5 \cdot 29$	29	
581	7.83	7,83	
582	2.3.97	97	
583	11.53	53,11	
584	$2^3 \cdot 73$	73	
585	$3^2 \cdot 5 \cdot 13$	13,5	
586	2.293	293	
587	587		
588	$2^2 \cdot 3 \cdot 7^2$	7	
589	19.31	31,19	
590	2.5.59	59,5	
591	3.197	197,3	
592	$2^4 \cdot 37$	37	
593	593		
594	$2 \cdot 3^3 \cdot 11$	11	
595	5.7.17	5	
596	$2^2 \cdot 149$	149	
597	3.199	199	
598	2.13.23	23,13	
599	599		
600	$2^3 \cdot 3 \cdot 5^2$		5
601	601		
602	2.7.43	43	
603	$3^2 \cdot 67$	67	
604	$2^2 \cdot 151$	151	
605	$5 \cdot 11^2$	11	
606	2.3.101	101	
607	607		
608	$2^5 \cdot 19$	19	
609	3.7.29	29	
610	2.5.61	61	

611	13.47	47,13	
612	$2^2 \cdot 3^2 \cdot 17$		
613	613		
614	2.307	307	
615	3.5.41	41	
616	$2^3 \cdot 7 \cdot 11$		
617	617		
618	2.3.103	103	
619	619		
620	$2^2 \cdot 5 \cdot 31$	31	
621	$3^3 \cdot 23$	23,3	
622	2.311	311	
623	7.89	89,7	
624	$2^4 \cdot 3 \cdot 13$	13	
625	5^4		
626	2.313	313	
627	3.11.19	11,19	
628	$2^2 \cdot 157$	157	
629	17.37	17,37	
630	$2 \cdot 3^2 \cdot 5 \cdot 7$		
631	631		
632	$2^3 \cdot 79$	79	
633	3.211	211	
634	2.317	317	
635	5.127	127,5	
636	$2^2 \cdot 3 \cdot 53$	53	
637	$7^2 \cdot 13$	13,7	
638	2.11.29	29,11	
639	$3^2 \cdot 71$	71,3	
640	$2^7 \cdot 5$		2
641	641		
642	2.3.107	107	
643	643		
644	$2^2 \cdot 7 \cdot 23$	23	
645	3.5.43	5,43	
646	2.17.19	17,19	
647	647		
648	$2^3 \cdot 3^4$		3
649	11.59	59,11	
650	$2 \cdot 5^2 \cdot 13$	13	
651	3.7.31	31,7	
652	$2^2 \cdot 163$	163	
653	653		
654	2.3.109	109	
655	5.131	131	
656	$2^4 \cdot 41$	41	
657	$3^2 \cdot 73$	73	
658	2.7.47	47,7	
659	659		
660	$2^2 \cdot 3 \cdot 5 \cdot 11$		