Algèbre – Devoir à la maison I

Problème 1. – (Groupes simples d'ordre $\leqslant 660$) L'objectif de ce problème est d'établir le théorème suivant.

> **Théorème. –** *Soit G un groupe simple non abélien d'ordre $n \leqslant 660$. Alors $n \in \{60, 168, 360, 504, 660\}$.*

La stratégie va simplement consister à montrer que tous les autres cardinaux ne sauraient donner lieu à un groupe simple.

Notations

Soit G un groupe fini de cardinal n.

- Pour tout $p \mid n$, on désignera par n_p le nombre de p-Sylow de G et $\mathrm{Syl}_p(G)$ l'ensemble de ses p-Sylow;
- Pour tout sous-groupe $H \leqslant G$, on rappelle que le normalisateur de H dans G est le sous-groupe $N_G(H) := \left\{g \in G \ : \ gHg^{-1} = H\right\}$ et son centralisateur dans G le sous-groupe $C_G(H) := \{g \in G \ : \ \forall h \in H,\ gh = hg\}$;
- Pour tous g et $h \in G$, on désignera par $[g, h]$ le commutateur $ghg^{-1}h^{-1}$.

Enfin, p désignera toujours un nombre premier et, pour tout entier naturel k et tout entier v, on notera $p^v || k$ si $p^v \mid k$ et $p^{v+1} \nmid k$.

Un premier tri via des outils élémentaires

1. Justifier qu'un p-groupe est simple si, et seulement s'il est d'ordre p.
   Cela permet de traiter 142 entiers parmi la liste des entiers inférieurs à 660 qui sont des puissances d'un nombre premier, dont 120 sont premiers et fournissent par conséquent des groupes simples.
2. Expliquer pourquoi un groupe de cardinal n tel qu'il existe un diviseur premier p de n tel que pour tout entier k, les conditions $k \mid n$ et $k \equiv 1 \pmod p$ impliquent $k = 1$ n'est pas simple.
   Ce critère permet de montrer que (pas moins de) 451 entiers $\leqslant 660$ ne donnent jamais lieu à un groupe simple.
3. Soit G un groupe fini simple non abélien de cardinal n et p un diviseur premier de n. Établir que $n \mid \dfrac{n_p!}{2}$ (on pourra penser à utiliser une action bien choisie et à composer par la signature). En déduire un nouveau critère permettant d'éliminer de nouveaux entiers.
   Ce critère permet d'éliminer 25 nouveaux entiers parmi les 61 qui nous restaient. Il reste donc 36 cardinaux possibles : 30, 56, 90, 105, 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.
4. Dans cette question, on se donne un groupe G d'ordre n que l'on suppose simple et on notera $\min_p(n)$ la plus petite valeur de n_p compatible avec les théorèmes de Sylow et la question **3.** Montrer qu'alors, on a au moins
$$1 + \sum_{\substack{p \mid n \\ p \| n}} (p-1)\min_p(n) + \sum_{\substack{p^v \| n \\ v \geqslant 2 \mid n}} p^v$$
éléments dans G. En déduire un nouveau critère pour éliminer de nouveaux entiers et justifer que l'on élimine ainsi tous les groupes d'ordre p^2q et pqr pour p, q, r des nombres premiers distincts.
   On élimine ainsi 13 nouveaux entiers et il nous en reste 23 : 90, 120, 144, 180, 210, 240, 252, 264, 288, 315, 336, 396, 400, 420, 432, 480, 525, 528, 540, 560, 576, 612 et 630.
5. Soit p un nombre premier impair. Préciser le cardinal des p-Sylow de $\mathfrak{A}_{p+1}$ et montrer que leur normalisateur sont d'ordre $\dfrac{p(p-1)}{2}$.
   On pourra commencer par vérifier que le nombre de p-Sylow de $\mathfrak{A}_{p+1}$ est donné par $[\mathfrak{A}_{p+1} : N_{\mathfrak{A}_{p+1}}(P)]$ pour tout p-Sylow P et relier le nombre de p-Sylow de $\mathfrak{A}_{p+1}$ au nombre déléments d'ordre p de $\mathfrak{A}_{p+1}$.
   Soit alors G un groupe simple non abélien d'ordre n et p un diviseur premier de n. Montrer alors que, si $n_p = p+1$, $n \mid \dfrac{(p-1)p(p+1)}{2}$.
   On élimine alors 8 nouveaux entiers. Il en reste 16 : 144, 180, 210, 240, 252, 288, 315, 400, 420, 432, 480, 525, 540, 576, 612 et 630.

Le cas des groupes d'ordre $2^\alpha p^\beta$ pour $\alpha \leqslant 5$ (ainsi que 480 et 576)

6. Montrer que si G est un groupe fini et $H \leqslant G$, alors $[N_G(H), C_G(H)] \mid \mathrm{Aut}(H)$.
7. Soit G un p-groupe et H un sous-groupe propre de G. À l'aide de l'équation aux classes pour l'action de H par translation à gauche sur G/H, montrer que $\#N_G(H) > \#H$.
8. Soit G un groupe, $P \in \mathrm{Syl}_p(G)$ et $Q \leqslant G$ un p-sous-groupe. Établir que $Q \cap N_G(P) = Q \cap P$.
   Indication : On pourra considérer la restriction de la surjection canonique $N_G(P) \to N_G(P)/P$ à Q.

9. Soit G un groupe de cardinal n et p un nombre premier divisant n. Montrer que si $n_p \not\equiv 1 \pmod{p^2}$, alors G possède deux p-Sylow P et P' pour lesquels $[P, P \cap P'] = p$. Montrer en utilisant la question prćédente qu'alors $\#N_G(P \cap P') = \#P \times m$ pour un certain entier $m > p$.
*Indication : On pourra considérer l'action d'un p-Sylow P sur $Syl_p(G) \setminus \{P\}$ et utiliser la question **7**. Puis, on pourra montrer que $N_P(P \cap P') = P$ et que $N_G(P \cap P')$ contient l'ensemble PP'.*

10. Utiliser la question précédente et la question **3.** pour éliminer l'entier 480.

11. Montrer que si G est d'ordre 288 ou 576 est simple, alors G possède deux 3-Sylow distincts T et T' d'intersection non triviale.

12. En utilisant les questions **6.** et **9.**, montrer que $\#C_G(I) \mid 18$, que $C_G(I)$ contient un élément c d'ordre 6. Enfin, en considérant l'action de G sur l'ensemble de ses 2-Sylow, montrer qu'on aboutit à une contradiction en regardant la permutation $\varphi(c)$ où $\varphi : G \to \mathfrak{A}(\mathrm{Syl}_2(G))$ est le morphisme associé à cette action.
Indication : On pourra montrer que $N_G(S)$ est un 2-groupe pour tout 2-Sylow S puis en dd́uire que $\varphi(c)$ n'a pas de point fixe. On étudiera ensuite les décompositions de $\varphi(c)$ en produit de k-cycles disjoints possibles.

13. Montrer qu'il n'existe pas de groupe simple d'ordre $2^\alpha p^\beta$ pour $\alpha \leqslant 5$. On pourra étudier les valeurs possibles de n_p et utiliser **9**.
Cela permet d'éliminer 144, 400 et 432. Il reste donc dix entiers qui résistent encore et toujours : 180, 210, 240, 252, 315, 420, 525, 540, 612 et 630.

Le transfert

Soit G un groupe fini.

14. Soit H un sous-groupe de G d'indice n. On note $x_1, \dots, x_n \in G$ un ensemble de représentants de G modulo H. L'action de G sur G/H induit une action de G sur $\{1, \dots, n\}$ et, pour tout $g \in G$ et $i \in \{1, \dots, n\}$, il existe $h_{i,g\cdot i} \in H$ tel que $g x_i = x_{g\cdot i} h_{i,g\cdot i}$. On note enfin $\pi : H \to H/D(H)$ la projection canonique. Établir que la formule

$$V(g) = \pi\left(\prod_{i=1}^{n} h_{i,g\cdot i}\right)$$

définit un morphisme de groupes $G \to H/D(H)$ indépendant du choix des représentants.

15. Avec les notations précédentes, soit $h \in H$. On considère l'action de $\langle h \rangle$ sur $X = G/H$ et on note $g_1, \dots, g_r$ des éléments de G tels que les classes $[g_i]$ des g_i dans X forment un ensemble de représentants pour cette action. Pour tout $i \in \{1, \dots, r\}$, on note n_i l'entier naturel minimal non nul tel que $h^{n_i} \cdot [g_i] = [g_i]$. Montrer que

$$V(h) = \pi\left(\prod_{i=1}^{r} g_i^{-1} h^{n_i} g_i\right).$$

16. Soient S un p-Sylow de G et $A, b \subseteq S$ des parties stables par conjugaison dans S. Montrer que si A et B sont conjuguées dans G, alors elles le sont dans $N_G(S)$ (on pourra considérer deux p-Sylow de $N_G(A)$).

17. Soit S un p-Sylow de G tel que $S \subseteq Z(N_G(S))$. Montrer que le morphisme $V : G \to S$ défini en **17.** est surjectif. En déduire qu'il existe un sous-groupe distingué H de G tel que S soit isomorphe à G/H.

18. En déduire que si G est simple non cyclique, alors le cardinal de G est divisible par 12 ou son plus petit facteur premier apparaît au moins au cube dans sa décomposition en facteurs premiers.
On élimine ainsi 210, 315, 525 *et 630. Il ne reste donc plus que 6 réfractaires : 180, 240, 252, 420, 540 et 612.*

La p-nilpotence de Burnside

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 (avec p' premier distinct de p) distingué N par n'importe lequel de ses p-Sylow. Un tel sous-groupe N est appelé *p-complément distingué*.

19. À quelle(s) condition(s) un groupe p-nilpotent peut-il être simple ?

20. Soient G un groupe fini, p un nombre premier et P un p-Sylow abélien. Montrer que si $x, y \in G$ sont conjugués dans G, ils le sont aussi dans $N_G(P)$.

21. Soit G un groupe fini, p un nombre premier et P un p-Sylow de G. Si $N_G(P) = C_G(P)$, montrer que G est p-nilpotent. On pourra établir que dans ce cas, le transfert $G \to P$ est surjectif restreint à P.

22. Éliminer 252 et 180.

23. En utilisant la structure des groupes d'ordre pq, éliminer 540 et 240.
Il ne reste finalement que deux survivants : 420 et 612 !

Le cas 420

On suppose qu'il existe un groupe simple d'ordre 420.

24. Montrer que si S est un 7-Sylow, alors $C_G(S)$ est d'ordre 14 ou 28 et qu'il existe un élément c d'ordre 14. Montrer que c ne normalise aucun autre 7-Sylow et conclure via l'action de G sur $\mathrm{Syl}_7(G)$.
On pourra montrer que cette action induit un morphisme $\varphi : G \to \mathfrak{A}_{15}$ et étudier $\varphi(c)$.

Le cas 612

On suppose qu'il existe un groupe simple d'ordre 612.

24. Montrer que G admet au moins deux 3-Sylow T et T' d'intersection non triviale. On pose alors $I = T \cap T'$. Montrer alors que $C_G(I)$ contient un élément c d'ordre 6. En considèrant l'action de G sur $\mathrm{Syl}_{17}(G)$, établir que c^3 normalise 6 17-Sylow de G. Soit S_{17} un 17-Sylow normalisé par c. Faire agir S par conjugaison sur $\mathrm{Syl}_{17}(G) \setminus \{S_{17}\}$et en déduire que G est 17-nilpotent. Conclure.
Indication : On pourra établir qu'il existe pour tout S', S'' normalisés par S_{17}, un élément $s \in S_{17}$ tel que $S'' = sS's^{-1}$ puis montrer que $[c^3, s] \in N_G(S'')$.

Existence de groupe(s) simple(s) d'ordres 60, 168, 360, 504, 660

25. Justifier qu'il existe un groupe simple d'ordre 60 et d'ordre 360.

▶ **Compléments. –** On peut montrer [1] que $\mathfrak{A}_5 \cong \mathrm{PSL}_2(\mathbf{F}_4) \cong \mathrm{PSL}_2(\mathbf{F}_5)$ est le seul groupe simple d'ordre 60 (à isomorphisme pr
'es) et que $\mathfrak{A}_6 \cong \mathrm{PSL}_2(\mathbf{F}_9)$ est le seul sous-groupe simple d'ordre 360 (à isomorphisme près). On peut par ailleurs montrer [2] que $\mathrm{PSL}_n(k)$ est simple pour tout $n \geqslant 2$ et k corps fini sauf pour $n = 2$ et $k = \mathbf{F}_2$ ou $\mathbf{F}_3$. Cela fournit un unique (à isomorphisme près) groupe simple d'ordre 168, à savoir $\mathrm{PSL}_2(\mathbf{F}_7) \cong \mathrm{PSL}_3(\mathbf{F}_2)$, un unique (à isomorphisme près) groupe simple d'ordre 504, à savoir $\mathrm{PSL}_2(\mathbf{F}_8)$ et un unique (à isomorphisme près) groupe simple d'ordre 660, à savoir $\mathrm{PSL}_2(\mathbf{F}_{11})$. Je rappelle que la classification (à isomorphisme près) des groupes finis simples est connue [3] et que les groupes simples se répartissent en quatre familles : les groupes abéliens d'ordre premier, les groupes alternés pour $n \geqslant 5$, les groupes de type Lie et les groupes sporadiques. On peut en réalité établir qu'à chaque fois, un groupe simple de cardinal n est unique à isomorphisme près (et alors on a ce que l'on appelle des isomorphismes exceptionnels entre deux groupes de deux familles différentes lorsque les cardinaux co^incident comme par exemple $\mathfrak{A}_5 \cong \mathrm{PSL}_2(\mathbf{F}_4) \cong \mathrm{PSL}_2(\mathbf{F}_5)$) sauf dans deux cas où on a deux classes d'isomorphismes : $\mathfrak{A}_8 \cong \mathrm{PSL}_4(\mathbf{F}_2) \ncong \mathrm{PSL}_3(\mathbf{F}_4)$ d'ordre [4] 20160 et les groupes $\mathrm{P}\Omega_{2n+1}(\mathbf{F}_q) \ncong \mathrm{PSp}_{2n}(\mathbf{F}_q)$ pour tout $n \geqslant 3$ et q puissance d'un nombre premier impair d'ordre [5]

$$q^{n^2} \prod_{i=1}^{n} \frac{q^{2i} - 1}{2}.$$

1. Voir par exemple le TD 2 de l'année 2020–2021 sur la page web de D. Harari pour les cas d'ordre 60, 168 et 360 mais aussi pour quelques isomorphismes exceptionnels.
2. Je vous renvoie par exemple au Perrin pour cela.
3. Mais difficile !
4. Vous pourrez en trouver une démonstration dans l'ouvrage *Histoires hédonistes des groupes* de Caldero et .
5. Voir ici pour des références.