Exercices Algèbre - Groupes II

Exercice 1.

1. Montrer que les groupes
$$\mathbf{Z}/12\mathbf{Z}\times\mathbf{Z}/90\mathbf{Z}\times\mathbf{Z}/25\mathbf{Z} \quad \text{et} \quad \mathbf{Z}/100\mathbf{Z}\times\mathbf{Z}/30\mathbf{Z}\times\mathbf{Z}/9\mathbf{Z}$$
sont isomorphes.
2. Montrer qu'un groupe abélien fini non cyclique possède un sous-groupe isomorphe à $\mathbf{Z}/p\mathbf{Z}\times\mathbf{Z}/p\mathbf{Z}$ pour un certain nombre premier p.
3. Combien y a-t-il de groupes abéliens de cardinal 360 ? Plus généralement de cardinal n avec $n \geqslant 1$ un entier naturel ?
4. Quels sont les entiers n tels que le groupe $(\mathbf{Z}/n\mathbf{Z})^\times$ soit cyclique ? Décomposer le groupe $G = (\mathbf{Z}/187\mathbf{Z})^\times$ sous la forme donnée par le théorème de structure des groupes abéliens de type fini.

Solution.

1. Par le théorème chinois, ces deux groupes sont isomorphes à
$$(\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/4\mathbf{Z})\times(\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/9\mathbf{Z})\times(\mathbf{Z}/5\mathbf{Z}\times\mathbf{Z}/25\mathbf{Z})\,.$$
Il s'agit de l'écriture en composantes p-primaires tandis que l'écriture en facteurs invariants est
$$\mathbf{Z}/30\mathbf{Z}\times\mathbf{Z}/900\mathbf{Z}.$$
2. On utilise le théorème de structure des groupes abéliens finis qui garantit que
$$G \cong \mathbf{Z}/d_1\mathbf{Z}\times\cdots\times\mathbf{Z}/d_r\mathbf{Z}$$
pour un certain $r \in \mathbf{N}$ et $d_i \geqslant 2$ pour $i \in \{1,\dots,r\}$ et $d_i \mid d_{i+1}$ pour $i \in \{1,\dots,r-1\}$. Comme G n'est pas cyclique, on a $r \geqslant 2$ et pour $p \mid d_1$ premier, $p \mid d_i$ pour tout $i \in \{1,\dots,r\}$. On sait alors que $\mathbf{Z}/p\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}/d_i\mathbf{Z}$ pour tout $i \in \{1,\dots,r\}$. On obtient ainsi un sous-groupe de G isomorphe à $(\mathbf{Z}/p\mathbf{Z})^r$ qui contient évidemment une copie de $\mathbf{Z}/p\mathbf{Z}\times\mathbf{Z}/p\mathbf{Z}$.
3. On a $360 = 2^3\times3^2\times5$. La composante 2-primaire d'un tel groupe (à isomorphisme près) est donc un groupe abélien d'ordre 8, à savoir $\mathbf{Z}/8\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/4\mathbf{Z}$ ou $(\mathbf{Z}/2\mathbf{Z})^3$. De même, la composante 3-primaire est isomorphe à $\mathbf{Z}/9\mathbf{Z}$ ou $(\mathbf{Z}/3\mathbf{Z})^2$ et la composante 5-primaire est isomorphe à $\mathbf{Z}/5\mathbf{Z}$. On obtient ainsi 6 classes d'isomorphismes de groupes abéliens de cardinal 360, à savoir
$$\begin{aligned}
\mathbf{Z}/8\mathbf{Z}\times\mathbf{Z}/9\mathbf{Z}\times\mathbf{Z}/5\mathbf{Z} &\cong \mathbf{Z}/360\mathbf{Z}\\
\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/4\mathbf{Z}\times\mathbf{Z}/9\mathbf{Z}\times\mathbf{Z}/5\mathbf{Z} &\cong \mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/180\mathbf{Z}\\
(\mathbf{Z}/2\mathbf{Z})^3\times\mathbf{Z}/9\mathbf{Z}\times\mathbf{Z}/5\mathbf{Z} &\cong (\mathbf{Z}/2\mathbf{Z})^2\times\mathbf{Z}/90\mathbf{Z}\\
\mathbf{Z}/8\mathbf{Z}\times(\mathbf{Z}/3\mathbf{Z})^2\times\mathbf{Z}/5\mathbf{Z} &\cong \mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/120\mathbf{Z}\\
\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/4\mathbf{Z}\times(\mathbf{Z}/3\mathbf{Z})^2\times\mathbf{Z}/5\mathbf{Z} &\cong \mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/60\mathbf{Z}\\
(\mathbf{Z}/2\mathbf{Z})^3\times(\mathbf{Z}/3\mathbf{Z})^2\times\mathbf{Z}/5\mathbf{Z} &\cong \mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/30\mathbf{Z}.
\end{aligned}$$
Dans le cas général, si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec $r \in \mathbf{N}^\times$, $p_1,\dots,p_r$ des nombres premiers distincts et $\alpha_i \geqslant 1$. Par le théorème de structure, on sait que les classes d'isomorphismes de groupes abéliens d'ordre n sont caractérisées par la liste des facteurs invariants $(d_1,\dots,d_s)$ pour un certain $s \in \mathbf{N}$ et $d_i \geqslant 2$ pour $i \in \{1,\dots,s\}$ et $d_i \mid d_{i+1}$ pour $i \in \{1,\dots,s-1\}$ et $d_1\cdots d_s = n$. Par conséquent, chaque d_i se décompose sous la forme $d_i = p_1^{\alpha_{i,1}}\cdots p_r^{\alpha_{i,r}}$ avec les contraintes que pour tout $i \in \{1,\dots,s-1\}$ et tout $j \in \{1,\dots,r\}$, $\alpha_{i,j} \leqslant \alpha_{i+1,j}$ et $\sum_{i=1}^{s} \alpha_{i,j} = \alpha_j$. Il s'ensuit que le nombre de choix possibles est de $\prod_{j=1}^{r} p(\alpha_j)$ où $p(.)$ désigne la fonction nombre de partitions croissantes d'entiers strictement positifs.
4. On pose $n = \prod_p p^{\alpha_p}$ la décomposition de n en produit de facteurs premiers. On sait alors d'après le cours que
$$(\mathbf{Z}/n\mathbf{Z})^\times \cong (\mathbf{Z}/2^{\alpha_2}\mathbf{Z})^\times \times \prod_{\substack{p\neq2\\ \alpha_p\geqslant1}} \mathbf{Z}/p^{\alpha_p-1}(p-1)\mathbf{Z}$$

Or, on sait que

$$(\mathbf{Z}/2^{\alpha_2}\mathbf{Z})^\times = \begin{cases} \{0\} \text{ si } \alpha_2 = 1 \\ \mathbf{Z}/2\mathbf{Z} \text{ si } \alpha_2 = 2 \\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{\alpha_2-2}\mathbf{Z} \text{ si } \alpha_2 \geqslant 3. \end{cases}$$

Un groupe cyclique ne pouvant contenir plus d'un élément, d'ordre 2, on voit que $(\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique si, et seulement si, $n = p^\alpha$ ou $n = 2p^\alpha$ avec p un nombre premier impair et $\alpha \geqslant 0$ ou $n = 4$.
Pour finir, on a $187 = 11 \times 17$ de sorte que

$$(\mathbf{Z}/187\mathbf{Z})^\times \cong \mathbf{Z}/10\mathbf{Z} \times \mathbf{Z}/16\mathbf{Z} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/80\mathbf{Z}.$$

Exercice 2. Soient G un groupe et H un sous-groupe de G d'indice fini m. On note G/H l'ensemble des classes de G modulo H (ceci n'est pas un groupe en général). Pour $g \in G$, on note $h_g : G/H \to G/H$ l'application $aH \mapsto gaH$.

1. Montrer que h_g est une bijection, et que l'application h qui envoie g sur h_g est un homomorphisme de G dans $\mathfrak{S}(G/H)$.
2. Montrer que $[G : \mathrm{Ker}\,(h)]$ divise $m!$.
3. Montrer que $\mathrm{Ker}\,(h)$ est contenu dans H.
4. Montrer que $[H : \mathrm{Ker}\,(h)]$ divise $(m-1)!$.
5. Application 1 : montrer que si H est d'indice 2 dans G, alors H est distingué dans G.
6. Application 2 : montrer que si G est un p-groupe, et si H est d'indice p dans G, alors H est distingué dans G.
7. Application 3 : Supposons que G est fini et que $m = [G : H]$ est le plus petit diviseur premier de l'ordre de G. Montrer que H est distingué dans G.

Solution.

1. Il est clair que h_g est injective car si $gaH = ga'H$, alors $a^{-1}a' \in H$ et $aH = a'H$ et de même pour la surjectivité car $h_g(g^{-1}aH) = aH$. On a donc bien une bijection [1]. Le fait qu'on ait un morphisme est clair aussi car $h_g \circ h_{g'} = h_{gg'}$. On fait en réalité ici agir G sur G/H.
2. Attention ici qu'on n'a pas supposé G fini et donc $[G : \mathrm{Ker}(h)]$ n'est pas donné par $\#G/\#\mathrm{Ker}(h)$. Le théorème de factorisation fournit un morphisme injectif $\tilde{h} : G/\mathrm{Ker}(h) \to \mathfrak{S}(G/H) \cong \mathfrak{S}_m$. On peut ainsi identifier $G/\mathrm{Ker}(h)$ à un sous-groupe de $\mathfrak{S}_m$ et en déduire par Lagrange que $[G : \mathrm{Ker}(h)] \mid m!$.
3. Soit $g \in \mathrm{Ker}(h)$. On a alors pour tout $a \in G$, $gaH = aH$ qui implique immédiatement que $g \in H$.
4. On considère de façon analogue $h_2 : H \to \mathfrak{S}(G/H \setminus \{H\})$ définie pour $g \in H$ par

$$h_2(g) : \begin{array}{ccc} G/H \setminus \{H\} & \longrightarrow & G/H \setminus \{H\} \\ aH & \longmapsto & gaH. \end{array}$$

   On vérifie de même qu'il s'agit bien d'une bijection bien définie et que h_2 est un morphisme de groupes de même noyau que h. Le même raisonnement qu'en question **2.** fournit alors la conclusion souhaitée $[H : \mathrm{Ker}(h)] \mid (m-1)!$ car $\mathfrak{S}(G/H \setminus \{H\}) \cong \mathfrak{S}_{m-1}$. En fait, on a restreint l'action précédente en une action de H sur G/H et utilisé le fait que puisque H est un point fixe de G/H pour cette action, cela donne lieu à une action de H sur $G/H \setminus \{H\}$ de même noyau que h.

   Noter qu'en TD, l'un d'entre vous a suggéré d'utiliser le troisième théorème d'isomorphisme. Je rappelle que ce théorème garantit que si $N \lhd G$ et $H \lhd G$ avec $N \leqslant H$, alors $H/N \lhd G/N$ et l'application $f : G/N \to G/H$ qui à gN associe gH est bien définie de noyau H/N et passe au quotient pour donner un isomorphisme $(G/N)/(H/N) \cong G/H$. L'hypothèse que les deux groupes sont distingués est importante sinon G/H ou G/N n'a pas de structure de groupe et H/N n'est pas nécessairement distingué dans G/N. Par ailleurs, comme vous le verrez dans le cours, le fait qu'on ait un isomorphisme $G/H \cong N$ **n'implique pas** que $G \cong H \times N$ et en particulier ici on n'a pas nécessairement $G/N \cong G/H \times H/N$ (penser par exemple à $G = \mathbf{H}_8$, $H = Z(\mathbf{H}_8) \cong \mathbf{Z}/2\mathbf{Z}$ et $N = G/H \cong (\mathbf{Z}/2\mathbf{Z})^2$. En revanche, on a bien dans tous les cas une **bijection** entre G/N et $G/H \times H/N$. Cela est évident par cardinalité si G est fini mais ici ce n'est pas dans les hypothèses et il faut alors remarquer que l'application ensembliste surjective (l'ensemble d'arrivée n'étant pas nécessairement un groupe) $f : G/\mathrm{Ker}(h) \to G/H$ qui à $g\mathrm{Ker}(h)$ associe gH est bien définie et passe au quotient pour la relation donnée par le groupe $H/\mathrm{Ker}(h)$ pour donner une application surjective (par surjectivité de f). En effet, si $gN = g'N$ avec $g'^{-1}g \in H$, alors on a bien $gH = g'H$. L'application quotient est alors injective si, et seulement si, $gH = g'H$ implique que gN et $g'N$ sont en relation pour la relation d'équivalence associée à H/N. Cela est clairement le cas et fournit la bijection souhaitée. En conclusion, il faut être prudent avec ce théorème d'isomorphisme et dans cette question, on ne pouvait pas l'utiliser directement mais uniquement en redémontrant une version "bijection" puisqu'un des sous-groupes, à savoir H, n'est pas supposé distingué et que G n'est pas supposé fini. Une fois la **bijection** $G/\mathrm{Ker}(h) \cong G/H \times H/\mathrm{Ker}(h)$ obtenue, on peut alors dire que $[G : \mathrm{Ker}(h)] = [G : H] \times [H : \mathrm{Ker}(h)]$ et donc $[G : H] \times [H : \mathrm{Ker}(h)] = m \times [H : \mathrm{Ker}(h)] \mid m!$ et finalement $[H : \mathrm{Ker}(h)] \mid (m-1)!$.
5. On a $m = 2$ et la question **4.** fournit alors que $[H : \mathrm{Ker}(h)] = 1$ soit $H = \mathrm{Ker}(h)$. Ainsi $H \lhd G$.

1. On pouvait aussi utiliser que les espaces d'arrivée et de départ avait le même cardinal.

6. On a donc que G et H sont finis de cardinal une puissance de p. Par **4.**, on a donc $\#H \mid (p-1)!\#\mathrm{Ker}(h)$. Mais $\#H$ est premier avec $(p-1)!$ donc $\#H \mid \#\mathrm{Ker}(h)$ et la question **3.** permet alors de conclure à nouveau à l'égalité $H = \mathrm{Ker}(h)$. Ainsi $H \lhd G$.
7. De même, $\#H \mid (m-1)!\#\mathrm{Ker}(h)$ et $\#H = \#G/m$ ne contient que des facteurs premiers $\geqslant m$ et donc $\#H$ est premier avec $(m-1)!$ et on conclut comme en question précédente.

Exercice 3. Soient G un groupe et H un sous-groupe d'indice fini $n \geqslant 2$.

1. Montrer qu'il existe un sous-groupe distingué K de G, contenu dans H, tel que $[G : K]$ divise $n!$. (On pourra considérer l'action de G sur G/H).
2. On suppose que G est fini. Montrer que G n'est pas la réunion des conjugués gHg^{-1} de H.
3. Montrer que **2.** reste vrai si G est infini.
4. Est-ce que **2.** reste vrai si on ne suppose plus que $[G : H]$ est fini ?
5. Soit G un groupe fini agissant transitivement sur un ensemble fini X tel que $\#X \geqslant 2$. Montrer qu'il existe $g \in G$ ne fixant aucun point de X.
6. Soit $k \geqslant 5$ un entier et soit H un sous-groupe de $\mathfrak{S}_k$ d'indice compris entre 2 et $k-1$. Montrer que $H = \mathfrak{A}_k$. On admettra le fait que les seuls sous-groupes distingués de $\mathfrak{S}_k$ sont $\{1\}$, $\mathfrak{A}_k$ et $\mathfrak{S}_k$.

Solution.

1. Faisant agir G sur G/H, on obtient un morphisme $f : G \to \mathfrak{S}(G/H) \cong \mathfrak{S}_n$ dont le noyau convient.
2. On a clairement que
$$\bigcup_{g\in G} gHg^{-1} = \bigcup_{\overline{g}\in G/H} gHg^{-1}$$
où gHg^{-1} ne dépend que de la classe de g dans G/H car $(gh)H(gh)^{-1} = gHg^{-1}$. Il vient par conséquent que (bien faire attention ici que e appartient à chacun des conjugués)
$$\begin{aligned}\#\left(\bigcup_{g\in G} gHg^{-1} \smallsetminus \{e\}\right) &= \#\left(\bigcup_{\overline{g}\in G/H} gHg^{-1} \smallsetminus \{e\}\right)\\ &\leqslant \sum_{\overline{g}\in G/H} \#\left(gHg^{-1} \smallsetminus \{e\}\right)\\ &\leqslant \sum_{\overline{g}\in G/H} \#(H \smallsetminus \{e\}) \leqslant \#(G/H)(\#H - 1) = \#G\left(1 - \frac{1}{\#H}\right) < \#G - 1\end{aligned}$$
car $H \neq G$ si bien que
$$\#\left(\bigcup_{g\in G} gHg^{-1} \smallsetminus \{e\}\right) < \#(G \smallsetminus \{e\}) \quad \text{et} \quad \bigcup_{g\in G} gHg^{-1} \neq G.$$
3. On dispose toujours de l'action de G sur G/H qui fournit un morphisme $\varphi : G \to \mathfrak{S}(G/H)$ avec $\mathfrak{S}(G/H)$ un groupe fini. On note alors K le sous-groupe de $\mathfrak{S}(G/H)$ des bijections fixant H et on a alors que $\varphi(H)$ est un sous-groupe de K. Par ailleurs, la transitivité de l'action garantit que $\varphi(G)$ n'est pas contenu dans K donc $\varphi(H)$ est un sous-groupe strict du groupe fini $\varphi(G)$ et
$$\bigcup_{g\in G} \varphi(g)\varphi(H)\varphi(g)^{-1} \neq \varphi(G).$$
Cela entraîne alors nécessairement que
$$\bigcup_{g\in G} gHg^{-1} \neq G.$$
4. Le résultat devient alors faux en général. On pose $G = \mathrm{GL}_n(\mathbf{C})$ et $H = T_n(\mathbf{C}) \cap G$ le sous-groupe des matrices triangulaires supérieures inversibles. On sait alors que toute matrice de G est trigonalisable, autrement dit conjuguée à une matrice de $T_n(\mathbf{C})$ de sorte que
$$\bigcup_{g\in G} gHg^{-1} = G$$
mais H est d'indice infini dans[2] G. Pour voir que l'indice est infini, on peut par exemple utiliser le fait que toute matrice M de $GL_n(\mathbf{C})$ s'écrit sous la forme $M = \exp(N) = \left(\exp\left(\frac{N}{n}\right)\right)^n$ et donc toute matrice de $GL_n(\mathbf{C})$ est une puissance n-ième pour tout entier naturel n. Supposons alors que $GL_n(\mathbf{C})$ possède un quotient fini, disons d'ordre r. Pour toute matrice $M \in GL_n(\mathbb{C})$, il existe B telle que $M = B^r$ et ainsi la classe de M est triviale si bien qu'un tel quotient est nécessairement trivial. Puisque $T_n(\mathbf{C}) \neq GL_n(\mathbf{C})$, on en déduit qu'il est d'indice infini.

2. Un autre exemple est $G = SO_3(\mathbf{R})$ et $H = SO_2(\mathbf{R})$ comme sous-groupe des rotations autour de l'axe des abscisses. Toute rotation étant conjuguée à une rotation d'axe fixé, cela fournit bien un autre contre-exemple.

5. On choisit $x_0 \in X$ et on note $H = \mathrm{Stab}_G(x_0)$. On a alors que H est un sous-groupe de G différent de G (sinon $X = \{x_0\}$ par transitivité). On peut donc trouver $g_0 \in G, g_0 \notin \bigcup_{g\in G} gHg^{-1}$. Soit alors $x \in X$. On sait qu'il existe $g \in G$ tel que $x = g \cdot x_0$ et alors $\mathrm{Stab}_G(x) = gHg^{-1}$ donc par construction $g_0 \notin \mathrm{Stab}_G(x)$, ce qui signifie que $g_0 \cdot x \neq x$ ce qui conclut la preuve.
6. Par **1.**, H contient un sous-groupe distingué K de $\mathfrak{S}_k$ d'indice divisant $[\mathfrak{S}_k : H]!$. Comme H n'est pas d'indice 1, ce groupe ne peut pas être $\mathfrak{S}_k$ tout entier sinon $H = \mathfrak{S}_k$ serait d'indice 1. Ce sous-groupe est donc (puisque $k \geqslant 5$) soit le groupe trivial soit le groupe alterné. Supposons qu'il s'agisse du groupe trivial. On a alors que $k!$ divise $[\mathfrak{S}_k : H]! \in \{2!, \dots, (k-1)!\}$ ce qui est absurde donc $K = \mathfrak{A}_k$ et $K \subseteq H$ donc $[G : H] \leqslant [G : K]$ si bien que $[G : H] = 2$ et $H = \mathfrak{A}_k$.

Exercice 4.

1. Soit G un groupe tel que $G/Z(G)$ est cyclique. Rappeler pourquoi G est abélien. Le résultat tient-il toujours si l'on suppose seulement que $G/Z(G)$ est abélien ?
2. Justifier que la probabilité que deux éléments d'un groupe non abélien commutent est $\leqslant \frac{5}{8}$.
3. Montrer qu'un p-groupe d'ordre p^n possède des sous-groupes d'ordre p^i pour tout $i \in \{0, \dots, n\}$ (on peut même imposer la condition que ces sous-groupes soient distingués comme dans l'exercice 6 du Perrin).
4. Soient p un nombre premier et P un p-Sylow de G. Montrer que $P \cdot Z(G)$ est un sous-groupe de G, et que $(P \cdot Z(G))/Z(G)$ est un p-Sylow de $G/Z(G)$.
5. Montrer que ceci induit une bijection entre les p-Sylow de G et les p-Sylow de $G/Z(G)$.

Solution.

1. On note $\overline{a}$ un générateur de $G/Z(G)$. Tout élément de G est alors de la forme $a^m z$ avec $m \in \mathbf{N}$ et $z \in Z(G)$ ce qui permet de conclure. Le résultat tombe en défaut si l'on suppose seulement abélien comme on le voit avec le contre-exemple des quaternions.
2. En effet, si G est non abélien, alors par l'exercice 7, $G/Z(G)$ ne peut pas être cyclique est est donc de cardinal au moins 4. Si l'on note $z = \#Z(G)$ et $n = \#G$, alors $n \geqslant 4z$. Si maintenant $x \in Z(G)$, pour tout $y \in G$, x et y commutent. Soit alors $x \in G \setminus Z(G)$. Les éléments y qui commutent avec x sont les éléments du centralisateur de x pour l'action par conjugaison. On obtient alors un sous-groupe strict car x n'est pas central, de cardinal $\leqslant \frac{n}{2}$. On obtient finalement que le nombre de paires $(x, y) \in G^2$ qui commutent vérifie
$$\leqslant zn + (n-z)\frac{n}{2} = \frac{nz}{2} + \frac{n^2}{2} \leqslant \frac{n^2}{8} + \frac{n^2}{2} = \frac{5}{8}n^2.$$
Il reste à diviser par $\#G^2 = n^2$ pour obtenir que la probabilité est bien $\leqslant \frac{5}{8}$. Noter que cette probabilité est optimale et est notamment pour les groupes[3] $\mathbf{H}_8$ et $\mathbf{D}_4$.
3. On raisonne par récurrence sur n. Pour $n = 0$, c'est évident. Supposons la propriété connue pour les groupes d'ordre p^n et soit G un groupe d'ordre p^{n+1}. Si $i = 0$, il n'y a rien à faire et on peut supposer que $i \geqslant 1$. On sait que $Z(G)$ est non trivial et en tant que p-groupe, il admet un élément d'ordre p donc un sous-groupe Z d'ordre p. Comme Z est central, il est distingué et on note $\pi : G \to G/Z$ la surjection canonique. Par hypothèse, G/Z est de cardinal p^n et possède donc un sous-groupe H' de cardinal p^{i-1}. Il est alors clair que $H = \pi^{-1}(H')$ est un sous-groupe de G de cardinal p^i ce qui conclut la preuve.
4. Par le théorème d'isomorphisme, on a que $PZ(G)/Z(G) \cong P/(P \cap Z(G))$ et est un sous-groupe de $G/Z(G)$ qui s'identifie à $\pi(P)$ où $\pi : G \to G/Z(G)$ est la surjection canonique. Ce qui suit est à rapprocher du théorème 2.13 et serait valable en remplaçant $Z(G)$ par n'importe quel sous-groupe H distingué dans G. Commençons par établir que $P \cap Z(G)$ est un p-Sylow de $Z(G)$. Le groupe P est un p-Sylow de $PZ(G)$ car contenu dans $PZ(G)$ et un p-groupe de cardinal maximal. On note alors $\#P = p^n$ et $\#PZ(G) = p^n s$ avec $p \nmid s$. On écrit alors $\#Z(G) = p^m r$ avec $p \nmid r$, $m \leqslant n$ et $r \mid s$. Par le théorème d'isomorphisme, on a $\#(P \cap Z(G)) = \#P\#Z(G)/\#PZ(G) = p^m \frac{r}{s}$. Mais $P \cap Z(G)$ est un p-groupe donc $s = r$ et $P \cap Z(G)$ est un p-Sylow de $Z(G)$. Posons alors $\#G = p^n t$ avec $p \nmid t$ et $s \mid t$. On a alors $\#(G/Z(G)) = p^{n-m}\frac{t}{s}$. Or, $PZ(G)/Z(G)$ est d'ordre p^{n-m}, il s'agit donc d'un p-Sylow de $G/Z(G)$.
5. On considère alors l'application bien définie f des p-Sylow de G dans les p-Sylow de $G/Z(G)$ qui à P associe $PZ(G)/Z(G)$ et vérifions qu'il s'agit bien d'une bijection. Définissons pour ce faire la bijection réciproque.
Soit à présent S un p-Sylow de $G/Z(G)$. On pose alors $H = \pi^{-1}(S)$. On remarque que $G/H \to \tilde{G}/S$ est une bijection[4] avec $\tilde{G} = G/Z(G)$ si bien que si l'indice de S dans $\tilde{G}$ est premier à p, il en est de même de celui[5] de H dans G. Ainsi un p-Sylow de H est un p-Sylow de G. Soit alors P un p-Sylow de H (et donc de G). Par ailleurs, par définition de H, on a $Z(G) \lhd H$ et ainsi le sous-groupe $PZ(G) \leqslant H$. On a aussi que $\pi(P) = PZ(G)/Z(G)$ est un p-Sylow de $\tilde{G}$ inclus dans S, donc égal à S. Ainsi $\pi(P) = S = \pi(H)$ et

3. Un autre exercice intéressant utilisant la formule de Burnside est de montrer que la probabilité cherchée est de $\frac{k}{n}$ où k est le nombre de classes de conjugaison et $n = \#G$. On peut essayer de majorer cela puisqu'a priori on ne connaît pas forcément k et une inégalité classique (dont la preuve utilise de choses très simples issues de la théorie des représentations) garantit que $n \geqslant 4k - \frac{3n}{d}$ avec $d = \#D(G)$. On obtient alors une borne $\leqslant \frac{1}{4} + \frac{3}{4d}$ qui redonne $\frac{5}{8}$ si $D(G)$ est d'ordre 2 et est meilleure sinon.

4. En effet, l'application $\pi' \circ \pi$ avec $\pi : G \to \tilde{G}$ la surjection canonique et $\pi' : \tilde{G} \to \tilde{G}/S$ (attention à ce qu'ici on n'a pas nécessairement de structure de groupe sur $\tilde{G}/S$) passe au quotient modulo H car si $g'^{-1}g \in H$, alors $\pi' \circ \pi(g') = \pi' \circ \pi(g)$ car $\pi(g')^{-1}\pi(g) \in S$. On obtient ainsi une application $f : G/H \to \tilde{G}/S$ telle que $f \circ \pi'' = \pi' \circ \pi$ pour $\pi'' : G \to G/H$ la surejction canonique. La surjectivité découle de la surjectivité de π et de π'. Enfin, si $f \circ \pi''(g) = f \circ \pi''(g')$ équivaut à ce que $\pi(g')^{-1}\pi(g) = \pi(g'^{-1}g) \in S$ soit à ce que $g'^{-1}g \in \pi^{-1}(S) = H$, ce qui fournit l'injectivité.

5. Attention que cela n'implique **pas** que H soit un p-Sylow de G !

on en déduit que $H \leqslant PZ(G)$ et donc que $H = PZ(G)$. Enfin, P est unique. En effet, si P' est un autre p-Sylow de H, alors il existe $g \in H$ tel que $P' = gPg^{-1}$. Mais on vient de voir que $H = PZ(G)$ de sorte que $g = g_1 g_2$ avec $g_1 \in P$ et $g_2 \in Z(G)$ si bien que

$$P' = gPg^{-1} \quad \text{et} \quad P' = g_1 g_2 P g_2^{-1} g_1^{-1} = g_1 P g_1^{-1} = P$$

car g_2 commute à tout élément de G et $g_1 \in P$. Finalement, on définit g de l'ensemble des p-Sylow de $\tilde{G} = G/Z(G)$ vers celui des p-Sylow de G qui à tout p-Sylow S de $\tilde{G}$ associe l'unique p-Sylow P de G tel que $\pi^{-1}(S) = PZ(G)$. Cette application est bien définie et est bien la réciproque de f. On pouvait aussi bien sûr utiliser ce qui précède pour démontrer que f est injective et surjective.

Exercice 5. Soient p un nombre premier et G un p-groupe fini. Soit $(A, +)$ un groupe abélien avec $A \neq \{0\}$. On suppose donnée une action de G sur A par automorphismes, c'est-à-dire que pour tout $g \in G$, la bijection $x \mapsto g \cdot x$ de A dans A est un automorphisme du groupe abélien A. On suppose de plus que A est *de torsion p-primaire*, *i.e.* pour tout $x \in A$, il existe $m \in \mathbf{N}$ tel que $p^m x = 0$.

1. Montrer que si A est fini, son cardinal est une puissance de p (on pourra utiliser la classification des groupes abéliens finis, ou encore le théorème de Sylow).
2. On suppose que A est fini. Montrer qu'il existe $x \neq 0$ dans A tel que pour tout $g \in G$, on ait $g \cdot x = x$.
3. On ne suppose plus A fini. Soit $a \neq 0$ dans A. Montrer que le sous-groupe B de A engendré par $\{g \cdot a, g \in G\}$ est fini.
4. En déduire que le résultat de **2.** vaut encore sans l'hypothèse A fini.

Solution.

1. L'hypothèse est que tout élément est d'ordre une puissance de p. Le théorème de structure des groupes abéliens finis garantit que

$$A \cong \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_r\mathbf{Z}$$

avec $d_1 \mid \cdots \mid d_r$. Si maintenant un des d_i possède un autre facteur premier que p, disons q, alors on sait que G va contenir un élément d'ordre q ce qui est absurde. D'où, tous les d_i sont des puissances de p et A est un p-groupe.
On peut aussi raisonner en disant que tout élément de A engendre un p-groupe et appartient donc à un p-Sylow mais puisque A est abélien, on a un unique p-Sylow et celui-ci contient A, il lui est donc égal.

2. L'action étant par automorphisme, $\mathrm{Fix}(g)$ est un sous-groupe de A pour tout $g \in G$. L'équation aux classes fournit

$$\#A = \#A^G + \sum_{\omega \in \Omega'} \frac{\#G}{\#\mathrm{Stab}_G(\omega)}$$

et puisque $\frac{\#G}{\#\mathrm{Stab}_G(\omega)}$ est une puissance de p car pour $\omega \in \Omega'$, la stabilisateur est un sous-groupe strict et G est un p-groupe. Par ailleurs, $p \mid \#A$ si bien que $p \mid \#A^G$. Mais $\#A^G \neq 0$ car $0 \in A^G$ (car on agit par automorphisme) et par conséquent $\#A^G \geqslant p$ et on a le résultat.

3. On peut utiliser le théorème de structure des groupes abéliens de type fini couplé au fait que tout élément de A est de torsion.
4. On applique simplement le résultat de **2.** à B et il existe $x \neq 0$ dans $B \subseteq A$ tel que pour tout $g \in G$, $g \cdot x = x$.

Exercice 6. Montrer que tout groupe d'ordre 255 est cyclique.

Solution. Soit G d'ordre $255 = 3 \times 5 \times 17$. On sait par les théorèmes de Sylow que le nombre n_3 de 3-Sylow vaut 1 ou 85 (car il divise 85 et est congru à 1 modulo 3), celui n_5 des 5-Sylow vaut 1 ou 51 et on a un unique 17-Sylow, que l'on notera S_{17}. On ne peut pas avoir $n_3 = 85$ et $n_5 = 51$ car sinon on obtiendrait au moins[6] $85 \times 2 + 51 \times 4 = 374$ éléments dans G. On a donc $n_3 = 1$ ou $n_5 = 1$. Supposons $n_3 = 1$ (l'autre cas se traitant de façon complètement analogue) et S_3 l'unique 3-Sylow. Notons alors S_5 un 5-Sylow quelconque. On a alors

a) $S_3 S_{17} \cong S_3 \times S_{17} \lhd G$ car $S_3 \lhd G$ et $S_{17} \lhd G$;

b) $S_3 S_{17} \cap S_5 = \{e\}$;

c) $S_3 S_5 S_{17} = G$.

On a donc $G = S_3 S_{17} \rtimes S_5$ associé à un morphisme $\varphi S_5 \longrightarrow \mathrm{Aut}(S_3 S_{17})$. On a alors[7] $\mathrm{Aut}(S_3 S_{17}) \cong \mathrm{Aut}(\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/17\mathbf{Z}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/16\mathbf{Z}$ donc le morphisme φ est nécessairement trivial et le produit direct. Par le lemme chinois, on obtient donc que

$$G \cong S_3 \times S_5 \times S_{17} \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/17\mathbf{Z} \cong \mathbf{Z}/255\mathbf{Z}.$$

6. En effet, il est clair qu'en considérant l'ordre d'un élément g de l'intersection d'un 3-Sylow et d'un 5-Sylow, que cet ordre doit divisier 3 et 5 et est donc égal à 1 si bien qu'un 3-Sylow et un 5-Sylow sont disjoints mais aussi que puisque les 3-Sylow (et les 5-Sylow) sont cycliques, que l'intersection de deux 3-Sylow (et de deux 5-Sylow) distincts est trivial.

7. En effet, pour deux groupes G_1 et G_2, l'application $\mathrm{Aut}(G_1 \times G_2) \longrightarrow \mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2)$ défini par $\varphi \mapsto ([g_1 \mapsto \varphi(g_1, 1)], [g_2 \mapsto \varphi(1, g_2)])$ est un isomorphisme de réciproque $\mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2) \longrightarrow \mathrm{Aut}(G_1 \times G_2)$ défini par $(\varphi_1, \varphi_2) \mapsto [(g_1, g_2) \mapsto (\varphi_1(g_1), \varphi_2(g_2))]$. On peut aussi utiliser que

$$\mathrm{Aut}\,(\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/17\mathbf{Z}) \cong \mathrm{Aut}\,(\mathbf{Z}/85\mathbf{Z}) \cong (\mathbf{Z}/85\mathbf{Z})^\times \cong (\mathbf{Z}/5\mathbf{Z})^\times \times (\mathbf{Z}/17\mathbf{Z})^\times \cong \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/16\mathbf{Z}.$$

Exercice 7 — Isomorphismes exceptionnels. Soit n un entier et $K = \mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ le corps fini à p éléments avec p un nombre premier. Soit E le K-ev K^n. On note $\mathbf{P}(E)$ l'ensemble des droite vectorielles de K^n (*espace projectif de dimension* $n-1$).

1. Montrer qu'il existe un morphisme injectif Φ de $\mathrm{PGL}_n(K)$ dans le groupe symétrique $\mathfrak{S}(\mathbf{P}(E))$.
2. Montrer que, si $n = 2$, $\mathbf{P}(E)$ est de cardinal $p+1$; on identifie Φ à un morphisme $\mathrm{PGL}_2(K) \longrightarrow \mathfrak{S}_{p+1}$.
3. On prend $p = 2$. Montrer que Φ induit des isomorphismes de $\mathrm{PGL}_2(\mathbf{F}_2)$ et $\mathrm{PSL}_2(\mathbf{F}_2)$ sur $\mathfrak{S}_3$.
4. On prend $p = 3$. Montrer que Φ induit un isomorphisme de $\mathrm{PGL}_2(\mathbf{F}_3)$ sur $\mathfrak{S}_4$ et de $\mathrm{PSL}_2(\mathbf{F}_3)$ sur $\mathfrak{A}_4$. Les groupes $\mathrm{PGL}_2(\mathbf{F}_3)$ et $\mathrm{SL}_2(\mathbf{F}_3)$ sont-ils isomorphes ?
5. On prend $p = 5$. Montrer que Φ induit un isomorphisme de $\mathrm{PGL}_2(\mathbf{F}_5)$ sur $\mathfrak{S}_5$ et de $\mathrm{PSL}_2(\mathbf{F}_5)$ sur $\mathfrak{A}_5$ (on rappelle que tout sous-groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$ pour $n \geqslant 5$, conséquence non triviale de la simplicité des groupes alternés).
6. Montrer que $\mathrm{SL}_3(\mathbf{F}_2)$ est simple.
7. Soit G simple d'ordre 168. Montrer que G est isomorphe à $\mathrm{PSL}_2(\mathbf{F}_7)$.
8. Montrer que l'on a un isomorphisme entre $\mathrm{SL}_3(\mathbf{F}_2)$ et $\mathrm{PSL}_2(\mathbf{F}_7)$.

Solution.
On rappelle qu'on sait que le cardinal de $\mathrm{GL}_n(K)$ est [8]

$$\#\mathrm{GL}_n(K) = (p^n-1)(p^n-p)\ldots(p^n-p^{n-1}).$$

Comme par définition $\mathrm{SL}_n(K)$ est le noyau du morphisme de groupes surjectif $\det : \mathrm{GL}_n(K) \longrightarrow K^\times$, son cardinal est celui de $\mathrm{GL}_n(K)$ divisé par $p-1$, soit

$$\#\mathrm{SL}_n(K) = (p^n-1)(p^n-p)\ldots(p^n-p^{n-2}).p^{n-1}.$$

D'autre part, on rappelle que $\mathrm{PGL}_n(K) = \mathrm{GL}_n(K)/Z(\mathrm{GL}_n(K))$ est ainsi le quotient de $\mathrm{GL}_n(K)$ par un groupe isomorphe à $K^\times$ (car le centre de $\mathrm{GL}_n(K)$ est constitué des matrices scalaires non nulles), donc $\#\mathrm{PGL}_n(K) = \#\mathrm{SL}_n(K)$. On obtient immédiatement par passage au quotient un morphisme injectif $\mathrm{PSL}_n(K) \longrightarrow \mathrm{PGL}_n(K)$.

Enfin, le cardinal de $\mathrm{PSL}_n(K)$ dont on rappelle qu'il est défini par $\mathrm{PSL}_n(K) = \mathrm{SL}_n(K)/Z(\mathrm{SL}_n(K))$ et que [9] $Z(\mathrm{SL}_n(K)) = Z(\mathrm{GL}_n(K)) \cap \mathrm{SL}_n(K) = \{\lambda I_n \ : \ \lambda^n = 1\}$. Or, il y a $\mathrm{pgcd}(n, p-1)$ racines n-ièmes de l'unité dans un corps K de cardinal p : en effet, on sait que $K^\times$ est un groupe cyclique d'ordre $p-1$, et on est donc ramené à compter le nombre de solutions x de $nx = 0$ dans $\mathbf{Z}/(p-1)\mathbf{Z}$, ce qui donne facilement le résultat puisque les solutions sont les éléments de $\mathbf{Z}/(p-1)\mathbf{Z}$ multiple de $\frac{p-1}{\mathrm{pgcd}(n,p-1)}$. Finalement,

$$\#\mathrm{PSL}_n(K) = \frac{(p^n-1)(p^n-p)\ldots(p^n-p^{n-2}).p^{n-1}}{\mathrm{pgcd}(n, p-1)}.$$

1. On fait opérer $\mathrm{PGL}_n(K)$ sur l'ensemble $\mathbf{P}(E)$ des droites vectorielles de E par $\bar{g}.D = g(D)$, où $g \in \mathrm{GL}_n(K)$ et $\bar{g}$ est son image dans $\mathrm{PGL}_n(K)$. Ceci est bien défini car si $\bar{g}_1 = \bar{g}_2$, alors g_1 et g_2 sont proportionnels donc $g_1(D) = g_2(D)$. L'opération est fidèle car les seuls $g \in \mathrm{GL}_n(K)$ qui stabilisent toutes les droites sont les homothéties. On obtient donc un morphisme injectif Φ de $\mathrm{PGL}_n(K)$ dans $\mathfrak{S}(\mathbf{P}(E))$.
2. Les droites vectorielles de E sont données par une équation $x = ay$ dans le plan (avec $a \in K$) ou par l'équation $y = 0$. On obtient ainsi $q+1$ droites. On pouvait aussi raisonner en dénombrant le nombre de vecteurs non nuls de E, à savoir p^2-1 puis en remarquant qu'une droite (isomorphe à $\mathbf{F}_p$ contient $p-1$ tels vecteurs non nuls) si bien qu'on retrouve bien $\frac{p^2-1}{p-1} = p+1$ droites [10].

   De manière plus explicite et en identifiant $\mathbf{P}(E)$ avec $\mathbf{P}^1(E) = K \cup \{\infty\}$, on obtient le morphisme suivant qui à la classe d'une matrice $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ avec $\alpha, \beta, \gamma, \delta \in \mathbf{F}_7$ tels que $\alpha\delta - \gamma\beta = 1$ associe la bijection $f_M : \mathbf{P}^1(E) \longrightarrow \mathbf{P}^1(E)$ donnée par

$$\forall a \in \mathbf{F}_7, \quad f_M(D_a) = D_{\frac{a\alpha+\beta}{a\gamma+\delta}} \quad \text{et} \quad f_M(D_\infty) = D_{\frac{\alpha}{\gamma}}$$

8. En effet, on a $p^n - 1$ choix de première colonne non nulle, puis $p^n - p$ choix de seconde colonne non colinéaire à la première, etc...

9. Cela résulte du fait plus général (sur un corps K quelconque) suivant : si un endomorphisme u de K^n commute avec tous les endomorphismes de déterminant 1, alors u est une homothétie. Il suffit pour cela (ce qui est classique) de voir que tout vecteur $x \neq 0$ de K^n est vecteur propre pour u. Complétons x en une base $(x, e_1, \ldots, e_{n-1})$ de K^n ; soit M la matrice de u dans cette base, alors M commute avec la matrice de Jordan $J_n = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & (0) \\ & & \ddots & \ddots & \\ & & & \ddots & \ddots \\ & (0) & & & 0 \ \ 1 \\ & & & & 0 \end{pmatrix}$, ce qui implique qu'elle laisse stable le noyau de J_n, lequel est $K.x$. Ainsi x est bien vecteur propre pour u comme on voulait. Je vous renvoie au chapitre IV du Perrin pour plus de détails sur les groupes linéaires.

10. Noter que ce raisonnement fournit que dans le cas général, on a $\frac{p^n-1}{p-1} = p^{n-1} + \cdots + 1$ droites dans $\mathbf{F}_p^n$.

où D_a est la droite d'équation $x = ay$ et D_∞ la droite d'équation $y = 0$ avec la convention que si $a\gamma + \delta = 0$, alors $\frac{a\alpha+\beta}{a\gamma+\delta} = \infty$ et car cela ne dépend pas du représentant M choisi et que $M\begin{pmatrix}a\\1\end{pmatrix} = \begin{pmatrix}a\alpha+\beta\\a\gamma+\delta\end{pmatrix}$ et $M\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\alpha\\\gamma\end{pmatrix}$. Autrement dit, le sous-groupe de $\mathfrak{S}_{q+1}$ isomorphe à $\mathrm{PSL}_2(K)$ correspond aux bijections de $\mathbf{P}^1(E)$ de la forme $a \mapsto \frac{a\alpha+\beta}{a\gamma+\delta}$ (appelées homographies) avec $\begin{pmatrix}\alpha & \beta\\\gamma & \delta\end{pmatrix} \in \mathrm{PSL}_2(K)$ avec $\alpha, \beta, \gamma, \delta \in \mathbf{F}_7$ tels que $\alpha\delta - \gamma\beta = 1$ (qui encore une fois ne dépend pas du représentant choisi). On voit ici poindre l'équivalence entre homographies et matrices de $\mathrm{PSL}_2(K)$ qui nous sera utile en question **7**.

3. Les groupes $\mathrm{PGL}_2(\mathbf{F}_2)$ et $\mathrm{PSL}_2(\mathbf{F}_2)$ sont égaux et de cardinal 6 par **1.**, qui est aussi le cardinal de $\mathfrak{S}_3$. Ainsi, le morphisme injectif Φ est aussi surjectif, d'où le résultat.

4. Le cardinal de $\mathrm{PGL}_2(\mathbf{F}_3)$ est ici $(3^2-1).3 = 24$. Comme $\mathfrak{S}_4$ est aussi de cardinal 24, Φ est bien un isomorphisme. De plus $\mathrm{PSL}_2(\mathbf{F}_3)$ est un sous-groupe [11] d'indice 2 de $\mathrm{PGL}_2(\mathbf{F}_3)$, car $\mathrm{pgcd}(2, 3-1) = 2$. Comme le seul sous-groupe d'indice 2 de [12] $\mathfrak{S}_4$ est $\mathfrak{A}_4$, on en déduit que Φ induit un isomorphisme de $\mathrm{PSL}_2(\mathbf{F}_3)$ sur $\mathfrak{A}_4$.

Bien qu'ils aient même cardinal, les groupes $\mathrm{PGL}_2(\mathbf{F}_3)$ et $\mathrm{SL}_2(\mathbf{F}_3)$ ne sont pas isomorphes, par exemple parce que $\mathrm{SL}_2(\mathbf{F}_3)$ a un centre non trivial (de cardinal 2, égal à $\{\pm I_2\}$) alors que le centre de $\mathrm{PGL}_2(\mathbf{F}_3) \simeq \mathfrak{S}_4$ est réduit au neutre. Noter du reste que la même preuve que pour calculer le centre de $\mathrm{GL}_n(K)$ et $\mathrm{SL}_n(K)$ (voir note de bas de page numéro 4) montre que les centres de $\mathrm{PGL}_n(K)$ et $\mathrm{PSL}_n(K)$ sont triviaux pour tout $n \geqslant 2$ (sur un corps quelconque).

5. Le cardinal de $\mathrm{PGL}_2(\mathbf{F}_5)$ est $(5^2-1).5 = 120$, ce qui montre que Φ induit un isomorphisme de $\mathrm{PGL}_2(\mathbf{F}_5)$ sur un sous-groupe d'indice 6 de $\mathfrak{S}_6$, lequel est isomorphe à $\mathfrak{S}_5$ (voir l'exercice 1 de la feuille I). Comme $\mathrm{pgcd}(2, 5-1) = 2$, on a encore que $\mathrm{PSL}_2(\mathbf{F}_5)$ est d'indice 2 dans $\mathrm{PGL}_2(\mathbf{F}_5) \simeq \mathfrak{S}_5$, et il est donc isomorphe via Φ à $\mathfrak{A}_5$.

On peut montrer que l'image de $\mathrm{PGL}_2(\mathbf{F}_5)$ par Φ, bien qu'isomorphe à $\mathfrak{S}_5$ n'est pas conjugué des sous-groupes de $\mathfrak{S}_6$ donnés par le stabilisateur d'un élément de $\{1, ..., 6\}$. Ce phénomène (existence d'un sous-groupe d'indice m non conjugué des stabilisateurs d'un point) ne se produit dans $\mathfrak{S}_m$ que pour $m = 6$, et explique la présence dans $\mathfrak{S}_6$ d'un automorphisme qui n'est pas intérieur. Voir l'exercice 12 pour plus de détails.

6. Concernant le cardinal, on applique la formule

$$\#\mathrm{PSL}_3(\mathbf{F}_2) = \frac{(2^3-1)(2^3-2)2^2}{\mathrm{pgcd}(3,1)} = 7 \times 6 \times 4 = 168.$$

On peut ainsi remarquer qu'on a $\mathrm{SL}_3(\mathbf{F}_2) = \mathrm{GL}_3(\mathbf{F}_2)$.

Un élément de $\mathrm{SL}_3(\mathbf{F}_2)$ admet pour polynôme minimal un polynôme de $\mathbf{F}_2[X]$ de degré inférieur ou égal à 3, donc parmi la liste suivante : $X+1, X^2+1, X^2+X+1, X^3+1, X^3+X+1, X^3+X^2+1, X^3+X^2+X+1$ et sa classe de conjugaison est déterminé par sa suite d'invariants de similitudes qui est ici déterminée par le polynôme minimal. Ainsi, un polynôme minimal donné correspond à une classe de conjugaison.

- La seule matrice de polynôme minimal $X+1$ est I_3 qui forme une classe de conjugaison ;
- Soit $A \in \mathrm{SL}_3(\mathbf{F}_2)$ de polynôme minimal $X^2+1 = (X+1)^2$. On a alors que $\mathrm{Im}(A+I_3) \subseteq \mathrm{Ker}(A+I_3)$ de dimension respective [13] 1 et 2 et une telle matrice est caractérisée par la donnée de la droite [14] $\mathrm{Im}(A+I_3)$ et du plan $\mathrm{Ker}(A+I_3)$. On a alors 7 choix de droites D puis 3 choix de plans P qui la contienne [15], soit 21 éléments d'ordre 2 qui forment une classe de conjugaison.
- Soit $A \in \mathrm{SL}_3(\mathbf{F}_2)$ de polynôme minimal X^2+X+1. Alors nécessairement, le polynôme caractéristique est $X^3+1 = (X+1)(X^2+X+1)$ et 1 est valeur propre de A mais 1 n'est pas racine de X^2+X+1. On a donc une contradiction et X^2+X+1 ne peut pas apparaître comme polynôme minimal [16].

11. Le fait qu'on obtienne un sous-groupe se voit grâce la composition de l'inclusion naturelle $i : \mathrm{SL}_n(\mathbf{F}_p) \to \mathrm{GL}_n(\mathbf{F}_p)$ avec la surjection canonique $\pi : \mathrm{GL}_n(\mathbf{F}_p) \to \mathrm{PGL}_n(\mathbf{F}_p)$. Il est facile de montrer que $\pi \circ i$ passe au quotient modulo $Z(\mathrm{SL}_n(\mathbf{F}_p))$ pour fournir un morphisme injectif $\mathrm{PSL}_n(\mathbf{F}_p) \to \mathrm{PGL}_n(\mathbf{F}_p)$ et ainsi on peut réaliser $\mathrm{PSL}_n(\mathbf{F}_p)$ comme un sous-groupe de $\mathrm{PGL}_n(\mathbf{F}_p)$.

12. Cela découle soit du fait que l'on connaît tous les sous-groupes de $\mathfrak{S}_n$ pour $n \leqslant 4$ et les sous-groupes distingués de $\mathfrak{S}_n$ pour $n \geqslant 5$ ou plus simplement du fait qu'un sous-groupe d'indice 2 donne lieu au quotient à un morphisme surjectif (donc non trivial) de $\mathfrak{S}_n \to \{\pm 1\}$. Or, le seul morphisme non trivial de $\mathfrak{S}_n$ dans le groupe multiplicatif $\{\pm 1\}$ est la signature. Cela se voit en montrant qu'une transposition est nécessairement envoyée sur -1 et en utilisant le fait que les transpositions engendrent $\mathfrak{S}_n$. Il existe au moins une transposition envoyée sur -1 sinon pusiqu'elles engendrent $\mathfrak{S}_n$, le morphisme est trivial mais alors puisque toutes les transpositions sont conjuguées et que $\{\pm 1\}$ est abélien, toutes les transpositions ont la même image, à savoir -1, ce qui permet de conclure.

13. En utilisant par exemple les résultats bien connus sur les matrices nilpotentes ou en trigonalisant sur une clôture algébrique.

14. En effet, par exemple, en se fixant $P = \mathrm{Ker}(A+I_3)$, la matrice A est de la forme

$$A = \begin{pmatrix}1 & 0 & a\\0 & 1 & b\\0 & 0 & 1\end{pmatrix}$$

avec a ou b non nul et alors il est clair que a et b sont fixés par $D = \mathrm{Im}(A+I_3)$ car

$$A + I_3 = \begin{pmatrix}0 & 0 & a\\0 & 0 & b\\0 & 0 & 0\end{pmatrix}.$$

15. Bien remarquer que tout plan de $\mathbf{F}_2^3$ contient 3 des 7 droites de $\mathbf{F}_2^3$ et est de cardinal 4.

16. On aurait aussi pu voir qu'on obtenait 168 éléments avec les autres polynômes minimaux.

— Soit $A \in \mathrm{SL}_3(\mathbf{F}_2)$ de polynôme minimal $X^3+1=(X+1)(X^2+X+1)$. Cela se produit lorsque la droite $\mathrm{Ker}(A+I_3)$ et le plan $\mathrm{Ker}(A^2+A+I_3)$ sont supplémentaires dans $\mathbf{F}_2^3$. Une telle matrice est donc entièrement caractérisée par la donnée d'une droite et d'un plan supplémentaire ainsi que d'une matrice de $\mathrm{SL}_2(\mathbf{F}_2)$ de polynôme caractéristique X^2+X+1. On a 7 choix de droites puis 4 choix de plan (en effet, on a 6 choix d'un vecteur non nul non colinéaire au vecteur de la droite choisie et alors on peut choisir tout vecteur différent de la somme du vecteur directeur de la droite choisie et du vecteur choisi. Ce faisant, on obtient 12 plans mais chacun étant compté trois fois) puis on voit qu'une matrice $\mathrm{SL}_2(\mathbf{F}_2)$ de polynôme caractéristique X^2+X+1 est de la forme $\begin{pmatrix} a & 1 \\ 1 & 1-a \end{pmatrix}$ avec $a \in \mathbf{F}_2$ et on a ainsi 2 possibilités, soit finalement 56 telles matrices, toutes d'ordre 3.

— Soit $A \in \mathrm{SL}_3(\mathbf{F}_2)$. Le polynôme minimal de A est irréductible de degré 3 si, et seulement si [17], pour tout $x \in \mathbf{F}_2^3$ non nul, la famille (x, Ax, A^2x) est une base de $\mathbf{F}_2^3$. Pour x non nul, on a donc 6 choix pour Ax et 4 choix pour A^2x (A^3x étant fixé par le polynôme minimal), ce qui fournit 24 matrices dans chacun des cas, d'ordre 7 car $X^7+1=(1+X)(X^3+X+1)(X^3+X^2+1)$. Noter que si A a pour polynôme minimal X^3+X+1 alors A^{-1} a pour polynôme minimal X^3+X^2+1 et inversement.

— Soit finalement $A \in \mathrm{SL}_3(\mathbf{F}_2)$ de polynôme minimal $X^3+X^2+X+1=(X+1)^3$. Cela arrive si, et seulement si, $\mathrm{Ker}(A+I_3)$ est une droite contenue dans le plan $\mathrm{Ker}(A+I_3)^2$ et tout vecteur hors de ce plan a une image dans le plan mais pas dans la droite. Ainsi, une telle matrice est déterminée par le choix d'une droite contenue dans un plan et de l'image par $A+I_3$ d'un vecteur hors de ce plan dans le plan mais pas dans la droite. On a ainsi $7\times 3\times 2=42$ telles matrices d'ordre 4 car $X^4+1=(X+1)^4$.

On a donc bien obtenu 168 éléments répartis en 6 classes de conjugaison [18]. Soit à présent $H \neq \{I_3\} \lhd \mathrm{SL}_3(\mathbf{F}_2)$. Supposons que H ne contienne ni élément d'ordre 3 ni élément d'ordre 7. Alors le cardinal de H divise $168/21=8$ donc H contient un élément d'ordre 2 donc les 21 éléments conjugués d'ordre 2 et H contient au moins 22 éléments, absurde. On sait donc que H contient un élément d'ordre 3 ou un élément d'ordre 7. Dans le premier cas, H contient 56 éléments d'ordre 7 donc $\#H \geqslant 57$ et $\#H \in \{84, 168\}$ donc H contient les 21 éléments d'ordre 2 et 24 éléments d'ordre 7 conjugués et $\#H \geqslant 57+24+21=102$ donc $\#H=168$. Dans le second cas, H contient 24 éléments d'ordre 7 et en fait les 48 car les classes de conjugaison sont échangées par inversion donc $\#H \geqslant 49$ et $\#H \in \{56, 84, 168\}$ donc H a un élément d'ordre 7 et on conclut de nouveau que $\#H=168$, ce qui conclut la preuve.

7. Par les théorèmes de Sylow, G admet huit 7-Sylow (car G étant simple, il ne peut pas en posséder un unique). Si l'on note X l'ensemble des 7-Sylow, l'action transitive de G par conjugaison sur X induit un morphisme de groupes injectif $\varphi : G \to \mathfrak{S}(X) \cong \mathfrak{S}_8$. Or, les éléments de $\mathfrak{S}_8$ sont d'ordre 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 15. Mais G n'admet pas d'élément d'ordre 15 donc tous les éléments de G sont d'ordre $\leqslant 12$.

En outre, on voit que pour tout 7-Sylow S de G, $\#N_G(S)=\frac{168}{\#X}=21$ donc en particulier $N_G(S)$ n'est pas cyclique (sinon on a un élément d'ordre 21). Montrons que S agit transitivement sur $X'=X\setminus\{S\}$. Comme il agit trivialement sur S, on voit que la restriction de φ induit un morphisme $\tilde{\varphi} : S \to \mathfrak{S}(X') \cong \mathfrak{S}_7$. Si $T \in X'$, alors S n'est pas contenu dans $N_G(T)$ sinon par un argument de Frattini on aurait $T=S$ (car T et S sont deux 7-Sylow de $N_G(T)$ et T y est normal). Ainsi, $S \cap N_G(T)=\{e\}$ (si $s \neq e \in S$ et $sTs^{-1}=T$ alors cela vaut pour tout élément de S qui est cyclique d'ordre 7 engendré par s et $S \leqslant N_G(T)$) et pour tous $g, g' \in S$, $gTg^{-1}=g'Tg'^{-1}$ si, et seulement si, $g=g'$ (car $gg'^{-1} \in S \cap N_G(T)$). Par conséquent, l'orbite de T sous l'action de S sur X' est de cardinal $7=\#X'$ et est donc transitive et *a fortiori* l'action de $N_G(S)$ sur X' est transitive.

Le stabilisateur de T pour cette action de $N_G(S)$ (de cardinal 21) sur X' n'est autre que $N_G(S) \cap N_G(T)$. Comme $\#X'=7$, il vient que $\#(N_G(S) \cap N_G(T))=3$.

On pose $n_3 \neq 1$ le nombre de 3-Sylow, congru à 1 modulo 3 et divisant 56 donc $n_3 \in \{4, 7, 28\}$. Le cas $n_3=4$ est impossible car $168 \nmid 48=24$ (faire agir G sur l'ensemble de ses 3-Sylow). Supposons $n_3=7$. Le sous-groupe $N_G(S)$ est d'ordre 21, il contient donc 1 ou sept 3-Sylow. S'il en contient un seul, il est distingué et on a nécessairement un unique 7-Sylow distingué et on peut alors en déduire que dans ce cas $N_G(S)$ serait le produit direct de ce 3-Sylow par son 7-Sylow et donc on a une contradiction avec le fait qu'il ne soit pas cyclique. On sait donc que $N_G(S)$ contient sept 3-Sylow qui sont nécessairement alors les 3-Sylow de G. Ceci valant pour tout 7-Sylow, on a donc pour $T \neq S$, $\#(N_G(S) \cap N_G(T)) \geqslant 7\times 2+1=15$, ce qui est absurde. Ainsi, $n_3=28$.

On pose alors $H=N_G(N_G(S) \cap N_G(T))$. Comme $N_G(S) \cap N_G(T)$ est un 3-Sylow de G, H est de cardinal $168/28=6$. Si H est cyclique, alors G a un élément x d'ordre 6 et $\langle x^2 \rangle$ est un 3-Sylow. Comme ces derniers sont conjugués, on voit que tout 3-Sylow est engendré par le carré d'un élément d'ordre 6. Ainsi G contient au moins $2\times 28=56$ éléments d'ordre 6. Il contiendrait aussi $2\times 28=56$ éléments d'ordre 3 et $8\times 6=48$ éléments d'ordre 7. On aboutit à 160 éléments, auxquels s'ajoutent au moins deux 2-Sylow de cardinal 8, soit au moins 9 éléments d'ordre divisant 8 et G aurait au moins 169 éléments, absurde. D'où, H n'est pas cyclique et $H \cong \mathfrak{S}_3$.

Fixons alors un générateur s du 7-Sylow S. Alors l'application $\tau : \{0, \dots, 6\} \to X'$ donnée par $\tau(k)=s^kTs^{-k}$ est bijective (par transitivité). En posant $\tau(\infty)=S$, on obtient une bijection $\tau : \mathbf{P}^1(\mathbf{F}_7)=\mathbf{F}_7 \cup \{\infty\} \to X$. Avec ces identifications, l'action de S sur $X \cong \mathbf{P}^1(\mathbf{F}_7)$ devient

$$\forall x \in \mathbf{P}^1(\mathbf{F}_7), \quad s \cdot x = x+1 \qquad (s \cdot s^kTs^{-k}=ss^kTs^{-k}s^{-1}=s^{k+1}Ts^{-k-1})$$

17. Polynôme minimal pas irréductible implique par le lemme des noyaux le fait qu'il existe un x qui ne vérifie pas l'hypothèse. Pour la réciproque, on voit que l'espace engendré par la famille (x, Ax, A^2x) est stable par A et si son supplémentaire est non réduit à 0, alors la matrice A dans une base de cet espace et de son supplémentaire est diagonale par blocs ce qui contredit l'irréductiblité du polynôme caractéristique.

18. On pouvait aussi raisonner en termes d'invariants de similitudes comme sur stackexchange.

avec la convention $\infty + 1 = \infty$. Autrement dit, elle est donnée par l'homographie de $\mathbf{P}^1(\mathbf{F}_7)$ de matrice (voir la fin de **2.**)

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{PSL}_2(\mathbf{F}_7)$$

et on atterrit bien dans le sous-groupe isomorphe à $\mathrm{PSL}_2(\mathbf{F}_7)$ de $\mathfrak{S}_8$ (voir toujours la fin de la question **2.**).

Choisissons $t \in N_G(S) \cap N_G(T)$ d'ordre 3. Le morphisme $c : \mathbf{Z}/3\mathbf{Z} \to \mathrm{Aut}(S) \cong \mathbf{Z}/6\mathbf{Z}$ donné par la conjugaison par les puissances de t est non trivial (sinon $N_G(S)$ serait engendré par s et t et cyclique car s et t commutent d'ordres premiers entre eux). Il est donc égal à $k \mapsto 2k$ ou $4k$ ce qui signifie que $tst^{-1} \in \{s^2, s^4\}$. Quitte à remplacer t par $t^2 = t^{-1}$, on peut supposer que $tst^{-1} = s^2$. On voit alors facilement que l'action de t sur X correspond à la bijection de $\mathbf{P}^1(\mathbf{F}_7)$ donnée par la formule $t \cdot x = 2x$ toujours avec la convention naturelle $2 \cdot \infty = \infty$. Autrement dit, elle est donnée par l'homographie de $\mathbf{P}^1(\mathbf{F}_7)$ de matrice

$$\begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix} \in \mathrm{PSL}_2(\mathbf{F}_7)$$

et on atterrit bien dans le sous-groupe isomorphe à $\mathrm{PSL}_2(\mathbf{F}_7)$ de $\mathfrak{S}_8$ (voir toujours la fin de la question **2.**).

Soient maintenant $u \in H \smallsetminus (N_G(S) \cap N_G(T))$. Comme $H \cong \mathfrak{S}_3$, u correspond à une transposition et t à un 3-cycle. Il est donc clair que $utu^{-1} = t^{-1} = t^2$. On en déduit que pour tout $x \in \mathbf{P}^1(\mathbf{F}_7)$, on a $u \cdot (2x) = 4u \cdot x$ (en effet, si l'on voit u comme une permutation de $\mathbf{P}^1(\mathbf{F}_7)$, cela signifie que $u(2x) = 4u(x)$ et cela se voit par le fait que $u \cdot (2x) = u \cdot (t \cdot x) = uts^k T s^{-k} t^{-1} u^{-1} = t^2 us^k T s^{-k} u^{-1} t^2$ soit $u \cdot (2x) = t^2 \cdot (u \cdot x) = 4u \cdot x$). Montrons que $G = \langle s, t, u \rangle$. Le groupe de droite est de cardinal > 21 et divisible par 21 donc vaut 42, 84 ou 168. Comme G est simple, il ne peut pas être d'indice 2. Supposons alors qu'il soit de cardinal 42, soit d'indice 4. On peut alors construire un morphisme non trivial $G \to \mathfrak{S}(G/\langle s, t, u \rangle) \cong \mathfrak{S}_4$. Par simplicité un tel morphisme est injectif ce qui est impossible par cardinalité. On a donc bien que $G = \langle s, t, u \rangle$.

Puisque $u(0) = 4u(0)$ et $u(\infty) = 4u(\infty)$, $u(0), u(\infty) \in \{0, \infty\}$ et alors nécessairement $u(0) = \infty$ et $u(\infty) = 0$ sinon u aurait deux points fixes et serait ainsi dans le normalisateur d'un 7-Sylow, d'ordre 21, ce qui est exclu car u est d'ordre 2. De même, $u(1) \neq 1$ et si $u(1) \in \{2, 4\}$, alors (par exemple) si $u(1) = 2$, $u(2) = 4u(1) = 1$ et $u(4) = 4u(2) = 4$ ce qui est exclu. D'où $a := u(1) \in \{3, 5, 6\}$. On vérifie alors que

$$\forall x \in \mathbf{P}^1(\mathbf{F}_7), \quad u \cdot x = \frac{a}{x}.$$

En effet, $u(2) = 4a = \frac{a}{2}$ et $u(4) = 4 \times \frac{a}{2} = \frac{a}{4}$. On a de même $u(3) = 2u(6)$ et $u(5) = 4u(6) = \frac{u(6)}{2}$. Mais (par exemple dans le cas $a = 3$), $u(3) = 1 = \frac{a}{3}$ et donc $u(6) = \frac{a}{6}$ et $u(5) = \frac{a}{5}$. Malheureusement pour l'instant on obtient une homographie de matrice $\begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}$ qui est dans $\mathrm{PGL}_2(\mathbf{F}_7)$ mais pas dans $\mathrm{PSL}_2(\mathbf{F}_7)$. Mais $a \in \{3, 5, 6\}$ si bien qu'on vérifie que $\frac{-1}{a} \in \{1, 2, 4\}$ est un carré modulo 7 et il existe $c \in \mathbf{F}_7^\times$ tel que $ac^2 = -1$ et on voit finalement que

$$\forall x \in \mathbf{P}^1(\mathbf{F}_7), \quad u \cdot x = \frac{ac}{cx}$$

et ainsi l'action de u sur X est donnée par l'homographie de $\mathbf{P}^1(\mathbf{F}_7)$ de matrice

$$\begin{pmatrix} 0 & ac \\ c & 0 \end{pmatrix} \in \mathrm{PSL}_2(\mathbf{F}_7)$$

et on atterrit bien dans le sous-groupe isomorphe à $\mathrm{PSL}_2(\mathbf{F}_7)$ de $\mathfrak{S}_8$.

Finalement, comme $\varphi(G) \cong G = \langle s, t, u \rangle$ est contenu dans le sous-groupe de $\mathfrak{S}_8$ isomorphe à $\mathrm{PSL}_2(\mathbf{F}_7)$ et on conclut alors par cardinalité que $G \cong \mathrm{PSL}_2(\mathbf{F}_7)$. Ouf!

8. Cela résulte de la combinaison des questions **6.** et **7.**. Si vous souhaitez un isomorphisme explicite entre ces deux groupes, je vous renvoie à http://mathem-all.fr/bw/PSL2GL32.pdf. On verra dans la partie Bonus que le théorème de transfert assure que tout groupe de cardinal $60 < n < 168$ n'est pas simple et ainsi cet exercice couplé aux exercices 6 (question **4.**) et 8 permet d'obtenir la classification de tous les sous-groupes finis simples d'ordre $\leqslant 168$. On verra aussi en bonus que les techniques de ce cours peuvent même être poussées plus loin!

La classification des groupes finis est un problème ambitieux et toujours ouvert. Une stratégie est de se ramener par une suite d'extension à l'étude des groupes simples finis. Si l'on sait alors classifier les extensions et les groupes finis simples, alors on peut classifier les groupes finis. On ne sait malheureusement pas classifié les extensions mais en revanche on sait classifier les groupes finis simples. Cette classification des groupes simples finis (dont un ingrédient fondamental a été le théorème de Feit-Thompson et dont les résultats ont été publiés entre 1953 et 1983 qui comprend des dizaines de milliers de pages répartis dans plus de 500 articles de recherches auxquels plus d'une centaine de mathématiciens ont contribué) se séparent en 4 catégories : les groupes cycliques d'ordre premier, les groupes alternés (avec $n \geqslant 5$), les groupes de type Lie (typiquement les $\mathrm{PSL}_n(k)$ qui sont simples pour k un corps commutatif sauf $n = 2$ et $k = \mathbf{F}_2$ ou $\mathbf{F}_3$, voir Perrin IV.4) et les 26 groupes sporadiques. Il est donc important de savoir si certains groupes appartiennent à deux de ces catégories, en général ce n'est pas le cas mais cela arrive et c'est ce que fournissent ces "isomorphismes exceptionnels". On peut mentionner qu'il en manque certains puisqu'on s'est

limité ici aux corps finis de cardinal premier mais vous pourrez essayer de démontrer (voir le Perrin également) que $\mathrm{PGL}_2(\mathbf{F}_4) = \mathrm{PSL}_2(\mathbf{F}_4) \cong \mathfrak{A}_5$, $\mathrm{PSL}_4(\mathbf{F}_2) \cong \mathfrak{A}_8$ et $\mathrm{PSL}_2(\mathbf{F}_9) \cong \mathfrak{A}_6$ mais malgré le fait qu'ils aient le même cardinal, on a $\mathrm{PSL}_3(\mathbf{F}_4) \ncong \mathfrak{A}_8$. Et la liste n'est pas exhaustive avec notamment des isomorphismes exceptionnels de groupes symplectiques et unitaires.

Exercice 8. Trouver un groupe fini G non réduit au neutre tel que : le centre de G est 1, le sous-groupe dérivé de G est G, mais G n'est pas simple.

Solution. Soit H un groupe simple non abélien, par exemple $H = \mathfrak{A}_n$ avec $n \geqslant 5$. Posons $G = H \times H$. On vérifie immédiatement que le centre de G est le produit du centre de H avec lui-même, donc est trivial [19]. De même, le sous-groupe dérivé $D(G)$ de G est $D(H) \times D(H) = H \times H$. Pourtant G n'est pas simple car $\{1\} \times H$ est un sous-groupe distingué non trivial de G.

Exercice 9. On suppose qu'il existe un groupe simple G d'ordre 180.

1. Montrer que G contient trente-six 5-Sylow.
2. Montrer que G contient dix 3-Sylow puis que deux 3-Sylow distincts ne peuvent pas contenir un même élément $g \neq e$.
3. Conclure.

Solution.

1. Notons n_5 le nombre de 5-Sylow. Par simplicité de G et les théorèmes de Sylow, $n_5 \neq 1$. On sait alors que n_5 est congru à 1 modulo 5 et divise $180/5 = 36$ donc $n_5 \in \{6, 36\}$. Supposons que $n_5 = 6$ alors l'action transitive de G sur l'ensemble de ses six 5-Sylow fournit un morphisme non trivial (donc injectif par simplicité de G) $G \to \mathfrak{S}_6$. Par ailleurs, en composant avec la signature, on obtient un morphisme $G \to \{\pm 1\}$ qui ne peut pas être injectif pour des raisons de cardinalité est donc nécessairement trivial (par simplicité de G). Il s'ensuit qu'en réalité, on a un morphisme injectif $G \to \mathfrak{A}_6$. Ainsi, G est isomorphe à un sous-groupe de $\mathfrak{A}_6$ d'indice 2 (car $\#\mathfrak{A}_6 = 360$) donc distingué. Puisque $6 \geqslant 5$ et que G est non trivial, on obtiendrait un sous-groupe distingué non trivial dans $\mathfrak{A}_6$, contredisant sa simplicité. Il s'ensuit que $n_5 \neq 6$ et donc $n_5 = 36$.
2. Comme en question précédente (et avec des notations évidentes), n_3 est congru à 1 modulo 3 et divise 20. Par simplicité de G, $n_3 \in \{4, 10\}$. Si $n_3 = 4$, on obtiendrait de même un morphisme injectif de G dans $\mathfrak{S}_4$ ce qui est absurde car $\#G > 24$. Ainsi, $n_3 = 10$.

   Soient S et T deux 3-Sylow distincts et $g \in S \cap T$. Supposons que $g \neq e$ et posons $Z = \{x \in G \ : \ xg = gx\}$ le centralisateur de g dans G. On sait qu'un groupe d'ordre 9 est abélien [20], Z contient S et T donc Z a au moins 10 éléments et son cardinal divise 180 tout en étant un multiple de 9 donc [21] $\#Z \in \{18, 36, 45, 90\}$. Or, l'action transitive de G sur G/Z (qui est donc de cardinal $\geqslant 2$) fournit (par simplicité), un morphisme injectif de G dans $\mathfrak{S}(G/Z)$. Pour des raisons de cardinalité, on a nécessairement $\#Z = 18$ car $180/36 = 5$ et $5! = 120 < 180$. Ainsi, S et T sont aussi deux 3-Sylow de Z mais par les théorèmes de Sylow, un groupe d'ordre 18 admet un unique 3-Sylow donc on aurait $S = T$ et une contradiction [22]. Finalement, on a bien $S \cap T = \{e\}$. On en déduit que G contient exactement $10 \times 8 = 80$ éléments d'ordre 3 ou 9.
3. Par **1.**, on a $36 \times 4 = 144$ éléments d'ordre 5 (car ce sont des groupes d'ordre 5 et donc deux à deux distincts car cycliques). On obtient ainsi en combinant avec **2.**, au moins $144 + 80 = 224$ éléments dans G. On aboutit à une contradiction et il n'existe aucun groupe simple d'ordre 180.

Exercice 10. Soient p et q deux nombres premiers distincts.

1. Soit G un groupe simple d'ordre $p^\alpha m$ avec $\alpha \geqslant 1$ et $p \nmid m$. On note n_p le nombre de p-Sylow de G. Montrer que $\#G$ divise $n_p!$.
2. Montrer qu'un groupe d'ordre $p^m q^n$ avec $p < q$, $1 \leqslant m \leqslant 2$ et $n \geqslant 1$ n'est pas simple.
3. Montrer qu'un groupe d'ordre $p^2 q$ ou $p^3 q$ n'est pas simple. Classifier les groupes d'ordre $p^2 q$.
4. Montrer qu'un groupe non commutatif d'ordre < 60 n'est pas simple.

Solution.
On rappelle que dans le cours, on a vu que les théorèmes de Sylow impliquent qu'un groupe d'ordre pq n'est pas simple pour p et q deux nombres premiers distincts et que si $p < q$ et $p \nmid q - 1$, alors tout groupe d'ordre pq est cyclique.

1. On fait agir (transitivement) G sur l'ensemble S_p des ses n_p p-Sylow. Par simplicité, $n_p > 1$ et on a alors un morphisme non trivial $G \to \mathfrak{S}(S_p) \cong \mathfrak{S}_{n_p}$. Par simplicité de G, ce morphisme est injectif et donc par Lagrange $\#G \mid n_p!$.

19. En effet, pour G_1, G_2 deux groupes, on a clairement que $Z(G_1) \times Z(G_2) \subseteq Z(G_1 \times G_2)$ et réciproquement il est clair que si $(g_1, g_2) \in Z(G_1 \times G_2)$, alors $g_1 \in Z(G_1)$ et $g_2 \in Z(G_2)$. De même, un commutateur de $G_1 \times G_2$ est clairement de la forme $([g_1, g_1'], [g_2, g_2'])$ avec $g_1, g_1' \in G_1$ et $g_2, g_2' \in G_2$ si bien que $D(G_1 \times G_2) = D(G_1) \times D(G_2)$.

20. Supposons que ce ne soit pas le cas. Alors le centre est non trivial car on a affaire à un 3-groupe et différent du groupe entier. Par Lagrange, il est de cardinal 3 mais alors le quotient du groupe par son centre est aussi de cardinal 3 donc cyclique. On sait alors que cela implique que le groupe soit abélien. On a donc une contradiction et tout groupe d'ordre 9 est abélien. Noter que ce raisonnement est valable pour tout groupe d'ordre p^2 avec p premier.

21. On peut éliminer 180 car sinon $g \neq e$ est dans $Z(G)$ qui est donc non trivial et distingué donc égal à G par simplicité, ce qui implique que G est abélien mais il ne peut alors pas être simple car 180 n'est pas premier.

22. Ou plus simplement ici, on peut remarquer que les 3-Sylow sont de cardinal 9 donc d'indice 2, donc distingués et ainsi nécessairement égaux car un 3-Sylow distingué est unique.

2. Si $m = 1$, alors comme dans la preuve du cas pq, on note n_q le nombre de q-Sylow. Par les théorèmes de Sylow, $n_q \mid p$ et n_q est congru à 1 modulo q^n. Comme $p < q$, on a nécessairement $n_q = 1$ et l'unique q-Sylow est distingué et G n'est pas simple[23].

Soit maintenant $m = 2$. Supposons G simple. On sait que n_q est congru à 1 modulo q et divise p^2. Ainsi par simplicité et car $p < q$, $n_q = p^2$ et $q \mid p^2 - 1 = (p+1)(p-1)$ donc par primalité de q, $q \leqslant p+1$ et comme $p < q$, on a $p = q+1$ si bien que $p = 2$ et $q = 3$. Ainsi $\#G = 4 \times 3^n$. Par **1.**, $4 \times 3^n \mid 4!$ donc $3^n \mid 6$ et donc $n = 1$ et G est de cardinal 12. On a alors par les théorèmes de Sylow et simplicité que $n_2 = 3$ et donc $\#G \mid 3!$, ce qui est absurde. Un tel groupe ne peut donc pas être simple.

3. Supposons un tel G simple. Si $q < p$, alors on applique **2.** en inversant les rôles de p et de q pour traiter le cas p^2q et si $p < q$, on applique directement **2.** et de même inverser les rôles de p et de q permet de traiter le cas p^3q avec $q < p$. Il suffit de traiter le cas p^3q avec $p < q$. On a toujours n_q congru à 1 modulo q et $n_q \mid p^3$. Comme $p < q$, $n_q \in \{p^2, p^3\}$. Comptons alors les éléments d'ordre q dans G. On en a exactement $n_q(q-1)$. Si alors $n_q = p^3$, G contient au moins $p^3(q-1) = \#G - p^3$ éléments d'ordre q. le complémentaire de ces éléments est donc d'ordre p^3 et donc un p-Sylow, ce qui assure son unicité (car il ne contient aucun élément d'ordre q). Ainsi $n_p = 1$ ce qui contredit la simplicité de G. On peut donc supposer que $n_q = p^2$. Dans ce cas, la condition n_q congru à 1 fournit que $p \mid p^2 - 1$ et donc que $q = p+1$ et $p = 2$, $q = 3$ si bien que $\#G = 24$. On a alors nécessairement, $n_2 = 3$ (par simplicité et les théorèmes de Sylow) et $\#G$ devrait diviser 3!, ce qui est absurde à nouveau. On en déduit donc bien qu'un tel groupe est non simple.

Venons-en à la classification des groupes d'ordre p^2q à isomorphisme près. Soit G un tel groupe. On note $n_p \in \{1, q\}$ et $n_q \in \{1, p, p^2\}$ le nombre de p-Sylow et de q-Sylow respectivement. Supposons dans un premier temps que $n_q = p^2$. Cela implique que $q \mid p^2 - 1$. Ainsi, G possède $p^2(q-1) = \#G - p^2$ éléments d'ordre q et le complémentaire de ces éléments est l'unique p-Sylow de G. On a donc $n_p = 1$. Si maintenant $n_q = p$, alors $q \mid p - 1$ et on ne peut pas avoir $n_p = q$ car alors $p \mid q - 1$ ce qui est absurde donc $n_p = 1$. On est donc dans un des 4 cas de figure suivants :

- On a $q \mid p^2 - 1$ et $n_p = 1$, $n_q = p^2$. Dans ce cas, on voit que l'unique p-Sylow S_p est distingué, que $S_p \cap S_q = \{e\}$ pour des raisons d'ordre pour un q-Sylow S_q quelconque et $S_pS_q = G$ pour des raisons de cardinalité si bien que $G = S_p \rtimes S_q$. Or, $S_q \cong \mathbf{Z}/q\mathbf{Z}$ et $S_p \cong \mathbf{Z}/p^2\mathbf{Z}$ si S_p contient un élément d'ordre p^2 et $S_p \cong (\mathbf{Z}/p\mathbf{Z})^2$ si tous les éléments non triviaux sont d'ordre p (on peut par exemple obtenir que ce groupe est abélien en raisonnant comme dans la note de bas de page numéro 9). Noter que ce produit direct est non trivial sinon le groupe serait abélien et tout sous-groupe serait distingué ce qui contredit le fait que $n_q \neq 1$;
- On a $q \mid p - 1$, $n_p = 1$ et $n_q = p$ et de même $G = S_p \rtimes S_q$ où le produit semi-direct est non trivial et $S_q \cong \mathbf{Z}/q\mathbf{Z}$ et $S_p \cong \mathbf{Z}/p^2\mathbf{Z}$ ou $S_p \cong (\mathbf{Z}/p\mathbf{Z})^2$;
- On a $p \mid q - 1$, $n_p = q$ et $n_q = 1$ et de même $G = S_q \rtimes S_p$ où le produit semi-direct est non trivial et $S_q \cong \mathbf{Z}/q\mathbf{Z}$ et $S_p \cong \mathbf{Z}/p^2\mathbf{Z}$ ou $S_p \cong (\mathbf{Z}/p\mathbf{Z})^2$;
- On a $n_p = n_q = 1$, auquel cas d'après le cours et en utilisant le même raisonnement que ci-dessus, $G \cong S_p \times S_q$ soit $G \cong \mathbf{Z}/q\mathbf{Z} \times \mathbf{Z}/p^2\mathbf{Z} \cong \mathbf{Z}/p^2q\mathbf{Z}$ soit $G \cong \mathbf{Z}/q\mathbf{Z} \times (\mathbf{Z}/p\mathbf{Z}) \cong \mathbf{Z}/pq\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$. On a là tous les groupes abéliens d'ordre p^2q à isomorphisme près.

Reste donc à classifier les produits semi-directs non triviaux $\mathbf{Z}/p^2\mathbf{Z} \rtimes \mathbf{Z}/q\mathbf{Z}$ et $(\mathbf{Z}/p\mathbf{Z})^2 \rtimes \mathbf{Z}/q\mathbf{Z}$.

- Puisque $\mathrm{Aut}\left(\mathbf{Z}/p^2\mathbf{Z}\right)$ est cyclique d'ordre $p(p-1)$, il existe un produit semi-direct non trivial $\mathbf{Z}/p^2\mathbf{Z} \rtimes \mathbf{Z}/q\mathbf{Z}$ si, et seulement si, $q \mid p - 1$ et dans ce cas on a une unique classe d'isomorphisme de tel groupe en utilisant le fait que $\mathbf{Z}/p(p-1)\mathbf{Z}$ possède un seul sous-groupe d'ordre q et en utilisant l'exercice 9 question **3.**
- De même, on a que $\mathrm{Aut}\left((\mathbf{Z}/p\mathbf{Z})^2\right) \cong \mathrm{GL}_2(\mathbf{F}_p)$ (car un tel automorphisme est donné par l'image des deux générateurs $(1,0)$ et $(0,1)$ dans $\mathbf{F}_p^2$ et qu'un tel morphisme est nécessairement $\mathbf{F}_p$-linéaire). Le cardinal de $\mathrm{GL}_2(\mathbf{F}_p)$ est de $(p^2-1)(p^2-p)$. Ainsi, un produit semi-direct non trivial existe si, et seulement si, $q \mid p^2 - 1$. Dénombrons alors sous cette hypothèse le nombre de telles classes d'isomorphisme. On a que deux morphismes non triviaux $\psi, \varphi : \mathbf{Z}/q\mathbf{Z} \to \mathrm{GL}_2(\mathbf{F}_p)$ sont isomorphes si, et seulement si, les deux sous-groupes $\psi\left(\mathbf{Z}/q\mathbf{Z}\right)$ et $\varphi\left(\mathbf{Z}/q\mathbf{Z}\right)$ sont conjugués dans $\mathrm{GL}_2(\mathbf{F}_p)$ (cela découle de la question **2.** de l'exercice 9). Le problème devient donc un problème d'algèbre linéaire où il s'agit de déterminer les classes de conjugaison de sous-groupes d'ordre q de $\mathrm{GL}_2(\mathbf{F}_p)$. On voit facilement que deux matrices non scalaires de $\mathrm{GL}_2(\mathbf{F}_p)$ sont conjuguées si, et seulement si, elles ont les mêmes valeurs propres[24] (car, par exemple, elles le sont si, et seulement si, elles ont la même suite d'invariant de similitude et qu'une matrice non scalaire de taille 2 a son polynôme minimal égal à son polynôme caractéristique). Or, deux matrices d'ordre q ont pour valeurs propres des racines q-ièmes de l'unité dans $\mathbf{F}_p$. Si les deux valeurs propres sont 1, la matrice est semblable[25] à $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et est d'ordre p, ce qui est absurde. On a donc les cas suivants :

23. Le résultat pq^n pour la résolubilité (en fait un groupe simple est résoluble si, et seulement si, il est commutatif) est dû à Frobenius, le cas p^2q^n à Jordan et le cas général p^mq^n à Burnside en utilisant la théorie des représentations.

24. Ou alors on remarque que si tout élément de $\mathbf{F}_p^2$ est vecteur propre si, et seulement si, M est scalaire.Il existe donc $v \in \mathbf{F}_p^2$ non nul qui n'est pas un vecteur propre. On voit alors que dans la base (v, Mv), la matrice M est donnée par $\begin{pmatrix} 0 & \det(M) \\ 1 & \mathrm{Tr}(M) \end{pmatrix}$ si bien que deux matrices non scalaires sont bien semblables si, et seulement si, elles ont mêmes valeurs propres (avec multiplicité).

25. On rappelle qu'on regarde les matrices non scalaires !

i) Si $q = 2$, on obtient trois classes de conjugaison de matrices d'ordre 2, à savoir $-I_2$, $\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et on obtient donc deux classes d'isomorphismes de produits semi-directs non triviaux $(\mathbf{Z}/p\mathbf{Z})^2 \rtimes \mathbf{Z}/q\mathbf{Z}$. On vérifie que ces trois classes d'isomorphismes ont trois générateurs x, y et z tels que $x^p = y^p = z^2 = e$, $xy = yx$ et[26] $zx = x^{-1}z$ et $zy = y^{-1}z$, $zx = x^{-1}z$ et $zy = xy^{-1}z$, $zx = xz$ et $zy = y^{-1}z$ respectivement. Noter que le dernier est isomorphe à $\mathbf{Z}/p\mathbf{Z} \times D_{2p}$;

ii) Si $q \neq 2$, $q \mid p-1$ et $q \nmid p+1$. Alors $\mathbf{F}_p^\times$ contient exactement q racines q-ièmes de l'unité. En effet, on sait que $\mathbf{F}_p^\times$ est cyclique engendré disons par un élément g. Les racines q-ièmes de l'unité sont les éléments vérifiant $x^q = 1$. Un tel x est de la forme g^m et on cherche donc les $m \in \{0, \dots, p-1\}$ tels que $g^{qm} = 1$. On cherche donc les m tels que $p-1 \mid qm$ soit $\frac{p-1}{q} \mid m$, ce qui fournit bien q éléments et en réalité l'ensemble de ces q racines forme un groupe cyclique d'ordre q. Notons ξ une racine q-ième primitive, autrement dit un générateur de ce groupe. Tout sous-groupe d'ordre q est alors engendré par un élément dont les valeurs propres sont ξ et ξ^r avec $0 \leqslant r < q$ (on a a priori ξ^s et ξ^r mais en prenant une puissance de cette matrice, on transforme la valeur propre ξ^s en ξ). Deux tels sous-groupes sont conjugués si, et seulement si, il existe $1 \leqslant s < q$ tel que $1 = s$ et $r = sr'$ ou $1 = r's$ et $r = s$ soit si, et seulement si, $r = r'$ ou ($r \neq 0$ et $r' = r^{-1}$ modulo q). On obtient donc $\frac{q-3}{2} + 3 = \frac{q+3}{2}$ (on a tous les couples (r, r^{-1}) avec $r \neq r^{-1}$ dans $\mathbf{F}_p^\times$ et les paires $(1,1)$, $(-1,-1)$ et $(1,0)$) tels groupes de cardinal q non conjugués 2 à 2, soit $\frac{q+3}{2}$ classes d'isomorphismes de produits semi-directs non triviaux $(\mathbf{Z}/p\mathbf{Z})^2 \rtimes \mathbf{Z}/q\mathbf{Z}$;

iii) Si $q \neq 2$ et $q \nmid p-1$ et $q \mid p+1$, le raisonnement précédent montre qu'on n'a aucune racine q-ième de l'unité dans $\mathbf{F}_p^\times$ à part 1. Ainsi, une matrice d'ordre q est de déterminant le produit de ses valeurs propres qui sont des racines q-ièmes (dans une clôture algébrique ou même un corps de décomposition) donc leur produit aussi mais est dans $\mathbf{F}_p^\times$ donc il vaut 1 et les deux valeurs propres sont inverses l'une de l'autre, différentes de 1. Par conséquent, pour deux matrices A et B d'ordre q, B est conjuguée à une puissance de A première à q (car on passe des valeurs propres de A à celles de B en prenant une puissance première à q). On obtient donc un unique groupe d'ordre q à conjugaison près et une unique classe d'isomorphisme de produits semi-directs non triviaux $(\mathbf{Z}/p\mathbf{Z})^2 \rtimes \mathbf{Z}/q\mathbf{Z}$;

iv) De même, il existe un produit semi-direct non trivial $\mathbf{Z}/q\mathbf{Z} \rtimes \mathbf{Z}/p^2\mathbf{Z}$ si, et seulement si, $p \mid q-1$. Si $p \mid q-1$ mais $p^2 \nmid q-1$, l'exercice 9 question **3.** garantit qu'on a une seule classe d'isomorphisme de tels produits semi-directs tandis que si $p^2 \mid q-1$ (alors un générateur de $\mathbf{Z}/p^2\mathbf{Z}$ peut être envoyé soit sur un élément d'ordre p soit sur un élément d'ordre p^2) on a deux classes d'isomorphisme de tels produits semi-directs ;

v) De même, il existe un produit semi-direct non trivial $\mathbf{Z}/q\mathbf{Z} \rtimes (\mathbf{Z}/p\mathbf{Z})^2$ si, et seulement si, $p \mid q-1$. Alors $\mathrm{Aut}\,(\mathbf{Z}/q\mathbf{Z})$ admet un unique sous-groupe d'ordre p et deux morphismes non triviaux de $(\mathbf{Z}/p\mathbf{Z})^2$ vers ce groupe diffèrent par un automorphisme de[27] $(\mathbf{Z}/p\mathbf{Z})^2$, ce qui assure par l'exercice 9 question **1.** qu'on a une seule classe d'isomorphisme de tels produits semi-directs.

En conclusion, on a la classification :

- Si $p \nmid q-1$ et $q \nmid p^2-1$, deux groupes abéliens $\mathbf{Z}/p^2q\mathbf{Z}$ et $\mathbf{Z}/p^{\mathbf{Z}} \times \mathbf{Z}/pq\mathbf{Z}$;
- Si $p \mid q-1$, $p^2 \nmid q-1$ et $q \nmid p^2-1$, on a deux groupes abéliens $\mathbf{Z}/p^2q\mathbf{Z}$ et $\mathbf{Z}/p^{\mathbf{Z}} \times \mathbf{Z}/pq\mathbf{Z}$, un produit semi-direct non trivial $\mathbf{Z}/q\mathbf{Z} \rtimes \mathbf{Z}/p^2\mathbf{Z}$ et un produit semi-direct non trivial $\mathbf{Z}/q\mathbf{Z} \rtimes (\mathbf{Z}/p\mathbf{Z})^2$;
- Si $p^2 \mid q-1$ et $q \nmid p^2-1$, on a deux groupes abéliens $\mathbf{Z}/p^2q\mathbf{Z}$ et $\mathbf{Z}/p^{\mathbf{Z}} \times \mathbf{Z}/pq\mathbf{Z}$, deux produits semi-directs non triviaux $\mathbf{Z}/q\mathbf{Z} \rtimes \mathbf{Z}/p^2\mathbf{Z}$ et un produit semi-direct non trivial $\mathbf{Z}/q\mathbf{Z} \rtimes (\mathbf{Z}/p\mathbf{Z})^2$;
- Si $q \mid p-1$ et $q \neq 2$, on a deux groupes abéliens $\mathbf{Z}/p^2q\mathbf{Z}$ et $\mathbf{Z}/p^{\mathbf{Z}} \times \mathbf{Z}/pq\mathbf{Z}$, un produit semi-direct non trivial $\mathbf{Z}/p^2\mathbf{Z} \rtimes \mathbf{Z}/q\mathbf{Z}$ et $\frac{q+3}{2}$ produits semi-directs non triviaux $(\mathbf{Z}/p\mathbf{Z})^2 \rtimes \mathbf{Z}/q\mathbf{Z}$;
- Si $q \mid p+1$, $q \neq 2$, on obtient deux groupes abéliens $\mathbf{Z}/p^2q\mathbf{Z}$ et $\mathbf{Z}/p^{\mathbf{Z}} \times \mathbf{Z}/pq\mathbf{Z}$ et un produit semi-direct non trivial $(\mathbf{Z}/p\mathbf{Z})^2 \rtimes \mathbf{Z}/q\mathbf{Z}$;
- Si $q = 2$, on a deux groupes abéliens $\mathbf{Z}/2p^2\mathbf{Z}$ et $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/2p\mathbf{Z}$, un produit semi-direct non trivial $\mathbf{Z}/p^2\mathbf{Z} \rtimes \mathbf{Z}/q\mathbf{Z}$ et deux produits semi-directs non triviaux $(\mathbf{Z}/p\mathbf{Z})^2 \rtimes \mathbf{Z}/q\mathbf{Z}$;
- Si $p = 2$ et $q = 3$, on retrouve les groupes d'ordre 12 et on a deux groupes abéliens $\mathbf{Z}/12\mathbf{Z}$ et $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$, un produit semi-direct non trivial $\mathbf{Z}/3\mathbf{Z} \rtimes \mathbf{Z}/4\mathbf{Z}$, un produit semi-direct non trivial $(\mathbf{Z}/2\mathbf{Z})^2 \rtimes \mathbf{Z}/3\mathbf{Z}$ et un produit semi-direct non trivial $\mathbf{Z}/3\mathbf{Z} \rtimes (\mathbf{Z}/2\mathbf{Z})^2$.

On rappelle qu'on peut procéder de même pour classifier les groupes d'ordre pq avec $p < q$ et qu'on obtient la classification suivante :

- Si $p \nmid q-1$, on a un unique groupe $\mathbf{Z}/pq\mathbf{Z}$;
- Si $p \mid q-1$, on a $\mathbf{Z}/pq\mathbf{Z}$ et un unique produit semi-direct $\mathbf{Z}/q\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}$.

On en déduit par exemple que tout groupe d'ordre $2q$ avec q premier impair est isomorphe soit à $\mathbf{Z}/2q\mathbf{Z}$ soit à D_q.

26. En gros on fait
$$(1,z)(x,1) = (z\dot{x}, z) = (x^{-1}, z) = (x^{-1}, 1)(1, z).$$

27. Notons g un générateur du groupe d'ordre p. Deux morphismes de $(\mathbf{Z}/p\mathbf{Z})^2$ vers ce groupe d'ordre p correspondent à se donner deux couples d'entiers de $\{0, \dots, p-1\}$, (k_i, ℓ_i), qui correspondent aux images de $(1,0)$ et $(0,1)$. Les morphismes étant non triviaux, $(k_i, \ell_i) \neq (0,0)$ et on peut les compléter en une base $((k_i, \ell_i), e_i)$ de $\mathbf{F}_p^2$ et il existe alors $M \in \mathrm{GL}_2(\mathbf{F}_p)$ tel que $(k_2, \ell_2) = {}^tM(k_1, \ell_1)$, ce qui se traduit par le fait que $\psi = \varphi M$ et que ψ et φ diffèrent par un automorphisme de $(\mathbf{Z}/p\mathbf{Z})^2$.

4. Soit G non commutatif de cardinal < 60. On peut éliminer tous les cardinaux une puissance de p car le centre d'un p-groupe est non trivial et distinct de G tout entier lorsque G est non abélien. cela fournit la non simplicité. Par les questions précédentes, on peut aussi enlever tous les groupes d'ordre pq, pq^n ou p^2q^n avec $p < q$ ainsi que ceux de la forme p^3q ou p^2q. En énumérant les entiers < 60, on voit que cela laisse les groupes d'ordre 30, 42 et 48.
   - Soit G d'ordre[28] $30 = 2 \times 3 \times 5$ que l'on suppose simple. Les théorèmes de Sylow assurent alors que $n_3 = 10$ et $n_5 = 6$ et l'intersection de deux 3-Sylow (respectivement 5-Sylow) de G est triviale ce qui fournit 20 éléments d'ordre 3 et 24 d'ordre 5. On a donc $\#G \geqslant 44$ et une contradiction. Un tel groupe G est donc non simple.
   - Soit G d'ordre $42 = 2 \times 3 \times 7$ alors $n_7 = 1$ et G admet un unique 7-Sylow distingué et n'est par conséquent pas simple ;
   - Soit G d'ordre $48 = 2^4 \times 3$ que l'on suppose simple. On a alors $n_2 = 3$ et la question **1.** garantit alors que $48 \mid 3! = 6$, ce qui est absurde. Un tel groupe est donc non simple.

Exercice 11 — Groupes résolubles.

1. Montrer que tout sous-groupe et tout groupe quotient d'un groupe résoluble est résoluble.
2. Montrer plus généralement que toute extension d'un groupe résoluble par un groupe résoluble est résoluble.
3. Donner un exemple d'un groupe résoluble qui n'est pas nilpotent.
4. Soient p et q deux nombres premiers distincts. Montrer que tout groupe d'ordre pq est résoluble.
5. Même question pour les groupes d'ordre pqr, si p, q, r sont trois nombres premiers (on pourra évaluer le nombre d'éléments d'ordre p et le nombre d'éléments d'ordre q).
6. Même question pour les groupes d'ordre p^2q.

Solution.

1. On utilise le fait que G est résoluble si, et seulement s'il existe un entier n tel que $D^n(G) = \{e\}$. On constate alors que si $H \leqslant G$, pour tout n, $D^n(H) \leqslant D^n(G)$ donc H est résoluble. Soit maintenant $H \lhd G$ et considérons le groupe quotient G/H. On a alors le morphisme surjectif canonique $\pi : G \to G/H$ et par surjectivité, $D^n(G/H) = \pi(D^n(G))$ pour tout n, ce qui permet de conclure. On voit alors que de façon plus générale si $f : G \to H$ est un morphisme de groupes surjectif avec G résoluble, alors H est résoluble. On peut évidemment aussi voir "à la main" en regardant la liste des sous-groupes de $\mathfrak{S}_3$ que ce dernier n'est pas nilpotent.
2. Soit $1 \to N \to G \to H \to 1$ une suite exacte avec H et N deux groupes résolubles et montrons que G est résoluble. On sait alors que l'application $p : G \to H$ est surjective donc comme en **1.**, il s'ensuit qu'il existe un entier n tel que $\{e\} = D^n(H) = p(D^n(G))$ si bien que $D^n(G) \subseteq \mathrm{Ker}(p) = \mathrm{Im}(i) \cong N$ où $i : N \to G$ est injective. Ainsi, il existe un entier m tel que $D^m(i(H)) = \{e\}$ et alors $D^{n+m}(G) = \{e\}$ et G est résoluble.
3. Un groupe nilpotent est résoluble mais la réciproque est fausse comme en témoigne l'exemple du groupe $\mathfrak{S}_3$ (on aurait aussi pu prendre $\mathfrak{A}_4$ ou $\mathfrak{S}_4$). Une preuve est donnée page 32 du polycopié de cours, on pouvait aussi utiliser le fait (pour $G = \mathfrak{S}_3$ par exemple) que $D(G) = \mathfrak{A}_3$ qui est abélien donc $D^2(G) = \{e\}$ pour obtenir la résolubilité et le fait qu'un groupe est nilpotent si, et seulement s'il existe un entier n tel que $C^n(G) = \{e\}$ où $C^0(G) = G$ et $C^{n+1}(G)$ est le groupe engendré par les commutateurs $ghg^{-1}h^{-1}$ avec $g \in G$ et $h \in C^n(G)$ (la preuve étant analogue à celle dans le cas résoluble). On a dans notre cas, $C^1(G) = D(G) = \mathfrak{A}_3$ et $C^2(G)$ est alors un sous-groupe non trivial de $C^1(G) = \mathfrak{A}_3$ car $\mathfrak{A}_3$ n'est pas central dans G si bien que nécessairement $C^2(G) = \mathfrak{A}_3$ et par récurrence immédiate, $C^n(G) = \mathfrak{A}_3 \neq \{e\}$.
4. On peut utiliser le fait qu'on sait qu'un tel groupe est non simple. Il existe donc $H \lhd G$. On peut supposer sans perte de généralité que H est de cardinal p donc abélien et ainsi G/H est de cardinal q donc abélien et la suite $\{e\} \subseteq H \subseteq G$ montre que G est résoluble.
   On pouvait aussi reprendre la preuve de la non simplicité de G d'ordre pq sui établit que si $p < q$, alors G possède un seul q-Sylow qui est donc distingué.
   Reste à traiter le cas de $p = q$ mais on sait qu'un groupe d'ordre p^2 est abélien (voir note de bas de page numéro 9) donc résoluble. De manière générale, on sait qu'un p-groupe est nilpotent et donc résoluble[29].
5. On a le résultat d'après ce qui précède si $p = q = r$. Si deux des nombres premiers sont égaux, on est ramené à la question précédente, on supposera donc que $p < q < r$. On a alors que $n_r \in \{1, pq\}$ et $n_q \in \{1, r, pr\}$. Supposons que $n_r, n_q \neq 1$. Alors G admet exactement $pq(r-1)$ éléments d'ordre r et au moins $r(q-1)$ éléments d'ordre q. cela fournit que

$$\#G \geqslant pq(r-1) + r(q-1).$$

   Mais on remarque que

$$pq(r-1) + r(q-1) = pqr + rq - pq - r = \#G + (r-p)(q-1) - p > \#G$$

   car $r - p > 1$ et $q - 1 \geqslant p$. Ainsi $n_r = 1$ ou $n_q = 1$ et G admet un sous-groupe distingué d'ordre premier, donc abélien tel que le quotient soit un groupe de cardinal le produit de deux nombres premiers, donc résoluble. Ainsi, G est résoluble. En effet, si un groupe $H \lhd G$ est résoluble et que G/H aussi, alors G est résoluble par **2.**

28. Ce cas (ainsi que le suivant) découle aussi de l'exercice suivant et de la résolubilité des groupes d'ordre pqr.

29. En effet, on procède par récurrence sur n. Un groupe d'ordre p est bien nilpotent et supposons alors que $\#G = p^{n+1}$. On sait que $\{e\} \neq Z(G) \lhd G$ et donc on peut appliquer l'hypothèse de récurrence au p-groupe $Z(G)$. Il existe ainsi $\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = Z(G) \subseteq G_{n+1} = G$ avec $G_i \lhd Z(G)$ et donc comme ils sont centraux $G_i \lhd G$ et G_i/G_{i-1} inclus dans le centre de $Z(G)/G_{i-1}$ lui-même inclus dans le centre de G/G_{i-1}.

6. On a vu que dans ce cas, dans tous les cas soit le p-Sylow soit le q-Sylow est distingué. Chacun de ces Sylow est abélien et le quotient est de cardinal p^2 ou q donc abélien, ce qui permet de conclure.

On peut montrer de même qu'un groupe d'ordre $p^\alpha q$ avec $p > q$ (car $n_p = 1$ et un p-groupe est résoluble et le quotient abélien aussi), d'ordre[30] $p^\alpha q^\beta$ avec $p^\alpha < q+1$ (car $n_q = 1$ et des p-groupes sont résolubles) et d'ordre $p^\alpha q$ avec $p^\alpha \nmid (q-1)!$ sont non simples et résolubles. Dans ce dernier cas, on peut par exemple raisonner par récurrence sur α. Les cas $\alpha = 0$ ou 1 sont clairs. Supposons alors $\alpha > 1$ et le résultat connu pour les groupes d'ordre $p^\beta q$ avec $\beta < \alpha$. On sait que $n_p \in \{1, q\}$. Si $n_p = 1$ alors l'unique p-Sylow est distingué et résoluble en tant que p-groupe et le quotient de G par ce p-Sylow est d'ordre q donc lui aussi résoluble et on a le résultat. Si $n_p = q$, alors on a q p-Sylow et on fait agir un de ces p-Sylow, noté S sur les $q-1$ autres par conjugaison, cela fournit un morphisme $S \to \mathfrak{S}_{q-1}$. Un élément $s \in S$ est dans le noyau, il normalise tous les autres p-Sylow mais le normalisateur d'un p-Sylow est de cardinal p^α donc aussi un p-Sylow et $N_G(S_i)$ contient S_i donc $N_G(S_i) = S_i$ et donc le noyau de ce morphisme est le sous-groupe I donné par l'intersection des q p-Sylow de G. Ce noyau ne peut être trivial car sinon $p^\alpha \mid (q-1)!$ et est donc un p-groupe non trivial, donc résoluble. Par ailleurs, on a que

$$I = \bigcap_{T\ p-\text{Sylow}} T = \bigcap_{g\in G} gSg^{-1}$$

pour un p-Sylow S et I est alors clairement caractéristique donc distingué dans G. Le quotient G/I est alors un groupe de cardinal $p^\beta q$ avec $\beta < \alpha$ donc résoluble par hypothèse de récurrence et ainsi G est résoluble.
On peut alors déduire de tout cela que tout groupe d'ordre < 60 est résoluble.
Je rappelle qu'un groupe simple est résoluble si, et seulement s'il est commutatif (car $D(G) \lhd G$ et $D(G) \neq \{e\}$ donc $D(G) = G$) et cela a alors lieu si, et seulement si c'est un groupe d'ordre premier. Pour la culture, je mentionne le théorème de Feit-Thompson (qui est très profond et difficile mais qui a joué un rôle majeur dans la classification des groupes finis simples) conjecturé par Burnside en 1911 démontré en 1963 et qui stipule que tout groupe d'ordre impair est résoluble. On a enfin le résultat suivant (sorte de réciproque partielle du théorème de Lagrange) : G est résoluble si, et seulement si, pour tout $d \mid n = \#G$ tel que $\text{pgcd}\left(d, \frac{n}{d}\right) = 1$, G possède un sous-groupe d'ordre d.

Exercice 12 — Groupes simples d'ordre 60. Soit G un groupe simple d'ordre 60. On veut montrer que G est isomorphe au groupe alterné $\mathfrak{A}_5$.

1. Montrer que G admet six 5-Sylow.
2. En déduire qu'il existe un sous-groupe G' de $\mathfrak{A}_6$, d'indice 6, qui est isomorphe à G.
3. En faisant agir G' sur le quotient $\mathfrak{A}_6/G'$, plonger G' dans $\mathfrak{S}_5$.
4. Conclure.

Solution.

1. On sait que n_5 est congru à 1 modulo 5 et divise 12 donc $n_6 = 1$ ou 6 mais $n_6 \neq 1$ par simplicité de G donc $n_6 = 6$.
2. On fait agir G (transitivement) par conjugaison sur l'ensemble X de ces 5-Sylow ce qui fournit un morphisme non trivial (donc injectif par simplicité) $G \to \mathfrak{S}(X) \cong \mathfrak{S}_6$. En composant avec la signature, on a un morphisme $G \to \{\pm 1\}$ dont le noyau vaut G ou $\{e\}$ par simplicité mais pour des raisons de cardinalité, G ne peut pas s'injecter dans un groupe d'ordre 2 si bien que le noyau est égal à G et le morphisme est trivial, ce qui implique que les permutations obtenues dans l'image du morphisme $G \to \mathfrak{S}_6$ sont de signature 1 et donc qu'en réalité on a un morphisme injectif $\varphi : G \to \mathfrak{A}_6$ ce qui montre bien que $G \cong G' := \varphi(G) \leqslant \mathfrak{A}_6$ est isormorphe à un sous-groupe de $\mathfrak{A}_6$. L'indice de G' est de $\#\mathfrak{A}_6/\#G = 360/60 = 6$.
3. On fait alors agir G' sur le quotient $\mathfrak{A}_6/G'$, ce qui donne lieu à un morphisme non trivial (donc injectif par simplicité) $G' \to \mathfrak{S}(\mathfrak{A}_6/G') \cong \mathfrak{S}_6$. Mais on remarque pour tout $g' \in G'$, $g'G' = G'$ si bien que les permuations obtenues ont toutes la classe G' comme point fixe et induisent donc toutes une permutation de $\mathfrak{S}_5$. On a donc en réalité un morphisme injectif $G' \to \mathfrak{S}_5$.
4. On a donc que G' et donc G est isomorphe à un sous-groupe de $\mathfrak{S}_5$ d'indice 2. Un tel sous-groupe est nécessairement distingué et isomorphe à $\mathfrak{A}_5$. On pouvait aussi voir que le morphisme avait pour image $\mathfrak{A}_5$ comme précédemment et conclure par cardinalité.

On peut aussi comme dans https://www.ljll.math.upmc.fr/micheld/agreg/GroupeSimpleOrdre60.pdf établir que $n_2 = 5$ et faire agir G sur l'ensemble de ses 2-Sylow. Et voici maintenant une preuve en sonnet (dû à A. Chambert-Loir ?) :

Que le groupe alterné, en cinq lettres au moins
Est simple. – Voilà, mon cher, ce qu'il faut démontrer.
C'est dans le cours d'algèbre du Professeur Perrin
Que j'appris cette preuve, je vais te la donner.

Tout y repose, en fait, sur l'observation
Qu'un sous-groupe normal est immanquablement
La réunion de classes de conjugaison
Dont les ordres s'ajoutent. – Oui, c'est ça l'argument !

Quand n égale 5, ces classes s'énumèrent

30. À rapprocher du théorème de Burnside mentionné plus haut !

Et leur ordre se comptent, s'il le faut, un par un :
Il y a un, quinze, douze (deux fois) et puis vingt.

Et quand on les combine, de quelconque manière,
À moins des cas triviaux, de soixante un facteur
L'addition ne peut être. Q.e.d. Quel bonheur!

Exercice 13. Soient H et N des groupes et soient φ et $\psi : H \longrightarrow \mathrm{Aut}(N)$ des morphismes. On veut trouver des conditions pour que $N \rtimes_\varphi H$ et $N \rtimes_\psi H$ soient isomorphes.

1. S'il existe un automorphisme α de H tel que $\psi = \varphi \circ \alpha$, montrer que l'on a le résultat attendu.
2. S'il existe un automorphisme u de N tel que
$$\forall h \in H, \quad \varphi(h) = u \circ \psi(h) \circ u^{-1},$$
montrer que la conclusion vaut encore.
3. Si H est cyclique et si $\varphi(H) = \psi(H)$, montrer que $N \rtimes_\varphi H$ et $N \rtimes_\psi H$ sont isomorphes.
4. Si N est abélien et qu'il existe un isomorphisme $f : N \rtimes_\psi H \longrightarrow N \rtimes_\varphi H$ tel que $f(N) = N$, montrer alors qu'il existe $u \in \mathrm{Aut}(N)$ et $\alpha \in \mathrm{Aut}(H)$ tels que
$$\forall h \in H, \quad \varphi \circ \alpha(h) = u \circ \psi(h) \circ u^{-1}.$$

Solution.

1. On pose
$$f : \left\{ \begin{array}{ccc} N \rtimes_\psi H & \longrightarrow & N \rtimes_\varphi H \\ (n,h) & \longmapsto & (n, \alpha(h)). \end{array} \right.$$
On obtient bien un morphisme puisque
$$f((n,h)(n',h')) = f(n\psi(h)(n'), hh') = (n\psi(h)(n'), \alpha(h)\alpha(h'))$$
et
$$f(n,h)f(n',h') = (n,\alpha(h))(n',\alpha(h')) = (n\varphi(\alpha(h))(n'), \alpha(h)\alpha(h')) = (n\psi(h)(n'), \alpha(h)\alpha(h').$$
Ce morphisme est alors clairement un isomorphisme car α est un automorphisme.
2. On pose cette fois
$$f : \left\{ \begin{array}{ccc} N \rtimes_\psi H & \longrightarrow & N \rtimes_\varphi H \\ (n,h) & \longmapsto & (u(n), h). \end{array} \right.$$
On obtient bien un morphisme puisque
$$f((n,h)(n',h')) = f(n\psi(h)(n'), hh') = (u(n)u(\psi(h)(n')), hh')$$
et
$$f(n,h)f(n',h') = (u(n),h)(u(n'),h') = (u(n)\varphi(h)(u(n')), hh') = (u(n)u(\psi(h)(n')), hh').$$
Ce morphisme est alors clairement un isomorphisme car u est un automorphisme. Noter que $f(N) = N$.
3. Sous ces hypothèses, le groupe H est isomorphe à un $\mathbf{Z}/n\mathbf{Z}$ et $\psi(H)$ et $\varphi(H)$ sont isomorphes à $\mathbf{Z}/m\mathbf{Z}$ pour un certain $m \mid n$. Il existe donc d premier à m tel que $\varphi(1) = d\psi(1)$ dans $\mathbf{Z}/m\mathbf{Z}$. L'application $(\mathbf{Z}/n\mathbf{Z})^\times \to (\mathbf{Z}/m\mathbf{Z})^\times$ qui à $\overline{m}$ associe $\overline{m}$ étant surjective, il existe $d' \in (\mathbf{Z}/n\mathbf{Z})^\times$ qui s'envoie sur d. La multiplication par d' est alors un automorphisme de $\mathbf{Z}/n\mathbf{Z}$ qui vérifie $\varphi = \psi \circ \alpha$ et on conclut par **1.**
4. L'application $u = f_{|N}$ est un automorphisme de N et f induit un isomorphisme[31] $\tilde{f} : N \rtimes_\psi H/N \cong H \longrightarrow N \rtimes_\varphi H/N \cong H$ donné par $\overline{(n,h)} \mapsto \overline{f(n,h)}$ bien défini et bijectif car $f(N) = N$. On pose alors $\alpha = \tilde{f}$ vu comme automorphisme de H. Soit alors $h \in H$, on a pour tout $n \in N$
$$u \circ \psi(h) \circ u^{-1}(n) = f((1,h)(f^{-1}(n),1)(1,h^{-1})).$$
En effet,
$$(1,h)(f^{-1}(n),1) = (\psi(h)(f^{-1}(n)), h) \quad \text{et} \quad f((1,h)(f^{-1}(n),1)(1,h^{-1})) = f(\psi(h)(f^{-1}(n)),1)$$
tandis que
$$u \circ \psi(h) \circ u^{-1}(n) = f(\psi(h)(f^{-1}(n)))$$
et où l'on identifie N avec les $(n,1)$, $n \in N$. On a donc
$$u \circ \psi(h) \circ u^{-1}(n) = f(1,h)f(f^{-1}(n),1)f(1,h^{-1}) = f(1,h)(n,1)f(1,h^{-1}).$$

31. On a un morphisme $N \rtimes H \longrightarrow H$ donné par $(n,h) \mapsto h$ de noyau isomorphe à N. Donc α envoie h sur la classe de $(1,h)$ qui est envoyé sur la classe de $f(1,h)$ mais il est aussi envoyé sur $\alpha(h)$ qui correspond à la classe de $(1,\alpha(h))$.

Par ailleurs,

$$\varphi(\alpha(h))(n) = (1, \alpha(h))(n, 1)(1, \alpha(h)^{-1})$$

car

$$(1, \alpha(h))(n, 1)(1, \alpha(h)^{-1}) = (\varphi(\alpha(h))(n), \alpha(h))(1, \alpha(h)^{-1}) = (\varphi(\alpha(h))(n), 1).$$

Maintenant $x = (1, \alpha(h))$ et $y = f(1, h)$ ont la même image dans $N \rtimes_\varphi H/N$ car z pour un certain $a \in N$. Il existe donc $n \in N$ tel que $x = ya$. On a alors en notant $b = (n, 1)$ que $xbx^{-1} = yaba^{-1}y^{-1} = yby^{-1}$ car N est abélien si bien qu'on a bien

$$u \circ \psi(h) \circ u^{-1}(n) = \varphi \circ \alpha(h)(n)$$

ce qui conclut la démonstration en utilisant **1.** et **2**.

Il est important de savoir qu'on a ici exhibé des conditions suffisantes (très utiles) pour garantir que des produits semi-directs sont isomorphes mais il n'existe pas de CNS générale et il faut raisonner au cas par cas. Par exemple, un article de recherche de 2011 concerne les classes d'isomorphismes de produits semi-directs avec le groupe cyclique infini[32] $\mathbf{Z}$.

Exercice 14.

1. Montrer que $\mathrm{SL}_2(\mathbf{F}_3)$ possède un unique 2-Sylow que l'on identifiera.
2. Classifier les groupes de cardinal $\leqslant 15$.

Solution.

1. Comme dans l'exercice 3, on voit que les éléments de $\mathrm{SL}_2(\mathbf{F}_3)$ (qui est de cardinal $24 = 8 \times 3$) d'ordre 2 sont :
   - La matrice I_2 d'ordre 1 ;
   - La matrice $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ d'ordre 2 ;
   - Les matrices $\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}$ d'ordre 4.

   Il y a donc un unique 2-Sylow constitué de ces 8 éléments et il est clairement isomorphe à $\mathbf{H}_8$.
2. Tout découle de la classification déjà effectuée dans la correction du TD I pour les groupes de cardinal $\leqslant 8$. Ensuite, on a vu (voir note de bas de page numéro 9) qu'un groupe de cardinal 9 est abélien et il en va de même des groupes d'ordre 11 et 13. Les groupes d'ordre 10, 14 et 15 sont des groupes d'ordre pq classifiés dans le cours ce qui laisse les groupes d'ordre 12 que l'on peut classifier en utilisant l'exercice 6 question **3.** ou que l'on peut refaire à la main de la façon suivante. On a par les théorèmes de Sylow que G admet 1 ou quatre 3-Sylow. S'il en admet un seul, G admet un sous-groupe distingué N isomorphe à $\mathbf{Z}/3\mathbf{Z}$ tel que G/N soit d'ordre 4. On a alors que G est produit semi-direct $N \rtimes H$, un tek produit semi-direct étant donné par un morphisme $\psi : H \to \mathrm{Aut}(\mathbf{Z}/3\mathbf{Z}) \cong \mathbf{Z}/2\mathbf{Z}$. Si H est cyclique d'ordre 4, on a un seul morphisme non trivial définissant un unique (à isomorphisme près) produit semi-direct $\mathbf{Z}/3\mathbf{Z} \rtimes \mathbf{Z}/4\mathbf{Z}$ en plus du produit direct $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ et si $H \cong (\mathbf{Z}/2\mathbf{Z})^2$ donne lieu à 3 morphismes non triviaux qui diffèrent 2 à 2 d'un automorphisme de H, ce qui fournit à nouveau un unique (à isomorphisme près) produit semi-direct $\mathbf{Z}/3\mathbf{Z} \rtimes (\mathbf{Z}/2\mathbf{Z})^2$ en plus du produit direct $\mathbf{Z}/3\mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})^2$. Enfin, si on a quatre 3-Sylow, G admet 8 éléments d'ordre 3 si bien que leur complémentaire auquel on ajoute e forme l'unique 2-Sylow N de G qui est donc distingué. Le quotient $H = G/N \cong \mathbf{Z}/3\mathbf{Z}$ et $G = N \rtimes H$. Un tel produit semi-direct est donné par un morphisme $\psi : \mathbf{Z}/3\mathbf{Z} \to \mathrm{Aut}(N)$. Si N est cyclique, alors $\mathrm{Aut}(N) \cong \mathbf{Z}/2\mathbf{Z}$ et un tel morphisme est nécessairement trivial, donnant lieu au produit direct $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ et si $N \cong (\mathbf{Z}/2\mathbf{Z})^2$, alors $\mathrm{Aut}(N) \cong \mathrm{GL}_2(\mathbf{F}_2) \cong \mathfrak{S}_3$ (car d'ordre 6 non abélien). Il existe donc deux morphismes non triviaux conjugués et donc isomorphes si bien qu'on obtient un unique (à isomorphisme près) produit semi-direct $(\mathbf{Z}/2\mathbf{Z})^2 \rtimes \mathbf{Z}/3\mathbf{Z}$ en plus du produit direct $(\mathbf{Z}/2\mathbf{Z})^2 \times \mathbf{Z}/3\mathbf{Z}$. Finalement on a obtenu la classification suivante :
   - Ordre 1 : $\{e\}$;
   - Ordre 2 : $\mathbf{Z}/2\mathbf{Z}$;
   - Ordre 3 : $\mathbf{Z}/2\mathbf{Z}$;
   - Ordre 4 : $\mathbf{Z}/4\mathbf{Z}$ et $(\mathbf{Z}/2\mathbf{Z})^2$;
   - Ordre 5 : $\mathbf{Z}/5\mathbf{Z}$;
   - Ordre 6 : $\mathbf{Z}/6\mathbf{Z}$ et $\mathfrak{S}_3$;
   - Ordre 7 : $\mathbf{Z}/7\mathbf{Z}$;
   - Ordre 8 : $\mathbf{Z}/8\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, $(\mathbf{Z}/2\mathbf{Z})^2$, $D_4 = \mathbf{Z}/4\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}$ et $\mathbf{H}_8$;
   - Ordre 9 : $\mathbf{Z}/9\mathbf{Z}$ et $(\mathbf{Z}/3\mathbf{Z})^2$;
   - Ordre 10 : $\mathbf{Z}/10\mathbf{Z}$ et $\mathbf{Z}/5\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z} \cong D_5$;
   - Ordre 11 : $\mathbf{Z}/11\mathbf{Z}$;

32. *Isomorphism versus commensurability for a class of finitely presented groups* de Arzhantseva, Lafont et Minasyan.

— Ordre 12 : $\mathbf{Z}/12\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$, $(\mathbf{Z}/2\mathbf{Z})^2 \rtimes \mathbf{Z}/3\mathbf{Z} \cong \mathfrak{A}_4$, $\mathbf{Z}/6\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z} \cong D_6$ et $\mathbf{Z}/3\mathbf{Z} \rtimes \mathbf{Z}/4\mathbf{Z}$;

— Ordre 13 : $\mathbf{Z}/13\mathbf{Z}$;

— Ordre 14 : $\mathbf{Z}/14\mathbf{Z}$ et $\mathbf{Z}/7\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z} \cong D_7$;

— Ordre 15 : $\mathbf{Z}/15\mathbf{Z}$.

Exercice 15. Soit p un nombre premier impair.

1. Déterminer les p-Sylow de $\mathrm{GL}_2(\mathbf{F}_p)$.
2. Soient φ et ψ des morphismes non triviaux de $\mathbf{F}_p$ dans $\mathrm{GL}_2(\mathbf{F}_p)$. En notant pour tout entier k, φ_k le morphisme défini par $\varphi_k(x) = \varphi(kx)$, montrer qu'il existe un entier k et une matrice $P \in \mathrm{GL}_2(\mathbf{F}_p)$ tels que $\psi = P\varphi_k P^{-1}$.
3. En déduire qu'il existe, à isomorphisme près, un unique produit semi-direct non trivial $(\mathbf{Z}/p\mathbf{Z})^2 \rtimes \mathbf{Z}/p\mathbf{Z}$.
4. Montrer que le centre de ce dernier groupe est isomorphe à $\mathbf{Z}/p\mathbf{Z}$.
5. Soit G un groupe d'ordre p^3 non cyclique, contenant un élément x d'ordre p^2. Montrer que $\langle x \rangle$ est distingué dans G et que G est produit semi-direct de $\mathbf{Z}/p\mathbf{Z}$ par $\langle x \rangle \cong \mathbf{Z}/p^2\mathbf{Z}$.
6. Décrire les classes d'isomorphisme de groupes de cardinal p^3 (on pourra raisonner par exemple suivant l'ordre maximal d'un élément du groupe).

Solution.

1. On sait que $\#\mathrm{GL}_2(\mathbf{F}_p) = (p^2-1)(p^2-p) = p(p-1)^2(p+1)$ donc les p-Sylow de $\mathrm{GL}_2(\mathbf{F}_p)$ sont d'ordre p et tous conjugués. Or, on en connaît un, à savoir le groupe $U(p)$ des matrices unipotentes supérieures $\left\{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbf{F}_p\right\}$. Ainsi, une matrice est dans un des p-Sylow si, et seulement si, elle est conjuguée à une telle matrice et on a vu en exercice 3 que cela est équivalent à ce que son polynôme caractéristique soit égal à $(X-1)^2$. On peut dénombrer à la main le nombre de telles matrices qui sont $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $ad - bc \neq 0$ et $a, b, c, d \in \mathbf{F}_p$ et $X^2 - (a+d)X + ad - bc = X^2 - 2X + 1$. On cherche donc les solutions dans $\mathbf{F}_p$ au système

$$\begin{cases} ad - bc = 1 \\ a + d = 2. \end{cases}$$

On a donc p choix pour a et alors $d = 2 - a$ est fixé et on a l'équation $bc = -a^2 + 2a - 1 = -(a-1)^2$ et si $a \neq 1$, on a alors $p-1$ choix pour b et c est alors fixé tandis que si $a = 1$, on a $b = 0$ et c quelconque ou l'inverse (attention qu'ici on compte deux fois le cas $b = c = 0$), ce qui fournit au total $(p-1)^2 + 2p - 1 = p^2$ telles matrices. Si maintenant on a n_p p-Sylow, on obtient $n_p(p-1)$ éléments d'ordre p et ainsi $1 + n_p(p-1)$ éléments dans la réunion des n_p p-Sylow. On a donc nécessairement $n_p = p + 1$. On constate que les conjugués de $U(p)$ par $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et les $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$ avec $a \in \mathbf{F}_p$ fournissent $p+1$ sous-groupes d'ordre p qui sont donc tous les p-Sylow de $\mathrm{GL}_2(\mathbf{F}_p)$.
2. Par simplicité de $\mathbf{Z}/p\mathbf{Z}$, un tel morphisme est injectif et les images de ψ et φ sont des p-Sylow et par conséquent conjugués par une matrice $P \in \mathrm{GL}_2(\mathbf{F}_p)$. Notons que

$$\varphi^{(P)} : \begin{cases} \mathbf{F}_p & \longrightarrow & \psi(\mathbf{F}_p) \\ x & \longmapsto & P\varphi(x)P^{-1} \end{cases}$$

est un isomorphisme. Dès lors, $\left(\varphi^{(P)}\right)^{-1} \circ \psi$ est un automorphisme de $\mathbf{Z}/p\mathbf{Z}$, donc de la forme $x \mapsto kx$ pour un certain k premier à p, ce qui permet de conclure.
3. Comme $\mathrm{Aut}\left((\mathbf{Z}/p\mathbf{Z})^2\right) \cong \mathrm{GL}_2(\mathbf{F}_p)$, la question **1.** garantit l'existence d'un tel produit semi-direct non trivial (considérer par exemple l'injection canonique d'un p-Sylow) qui correspond à un morphisme non trivial $\mathbf{Z}/p\mathbf{Z} \longrightarrow \mathrm{GL}_2(\mathbf{F}_p)$ et la question **2.** combinée à l'exercice 9 montre l'unicité à isomorphisme près.
4. On a affaire à un p-groupe dont le centre est non trivial. Ainsi, le centre de $(\mathbf{Z}/p\mathbf{Z})^2 \rtimes \mathbf{Z}/p\mathbf{Z}$ est d'ordre p, p^2 ou p^3. S'il est d'ordre p^2 ou p^3, alors le quotient du groupe par son centre est d'ordre p ou p^2 donc abélien, ce qui est absurde car le produit semi-direct est non trivial. Ainsi, le centre est d'ordre p et par conséquent isomorphe à $\mathbf{Z}/p\mathbf{Z}$.
5. Le sous-groupe $\langle x \rangle$ est d'indice p donc l'exercice 3 du TD I permet d'affirmer qu'il est distingué dans G. Le quotient $G/\langle x \rangle$ est d'ordre p donc isomorphe à $\mathbf{Z}/p\mathbf{Z}$. Soit alors $y \in G \setminus \langle x \rangle$. On a alors que $y^p \in \langle x \rangle$ car $\overline{y^p} = \langle x \rangle$ dans le quotient et $y^{p^2} = e$ car y ne peut pas être d'ordre p^3, G étant non cyclique. Il existe donc $k \in \mathbf{Z}$ tel que $y^p = x^{pk}$. Comme $\langle x \rangle \lhd G$, il existe $r \geqslant 0$ tel que $y^{-1}xy = x^r$ et donc pour tout $\alpha \in \mathbf{N}$, $x^\alpha y = yx^{\alpha r}$. On cherche alors à trouver $z \in G \setminus \langle x \rangle$ d'ordre p. Cherchons z sous la forme $z = yx^n$. Ainsi $z^p = (yx^n)^p = yx^n yx^n \cdots yx^n$ et par une récurrence immédiate, il vient

$$z^p = y^p x^{n(r^{p-1}+\cdots+r+1)} = x^{pk+n(r^{p-1}+\cdots+r+1)}.$$

L'élément z est donc d'ordre p si, et seulement si, $p^2 \mid pk + n(r^{p-1} + \cdots + r + 1)$ où l'inconnue est n. Notons $S := r^{p-1} + \cdots + r + 1$. On a alors $(r-1)S = r^p - 1$ qui est congru à $r - 1$ modulo p. Cela est donc équivalent au fait que $r \not\equiv 1$ modulo p et $S \equiv 1$ modulo p (auquel cas l'équation admet immédiatement une solution n_0) ou $r \equiv 1$ modulo p. Dans ce dernier cas, si $r = 1 + \ell p$, alors

$$S = 1 + 1 + \cdots + 1 + \ell p \sum_{i=0}^{p-1} i + p^2 t = p + \ell p \frac{p(p-1)}{2} + p^2 t = p + p^2 t'$$

où t' est un entier car $p - 1$ est divisible par 2. On a sonc $S \equiv p$ modulo p^2 et on voit qu'on peut à nouveau trouver une solution n_0. On a donc $z = y x^{n_0} \in G \smallsetminus \langle x \rangle$ est d'ordre p. On a donc par propriété du produit semi-direct que $G = \langle x \rangle \rtimes \langle z \rangle \cong \mathbf{Z}/p^2\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}$.

6. Soit G d'ordre p^3. On note p^r l'ordre maximal d'un élément de G (autrement dit son exposant).

- Si $r = 3$, on a $G \cong \mathbf{Z}/p^3\mathbf{Z}$;
- Si $r = 2$, la question **5.** garantit que $G \cong \mathbf{Z}/p^2\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}$. Un tel produit semi-direct est équivalent à la donnée d'un morphisme $\psi : \mathbf{Z}/p\mathbf{Z} \to \mathrm{Aut}(\mathbf{Z}/p^2\mathbf{Z}) \cong \mathbf{Z}/p(p-1)\mathbf{Z}$. Le groupe cyclique $\mathbf{Z}/p(p-1)\mathbf{Z}$ admet un unique sous-groupe d'ordre p donc l'exercice 9 garantit qu'on a un unique produit semi-direct non trivial $\mathbf{Z}/p^2\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}$ et évidemment le groupe abélien correspondant au produit semi-direct trivial $\mathbf{Z}/p^2\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$;
- Si $r = 1$, alors tout sous-groupe de G d'ordre p^2 (et on sait qu'il en existe, *cf.* feuille de TD I) est distingué (car d'indice p) et isomorphe à $(\mathbf{Z}/p\mathbf{Z})^2$ et tout élément du complémentaire est d'ordre p, ce qui assure que $G \cong (\mathbf{Z}/p\mathbf{Z})^2 \rtimes \mathbf{Z}/p\mathbf{Z}$. La question **3.** garantit alors qu'on a un unique produit semi-direct non trivial $(\mathbf{Z}/p\mathbf{Z})^2 \rtimes \mathbf{Z}/p\mathbf{Z}$ et un groupe abélien $(\mathbf{Z}/p\mathbf{Z})^3$.

Pour conclure, on a obtenu cinq classes d'isomorphismes :

$$(\mathbf{Z}/p\mathbf{Z})^3, \quad \mathbf{Z}/p^2\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}, \quad \mathbf{Z}/p^3\mathbf{Z}, \quad (\mathbf{Z}/p\mathbf{Z})^2 \rtimes \mathbf{Z}/p\mathbf{Z}, \quad \mathbf{Z}/p^2\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}.$$

Exercice 16 — Groupes nilpotents.

1. Soient G un groupe fini, $N \lhd G$, $H \leqslant G$ et $\pi : G \to G/N$ la surjection canonique. Établir que $\pi(H) \leqslant Z(G/N)$ si, et seulement si, $[H, G] \leqslant N$ où, pour $H_1, H_2 \leqslant G$, on note $[H_1, H_2]$ le sous-groupe de G engendré par les commutateurs de la forme $h_1 h_2 h_1^{-1} h_2^{-1}$ avec $h_1 \in H_1$ et $h_2 \in H_2$.
On définit alors *la suite centrale descendante* associée à G par $C^1(G) = G$ et $C^{n+1}(G) = [G, C^n(G)]$ pour $n \in \mathbf{N}^\times$. En déduire que G est nilpotent si, et seulement si, il existe $n_0 \in \mathbf{N}^\times$ tel que $C^{n_0}(G) = \{e\}$.

2. Montrer qu'un groupe nilpotent est résoluble. Que dire de la réciproque ?

3. Montrer que le centre d'un groupe nilpotent est non trivial.

4. Montrer que si G est nilpotent et que H est un sous-groupe de G, alors H est nilpotent.

5. Montrer que si $H \lhd G$ et que G est nilpotent, alors G/H est nilpotent.

6. On suppose H et G/H nilpotents. Le groupe G est-il nilpotent ?

7. Soient p, q, r trois nombres premiers. Montrer que tout groupe d'ordre pqr est résoluble. Un tel groupe est-il nilpotent ?

8. On suppose G fini. Montrer que G est nilpotent si, et seulement si, tout sous-groupe maximal de G est distingué et si, et seulement si, G est produit direct de ses p-Sylow pour tout nombre premier p divisant $\#G$.

Solution.

1. La condition que $\pi(H) \leqslant Z(G/N)$ équivaut à $[\pi(H), G/N] = \{\overline{e}\}$. On a clairement que $[\pi(H), G/N] = [\pi(H), \pi(G)] = \pi([H, G])$ par surjectivité du morphisme de groupes π. Ainsi, on a immédiatement que $[\pi(H), G/N] = \{\overline{e}\}$ si, et seulement si, $[H, G] \leqslant N$.
Si G est nilpotent, il existe une suite de groupes

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

avec pour tout $i \in \{1, \ldots, n\}$, $G_i \lhd G$ et pour tout $i \in \{1, \ldots, n-1\}$, $G_{i+1}/G_i \leqslant Z(G/G_i)$, soit $[G, G_{i+1}] \leqslant G_i$ d'après ce qui précède. On a donc $C^1(G) \leqslant G_n$ puis $C^2(G) = [G, C^1(G)] \leqslant [G, G_n] \leqslant G_{n-1}$ et de proche en proche $C^{n+1}(G) \leqslant G_0 = \{e\}$ ce qui permet de conclure. Réciproquement, supposons que $C^n(G) = \{e\}$, on pose alors $G_{n-1} = G$, $G_{n-2} = C^2(G), \ldots, G_0 = C^n(G)$ et on a alors

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{n-1} = G$$

avec $G_i \lhd G$ car les $C^i(G)$ sont des sous-groupes caractéristiques de G et $[G, G_{i+1}] = G_i$ par définition, ce qui permet bien de montrer que G est nilpotent.

2. C'est du cours et évident à partir des définitions ou des caractérisations en termes de D^n et C^n. La réciproque est fausse comme on l'a vu dans l'exercice 7 question **2.**

3. Soit G un groupe nilpotent. Il existe $n \geqslant 0$ maximal tel que $C^n(G) \neq \{e\}$. On a alors $C^{n+1}(G) = \{e\}$ soit $[G, C^n(G)] = \{e\}$. Cela signifie que le sous-groupe non trivial $C^n(G)$ est contenu dans $Z(G)$ qui est donc non trivial.

Plus généralement, si $N \neq \{e\} \lhd G$, alors $N \cap Z(G) \neq \{e\}$ (si l'on ne suppose plus N normal, le résultat tombe en défaut comme on le voit avec D_8 et N d'ordre 2 dans D_8 non contenu dans le sous-groupe cyclique d'ordre 4). En effet, il est immédiat de voir qu'un groupe est nilpotent si, et seulement si, il existe un entier n et des groupes

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$$

avec $[G, G_i] \subseteq G_{i+1}$. En effet, si G est nilpotent, $G_i = C^i(G)$ convient et réciproquement par récurrence on établit que $C^i(G) \subseteq G_i$. En posant dans notre cas $N_i = N \cap C^i(G)$, on a une suite d'extensions

$$N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_n = \{e\}$$

où on vérifie que $[G, N_i] \subseteq N_{i+1}$. Choisissons alors l'entier k maximal tel que $N_k \neq \{e\}$. On a $N_k \leqslant N$ et $[G, N_k] \subseteq N_{k+1} = \{e\}$ donc $N_k \subseteq Z(G)$.

4. Une récurrence simple assure que pour tout $n \geqslant 0$, $C^n(H) \subseteq C^n(G)$, ce qui entraîne immédiatement le résultat. On a également que l'image d'un groupe nilpotent par un morphisme de groupes (car $f(C^n(G)) \subseteq C^n(f(G))$ avec égalité si le morphisme est surjectif) est nilpotent en raisonnant comme dans le cas résoluble.

5. On raisonne comme dans le cas résoluble en établissant que $\pi(C^n(G)) = C^n(G/H)$.

6. C'est faux comme on peut le voir avec $G = \mathfrak{S}_3$, $H = \mathfrak{A}_3$ et $G/H = \{\pm 1\} \cong \mathbf{Z}/2\mathbf{Z}$. On a alors H et G/H abéliens donc nilpotents mais G non nilpotent.

On a en revanche le résultat plus faible suivant : si $H \leqslant G$ est un sous-groupe central (donc en particulier nilpotent), alors G/H nilpotent implique G nilpotent. En effet, on a l'existence d'un n tel que $C^n(G/H) = \{e\}$ donc $\pi(C^n(G)) = \{e\}$ soit $C^n(G) \leqslant H$ et donc $C^n(G)$ est central et $C^{n+1}(G) = \{e\}$.

7. On a déjà traité la résolubilité. On sait que tout p-groupe est nilpotent donc si $p = q = r$, on obtient donc un groupe nilpotent.

Si maintenant (sans perte de généralité), $p = q \neq r$, un tel groupe n'est pas nécessairement nilpotent comme en témoigne l'exemple de $\mathfrak{S}_3 \times \mathbf{Z}/2\mathbf{Z}$ (qui s'il était nilpotent entraînerait que $\mathfrak{S}_3$ est nilpotent).

Supposons pour finir que $p < q < r$. Un tel groupe n'est pas non plus nécessairement nilpotent comme en témoigne l'exemple de $\mathfrak{S}_3 \times \mathbf{Z}/5\mathbf{Z}$ (qui s'il était nilpotent entraînerait que $\mathfrak{S}_3$ est nilpotent comme quotient par le sous-groupe distingué $\mathbf{Z}/5\mathbf{Z}$).

8. Supposons dans un premier temps que G est produit direct de ses p-Sylow. On a alors que chacun des p-Sylow est nilpotent en tant que p-groupe et on peut vérifier qu'un produit direct de groupes nilpotents est nilpotent (tout se passe composante par composante), ainsi G est nilpotent.

Réciproquement, supposons que G est nilpotent. Soit $M \leqslant G$ un sous-groupe maximal (voir l'exercice suivant pour une justification de l'existence d'un tel sous-groupe). Puisqu'il existe un n_0 tel que $C^{n_0}(G) = \{e\}$, il existe un entier minimal n tel que $C^n(G) \leqslant M$ et par minimalité de n, il existe $g \in C^{n-1}(G) \setminus M$. Alors, on a $[g, M] \subseteq [C^{n-1}(G), G] = C^n(G) \subseteq M$ ce qui assure que $gMg^{-1} \subseteq M$ et $g \in N_G(M) \setminus M$. Par conséquent, $N_G(M)$ est un sous-groupe de G contenant M, distinct de M donc égal à G par maximalité. On a donc $N_G(M) = G$ et M est distingué dans G. On a donc que tout sous-groupe maximal est distingué. Soit S un p-Sylow de G. Supposons que $N_G(S) \neq G$. Alors $N_G(S)$ est contenu dans un sous-groupe maximal M de G. Par hypothèse, M est distingué dans G donc pour tout $g \in G$, $gSg^{-1} \subseteq gMg^{-1} = M$ donc S et gSg^{-1} sont deux p-Sylow de M, donc conjugués dans M. Il existe ainsi $m \in M$ tel que $gSg^{-1} = mSm^{-1}$ donc $m^{-1}g \in N_G(S) \subseteq M$ donc $g \in M$ ce qui implique que $M = G$, ce qui est absurde par définition d'un sous-groupe maximal. Ainsi $N_G(S) = S$ et S est distingué et l'unique p-Sylow de G.

Considérons alors l'application $\varphi : \prod_{p \mid \#G} S_p \to G$ défini par le produit dans G et où S_p désigne l'unique p-Sylow. Comme les p-Sylow ont des cardinaux premiers entre eux, on voit que les éléments d'un sous-groupe de Sylow commutent avec ceux d'un autre. En effet, soit $x \in S_p$ et $y \in S_q$ distincts de e, alors $xyx^{-1} \in S_q$ et il existe k tel que $xy = y^k x$ mais alors $xy^{1-k} = y^k xy^{-k}$ soit $y^{1-k} = x^{-1}y^k xy^{-k} \in S_p$ car $x, y^k xy^{-k} \in S_p$ et ainsi, $y^{1-k} \in S_p \cap S_q = \{e\}$ et $k = 1$. Cela entraîne qu'on a un morphisme de groupes et ce dernier est clairement injectif (car par commutativité et le fait que les ordres soient premiers entre eux, l'ordre d'un élément $s_1 \cdots s_r$ est le ppcm des ordre des s_i donc un élément du noyau est nécessairement trivial). On en déduit le résultat. On aurait pu utiliser une généralisation de la Remarque 3.8 page 25 du polycopié en remarquant que les intersections sont deux à deux triviales, que chaque sous-groupe est distingué et que le produit des cardinaux est égal au cardinal de G.

On termine par lister une propriété supplémentaires des groupes nilpotents : un groupe G est nilpotent si, et seulement si, $G/Z(G)$ est nilpotent (en effet le sens direct découle de l'exercice et dans le sens indirect si $\pi : G \to G/Z(G)$ et si $C^n(G/Z(G)) = \{e\}$ et $C^{n-1}(G/Z(G)) \neq \{e\}$, alors $C^n(G) \subseteq Z(G)$ et $C^{n-1}(G) \not\subseteq Z(G)$ donc $[G, C^n(G)] = \{e\}$).

Exercice 17 — Sous-groupe de Frattini. Soit G un groupe de type fini. On dit qu'un sous-groupe H de G est maximal si $H \neq G$ et qu'aucun sous-groupe propre de G n'est compris strictement entre H et G. On définit alors le *sous-groupe de Frattini* de G, et on note $\phi(G)$, l'intersection des sous-groupes maximaux de G.

1. Montrer que $\mathbf{Q}$ ne possède pas de sous-groupe maximal.

2. Montrer que G admet au moins un sous-groupe maximal. La démonstration se simplifie-t-elle si G est fini ?
3. Déterminer $\phi(\mathbf{Z})$ et $\phi(\mathfrak{S}_n)$.
4. Montrer que $\phi(G)$ est caractéristique. On notera $\pi : G \to G/\phi(G)$ la projection canonique.
5. Soit $S \subseteq G$ une partie de G. Montrer que S engendre G si, et seulement si, $\pi(S)$ engendre $G/\phi(G)$.
6. Montrer que $\phi(G)$ est exactement l'ensemble des éléments $g \in G$ tels que pour toute partie $S \subseteq G$, on a $\langle S, g\rangle = G \quad \Rightarrow \langle S\rangle = G$.
7. Montrer que si G est fini, $\phi(G)$ est nilpotent.
8. On suppose G fini. Montrer que G est nilpotent si, et seulement si, $D(G) \subseteq \phi(G)$.
9. On suppose dans cette question que G est un p-groupe pour p un nombre premier.
   (a) Montrer que tout sous-groupe maximal de G contient $D(G)$ et le sous-groupe G^p engendré par les puissances p-ièmes dans G.
   (b) Montrer que $G/\phi(G)$ est le plus grand quotient abélien de G d'exposant p.
   (c) Que peut-on en déduire sur le nombre minimal de générateurs de G ?
   (d) Montrer que $\phi(G) = D(G) \cdot G^p$.

Solution.

1. Montrons le résultat plus général suivant. Un groupe additif G est dit *divisible* si pour tout $x \in G$, pour tout entier naturel n non nul, il existe $y \in G$ tel que $x = ny$. Un groupe additif divisible G n'a alors pas de sous-groupe maximal (noter que cela recouvre bien le cas de $\mathbf{Q}$, $\mathbf{Q}/\mathbf{Z}$ ou $\mathbf{U}$ des complexes de module 1). Supposons que G admet un sous-groupe H maximal. Il existe $a \in G \setminus H$. Par maximalité, $G = H + a\mathbf{Z}$. Il existe alors par divisibilité $a' \in G$ tel que $a = 2a'$ et $h \in H$, $n \in \mathbf{Z}$ tel que $a' = b + na$ ce qui entraîne que $a = 2b + 2na$. Par conséquent, $ma \in H$ avec $m = |2n - 1|$ qui est élément de $\mathbf{N}^\times$. Il existe également $a'' \in G$ tel que $ma'' = a$ et $c \in H$, $p \in \mathbf{Z}$ tels que $a'' = c + pa$. D'où, $a = mc + pma \in H$, ce qui est absurde !
2. On suppose $G \neq \{e\}$ et $G = \langle a_1, \dots, a_n\rangle$. On considère l'ensemble $\mathcal{E}$ des sous-groupes stricts de G. C'est un ensemble non vide muni de la relation d'ordre donnée par l'inclusion. Montrons que toute partie non vide totalement ordonnée $\mathcal{F}$ de $\mathcal{E}$ admet un majorant dans $\mathcal{E}$. Soit $\mathcal{F}$ une telle partie. On définit alors
$$M = \langle H \ : \ H \in \mathcal{F}\rangle = \bigcup_{H \in \mathcal{F}} H.$$
Il est clair que M est un sous-groupe de G contenant chacun des $H \in \mathcal{F}$. Montrons que $M \neq G$. Sinon, pour tout $i \in \{1, \dots, n\}$, $a_i \in M$ donc il existe $H_i \in \mathcal{F}$ tel que $a_i \in H_i$. Or, $\mathcal{F}$ est totalement ordonné donc il existe $H \in \mathcal{F}$ tel que pour tout $i \in \{1, \dots, n\}$, $a_i \in H$ et donc $G = H$. Cela donne une contradiction puisque H est un sous-groupe strict. On a donc $M \neq G$ et donc $M \in \mathcal{E}$ est un majorant. On peut donc appliquer le lemme de Zorn pour en déduire que $\mathcal{E}$ possède un élément maximal, autrement dit que G admet un sous-groupe maximal.
Si G est fini, $\mathcal{E}$ est fini et on n'a pas besoin de recourir au lemme de Zorn pour en déduire que $\mathcal{E}$ admet un élément maximal.
3. Les sous-groupes de $\mathbf{Z}$ sont les $a\mathbf{Z}$ avec $a \in \mathbf{Z}$. On a donc que les sous-groupes maximaux sont les $p\mathbf{Z}$ avec p premier et il est clair que $\Phi(\mathbf{Z}) = \{0\}$. On peut montrer que H est maximal dans $\mathbf{Z}/n\mathbf{Z}$ si, et seulement si, $\pi^{-1}(H)$ est un sous-groupe maximal de $\mathbf{Z}$ contenant $n\mathbf{Z}$, autrement dit de la forme $p\mathbf{Z}$ pour p premier divisant n. On note alors r le radical de n, à savoir le produit des diviseurs premiers de n. Alors on en déduit que $\Phi(\mathbf{Z}/n\mathbf{Z}) = r\mathbf{Z}/n\mathbf{Z}$.

   Passons au cas du groupe symétrique. Posons $\mathfrak{S}_n(i)$ l'ensemble des permutations fixant i et montrons que ces sous-groupes sont maximaux. Pour cela, montrons que si $\sigma \in \mathfrak{S}_n \setminus \mathfrak{S}_n(i)$, alors $\langle \mathfrak{S}_n(i), \sigma\rangle = \mathfrak{S}_n$. On décompose σ en produit de cycles à supports disjoints $\sigma = \sigma_1\sigma_2 \cdots \sigma_k$. Comme $\sigma \in \mathfrak{S}_n(i)$, $j = \sigma(i) \neq i$. Puisque les cycles commutent, on peut supposer que $\sigma_1(i) = j$ et que $\sigma_2, \dots, \sigma_k \in \mathfrak{S}_n(i)$. Il vient que $\langle \mathfrak{S}_n(i), \sigma\rangle = \langle \mathfrak{S}_n(i), \sigma_1\rangle := H$. Écrivons $\sigma_1 = (ijj_1 \cdots j_s)$. Soit $\tau = (jj_1 \cdots j_s)$. On a alors $\sigma_1 = (ij)\tau$ et $\tau \in \mathfrak{S}_n(i)$ si bien que $(ij) \in H$. Mais pour tout $k \in \{1, \dots, n\}$, avec $k \neq i, j$, on a $(jk)(ij)(jk) = (ik) \in H$ (car $(jk) \in \mathfrak{S}_n(i)$) et H contient toutes les transpositions qui engendrent $\mathfrak{S}_n$ si bien que $H = \mathfrak{S}_n$ et $\mathfrak{S}_n(i)$ est maximal. On a donc que $\Phi(\mathfrak{S}_n) \subseteq \bigcap_{i=1}^n \mathfrak{S}_n(i) = \{\mathrm{Id}\}$ de sorte que $\Phi(\mathfrak{S}_n) = \{\mathrm{Id}\}$.
4. Soit φ un automorphisme de G. Alors, pour tout sous-groupe maximal H de G, $\varphi(H)$ est aussi un sous-groupe maximal et l'application $H \mapsto \varphi(H)$ est une permutation de l'ensemble des sous-groupes maximaux de G. Par conséquent,
$$\varphi(\Phi(G)) = \bigcap_{H \subseteq G \text{maximal}} \varphi(H) = \bigcap_{H \subseteq G \text{maximal}} H = \Phi(G)$$
si bien que $\Phi(G)$ est caractéristique.
5. Le sens direct est immédiat par surjectivité de π. Supposons alors réciproquement que $\pi(S)$ engendre $G/\Phi(G)$ mais que $H = \langle S\rangle \neq G$. Alors H est contenu dans un sous-groupe maximal M de G. Comme M contient $\Phi(G)$, $\pi(M)$ s'identifie avec $M/\Phi(G)$ qui est un sous-groupe strict de $G/\Phi(G)$ (sinon $\pi(M) = \pi(G)$ mais alors pour tout $g \in G$, il existe $g' \in \Phi(G)$, $m \in M$ tel que $g'm = g$ donc $g \in M$ et $G = M$). Ainsi le sous-groupe engendré par $\pi(S)$ est inclus dans ce sous-groupe strict $M/\Phi(G)$, ce qui est une contradiction. Ainsi, $H = G$ et S engendre G.

6. La question précédente assure que si $g \in \Phi(G)$, alors pour tout $S \subseteq G$, on a $\langle S, g\rangle = G \Rightarrow \langle S\rangle = G$. Soit maintenant $g \in G \setminus \Phi(G)$. Il existe alors un sous-groupe maximal H de G tel que $g \notin H$. On considère $S = H \subseteq G$. Il est clair que $\langle S\rangle = H \neq G$ alors que $\langle S, g\rangle = G$ par maximalité. D'où la caractérisation souhaitée.

7. Soit P un p-Sylow de $\Phi(G)$. Comme $\Phi(G)$ est caractéristique donc distingué dans G, on en déduit que[33] $G = \Phi(G)N_G(P)$. Par **5.**, on a $N_G(P) = G$ et donc $P \lhd G$ donc a fortiori $P \lhd \Phi(G)$ et est l'unique p-Sylow de $\Phi(G)$. En raisonnant comme dans l'exercice 12, il vient que $\Phi(G)$ est produit de ses p-Sylow et donc nilpotent.

8. On suppose dans un premier temps G nilpotent. On sait alors d'après l'exercice précédent que tout sous-groupe maximal H est distingué dans G et donc G/H est un groupe simple (par maximalité) nilpotent. On a alors que cela implique que G/H est cyclique (utiliser par exemple la caractérisation comme produit de ses Sylow) d'ordre premier et en particulier abélien. Ainsi $D(G) \subseteq H$ et $D(G) \subseteq \Phi(G)$. Réciproquement, si $D(G) \subseteq \Phi(G)$, alors tout sous-groupe maximal H de G contient $D(G)$ donc est distingué (car pour tout $g \in G$ et $h \in H$, $xhx^{-1}h \in D(G) \subseteq H$ donc $xhx^{-1} \in H$) donc G est nilpotent.

9. (a) Soit H un sous-groupe maximal de G qui est nilpotent car un p-groupe. Ainsi la question précédente assure que H est distingué dans G et que G/H est cyclique d'ordre p donc $D(G) \subseteq H$ et $G^p \subseteq H$.

(b) La question précédente assure que $G/\Phi(G)$ est abélien d'exposant p car $D(G) \subseteq \Phi(G)$ et $G^p \subseteq \Phi(G)$. Soit à présent H un sous-groupe distingué de G tel que G/H soit abélien d'exposant p. Notons $\pi_H : G \to G/H$ la surjection canonique. On sait qu'on a $G/H \cong (\mathbf{Z}/p\mathbf{Z})^r$ pour un certain entier r non nul. On considère alors les r projections $\pi_i : (\mathbf{Z}/p\mathbf{Z})^r \to \mathbf{Z}/p\mathbf{Z}$ et il est clair que $H = \bigcap_{i=1}^r H_i$ avec $H_i = \mathrm{Ker}(\pi_i \circ \pi_H)$. Les H_i sont des sous-groupes maximaux de G car d'indice p donc $\Phi(G) \subseteq H$, ce qui assure l'existence d'un morphisme $\pi' : G/\Phi(G) \to G/H$ surjectif de noyau $H/\Phi(G)$ induisant un isomorphisme (troisième théorème d'isomorphisme) $(G/\Phi(G))/(H/\Phi(G)) \cong G/H$ et tel que $\pi_H : \pi' \circ \pi$ avec $\pi : G \to G/\Phi(G)$. Ainsi $G/\Phi(G)$ est bien le plus grand quotient abélien d'exposant p.

(c) Soit $g_1, \dots, g_m$ une famille génératrice de G. Alors $\pi(g_1), \dots, \pi(g_m)$ engendrent $G/\Phi(G)$ donc[34] $m \geqslant \dim_{\mathbf{F}_p}(G/\Phi(G))$. Or, $G/\Phi(G)$ admet une partie génératrice minimale de cardinal $\dim_{\mathbf{F}_p}(G/\Phi(G))$ et en choisissant des relevés de ces générateurs dans G, on obtient une famille génératrice par **5.** de G de cardinal $\dim_{\mathbf{F}_p}(G/\Phi(G))$. Cela assure que le nombre minimal de générateurs de G est égal à $\dim_{\mathbf{F}_p}(G/\Phi(G))$.

(d) La question **9.**(a) garantit que $D(G)G^p \subseteq \Phi(G)$. Or, $G/D(G)G^p$ est clairement un groupe abélien d'exposant p donc par **9.**(b), $\Phi(G) \subseteq D(G)G^p$ et finalement $\Phi(G) = D(G)G^p$. On retrouve par exemple avec cela que $\Phi(\mathbf{Z}/p\mathbf{Z}) = \{0\}$.

Exercice 18. Soit $n \geqslant 1$.

1. Soit $\phi \in \mathrm{Aut}(\mathfrak{S}_n)$ tel que ϕ transforme toute transposition en une transposition. Montrer que ϕ est intérieur.

2. Soit $\sigma \in \mathfrak{S}_n$. Déterminer le cardinal du commutant $Z(\sigma) = \left\{\tau \in \mathfrak{S}_n \ : \ \tau\sigma\tau^{-1} = \sigma\right\}$ de σ.

3. En déduire que si $n \neq 6$, on a $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$.

4. Soit $n \geqslant 5$ tel que $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$. Montrer que tous les sous-groupes d'indice n de $\mathfrak{S}_n$ sont conjugués.

5. En utilisant les 5-Sylow de $\mathfrak{S}_5$, montrer qu'il existe un sous-groupe H d'indice 6 de $\mathfrak{S}_6$ opérant transitivement sur $\{1, \dots, 6\}$.

6. Construire géométriquement un sous-groupe H' de $\mathfrak{S}_6$ vérifiant les mêmes propriétés que H.

7. En déduire que $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Int}(\mathfrak{S}_6)$.

Solution.

1. On peut supposer[35] $n \geqslant 4$ puisque tout automorphisme de $\mathfrak{S}_n$ avec $n \leqslant 3$ est intérieur[36]. Le groupe $\mathfrak{S}_n$ est engendré par les transpositions[37] $\tau_i = (1i)$ pour $i \in \{2, \dots, n\}$ et τ_i et τ_j ne commutent pas pour $i \neq j$. Ainsi, $\phi(\tau_i)$ et $\phi(\tau_j)$ sont deux transpositions disjointes qui ne commutent pas et donc qui ont un élément en commun dans leur support. On note α cet élément et on a alors que pour tout $i \in \{2, \cdots, n\}$, il existe α_i tel que $\phi(\tau_i) = (\alpha\alpha_i)$ et $\{\alpha, \alpha_2, \dots, \alpha_n\} = \{1, \dots, n\}$. On définit alors un élément $\sigma \in \mathfrak{S}_n$ par $\sigma(1) = \alpha$ et $\sigma(i) = \alpha_i$ et on vérifie alors que pour tout $\rho \in \mathfrak{S}_n$, $\phi(\rho) = \sigma\rho\sigma^{-1}$. En effet, on a cette relation pour chaque τ_i qui engendrent $\mathfrak{S}_n$ car $\phi(\tau_i) = (\alpha\alpha_i)$ et $\sigma\tau_i\sigma^{-1} = (\alpha\alpha_i)$.

2. On décompose σ en produit de cycles à supports disjoints avec k_1 cycles de longueur 1, k_2 cycles de longueurs $2, \dots, k_n$ cycles de longueurs n avec $k_i \in \{0, \dots, n\}$ pour $i \in \{1, \dots, n\}$ et $k_1 + 2k_2 + \cdots + nk_n = n$. On a vu dans le TD I que les conjugués de σ sont précisément les permutations qui préservent la forme de la décomposition en produit de cycles à supports disjoints donc un élément

33. C'est en effet, un argument classique dû à Frattini. Soit $g \in G$. Alors comme $P \leqslant \Phi(G)$ et que $\Phi(G)$ est distingué, $gPg^{-1} \leqslant \Phi(G)$ est un p-Sylow de $\Phi(G)$, donc conjugué (dans $\Phi(G)$ à P). Il existe donc $h \in \Phi(G)$ tel que $h^{-1}gP(h^{-1}g)^{-1} = P$ soit $h^{-1}g \in N_G(P)$ et $g \in \Phi(G)N_G(P)$.

34. Le r de la question précédente.

35. Même si cela n'est pas nécessaire dans le raisonnement qui suit.

36. Si $n = 1$ ou 2 c'est évident car on a un groupe abélien d'ordre 1 ou 2 dont le groupe d'automorphisme est trivial et pour $G = \mathfrak{S}_3 = \langle\tau, \sigma\rangle$ avec $\tau = (12)$ et $\sigma = (123)$, un automorphisme de G envoie nécessairement τ sur une transposition et σ sur un 3-cycle donc on a au plus 6 éléments. Mais, on sait que $\mathrm{Int}(G) \cong G/Z(G) \cong G$ si bien que nécessairement $\mathrm{Aut}(G) \cong \mathrm{Int}(G) \cong G$. On peut aussi montrer à la main que le morphisme $\mathfrak{S}_3 \to \mathrm{Aut}(\mathfrak{S}_3)$ donné par $\rho \mapsto [\sigma \mapsto \rho\sigma\rho^{-1}]$ est surjectif et conclure par cardinalité.

37. En effet, il est engendré par les transpositions comme on peut le montrer par récurrence sur n ou à partir de la décomposition en produit de cycles à supports disjoints en décomposant un cycle en produit de transpositions. C'est vrai pour $n = 1$ et si c'est vrai pour n et si $\sigma(n+1) = n+1$, alors en fait $\sigma \in \mathfrak{S}_n$ et on a la résultat par hypothèse de récurrence et sinon $\sigma(n+1) \neq n+1$ $(n+1\sigma(n+1)) \circ \sigma$ fixe $n+1$ et on conclut à nouveau par hypothèse de récurrence. On écrit alors toute transposition $(ij) = (1i)(1j)(1i)$.

de $\tau\sigma\tau^{-1}$ correspond à une permutation dont la décomposition est de la même forme. Pour que cette permutation soit égale à σ, il faut envoyer pour tout $j \in \{1,\dots,n\}$ un cycle de longueur j de σ sur un des k_j cycles de longueurs j de sigma, ce qui fournit k_j choix et ensuite on a j façon d'envoyer un j-cycles $(c_1,\dots,c_j)$ sur un autre $(c'_1,\dots,c'_j)$ (on choisit si l'on envoie c_1 sur $c'_1, c'_2, \dots, c'_j$). Puis pour le second cycle de longueur j, on a $k_j - 1$ choix du j-cycles sur lequel on l'envoie puis j façons de procéder et ainsi de suite donnant lieu à $k_j! j^{k_j}$ possibilités. Comme ce qui se passe pour chaque longueur de cycle est indépendant des autres longueurs, il vient que

$$\#Z(\sigma) = \prod_{j=1}^{n} k_j! j^{k_j}.$$

Cela permet de retrouver que le cardinal de la classe de conjugaison de $\mathfrak{S}_n$ associé à cette décomposition en produit de cycles à supports disjoints est de cardinal (considérer l'action par conjugaison)

$$\frac{n!}{\prod_{j=1}^{n} k_j! j^{k_j}}.$$

3. Soit φ un automorphisme de $\mathfrak{S}_n$. Si τ est une transposition de $\mathfrak{S}_n$, alors $\varphi(\tau)$ est d'ordre 2 et est donc un produit de transpositions à supports disjoints, disons de k transpositions à supports disjoints. Mais, on a $\#Z(\tau) = \#Z(\varphi(\tau))$ et par **2.**, cela fournit que $2(n-2)! = 2^k k!(n-2k)!$. Cela entraîne que si $n \neq 6$ (auquel cas $n = 6$ et $k = 3$ convient) que $k = 1$ et on conclut par **1.** En effet, la relation équivaut à

$$2^{k-1} = \frac{(n-2)!}{k!(n-2k)!} = \binom{n-k}{k}(n-2)\cdots(n-k+1)$$

et si $k > 1$, alors $n - 2 \neq n - k + 1$ car sinon on a nécessairement un facteur impair donc $n - 2 = n - k + 1$ soit $k = 3$ et

$$4 = \binom{n-3}{3}(n-2)$$

soit $n - 2 \leqslant 4$ mais on a aussi $n \geqslant 2k = 6$, alors $n = 6$.

4. Soit $H \subseteq \mathfrak{S}_n$ d'indice n. L'action transitive de $\mathfrak{S}_n$ sur $\mathfrak{S}_n/H$ induit un morphisme de groupes $\phi : \mathfrak{S}_n \to \mathfrak{S}(\mathfrak{S}_n/H) \cong \mathfrak{S}_n$. On sait alors que son noyau est distingué dans $\mathfrak{S}_n$ et est donc égal à $\{\mathrm{Id}\}$, $\mathfrak{A}_n$ ou $\mathfrak{S}_n$ car $n \geqslant 5$. Mais par définition, $\mathrm{Ker}(\phi)$ agit trivialement sur la classe de H dans $\mathfrak{S}_n/H$ donc $\mathrm{Ker}(\phi) \subseteq H$ donc $\mathrm{Ker}(\phi) = \{\mathrm{Id}\}$ par cardinalité et ϕ est injective et donc $\phi \in \mathrm{Aut}(\mathfrak{S}_n)$. Par hypothèse, il existe $\sigma \in \mathfrak{S}_n$ tel que ϕ soit l'automorphisme de conjugaison par σ mais par construction, ϕ envoie H sur le stabilisateur d'un point (la classe de H) dans $\mathfrak{S}(\mathfrak{S}_n/H) \cong \mathfrak{S}_n$. Reste à voir que dans $\mathfrak{S}_n$, les stabilisateurs d'un point sont tous conjugués. En effet, si on note $\mathfrak{S}_n(i) = \{\sigma \in \mathfrak{S}_n \ : \ \sigma(i) = i\}$ pour $i \in \{1,\dots,n\}$. On a alors clairement que pour tout $i \neq j$, $(ij)\mathfrak{S}_n(j)(ij) = \mathfrak{S}_n(i)$. Et finalement comme le conjugué d'un $\mathfrak{S}_n(i)$ est un $\mathfrak{S}_n(j)$, on voit que les $\mathfrak{S}_n(1),\dots,\mathfrak{S}_n(n)$ sont les seuls sous-groupes d'indice n et ils sont tous conjugués.

5. On a par les théorèmes de Sylow que $\mathfrak{S}_5$ admet un ou six 5-Sylow. Par simplicité[38] de $\mathfrak{A}_5$ (remarquer qu'un 5-Sylow de $\mathfrak{A}_5$ est un 5-Sylow de $\mathfrak{S}_5$), on déduit que $n_5 = 6$. Notons X l'ensemble de ces 5-Sylow, l'action transitive de $\mathfrak{S}_5$ sur X donne lieu à un morphisme $\mu : \mathfrak{S}_5 \to \mathfrak{S}(X) \cong \mathfrak{S}_6$ dont le noyau est trivial (car distingué, distinct de $\mathfrak{S}_5$ car le morphisme est non trivial et distinct de $\mathfrak{A}_5$ car l'action est transitive). On en déduit donc que l'image de G, $H = \mu(\mathfrak{S}_5)$ est un sous-groupe d'indice 6 qui opère transitivement sur $\{1,\dots,6\}$.

6. Le groupe $H' = \mathrm{PGL}_2(\mathbf{F}_5)$ vu comme sous-groupe de $\mathfrak{S}_6$ par action sur $\mathbf{P}^1(\mathbf{F}_5)$ (voir exercice 3) est d'indice 6 qui opère transitivement sur $\{1,\dots,6\}$.

7. Supposons que $\mathrm{Aut}(\mathfrak{S}_6) = \mathrm{Int}(\mathfrak{S}_6)$. Les questions **4.** et **5.** (ou **6.**) assurent alors que le groupe $\mathfrak{S}_6$ possède un sous-groupe d'indice 6 opérant transitivement sur $\{1,\dots,6\}$. Mais on a vu qu'un tel sous-groupe est nécessairement le stabilisateur d'un élément i, ce qui est une contradiction et finalement $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Int}(\mathfrak{S}_6)$.

Pour $n = 1, 2$, on a $\mathrm{Aut}(\mathfrak{S}_n) = \{\mathrm{Id}\}$ et pour $n \geqslant 3$, $n \neq 6$, on sait qu'on a la suite exacte $1 \to Z(\mathfrak{S}_n) \to \mathfrak{S}_n \to \mathrm{Int}(\mathfrak{S}_n) \to 1$. Mais, on sait que $Z(\mathfrak{S}_n) = \{e\}$ (sous-groupe distingué différent de $\mathfrak{A}_n$ pour $n \geqslant 5$ et se fait à la main pour $n = 3$ ou 4), ce qui implique que $\mathrm{Int}(\mathfrak{S}_n) \cong \mathfrak{S}_n$. On pouvait aussi procéder différemment comme suit, l'application $\mathfrak{S}_n \to \mathrm{Aut}(\mathfrak{S}_n)$ qui à une permutation associe l'automorphisme par conjugaison par cette permutation est de noyau $Z(\mathfrak{S}_n)$ qui est trivial si bien qu'il est injectif et l'exercice démontre qu'il est surjectif donc $\mathrm{Aut}(\mathfrak{S}_n) \cong \mathfrak{S}_n$.
Dans le cas $n = 6$, on a toujours de même $\mathrm{Int}(\mathfrak{S}_6) \cong \mathfrak{S}_6$ et on a la suite exacte $1 \to \mathrm{Int}(\mathfrak{S}_6) \to \mathrm{Aut}(\mathfrak{S}_6) \to \mathrm{Aut}(\mathfrak{S}_6)/\mathrm{Int}(\mathfrak{S}_6) \to 1$. Reprenant la démonstration et notant $\mathcal{I}_k$ l'ensemble des produits de k transpositions disjointes, on a qu'un automorphisme extérieur (non intérieur) envoie $\mathcal{I}_1$ sur $\mathcal{I}_3$ (car un automorphisme envoie une classe de conjugaison sur une classe de conjugaison et que les $\mathcal{I}_k$ forment chacun une classe de conjugaison et s'il envoie $\mathcal{I}_1$ sur lui-même, par **1.**, l'automorphisme est intérieur) et inversement. Ainsi pour tout $\phi, \psi \in \mathrm{Aut}(\mathfrak{S}_6) \setminus \mathrm{Int}(\mathfrak{S}_6)$, on a $\phi \circ \psi(\mathcal{I}_1) = \mathcal{I}_1$ ce qui implique par **1.** que $\phi \circ \psi \in \mathrm{Int}(\mathfrak{S}_6)$ et permet de montrer que $\mathrm{Int}(\mathfrak{S}_6)$ est d'indice 2 dans

38. Ou en utilisant qu'on connaît les sous-groupes distingués de $\mathfrak{S}_5$ et aucun n'est de cardinal 5.

$\mathrm{Aut}(\mathfrak{S}_6)$. D'où $\#\mathrm{Aut}(\mathfrak{S}_6) = 1440$. On en déduit qu'il y a 12 groupes d'indice 6 dans $\mathfrak{S}_6$, à savoir $\mathfrak{S}_6(1), \dots, \mathfrak{S}_6(n), \phi(\mathfrak{S}_6(1)), \dots, \phi(\mathfrak{S}_6(n))$ pour $\phi \in \mathrm{Aut}(\mathfrak{S}_6) \setminus \mathrm{Int}(\mathfrak{S}_6)$. Enfin, on obtient que $\mathrm{Aut}(\mathfrak{S}_6) = \mathrm{Int}(\mathfrak{S}_6) \rtimes \mathbf{Z}/2\mathbf{Z}$. On a donc la suite exacte courte $1 \to \mathfrak{S}_6 \to \mathrm{Aut}(\mathfrak{S}_6) \to \mathbf{Z}/2\mathbf{Z} \to 1$ et pour obtenir le résultat (un tel produit semi-direct non trivial est nécessairement unique à isomorphisme près), il suffit de montrer que $\mathrm{Aut}(\mathfrak{S}_6) \setminus \mathrm{Int}(\mathfrak{S}_6)$ contient un élément d'ordre 2. Soit $\phi \in \mathrm{Aut}(\mathfrak{S}_6) \setminus \mathrm{Int}(\mathfrak{S}_6)$. l'image d'un 5-cycle est un élément d'ordre 5 donc un 5-cycle. Il existe donc (la classe de conjugaison d'un 5-cycle est l'ensemble des 5-cycles) $\sigma \in \mathfrak{S}_6$ tel que

$$\mathrm{Int}(\sigma) \circ \phi(12345) = (12345) := c.$$

On a $\psi = \mathrm{Int}(\sigma) \circ \phi \in \mathrm{Aut}(\mathfrak{S}_6) \setminus \mathrm{Int}(\mathfrak{S}_6)$ et $\psi^2 \in \mathrm{Int}(\mathfrak{S}_6)$ (car d'indice 2). Il existe donc $\alpha \in \mathfrak{S}_6$ tel que $\psi^2 = \mathrm{Int}(\alpha)$. Comme ψ^2 fixe c, α et c commutent donc $\alpha c \alpha^{-1} = (\alpha(1)\alpha(2)\alpha(3)\alpha(4)\alpha(5)) = (12345)$ et $\alpha = c^k$ pour un entier k. Finalement $\psi^5 \in \mathrm{Aut}(\mathfrak{S}_6) \setminus \mathrm{Int}(\mathfrak{S}_6)$ et est d'ordre 2.

Exercice 19. Soit G un groupe simple d'ordre 360.

1. Montrer que G admet dix 3-Sylow.
2. Montrer que G est isomorphe à un sous-groupe de $\mathfrak{A}_{10}$. On supposera désormais que G est un sous-groupe de $\mathfrak{A}_{10}$.
3. Soit S un 3-Sylow de G. Montrer que S n'est pas cyclique, et que l'on peut supposer que $N_G(S)$ est le stabilisateur de 10 dans G.
4. Montrer que tout élément non trivial de S ne fixe aucun point de $\{1, \dots, 9\}$.
5. Montrer que l'on peut supposer que S est engendré par les éléments $x = (123)(456)(789)$ et $y = (147)(258)(369)$.
6. Montrer que le stabilisateur P de 1 dans $N_G(S)$ est cyclique d'ordre 4 et est un 2-Sylow de $N_G(S)$. On note z un générateur de P.
7. Montrer qu'on peut supposer que $z = (2437)(5698)$.
8. Soit T un 2-Sylow de G contenant z. Montrer que $T = \langle z, t \rangle$ avec t d'ordre 2.
9. Montrer que l'on peut supposer que $t = (1\ 10)(23)(56)(89)$.
10. Montrer que $G = \langle x, y, z, t \rangle$.
11. Que peut-on en conclure pour les groupes simples d'ordre 360 ?
12. Montrer que $\mathrm{PSL}_2(\mathbf{F}_9) \cong \mathfrak{A}_6$.

Solution.

1. On note n_3 le nombre de 3-Sylow. On a par les théorèmes de Sylow que $n_3 \in \{1, 4, 10, 40\}$. On ne peut pas avoir $n_3 = 1$ par simplicité et si $n_3 = 4$, l'action sur l'ensemble des 3-Sylow donne un morphisme injectif $G \to \mathfrak{S}_4$ ce qui est absurde par cardinalité. Montrons alors que $n_3 = 40$ abouti aussi à une contradiction. Supposons $n_3 = 40$. Alors pour tout 3-Sylow S, $N_G(S)$ est un sous-groupe de G d'indice 40 et est donc de cardinal 9, autrement dit, c'est un 3-Sylow contenant S et $N_G(S) = S$. Par ailleurs, un groupe de cardinal 9 étant abélien, $S = Z(N_G(S))$ et le théorème de transfert de Burnside démontré en bonus assure que G n'est pas simple, ce qui est contradictoire.

   De façon plus élémentaire, si $n_3 = 40$, on voit qu'il existe deux 3-Sylow S et T tels que $I = S \cap T$ ne soit pas trivial[39] et donc d'ordre 3. Alors $N_G(I)$ contient S et T (car par exemple pour $s \in S$ et $i \in I \subseteq S$, $sis^{-1} = i$ car S est abélien) donc $\#N_G(I)$ est un multiple de 9, distinct de 9 (car il a plus de 9 éléments avec $S \cup T$) et divisant 360. Mais $\#N_G(I) \neq 18, 45$ car un groupe d'ordre 18 ou 45 a un unique

39. Pour le voir, nous allons utiliser le résultat suivant (un peu plus fort que celui démontré dans le cours). Soit G un groupe fini et $p \mid \#G$ un nombre premier. On considère alors a tel que

$$p^a = \min\left\{ \frac{|S|}{|S \cap T|} \ : \ S \neq T \ p\text{-Sylow} \right\}.$$

Alors $n_p \equiv 1 \pmod{p^a}$. En effet, soient S et S' deux p-Sylow tels que $p^a = \frac{|S|}{|S \cap S'|}$ et faisons agir S sur l'ensemble X de tous ses p-Sylow par conjugaison. Par la formule des classes, on a

$$n_p = \text{ nombre d'orbites de taille } 1 + \sum_{\substack{\omega \\ |\omega|>1}} |\omega|$$

avec $|\omega| = \frac{|S|}{\mathrm{Stab}(T)}$ pour tout $T \in \omega$. La seule orbite de cardinal 1 est celle de S (voir les notes de cours) et pour les autres orbites, on a $\mathrm{Stab}(T) = \{g \in S \ : \ gTg^{-1} = T\} = S \cap N_G(T)$. Mais alors $S \cap N_G(T) = S \cap T$. L'inclusion $S \cap T \leqslant S \cap N_G(T)$ est triviale et pour l'inclusion réciproque, remarquer que $T \leqslant N_G(T)$ est un p-Sylow distingué de $N_G(T)$ donc le p-groupe $S \cap N_G(T)$ de $N_G(T)$ doit être inclus dans T. On a donc $|\omega| = \frac{|S|}{|S \cap T|}$ et on peut par conséquent en conclure que

$$\sum_{\substack{\omega \\ |\omega|>1}} |\omega| \equiv 0 \pmod{p^a}$$

et finalement que $n_p \equiv 1 \pmod{p^a}$.

Si maintenant $n_3 = 40 \not\equiv 1 \pmod 9$, le résultat précédent implique immédiatement qu'il existe deux 3-Sylwo tels que $S \cap T \neq \{e\}$ puisque sinon

$$9 = \min\left\{ \frac{|S|}{|S \cap T|} \ : \ S \neq T \ 3\text{-Sylow subgroups} \right\}.$$

3-Sylow d'après les théorèmes de Sylow. Si $\#N_G(I) \geqslant 72$, alors il s'agit d'un sous-groupe de G d'indice $\leqslant 5$ et par simplicité de G et en faisant agir G sur $G/N_G(I)$, on aurait que G s'injecte dans $\mathfrak{S}_n$ avec $n \leqslant 5$ ce qui est impossible pour des raisons de cardinalité. Donc $\#N_G(I) = 36$ et $N_G(I)$ admet un unique 2-Sylow P, par conséquent distingué dans $N_G(I)$. Mais $N_G(P)$ contient $N_G(I)$ (car un élément g de $N_G(I)$ stabilise I et donc gPg^{-1} est un 2-Sylow de $N_G(I)$ égal à P par unicité) et P est contenu comme sous-groupe d'indice 2 dans un 2-Sylow Q de G (donc distingué dans Q). Ainsi, $Q \subseteq N_G(P)$ et $\#N_G(P)$ est un multiple de 8 et mutliple de 72 car contenant $N_G(I)$ et distinct de 360 (par simplicité) donc G a un sous-groupe d'indice 5 ce qui fournit là encore une contradiction par simplicité. Ainsi, on a bien $n_3 = 10$.

2. On fait agir par conjugaison sur l'ensemble X des 3-Sylow. Pour voir qu'on arrive dans $\mathfrak{A}_{10}$, on compose par la signature et par cardinalité, le morphisme ne peut pas être injectif et donc il est trivial.

On peut aussi partir du morphisme injectif $\varphi : G \to \mathfrak{S}_{10}$ et remarquer que $\varphi(G) \cap \mathfrak{A}_{10}$ est distingué non trivial dans le groupe simple $\varphi(G)$ donc $\varphi(G) \subseteq \mathfrak{A}_{10}$.

3. Comme $N_G(S)$ fixe $S \in X$, le groupe $N_G(S)$ s'identifie bien au stabilisateur du point $S \in X$ dans G. Il suffit alors de numéroter les éléments de X avec S en dixième position.

Supposons S cyclique. Un générateur de S est alors d'ordre 9 dans $\mathfrak{A}_{10}$ donc un 9-cycle. Ainsi $N_G(S)$ est constitué des éléments de $\mathfrak{A}_9$ (car $N_G(S)$ fixe 10) normalisant un 9-cycle. Or, le centralisateur d'un 9-cycle est précisément le sous-groupe engendré par ce 9-cycle donc cela assure que le morphisme naturel $N_G(S) \to \mathrm{Aut}(S)$ qui à g associe $s \mapsto gsg^{-1}$ est de noyau S et passe au quotient en un morphisme injectif $N_G(S)/S \to \mathrm{Aut}(S)$. Or, $\#N_G(S)/S = 36/9 = 4$ et $\#\mathrm{Aut}(S) = \varphi(9) = 6$ ce qui est absurde. Ainsi S n'est pas cyclique.

4. Supposons qu'il existe $s \in S \setminus \{\mathrm{Id}\}$ fixant un point $i \in \{1, \dots, 9\}$. Alors s est d'ordre 3 (car S n'est pas cyclique) et $s \in S \cap T$ où T est le 3-Sylow de G correspondant au point $i \in \{1, \dots, 9\}$ et on aboutit à une contradiction comme en **1**. En effet, si par exemple on note $\{S_1, \cdots, S_9\}$ les Sylow distincts de S. L'hypothèse fournit qu'il existe $i \in \{1, \dots, 9\}$ tel que $sS_is^{-1} = S_i$. On a alors que $\#N_G(S_i) = 36$ et S_i est donc un 3-Sylow de $N_G(S_i)$ distingué donc unique. Mais $s \in N_G(S_i)$ et d'ordre 3 donc il est dans l'unique 3-Sylow de $N_G(S_i)$, à savoir dans S_i.

5. Les question **3.** et **4.** assurent que S est engendré par deux éléments x et y de $\mathfrak{A}_9$ d'ordre 3 qui commutent et qui ne fixent aucun point de $\{1, \dots, 9\}$. Cela implique que chacun de ces deux éléments sont des produits de trois 3-cycles à supports disjoints. Notons $x = (abc)(def)(ghi)$ avec $\{a, b, c, d, e, f, g, h, i\} = \{1, \dots, 9\}$. Comme y commute à x, y permute les supports des trois 3-cycles en respectant l'ordre cyclique sur ces supports et aucun 3-cycle de y ne peut avoir le même support qu'un 3-cycle de x sinon un élément non trivial de S fixe les trois points de ce support. Autrement dit, on sait que $yxy^{-1} = (y(a)y(b)y(c))(y(d)y(e)y(f))(y(g)y(h)y(i)) = x$ et $y(a) \in \{b, c\}$ (car $y(a) \neq a$ car on n'a aucun point fixe) alors si par exemple $y(a) = b$, $y(b) = c$ et $y(c) = a$ et $x^{-1}y$ fixe a, b, c. Quitte à échanger (def) et (ghi), on peut donc supposer que $y = (adg)(beh)(cfi)$ et quitte à renuméroter les éléments de $\{1, \dots, 9\}$, on peut supposer que $x = (123)(456)(789)$ et $y = (147)(258)(369)$.

6. Par **4.**, $S \subseteq N_G(S)$ agit transitivement sur $\{1, \dots, 9\}$, donc $\#P = 4$ (cardinal de l'orbite de l'action de $N_G(S) \subseteq \mathfrak{A}_9$ sur $\{1, \dots, 9\}$ transitive) et P est un 2-Sylow de $N_G(S)$ (dont on rappelle qu'il est de cardinal 36). Ainsi $N_G(S) = SP$ car $P \cap S = \{e\}$ et par cardinalité (en fait comme $S \lhd N_G(S)$, on a $N_G(S) = S \rtimes P$) et $P \cong N_G(S)/S$. On vérifie alors que le centralisateur de S dans $\mathfrak{A}_9$ est un 3-groupe (on montre en utilisant les résultats de l'exercice 1 du TD I que la classe de conjugaison d'un produit de trois 3-cycles dans $\mathfrak{A}_9$ et dans $\mathfrak{S}_9$ sont les mêmes et donc le cardinal du centralisateur d'un produit de trois 3-cycles dans $\mathfrak{A}_9$ est de 3^4, on a alors qu'un élément du centralisateur de S est dans le centralisateur d'un générateur et est donc d'ordre divisant 3 donc tout élément est d'ordre une puissance de 3 et par le lemme de Cauchy par exemple cela implique qu'on a un 3-groupe). Ainsi $Z_G(S) = S$ où $Z_G(S)$ désigne le centralisateur de S dans G qui est donc un 3-groupe de G contenant S donc égal à S. Ainsi $P \cong N_G(S)/S = N_G(S)/Z_G(S)$ s'injecte dans $\mathrm{Aut}(S)$ car l'application $N_G(S) \to \mathrm{Aut}(S)$ donnée par $g \mapsto [s \mapsto gsg^{-1}]$ est de noyau $Z_G(S)$. Or, $\mathrm{Aut}(S) \cong \mathrm{GL}_2(\mathbf{F}_3)$. Dans $\mathrm{GL}_2(\mathbf{F}_3)$, on voit facilement que les éléments d'ordre 2 sont ceux conjugués à $-I_2$ (I_2 est d'ordre 1 et $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} -1 & a \\ 0 & -1 \end{pmatrix}$ sont d'ordre 3) et $M_a = \begin{pmatrix} 1 & a \\ 0 & -1 \end{pmatrix}$ avec $a \in \mathbf{F}_3$ et on constate que deux matrices M_a et M_b commutent si, et seulement si, $a = b$. Ainsi $\mathrm{GL}_2(\mathbf{F}_3^\times)$ ne contient triplet d'éléments d'ordre 2 qui commutent deux à deux donc $P \ncong (\mathbf{Z}/2\mathbf{Z})^2$ et nécessairement P est cyclique.

7. L'élément z est dans P donc fixe 1 et 10 donc $z \in \mathfrak{A}(\{2, \dots, 9\})$ et est d'ordre 4 donc z est un produit de deux 4-cycles à supports disjoints et n'a donc en particulier pas d'autre point fixe que 2 et 10. Notons $a \in \{3, \dots, 9\}$ l'image de 2 par z. Puisque z normalise S et est d'ordre 4, nécessairement $a \in \{4, 7\}$. En effet, un élément de $N_G(S)$ est déterminé par l'image de 1 (si $g_1, g_2 \in N_G(S)$ envoient tous deux 1 sur le même point, $g_1g_2^{-1}$ fixe 1 et serait donc dans P d'ordre divisant 3 donc $g_1 = g_2$). On écrit explicitement

$$\begin{aligned} N_G(S) = \{&\mathrm{Id}, (123)(456)(789), (132)(465)(798), (147)(258)(369), (174)(285)(396), \\ &(159)(267)(348), (186)(294)(375), (195)(276)(384), (168)(249)(357)\} \end{aligned}$$

Imaginons que $z(2) = 3$ alors $zxz^{-1} = x$ et alors $(z(1)z(2)z(3)) = (123)$ mais $(z(1)z(2)z(3)) = (13z(3))$ ce qui est absurde. Si maintenant $z(2) = 5$, alors $zxz^{-1} = (159)(267)(348)$ et $(z(1)z(2)z(3)) = (15z(3))$ donc $z(3) = 9$. On a aussi $(z(4)z(5)z(6))(z(7)z(8)z(9)) = (267)(348)$. On a $z(5) \neq 2$ sinon on a une transposition et $z(9) \neq 3$. On peut donc avoir $z(5) = 6$, auquel cas $z(6) = 7$ et $z(4) = 2$ mais on a au moins un 5-cycle. D'où, $z(5) \neq 6$ et si $z(5) = 7$, alors $z(6) = 2$ et $z(4) = 6$ et on a un cycle de longueur supérieure

à 4. D'où $z(5) \in \{4, 8\}$. Mais alors si $z(5) = 4$, $z(6) = 8$ et $z(4) = 3 = z(2)$ ce qui est exclu et idem si $z(5) = 8$. On aboutit de même à une contradiction lorsque $z(2) = 6, 8, 9$ si bien que $a \in \{4, 7\}$. Imaginons alors que $z(2) = 4$, cela implique que $z(3) = 7$ et $zx^{-1} = (147)(z(4)z(5)z(6))(z(7)z(8)z(9))$ de sorte que $(z(4)z(5)z(6))(z(7)z(8)z(9)) = (258)(369)$. Mais $z(4) \neq 2$ et $z(7) \neq 3$. Si $z(4) = 5$, alors $z(5) = 8$ et $z(6) = 2$ et on a un cycle de longueur au moins 5. D'où $z(4) \neq 5$. Si $z(4) = 8$, alors $z(5) = 2$ et $z(6) = 5$ et de même on a un cycle de longueur au moins 5. On a alors $z(4) \in \{3, 6, 9\}$. Si $z(4) = 6$, alors $z(5) = 9$, $z(6) = 3$ et on a un cycle trop long. Si $z(4) = 9$, alors $z(5) = 3$, $z(6) = 6$ et on a un point fixe donc nécessairement $z(4) = 3$, $z(5) = 6$ et $z(6) = 9$ et alors nécessairement $z(7) = 2$ et $z(8) = 5$ et $z(9) = 8$ si bien que $z = (2437)(5698)$. Si $z(2) = 7$, le même raisonnement fournit $(2734)(5896)$, autrement dit l'inverse de z qui engendre bien le même groupe. On peut donc bien supposer que $z = (2437)(5698)$.

8. Comme $\langle z\rangle$ est d'indice 2 dans T ($T = \langle z\rangle \cup t\langle z\rangle$), il existe $t \in T$ tel que $T = \langle z, t\rangle$. Comme G est simple, T ne peut pas être cyclique[40]. Ainsi, t est d'ordre 2 ou 4. Or, $t \notin N_G(S)$ donc $t(10) \neq 10$ et comme z fixe 1 et 10, on voit que nécessairement t échange 1 et 10. En effet, puisque $\langle z\rangle \lhd T$ (car d'indice 2), on a que $\sigma = tzt^{-1}$ doit fixer 1 et en prenant l'image par $t(1)$, on a que $\sigma(t(1)) = t(1)$ et de même $\sigma(t(10)) = t(10)$ mais une permutation de $\langle z\rangle$ fixe uniquement 1 et 10 et comme $t(10) \neq 10$, on a $t(10) = 1$ et $t(1) = 1$. Supposons alors t d'ordre 4. Comme t est paire et contient la transposition $(1\ 10)$ dans sa décomposition, la restriction de t à $\{2, \dots, 9\}$ est soit un 4 cycle soit un produit d'un 4-cycles par une double transposition à supports disjoints. Dans les deux cas, t^2 est une double transposition alors que $t^2 \in \langle z\rangle$ et même par ordre $t^2 = z^2$ est un produit de 4 transpositions. On a une contradiction et donc t est bien d'ordre 4.

9. La question précédente assure que t est un produit de $(1\ 10)$ et de 3 transpositions à support disjoints et donc tout élément de $T \setminus \langle z\rangle$ est d'ordre 2, cela implique (voir la classification des groupes d'ordre 8) que $T \cong D_4$. Comme t normalise $P = \langle z\rangle$ (propriété de D_4), une étude au cas par cas assure que (quitte à multiplier par une puissance de z, ce qui est bien acceptable) que l'on peut supposer que t a la forme souhaitée. En effet, $t = (1\ 10)(ab)(cd)(ef)$ avec $\{a, b, c, d, e, f\} \subseteq \{2, 3, 4, 5, 6, 7, 8, 9\}$. De plus, t normalise P et tzt^{-1} est d'ordre 4 donc vaut soit z soit z^{-1}. S'il vaut z, on a que $(t(2)t(4)t(3)t(7)) = (2437)$ ou (5698). Dans le premier cas, puisque t fixe au plus 2 points (car produit de 4 transpositions à supports disjoints), on ne peut pas avoir $t(2) = 2$. Si $t(2) = 4$, alors $t(4) = 3$, $t(4) = 7$ et $t(7) = 2$ et on a un 4-cycle, ce qui est absurde (de même si $t(2) = 3$ ou 7). On a donc $(t(2)t(4)t(3)t(7)) = (5698)$ et $(t(5)t(6)t(9)t(8)) = (2437)$ et si par exemple $t(2) = 5$, $t(4) = 6$, $t(3) = 9$, $t(7) = 8$ et alors on doit avoir $t(5) = 2$ mais $t(6) = 4$, $t(9) = 3$ et $t(8) = 7$ et t est un produit de 5 transpositions ce qui est à nouveau absurde. On a donc $tzt^{-1} = z^{-}1$ si bien que $(t(2)t(4)t(3)t(7)) = (2734)$ ou (5896). Si $t(2) = 2$, alors $t(4) = 7$, $t(3) = 3$ et $t(7) = 4$ et $(t(5)t(6)t(9)t(8)) = (5896)$ et $t(5) \neq 5$ (sinon on a trop de points fixes) et on peut avoir $t(5) = 8$, $t(6) = 9$, $t(9) = 6$ et $t(8) = 5$ si bien que $t = (1\ 10)(47)(58)(69)$ ou $t(5) = 6$ (si $t(5) = 9$ on a aussi trop de points fixes), $t = (1\ 10)(47)(56)(89)$.

Si $t(2) = 7$, $t(4) = 3$, $t(3) = 4$, $t(7) = 2$ et on a deux possibilités $t(5) = 5$, $t(6) = 8$, $t(9) = 9$ et $t(8) = 6$ de sorte que $t = (1\ 10)(27)(34)(68)$ ou $t(5) = 9$, $t(6) = 6$, $t(9) = 5$ et $t(8) = 8$ de sorte que $t = (1\ 10)(27)(34)(59)$.

Si $t(2) = 3$, $t(4) = 4$, $t(3) = 2$, $t(7) = 7$ et on a deux possibilités $t(5) = 8$, $t(6) = 9$, $t(9) = 6$ et $t(8) = 5$ de sorte que $t = (1\ 10)(23)(58)(69)$ ou $t(5) = 6$, $t(6) = 5$, $t(9) = 8$ et $t(8) = 9$ de sorte que $t = (1\ 10)(23)(56)(98)$.

Si $t(2) = 4$, $t(4) = 2$, $t(3) = 7$, $t(7) = 3$ et on a deux possibilités $t(5) = 5$, $t(6) = 8$, $t(9) = 9$ et $t(8) = 6$ de sorte que $t = (1\ 10)(24)(37)(68)$ ou $t(5) = 9$, $t(6) = 6$, $t(9) = 5$ et $t(8) = 8$ de sorte que $t = (1\ 10)(24)(37)(59)$.

On a aussi la possibilité que $(t(2)t(4)t(3)t(7)) = (5896)$ et $(t(5)t(6)t(9)t(8)) = (2734)$. Si $t(2) = 5$, $t(4) = 8$, $t(3) = 9$, $t(7) = 6$ et nécessairement $t(5) = 2$, $t(6) = 7$, $t(9) = 3$ et $t(8) = 4$ et on a trop de transpositions et de même dans les autres cas. On a donc 8 possibilités pour t. Maintenant, si on part de $\sigma = (1\ 10)(23)(56)(98)$, alors on vérifie que $z\sigma$, $z^2\sigma$ et $z^3\sigma$ donne trois autres t acceptables. De même, $\sigma' = (1\ 10)(47)(58)(69)$, $z\sigma$, $z^2\sigma$, $z^3\sigma$ donne les 4 autres. Par ailleurs, $z\sigma' z^{-1} = \sigma$ et donc on peut bien supposer que t a la forme souhaitée.

10. Par construction, $\langle x, y, z, t\rangle \subseteq G$ est un sous-groupe de cardinal $\geqslant 72$ et par simplicité G n'admet aucun sous-groupe strict d'indice $\leqslant 5$. Cela garantit que nécessairement $G = \langle x, y, z, t\rangle$.

11. Les questions précédentes assurent que tout groupe simple d'ordre 360 est isomorphe au sous-groupe G_0 de $\mathfrak{A}_{10}$ engendré par les éléments $x, y, z, t \in \mathfrak{A}_{10}$ (ces éléments ne dépendant pas de G). En particulier, cela implique que tous les groupes simples d'ordre 360 sont isomorphes.

12. Ces deux groupes sont simples d'ordre 360 donc on conclut par **11**.

40. Sinon il existe un élément d'ordre 8 et on fait agir G sur lui-même par multiplication à gauche fournissant un homomorphisme $G \to \mathfrak{S}(G) \cong \mathfrak{S}_{360}$. En composant avec la signature, on obtient un morphisme $G \to \mathbf{Z}/2\mathbf{Z}$ qui est surjectif comme on le voit en prenant l'image de notre élément d'ordre 8. La permutation obtenue se décompose en produit de $\#G/8$ cycles de la forme $(g, xg, x^2g, \dots, x^7g)$ de longueur 8 (les orbites étant indexées par un système de représentant de $G/\langle x\rangle$. On obtient que la signature est donnée par $(-1)^{\#G/8} = -1$. Le noyau de ce morphisme est alors d'indice 2 et contredit la simplicité de G. Cela se généralise bien sûr à tout 2-Sylow d'un groupe simple (qui ne peut donc pas être cyclique).

Bonus

On donne ici une notion supplémentaire qui se révèle fondamental dans la théorie des groupes finis et pour la classification des groupes simples finis.

Exercice 20 — Transfert de Burnside. Soit G un groupe fini.

1. 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.
2. 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
$$V(h) = \pi\left(\prod_{i=1}^{r} g_i^{-1} h^{n_i} g_i\right).$$
3. 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 $N_G(A)$).
4. 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 **1.** est surjectif. En déduire qu'il existe un sous-groupe distingué H de G tel que S soit isomorphe à G/H.
5. En déduire que si G est simple non cyclique, alors le cardinal de G est divisible par 12 ou son plus petit facteur premier appraît au moins au cube dans sa décomposition en facteurs premiers.

Solution.

1. On sait que le groupe $H/D(H)$ est abélien donc l'ordre des produits effectués dans ce groupe est sans importance. Soient $g, g' \in G$. On a par définition
$$V(gg') = \pi\left(\prod_{i=1}^{n} h_{i,(gg')\cdot i}\right),$$
avec les $h_{i,(gg')\cdot i} \in H$ définis par
$$(gg')x_i = x_{(gg')\cdot i} h_{i,(gg')\cdot i}$$
Or, $(gg')x_i = g(g' x_i)$ si bien que
$$x_{(gg')\cdot i} h_{i,(gg')\cdot i} = g\left(x_{g'\cdot i} h_{i,g'\cdot i}\right) = x_{g\cdot(g'\cdot i)} h_{g'\cdot i, g\cdot(g'\cdot i)} h_{i,g'\cdot i}.$$
et $h_{i,(gg')\cdot i} = h_{g'\cdot i, g\cdot(g'\cdot i)} h_{i,g'\cdot i}$. Puisque $H/D(H)$ est abélien, on a
$$V(gg') = \pi\left(\prod_{i=1}^{n} h_{g'\cdot i, g\cdot(g'\cdot i)}\right)\pi\left(\prod_{i=1}^{n} h_{i,g'\cdot i}\right) = V(g)V(g')$$
du fait que l'application $i \mapsto g'\cdot i$ est une bijection de $\{1, \dots, n\}$. Par ailleurs, on a clairement $V(1) = 1$ et V défini bien un morphisme de groupes.

Montrons maintenant que V est indépendant du choix des x_i. La commutativité de $H/D(H)$ assure que V ne change pas même si l'on permute les x_i. Si maintenant $x'_1, \dots, x'_n$ est un autre système de représentants de G modulo H définissant un morphisme V'. Alors quitte à permuter les x'_i, on peut supposer que x'_i est équivalent à x_i pour tout $i \in \{1, \dots, n\}$, autrement dit qu'il existe $k_i \in H$ tel que $x'_i = x_i k_i$. Par conséquent, on voit que l'on a
$$h_{i,g\cdot i} = k_{g\cdot i} h'_{i,g\cdot i} k_i^{-1}$$
et on conclut par commutativité de $H/D(H)$ que
$$V(g) = \pi\left(\prod_{i=1}^{n} h_{i,g\cdot i}\right) = \pi\left(\prod_{i=1}^{n} k_{g\cdot i} h'_{i,g\cdot i} k_i^{-1}\right) = \pi\left(\prod_{i=1}^{n} h'_{i,g\cdot i}\right) = V'(g)$$
car le produit des $k_{g\cdot i}$ est le même que celui des k_i. On a donc bien indépendance en le choix du système de représentants.

2. Il est clair qu'un ensemble de représentants de G modulo H est donné par

$$g_1, hg_1, \dots, h^{n_1-1}g_1, g_2, \dots, h^{n_2-1}g_2, \dots, g_r, \dots, h^{n_r-1}g_r.$$

Avec ces choix pour les x_i, on voit immédiatement que

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

3. On suppose qu'il existe $g \in G$ tel que $B = gAg^{-1}$. Les hypothèses assurent que l'on a les inclusions

$$S \subseteq N_G(A) \quad \text{et} \quad g^{-1}Sg \subseteq N_G(A).$$

Or, S et $g^{-1}Sg$ sont deux p-Sylow de $N_G(A)$ donc conjugués dans $N_G(A)$. Autrement dit, il existe $h \in N_G(A)$ tel que $g^{-1}Sg = hSh^{-1}$ soit tel que $gh \in N_G(S)$. Enfin, on a

$$(gh)A(gh)^{-1} = g(hAh^{-1})g^{-1} = gAg^{-1} = B$$

car h normalise A, ce qui permet de conclure.

4. Noter que puisque $S \subseteq N_G(S)$, l'hypothèse $S \subseteq Z(N_G(S)$ implique que S est abélien et donc $S/D(S) \cong S$. Soit $s \in S$. On a par **2.** que

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

On pose alors $A = \{g_i^{-1}s^{n_i}g_i\}$ et $B = \{s^{n_i}\}$. Comme S est abélien, A et B vérifient les hypothèses de **3.** donc par **3.**, il existe $y_i \in N_G(S)$ tel que $g_i^{-1}s^{n_i}g_i = y_i s^{n_i} y_i^{-1}$ pour tout i. Or, par hypothèse, $S \subseteq Z(N_G(S))$, ce qui assure que

$$g_i^{-1}s^{n_i}g_i = y_i s^{n_i} y_i^{-1} = s^{n_i} \quad \text{donc} \quad V(s) = \prod_{i=1}^{r} s^{n_i} = s^{\sum_{i=1}^{r} n_i} = s^{[G:S]}.$$

Enfin, comme S est un p-Sylow de G, $[G : S]$ est premier au cardinal de S (qui est abélien) ce qui assure que le morphisme $S \longrightarrow S$ défini par $s \mapsto s^{[G:S]}$ est un isomorphisme (car injectif par Lagrange puis on conclut à la bijectivité par cardinalité). Ainsi, la restriction de V à S est un automorphisme de S ce qui assure la surjectivité de $V : G \longrightarrow S$. Ainsi $H = \mathrm{Ker}(V)$ est un sous-groupe normal de G tel que $G/H \cong S$ via V.

5. Soit G un groupe non cyclique. On note p le plus petit facteur premier de $\#G$ et on suppose que $p^3 \nmid \#G$. Soit S un p-Sylow de G qui est donc de cardinal p ou p^2 donc abélien. L'action par conjugaison induit un morphisme de groupes $\varphi : N_G(S)/S \longrightarrow \mathrm{Aut}(S)$ dont la trivialité équivaut à la condition $S \subseteq Z(N_G(S))$. Or, tous les facteurs premiers du cardinal de $N_G(S)/S$ sont $> p$ alors que $\mathrm{Aut}(S)$ est isomorphe à $\mathbf{Z}/(p-1)\mathbf{Z}$ si S est d'ordre p et $\mathrm{GL}_2(\mathbf{F}_p)$ si S est d'ordre p^2 non cyclique et $\mathbf{Z}/p(p-1)\mathbf{Z}$ si S est d'ordre p^2 cyclique. Les cardinaux de ces trois groupes sont respectivement $p-1$, $p(p-1)^2(p+1)$, $p(p-1)$. Par conséquent, dans les trois cas, les facteurs premiers de ce cardinal sont tous $\leqslant p+1$. On a alors deux cas : si $p > 2$, alors $p+1$ n'est pas premier et donc le morphisme φ est toujours trivial, soit $p = 2$ et $p+1 = 3$ et φ est trivial sauf lorsque $p^2 = 4$ et $p+1 = 3$ divisent $\#G$. Finalement, on a $S \subseteq Z(N_G(S))$ dans tous les cas sauf si $p = 2$ et $12 \mid \#G$. Ainsi par **4.**, G admet un sous-groupe distingué non trivial d'indice $\#S$ sauf si $12 \mid \#G$. Ainsi on peut en conclure que G n'est pas simple sauf si éventuellement $12 \mid G$ ou son plus petit facteur premier apparaît au cube dans sa décomposition en produit de facteurs premiers.

Une application de ce théorème de transfert couplé à l'exercice 6 permet d'établir qu'aucun groupe d'ordre compris entre 61 et 167 n'est simple. En effet, les seuls candidats possibles sont les groupes d'ordre 72, 80, 88, 96, 104, 112, 120, 135, 136, 144, 152, 156 et 160 que l'on peut traiter au cas par cas à l'aide des théorèmes de Sylow. Pour aller plus loin, je vous renvoie aussi pour plus de détails à l'exercice 8 du Perrin qui permet d'établir Feit-Thompson pour les groupes d'ordre < 2000 (modulo un théorème de Burnside mentionné plus haut) mais aussi à http://christophebertault.fr/documents/articles/Article-Lesgroupesfinissimplesd'ordreinferieurc