Feuille TD 1 – Exercices Algèbre – Groupes – Corrigé

1 Généralités

Exercice 1 — Morphismes ou non ?.
Soit G un groupe. Les applications suivantes de G dans G sont-elles toujours des morphismes ?

1. $f_a : x \mapsto ax$, avec $a \in G$ fixé ;
2. $f_n : x \mapsto x^n$ pour $n \in \mathbf{N}^*$;
3. $g : x \mapsto x^{-1}$.

Solution.

1. On remarque que si $a \neq e$, alors $f_a(e) = a \neq e$ et on a donc pas un morphisme de groupes. En revanche, si $a = e$, on a l'identité qui est bien un morphisme de groupes.
   Une autre façon de le voir est de constater qu'en général, pour $x, y \in G$, $a(xy) \neq (ax)(ay)$ (sauf si $a = e$).
2. Ici on a bien $f_n(e) = e$ mais de on n'a pas un morphisme en général si G n'est pas abélien car $(xy)^n \neq x^n y^n$.
3. Idem, non en général si G n'est pas abélien car $(xy)^{-1} = y^{-1}x^{-1} \neq x^{-1}y^{-1}$.

Exercice 2 — Groupes, intersections et réunions.

1. Montrer que l'intersection d'une famille quelconque de sous-groupes d'un groupe G est aussi un sous-groupe.
2. Soient A et B deux sous-groupes d'un même groupe G. Montrer que $A \cup B$ est un sous-groupe de G si, et seulement si, $A \subseteq B$ ou $B \subseteq A$.
3. Que se passe-t-il si l'on considère la réunion d'au moins trois sous-groupes ?

Solution.

1. Soient $(G_i)_{i\in I}$ une famille de sous-groupes de G. On a clairement que $e \in \bigcap_{i\in I} G_i$. Par ailleurs, pour tous $x, y \in \bigcap_{i\in I} G_i$, on a que pour tout $i \in I$, $x, y \in G_i$ qui est un sous-groupe de G. Par conséquent, pour tout $i \in I$, $x, y \in G_i$, $xy^{-1} \in G_i$ et $xy^{-1} \in \bigcap_{i\in I} G_i$ et on a gagné !
2. C'est clair si $B \subseteq A$ ou $A \subseteq B$. Réciproquement, supposons que $A \cup B$ soit un sous-groupe de G. Supposons par l'absurde que $B \not\subseteq A$ ou $A \not\subseteq B$. On dispose alors de $x \in A$, $x \notin B$ et de $y \in B$, $y \notin A$. Mais $x, y \in A \cup B$ qui est un groupe donc $xy \in A \cup B$. On a alors soit $xy \in A$ soit $xy \in B$ par définition. Si $xy \in A$, alors
$$y = x^{-1}(xy) \in A \quad \text{car} \quad x, xy \in A,$$
   ce qui est absurde. De même, si $xy \in B$, alors $x \in B$ et on aboutit à une contradiction. En conclusion, on a bien $B \subseteq A$ ou $A \subseteq B$.
3. Par exemple
$$\mathfrak{S}_3 = \mathfrak{A}_3 \cup \langle(12)\rangle \cup \langle(13)\rangle \cup \langle(23)\rangle \quad \text{ou} \quad (\mathbf{Z}/2\mathbf{Z})^2 = \langle(\overline{1},\overline{0})\rangle \cup \langle(\overline{0},\overline{1})\rangle \cup \langle(\overline{1},\overline{1})\rangle.$$
   En revanche, dans le cas d'un espace vectoriel E sur un corps k **infini**, on a bien que
$$E \neq F_1 \cup F_2 \cup \cdots \cup F_n$$
   pour tous $F_1, F_2, \ldots, F_n$ des sous-espaces vectoriels stricts de E. En effet, sinon on peut supposer que $E = F_1 \cup F_2 \cup \cdots \cup F_n$ et que $F_n \not\subseteq F_1 \cup F_2 \cup \cdots \cup F_{n-1}$ (sinon il suffit de se débarrasser de F_n !). On peut alors choisir $x \in F_n \setminus F_1 \cup F_2 \cup \cdots \cup F_{n-1}$ et $y \notin F_n$. On a alors que pour tout $\lambda \in k$, $\lambda x + y \notin F_n$ et pour tout $i \leqslant n-1$, il existe au plus un $\lambda \in k$ tel que $\lambda x + y \in F_i$. En effet, si on dispose de $\lambda \neq \mu$ tels que $\lambda x + y$ et $\mu x + y$ sont dans F_i, alors $(\lambda - \mu)x \in F_i$ ce qui est absurde ! Mais comme $E = F_1 \cup F_2 \cup \cdots \cup F_n$, il existe au moins un $i \leqslant n-1$ tel que $\lambda x + y \in F_i$, ce qui vient contredire le caractère infini du corps k !

Exercice 3 — Botanique des groupes de petit cardinal. Décrire, à isomorphisme près, tous les groupes de cardinal $\leqslant 7$.

Solution. On a en fait la classification à isomorphisme près des groupes d'ordre $\leqslant 11$.

- Le seul groupe d'ordre 1 est le groupe trivial ;

- Si G est d'ordre p avec p premier alors nécessairement tout élément $g \in G$ distinct de l'identité est d'ordre p et engendre G si bien que[1] $G \cong \mathbf{Z}/p\mathbf{Z}$. Cela résout les cas $2, 3, 5, 7, 11$;
- Si G est d'ordre 4, on a que $G \cong \mathbf{Z}/4\mathbf{Z}$ si G contient un élément d'ordre 4 et sinon $G \cong (\mathbf{Z}/2\mathbf{Z})^2$ et G est engendré par toute paire d'éléments d'ordre 2 (qui commutent). En effet, l'ordre d'un élément non trivial de G divise 4 par Lagrange et vaut donc 2 ou 4. Si on a un élément d'ordre 4, alors G est cyclique et $G \cong \mathbf{Z}/4\mathbf{Z}$. Sinon, tout élément non trivial est d'ordre 2 et on peut faire appel à l'exercice 11 ou raisonner à la main. On doit avoir (puisque G est d'ordre 4) au moins un élément d'ordre 2, que nous pouvons appeler x. Puisque $x^2 = e$, $x^{-1} = x$ et donc on doit nécessairement avoir dans G un autre élément $y \neq x$ d'ordre 2. On a ainsi

$$\{e, x, y, xy\} \subseteq G \quad \text{et donc} \quad G = \{e, x, y, xy\}.$$

  Noter qu'ici on a utilisé que $xy \neq e, x, y$. On en déduit que $yx \in G$ et $yx \neq e, x, y$ donc $yx = xy$ et cela permet d'écrire la table de G. On reconnaît celle de $(\mathbf{Z}/2\mathbf{Z})^2$ si bien que $G \cong (\mathbf{Z}/2\mathbf{Z})^2$.
- Si G est d'ordre 6, on a que $G \cong \mathbf{Z}/6\mathbf{Z}$ si[2] G contient un élément d'ordre 6 (ou deux éléments d'ordre 2 et 3 respectivement qui commutent) et sinon[3] $G \cong \mathfrak{S}_3$ et G est engendré par un élément τ d'ordre 2 et un élément σ d'ordre 3 tels que $\tau\sigma\tau = \sigma^2$. En effet, l'ordre d'un élément non trivial de G vaut (par Lagrange) 2, 3 ou 6. Si on a un élément d'ordre 6, alors G est cyclique et $G \cong \mathbf{Z}/6\mathbf{Z}$. On peut donc supposer que tout élément non trivial est d'ordre 2 ou 3. On va montrer qu'il existe un élément d'ordre 2 et un élément d'ordre 3. En effet, si tous les éléments sont d'ordre 2, il vient qu'alors G est abélien[4] et contient au moins deux éléments d'ordre 2 distincts qui commutent. Le sous-groupe engendré par ces deux éléments est alors isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$ donc d'ordre 4, ce qui contredit le théorème de Lagrange. De même, si l'on avait que des éléments d'ordre 3, alors on disposerait d'au moins deux éléments x, y avec $y \neq x, x^2$ d'ordre 3 et

$$\{e, x, x^2, y, y^2, xy\} \subseteq G,$$

  où $xy \neq e, x, x^2, y, y^2$. On a alors que $xy^2 \neq e, x, x^2, y, y^2, xy$ et on aurait alors au moins 7 éléments dans G. On peut donc supposer que l'on dispose d'un élément τ d'ordre 2 et un élément σ d'ordre 3 et alors

$$\{e, \tau, \sigma, \sigma^2, \tau\sigma, \tau\sigma^2\} \subseteq G \quad \text{et donc} \quad G = \{e, \tau, \sigma, \sigma^2, \tau\sigma, \tau\sigma^2\}$$

  et où tous ces éléments sont deux à deux distincts. Alors, $\sigma\tau \in G$ et comme $\sigma\tau \neq \tau\sigma$, sinon le produit fournit un élément d'ordre[5] 6, on a nécessairement que $\tau\sigma\tau = \sigma^2$. Cela permet de dresser la table de multiplication du groupe G et on reconnaît celle de $\mathfrak{S}_3$ si bien que $G \cong \mathfrak{S}_3$.
- Si G est d'ordre 8, les exercices sur le groupe diédral et les quaternions ainsi le cours sur les produits semi-directs garantira que G est isomorphe soit à $(\mathbf{Z}/2\mathbf{Z})^3$, soit à $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, soit à $\mathbf{Z}/8\mathbf{Z}$, soit au groupe diédral $\mathbf{D}_4$ soit au groupe des quaternions $\mathbf{H}_8$.
- Si G est d'ordre $9 = 3^2$, le cours garantira que G est abélien et donc le théorème de structure des groupes abéliens de type fini garantit que $G \cong \mathbf{Z}/9\mathbf{Z}$ ou $G \cong (\mathbf{Z}/3\mathbf{Z})^2$;
- Si G est d'ordre $10 = 2 \times 5$ avec $2 \mid 5 - 1$, le cours sur le produit semi-direct garantira que G est soit abélien et isomorphe à $\mathbf{Z}/10\mathbf{Z} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$ soit isomorphe à l'unique produit semi-direct non trivial $\mathbf{Z}/2\mathbf{Z} \rtimes \mathbf{Z}/5\mathbf{Z}$ (qui est en fait isomorphe au groupe diédral[6] $\mathbf{D}_5$).

Pour aller plus loin, je vous renvoie aux feuilles de TD des annés précédentes[7] pour le cours d'Algèbre M1 MF, on peut classifier les groupes d'ordre p^2q avec p et q deux nombres premiers distincts ce qui traite le cas de 12 (qui peut également se traiter "à la main"), 13 est premier, 14 et 15 sont alors couverts par le cours sur le produit semi-direct ! On remarquera donc qu'il y a quelque chose qui semble se passer pour les

1. En effet, pour $x \in G \smallsetminus \{e\}$, $G = \{e, x, x^2, \ldots, x^{p-1}\}$. On pose alors l'application

$$\varphi : \left\{ \begin{array}{ccc} \mathbf{Z}/p\mathbf{Z} & \longrightarrow & G \\ \overline{k} & \longmapsto & x^k. \end{array} \right.$$

On vérifie comme toujours qu'une application définie sur un quotient est bien définie. Soient pour cela $\overline{k} = \overline{k'}$ pour $k, k' \in \mathbf{Z}$. Par définition, on a $k = k' + p\ell$ pour un certain entier ℓ. On a alors

$$x^k = x^{k'+p\ell} = x^{k'} \left(x^p\right)^\ell = x^{k'}$$

puisque $x^p = e$. L'application est donc bien définie et surjective vue la description de G plus haut. Comme $\#G = \#\left(\mathbf{Z}/p\mathbf{Z}\right) = p$, on a une bijection. Par ailleurs, il s'agit d'un morphisme de groupes puisque pour tous $\overline{k}, \overline{k'}$ dans $\mathbf{Z}/p\mathbf{Z}$ (attention ici que la loi de groupe sur $\mathbf{Z}/p\mathbf{Z}$ est **additive** tandis que celle sur G est **multiplicative**),

$$f\left(\overline{k} + \overline{k'}\right) = f\left(\overline{k+k'}\right) = x^{k+k'} = x^k x^{k'} = f\left(\overline{k}\right) f\left(\overline{k'}\right).$$

On a donc bien un isomorphisme et le résultat !

2. Noter que par théorème chinois, puisque 3 et 2 sont premiers entre eux, $G \cong \mathbf{Z}/6\mathbf{Z} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$.

3. On a aussi que $G \cong \mathfrak{S}_3 \cong \mathbf{D}_3$ le groupe des isométries laissant invariant le triangle équilatéral formé des racines cubiques de l'unité et $\mathfrak{S}_3 \cong \mathbf{Z}/3\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}$ est le seul produit semi-direct non trivial d'ordre 6.

4. En effet, pour tous $g, h \in G$, on a $(gh)^2 = e$ de sorte que $ghgh = e$ et en multipliant par h à droite il vient $ghg = h$ (car $h^2 = e$) et enfin en multipliant par g à droite on obtient $gh = hg$ (car $g^2 = e$).

5. En effet, $(\sigma\tau)^6 = \sigma^6\tau^6$ car G est abélien si $\sigma\tau = \tau\sigma$. Mais comme $\tau^2 = \sigma^3 = e$, on a $(\tau\sigma)^6 = e$. L'ordre de $\tau\sigma$ (qui est différent de e) vaut donc 2, 3 ou 6 mais $(\tau\sigma)^2 = \tau^2\sigma^2$ (toujours par caractère abélien de G) et donc $(\tau\sigma)^2 = \sigma^2 \neq e$ car $\tau^2 = e$ et σ est d'ordre 3. De même, $(\tau\sigma)^3 = \tau \neq e$ et l'ordre de $\tau\sigma$ est bien 6.

6. Voir l'exercice 5.

7. Disponibles sur la page web de David Harari.

groupes d'ordre 8 ou 12 (on a plus de travail et plus de classes d'isomorphismes). On peut aussi classifier [8] (à isomorphisme près) les groupes de cardinal $\leqslant 15$ on s'arrête à 15 pour une bonne raison, à savoir que le cardinal 16 est plus délicat et qu'on obtient beaucoup de classes d'isomorphismes (précisément 14). En fait, on peut voir que plus l'ordre du groupe possède de facteurs premiers de multiplicité grande, plus cela donne de la marge et donne lieu à de nombreuses classes d'isomorphismes. Pour une taille de cardinal donnée, l'ordre qui va maximiser ces critères est la puissance de 2. On peut par exemple l'illustrer par le fait que parmi tous les groupes d'ordre $\leqslant 2000$ (à isomorphisme près), $99,2\%$ sont d'ordre [9] $2^{10} = 1024$. En fait, on conjecture que presque tous les groupes finis sont des 2-groupes dans le sens où

$$\lim_{N\to+\infty} \frac{\#\left\{\text{classes d'iso. de 2-groupes } G \text{ de cardinal } \leqslant N\right\}}{\#\left\{\text{classes d'iso. de groupes } G \text{ de cardinal } \leqslant N\right\}} = 1$$

et même

$$\lim_{N\to+\infty} \frac{\#\left\{\text{classes d'iso. de 2-groupes } G \text{ de cardinal } 2^{\left\lceil \frac{\log(N)}{\log(2)} \right\rceil}\right\}}{\#\left\{\text{classes d'iso. de groupes } G \text{ de cardinal } \leqslant N\right\}} = 1.$$

Exercice 4 — Groupe symétrique. Soit $\mathfrak{S}_n$ le groupe symétrique sur n lettres.

1. Quel est l'ordre maximal d'un élément de $\mathfrak{S}_3$? de $\mathfrak{S}_4$? de $\mathfrak{S}_5$? de $\mathfrak{S}_n$?
2. Donner le treillis [10] des sous-groupes de $\mathfrak{S}_3$, en précisant à chaque fois lesquels des sous-groupes sont distingués. Répéter l'exercice avec le groupe alterné $\mathfrak{A}_4$.
   Soient G un groupe et $K \subseteq H$ deux sous-groupes de G. On suppose que $K \lhd H$ et que $H \lhd G$. A-t-on $K \lhd G$? Démontrer que si K est caractéristique dans H et que H est caractéristique dans G, alors K est caractéristique dans G.
3. Une *partition d'un entier* n est une suite $0 < \lambda_1 \leqslant \lambda_2 \leqslant \cdots \leqslant \lambda_r$ d'entiers tels que $\sum_{i=1}^{r} \lambda_i = n$. Montrer que les classes de conjugaison de $\mathfrak{S}_n$ sont en bijection avec les partitions de n.
4. Déterminer le centre de $\mathfrak{S}_n$.

Solution. Je vous renvoie pour des rappels sur le groupe symétrique et l'essentiel de ce qu'il faut connaître au premier chapitre du *Cours d'algèbre* de Daniel Perrin, un grand classique de l'agrégatif ou de l'agrégative !

1. Plusieurs façons de faire : décrire tous les éléments de $\mathfrak{S}_3$: $\mathrm{Id}, (12), (13), (23), (123), (132)$ ou alors en utilisant la décomposition de toute permutation en produit de cycles à supports disjoints dont l'ordre est alors le ppcm des longueurs des cycles [11] ou encore en utilisant le théorème de Lagrange et le fait que $\mathfrak{S}_3$ n'est pas cyclique car non abélien. Bref, on trouve 3 pour chacun des deux 3-cycles. De même, pour $\mathfrak{S}_4$, on trouve 4 atteint pour les six 4-cycles. Pour $\mathfrak{S}_5$, on obtient 6 pour chacun des 20 produits d'une transposition et d'un 3-cycle à supports disjoints. De manière générale, on voit que l'ordre maximal dans $\mathfrak{S}_n$ est donné par

   $$g(n) = \max_{\substack{0<\lambda_1\leqslant\cdots\leqslant\lambda_r \\ \lambda_1+\cdots+\lambda_r=n}} \mathrm{ppcm}(\lambda_1,\ldots,\lambda_r).$$

   On retrouve bien les résultats précédents puisqu'on a les partitions suivantes :

   $$3 = 1{+}1{+}1 = 1{+}2 = 3, \quad 4 = 1{+}1{+}1{+}1 = 2{+}2 = 1{+}3 = 4 \quad \text{et} \quad 5 = 1{+}1{+}1{+}1{+}1 = 1{+}1{+}1{+}2 = 1{+}1{+}3 = 1{+}4 = 2{+}3 = 5.$$

   On obtient par le théorème de Lagrange que $g(n) \mid n!$ et g est croissante. On a par exemple

n	3	4	5	6	7	8	9	10	11	12	13
g(n)	3	4	6	6	12	15	20	30	30	60	60

   Landau a démontré [12] en 1909 l'équivalent

   $$\log g(n) \underset{n\to+\infty}{\sim} \sqrt{n\log(n)}.$$

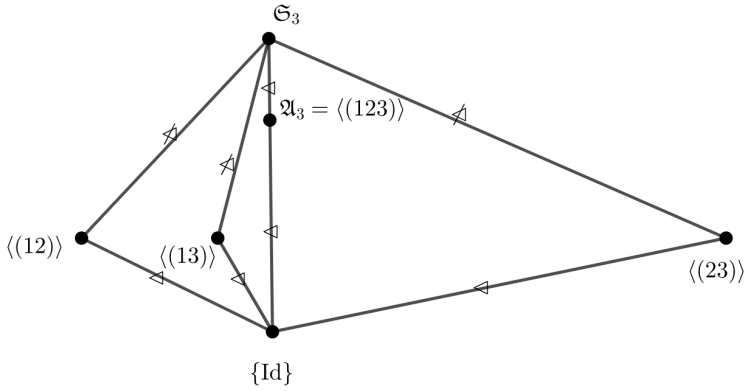
   ▶ **Compléments . –** C'est aussi un exercice intéressant de les dénombrer le nombre de partitions dont la décomposition en cycle à supports disjoints correspond à une partition $\boldsymbol{\lambda} = (\lambda_1,\ldots,\lambda_r)$ tel que $n = \lambda_1 + \cdots + \lambda_r$ vaut

   $$\frac{n!}{\prod_{j=1}^{n} a_j(\boldsymbol{\lambda})! j^{a_j(\boldsymbol{\lambda})}}$$

8. Voir à nouveau les feuilles de TD de l'an dernier.
9. Voir Besche, Eick et O'Brien, *The groups of order at most 2000*.
10. C'est-à-dire le graphe non orienté dont les sommets sont les sous-groupes de G et où une arête relie deux sous-groupes H_1 et H_2 si, et seulement si, $H_1 \subseteq H_2$ ou $H_2 \subseteq H_1$.
11. Car on vérifie immédiatement qu'un cycle de longueur ℓ est d'ordre ℓ et le fait que les cycles soient à support disjoints entraîne qu'ils commutent.
12. En utilisant des résultats d'arithmétique notamment sur la répartition des nombres premiers. Si l'article vous intéresse (et que vous lisez l'allemand), je peux vous transmettre l'article ! Vous trouverez une version en français ici.

où $a_j(\boldsymbol{\lambda})$ désigne le nombre de λ_k égaux à j. On peut faire pour cela agir G sur lui-même par conjugaison et on montre que le cardinal du stabilisateur de σ est donné par $\prod_{j=1}^{n} a_j(\boldsymbol{\lambda})! j^{a_j(\boldsymbol{\lambda})}$. En effet, pour envoyer σ sur lui-même par conjugaison, on procède cycle par cycle. Le premier cycle de longueur j est envoyé sur un autre cycle de longueur j. On a alors $a_j(\boldsymbol{\lambda})$ choix parmi tous les cycles de longueur j. Ensuite, on a j manières d'envoyer par conjugaison un j-cycle sur un autre j-cycle. Pour le second cycle de longueur j, il reste $a_j(\boldsymbol{\lambda})-1$ choix parmi tous les cycles de longueur j et toujours j manières d'envoyer par conjugaison un j-cycle sur un autre j-cycle. On obtient finalement un facteur $a_j(\boldsymbol{\lambda})! j^{a_j(\boldsymbol{\lambda})}$ et le produit apparaît lorsqu'on parcourt toutes les longueurs de cycles possibles.

2. On obtient facilement le treillis suivant [13]



car les sous-groupes sont d'ordre 1, 2, 3 ou 6 et les groupes d'ordre 2 et 3 sont nécessairement cycliques. Un groupe d'ordre 2 est alors simplement engendré par un élément d'ordre 2, autrement dit ici une transposition et donc de la forme $\langle(ab)\rangle = \{\mathsf{Id}, (ab)\}$ tandis qu'un sous-groupe d'ordre 3 est engendré par un élément d'ordre 3, autrement dit un 3-cycle et est alors donné par $\langle(abc)\rangle = \{\mathsf{Id}, (abc), (acb)\}$ si bien qu'on a un unique sous-groupe d'ordre 3, à savoir

$$\mathfrak{A}_3 = \langle(123)\rangle = \{\mathsf{Id}, (123), (132)\}\,.$$

Par ailleurs, on sait que $\mathfrak{A}_3$ est distingué dans $\mathfrak{S}_3$ et puisque

$$(abc)(ab)(acb) = (bc)$$

si $\{a,b,c\} = \{1,2,3\}$, aucun des sous-groupes d'ordre 2 ne sont distingués [14] dans $\mathfrak{S}_3$.
Passons à $\mathfrak{A}_4$. On sait que

$$\mathfrak{A}_4 = \{\mathsf{Id}, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}\,.$$

De plus, $\#\mathfrak{A}_4 = 12$ donc les sous-groupes non triviaux sont d'ordre 6, 4, 3 ou 2. Or, on sait qu'un sous-groupe d'ordre 6 [15] est soit cyclique soit isomorphe à $\mathfrak{S}_3$. ici la seule option serait $\mathfrak{S}_3$ car on n'a pas d'élément d'ordre 6 mais dans $\mathfrak{S}_3$ aucune paire d'éléments d'ordre 2 ne commutent tandis qu'ici tous les éléments d'ordre 2 commutent

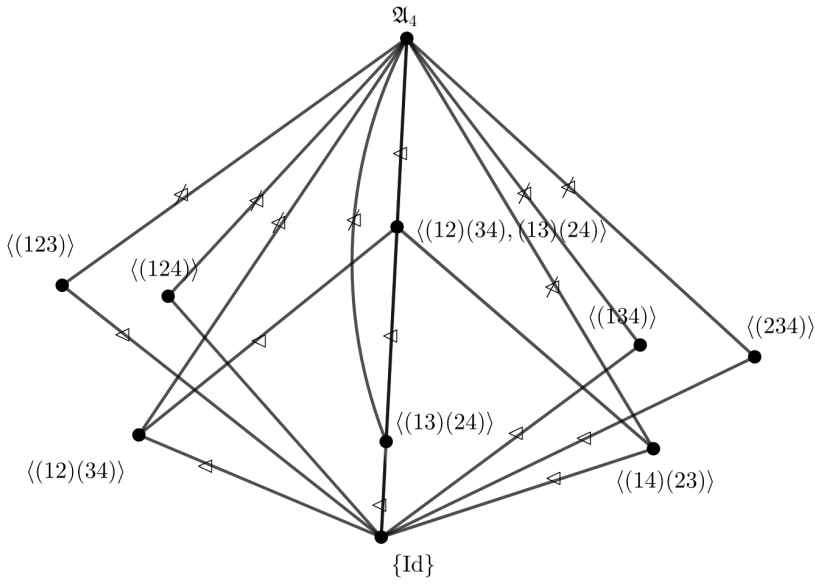
$$(12)(34)(13)(24) = (13)(24)(12)(34).$$

Pour les groupes d'ordre 4, on a deux possibilités [16] $\mathbf{Z}/4\mathbf{Z}$ et $(\mathbf{Z}/2\mathbf{Z})^2$. Ici, pas d'élément d'ordre 4 donc la seule possibilité est la seconde et on voit qu'on a un seul tel sous-groupe engendré par n'importe quelle paire d'éléments d'ordre 2 qui commutent, autrement dit par n'importe quelle paire de doubles transpositions

$$\langle(12)(34), (13)(24)\rangle \cong (\mathbf{Z}/2\mathbf{Z})^2\,.$$

Pour les sous-groupes d'ordre 2, on en a autant que de doubles transpositions et pour ceux d'ordre 3, moitié moins que de 3-cycles. Il s'ensuit le treillis suivant :

13. Cela est par exemple utile quand on étudie la théorie de Galois mais quand on classifie les revêtements galoisiens!
14. On pouvait le déduire sans calcul des théorèmes de Sylow, puisque ces sous-groupes d'ordre 2 sont les 2-Sylow de $\mathfrak{S}_3$.
15. Voir exercice 1.
16. Idem voir exercice 1.

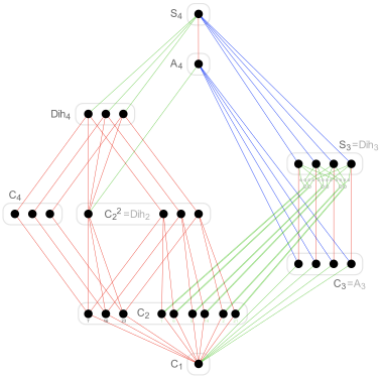


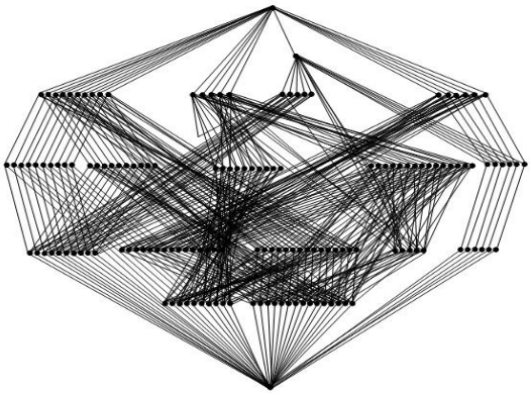
Le groupe trivial est toujours distingué, les sous-groupes d'ordre 2 sont d'indice 2 dans le groupe de Klein donc distingué dans celui-ci. Par ailleurs [17], les sous-groupes d'ordre 3 sont tous conjugués et donc non distingués et de même pour les sous-groupes d'ordre 2. On peut le voir à la main [18] du fait que

$$(ab)(cd)(abc)(ab)(cd) = (adb) \quad \text{et} \quad (abc)(ab)(cd)(acb) = (ad)(bc) \quad \text{si} \quad \{a,b,c,d\} = \{1,2,3,4\}$$

Reste à traiter le cas du groupe de Klein qui est distingué dans $\mathfrak{A}_4$. Cela découle de la question suivante ou des théorèmes de Sylow mais peut se voir aussi à la main grâce aux calculs précédents. En particulier, on a montré que $\mathfrak{A}_4$ est engendré par une double transposition et un 3-cycle et on retrouve le fait qu'être distingué n'est pas une relation transitive car $\langle(12)(34)\rangle \lhd \langle(12)(34),(13)(24)\rangle \lhd \mathfrak{A}_4$ mais $\langle(12)(34)\rangle \not\lhd \mathfrak{A}_4$.

On peut continuer avec $\mathfrak{S}_4$ ou $\mathfrak{S}_5$ mais la situation devient vite plus pénible avec les treillis respectifs suivants :





Supposons à présent que $K \lhd H$ et que $H \lhd G$. A-t-on $K \lhd G$? Démontrer que si K est caractéristique dans H et que H est caractéristique dans G et montrons qu'alors K est caractéristique dans G. Pour ce faire, soit $\varphi \in \mathtt{Aut}(G)$. Il s'agit d'établir que $\varphi(K) \subseteq K$. Puisque H est caractéristique dans G, $\varphi(H) \subseteq H$ et donc $\varphi_{|_H}$ est un morphisme de groupes de H dans H qui est bijectif. En effet, $\varphi^{-1} \in \mathtt{Aut}(G)$ et donc $\varphi^{-1}(H) \subseteq H$ soit $H \subseteq \varphi(H)$ car φ est surjective. Par ailleurs, $\mathrm{Ker}(\varphi_{|_H}) = \mathrm{Ker}(\varphi) \cap H = \{e\}$ car φ est injective. On a donc un élément de $\mathtt{Aut}(H)$ et comme $K \subseteq H$, $\varphi(K) = \varphi_{|_H}(K) \subseteq K$ car K est caractéristique dans H, ce qu'il fallait démontrer !

3. Le résultat découle du fait que la classe de conjugaison d'un élément de $\mathfrak{S}_n$ est entièrement déterminée par la forme de sa décomposition en produit de cycles à supports disjoints. Soit $c = (a_1, \ldots, a_k)$ un k-cycle de $\mathfrak{S}_n$. Alors pour tout $\sigma \in \mathfrak{S}_n$, on a

$$\sigma c \sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k)).$$

Toute permutation se décompose alors de façon unique en produit de cycles à support disjoints et on voit que tout conjugué d'une décomposition donnée possède une décomposition de la même forme et réciproquement il n'est pas difficile pour deux permutations

17. On peut là encore le voir grâce aux théorèmes de Sylow avec les 3-Sylows de $\mathfrak{A}_4$.
18. Plus généralement, c'est aussi une conséquence de la question suivante.

σ_1, σ_2 ayant le même type de décomposition en produit de cycles à supports disjoints de construire $\mu \in \mathfrak{S}_n$ tel que $\sigma_1 = \mu\sigma_2\mu^{-1}$. La classe de conjugaison correspondant à une partition donnée est l'ensemble des permutations dont la décomposition en cycles à support disjoint fait intervenir des cycles de longueurs $\lambda_1, \lambda_2, \ldots, \lambda_r$. Par exemple, dans $\mathfrak{S}_4$, la classe de conjugaison des doubles transpositions correspond à la partition $2+2=4$ et un 3-cycles à $3+1=4$.

► **Compléments . –** Pour $\mathfrak{A}_n$, c'est un peu plus subtil. Comme $\mathfrak{A}_n \lhd \mathfrak{S}_n$, la classe de conjugaison d'un élément de $\mathfrak{A}_n$ dans $\mathfrak{S}_n$ est contenue dans $\mathfrak{A}_n$. Par ailleurs, comme $[\mathfrak{S}_n : \mathfrak{A}_n] = 2$, on a que la classe de conjugaison d'un élément de $\mathfrak{A}_n$ est soit égale à la classe de conjugaison de cet élément dans $\mathfrak{S}_n$ soit la moitié de la classe de conjugaison de cet élément dans $\mathfrak{S}_n$ (dit autrement la classe de conjugaison d'un élément $\sigma \in \mathfrak{A}_n$ dans $\mathfrak{S}_n$ est soit égale à la classe de conjugaison de cet élément dans $\mathfrak{A}_n$ soit la réunion de deux classes de conjugaison de même cardinal dans $\mathfrak{A}_n$). En effet, on sait que la classe de conjugaison d'un élément est l'orbite par l'action de conjugaison et il est facile de voir que pour $\sigma \in \mathfrak{A}_n$

$$\#\mathsf{Cl}_{\mathfrak{S}_n}(\sigma) = \frac{n!}{\#Z_{\mathfrak{S}_n}(\sigma)} \quad \text{et} \quad \#\mathsf{Cl}_{\mathfrak{A}_n}(\sigma) = \frac{n!}{2\#Z_{\mathfrak{A}_n}(\sigma)}$$

avec

$$Z_{\mathfrak{S}_n}(\sigma) = \left\{\mu \in \mathfrak{S}_n \ : \ \mu\sigma\mu^{-1} = \sigma\right\} \quad \text{et} \quad Z_{\mathfrak{A}_n}(\sigma) = \left\{\mu \in \mathfrak{A}_n \ : \ \mu\sigma\mu^{-1} = \sigma\right\}.$$

Soit $Z_{\mathfrak{S}_n}(\sigma) = Z_{\mathfrak{A}_n}(\sigma)$ soit $Z_{\mathfrak{A}_n}(\sigma) \subsetneq Z_{\mathfrak{S}_n}(\sigma)$ strictement et il existe $\mu_0 \in \mathfrak{S}_n \setminus \mathfrak{A}_n$ tel que $\mu\sigma\mu^{-1} = \sigma$. Alors, le groupe alterné étant d'indice 2, $\mathfrak{S}_n = \mathfrak{A}_n \sqcup \mathfrak{A}_n\mu_0$ si bien que

$$\begin{array}{ccc} \left\{\mu \in \mathfrak{S}_n \setminus \mathfrak{A}_n \ : \ \mu\sigma\mu^{-1} = \sigma\right\} & \longrightarrow & Z_{\mathfrak{A}_n}(\sigma) \\ \mu & \longmapsto & \mu\mu_0 \end{array}$$

est une bijection qui montre que $Z_{\mathfrak{S}_n}(\sigma) = Z_{\mathfrak{A}_n}(\sigma) \sqcup \left\{\mu \in \mathfrak{S}_n \setminus \mathfrak{A}_n \ : \ \mu\sigma\mu^{-1} = \sigma\right\}$ avec

$$\#Z_{\mathfrak{A}_n}(\sigma) = \#\left\{\mu \in \mathfrak{S}_n \setminus \mathfrak{A}_n \ : \ \mu\sigma\mu^{-1} = \sigma\right\}.$$

Reste à déterminer quand une classe dans $\mathfrak{S}_n$ reste entière et quand elle se scinde en deux. Montrons qu'elle se scinde en deux si, et seulement si, la décomposition de σ ne comporte que des cycles de longueur impaire 2 à 2 distinctes. Si tel est le cas, σ commute avec le sous-groupe engendré par les cycles apparaissant dans sa décomposition en produit de cycles à supports disjoints. En effet, si τ commute à σ, comme la conjugaison préserve le type de décomposition en produit de cycles à supports disjoints et que tous les cycles apparaissant dans celle de σ sont de longueur différente, cela implique que τ commute à chacun de ces cycles individuellement. Fixons à présent la décomposition en cycle de $\sigma = c_1c_2\cdots c_r$. On utilise alors que si c est un cycle de longueur ℓ, alors le centralisateur de c est donné par

$$\left\{c^i\mu \ : \ i \in \{0, \ldots, \ell-1\},\ \mu \in \mathfrak{S}_{n-\ell}\right\}$$

avec $\mathfrak{S}_{n-\ell}$ le sous-groupe de $\mathfrak{S}_n$ fixant tous les éléments du support de c. Il est clair que toutes les permutations de cette forme commutent à c et on conclut par un argument de cardinalité, puisque le cardinal de ce centralisateur est simplement le $n!$ divisé par le cardinal de la classe de conjugaison de c, à savoir le nombre de ℓ-cycles, soit $\frac{n(n-1)\cdots(n-\ell+1)}{\ell}$ On obtient ainsi bien que les deux ensembles ont même cardinal $\ell \times (n-\ell)!$. On en déduit donc puisque τ commute à c_1 que $\tau = c_1^i\tau_1$ avec τ_1 de support disjoint à celui de c_1. On obtient que τ_1 commute à σ et donc τ_1 commute à c_2 et donc $\tau_1 = c_2^j\tau_2$ et de proche en proche τ appartient au sous-groupe engendré par $c_1, \ldots, c_r$. Il en résulte, puisque tous les cycles de σ sont de longueur impaire que τ est de signature $+1$ et $Z_{\mathfrak{S}_n}(\sigma) = Z_{\mathfrak{A}_n}(\sigma)$. On pouvait aussi calculer le cardinal de $Z_{\mathfrak{S}_n}(\sigma)$ (voir la note de bas de page 19) et constater qu'il est impair de sorte que tout élément de $Z_{\mathfrak{S}_n}(\sigma)$ est d'ordre impair. Or, tout élément de $\mathfrak{S}_n \setminus \mathfrak{A}_n$ étant d'ordre pair, on a le résultat ! Réciproquement, si on a un cycle de longueur paire c, on voit alors que

$$\forall \mu \in \mathfrak{S}_n, \quad \mu\sigma\mu^{-1} = (\mu c)\sigma(\mu c)^{-1}$$

et donc $Z_{\mathfrak{S}_n}(\sigma) \subsetneq Z_{\mathfrak{A}_n}(\sigma)$ strictement. Alternativement, si σ comporte deux cycles $c = (a_1, \ldots, a_k)$ et $c' = (a'_1, \ldots, a'_k)$ de même longueur impaire, alors, notant $d = (a_1\ a'_1)\cdots(a_k\ a'_k)$ (de signature -1), on a

$$\forall \mu \in \mathfrak{S}_n, \quad \mu\sigma\mu^{-1} = (\mu d)\sigma(\mu d)^{-1}$$

et donc à nouveau $Z_{\mathfrak{S}_n}(\sigma) \subsetneq Z_{\mathfrak{A}_n}(\sigma)$ strictement.

4. Dans le cas $n = 1$ ou $n = 2$, $\mathfrak{S}_n$ est abélien donc $Z(\mathfrak{S}_n) = \mathfrak{S}_n$. Supposons à présent que $n \geqslant 3$. Soit $\sigma \neq \mathrm{id}$. On peut alors choisir $a \neq b$ tels que $\sigma(a) = b$. Puisque $n \geqslant 3$, il existe $c \in \{1, \ldots, n\} \setminus \{a, b\}$. On considère alors $\tau = (a\ c)$ et on constate que $\sigma\tau\sigma^{-1} = (\sigma(a)\ \sigma(c)) = (b\ \sigma(c))$. On constate alors que c est dans le support de $\sigma\tau\sigma^{-1}$ mais pas dans celui de τ par définition ! Il s'ensuit que $\sigma\tau\sigma^{-1} \neq \tau$ et σ ne commute pas avec τ et n'est donc pas dans $Z(\mathfrak{S}_n)$. On en conclut que, lorsque $n \geqslant 3$, $Z(\mathfrak{S}_n) = \{\mathrm{Id}\}$.

Exercice 5 — Groupe diédral. On considère les deux transformations suivantes du plan euclidien : la rotation ρ de centre O et d'angle $\frac{\pi}{2}$, et la symétrie orthogonale σ par rapport à l'axe des abscisses. Le groupe *diédral* $\mathbf{D}_4$ est le sous-groupe des isométries du plan engendré par ρ et σ.

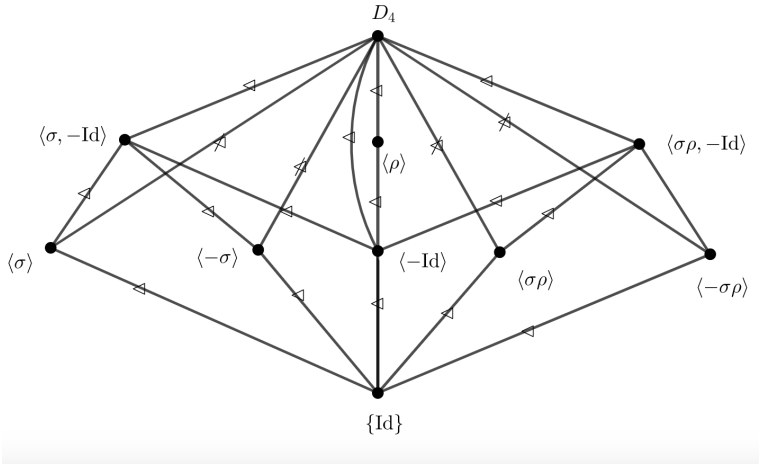
1. Calculer l'ordre de σ et de ρ. Décrire l'isométrie $\sigma\rho\sigma^{-1}$.
2. Montrer que $\mathbf{D}_4$ contient 8 éléments; caractériser ces éléments géométriquement.
3. Déterminer les classes de conjugaison dans $\mathbf{D}_4$.
4. Donner le treillis des sous-groupes de $\mathbf{D}_4$, en précisant les sous-groupes distingués.
5. Pour un entier $n > 0$, le groupe diédral $\mathbf{D}_n$ est le sous-groupe des isométries du plan engendré par σ et par la rotation ρ' de centre O et d'angle $\frac{2\pi}{n}$. Montrer que $\mathbf{D}_n$ contient $2n$ éléments et correspond au groupe des isométries du plan préservant le polygone régulier du plan à n côtés de sommet les racines n-ièmes de l'unité.

Solution.

1. On vérifie aisément[19] que $\sigma^2 = \mathrm{Id}$ et donc σ est d'ordre 2 tandis que $\rho^4 = \mathrm{Id}$ donc ρ est d'ordre 2 ou 4 mais ρ^2 est la rotation d'angle π donc ρ est d'ordre 4.
   On se convainc aisément sur un dessin que $\sigma\rho\sigma^{-1} = \sigma\rho\sigma$ est la rotation d'angle $-\frac{\pi}{2}$, à savoir ρ^{-1}. On peut le démontrer en utilisant le fait que les matrices de σ et ρ sont respectivement
   $$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$
   de sorte que la matrice de $\sigma\rho\sigma$ est bien donnée par
   $$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$
   qui est bien la matrice de la rotation de centre l'origine et d'angle $-\frac{\pi}{2}$. Plus simplement, on peut voir que $\sigma\rho\sigma$ est un automorphisme orthogonal de déterminant 1 donc une rotation et on détermine son angle en calculant l'image de $e_1 = (1, 0)$.
2. Il est facile de voir que $\mathbf{D}_4$ contient au moins 8 éléments distincts[20] : Id, la symétrie σ, les rotations ρ, ρ^2 et ρ^3 d'angle $\frac{\pi}{2}, \pi$ et $\frac{3\pi}{2}$ ainsi que $\sigma\rho$, $\sigma\rho^2$ et $\sigma\rho^3$ qui sont respectivement des symétries orthogonales par rapport à la droite d'angle respectivement $\frac{\pi}{4}$, l'axe des ordonnées et $\frac{3\pi}{4}$. On voit alors qu'on a ainsi tous les éléments de $\mathbf{D}_4$ grâce à la relation $\sigma\rho\sigma = \rho^{-1}$. En effet, par définition d'un groupe engendré par deux élément, tout élément de D_4 est de la forme $\sigma^k\rho^{r_1}\sigma\rho^{r_2}\sigma\cdots\rho^{r_s}\sigma^\ell$ avec $k, \ell \in \{0, 1\}$ et $r_1, \ldots, r_s \in \{1, \ldots, 3\}$ et la relation $\sigma\rho\sigma = \rho^{-1}$ permet de voir qu'un tel élément est de la forme $\sigma^s\rho^r$ avec $s \in \{0, 1\}$ et $r \in \{0, 1, 2, 3\}$ car σ est d'ordre 2 et ρ d'ordre 4. En dehors de l'identité, on a donc deux éléments d'ordre 4 ($\pm\rho$) et 5 éléments d'ordre 2.
3. Il est clair que la classe de conjugaison de l'identité est réduite à $\{\mathrm{Id}\}$ tout comme celle de $\rho^2 = -\mathrm{Id}$ est donnée par $\{-\mathrm{Id}\}$. La relation $\sigma\rho\sigma^{-1}$ montre que la classe de conjugaison de ρ est donnée par $\{\rho, \rho^3\} = \{\rho, -\rho\}$ (le conjugué d'une rotation est une rotation). Enfin, la relation $\sigma\rho\sigma = \rho^3$ fournit que $\rho\sigma\rho^{-1} = -\sigma$ qui implique facilement que la classe de conjugaison de σ est $\{\sigma, \sigma\rho^2 = -\sigma\}$ et enfin la classe de conjugaison de $\sigma\rho$ est $\{\sigma\rho, \sigma\rho^3\} = \{\sigma\rho, -\sigma\rho\}$.
4. Les sous-groupes potentiels sont d'ordre 1, 2, 4 ou 8. les sous-groups d'ordre 1 et 8 sont immédiats. Pour les sous-groupes d'ordre 2, ils sont cycliques engendrés par un élément d'ordre 2, on en a donc cinq engendrés respectivement par σ, $-\sigma$, $-\mathrm{Id}$ (qui est le centre de $\mathbf{D}_4$ car le centre est la réunion des éléments dont la classe de conjugaison est réduite à un singleton), $\sigma\rho$ et $-\sigma\rho$. Pour les sous-groupes d'ordre 4, on sait qu'un tel sous-groupe est soit cyclique engendré par un élément d'ordre 4 soit par deux éléments d'ordre 2 qui commutent. Dans le premier cas, on obtient ici le sous-groupe engendré par ρ et dans le second on obtient deux sous-groupes (car on n'a pas d'autres éléments d'ordre 2 qui commutent) $\{\mathrm{Id}, -\mathrm{Id}, \sigma, -\sigma\}$ et $\{\mathrm{Id}, -\mathrm{Id}, \sigma\rho, -\sigma\rho = \sigma\rho^3\}$ isomorphes à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. On obtient le treillis suivant

19. Soit géométriquement soit via les matrices.

20. On rappelle que les isométries du plan forment un groupe pour la loi de composition des applications et qu'une isométrie du plan est soit une rotation d'angle θ si elle est de déterminant 1, auquel cas sa matrice dans la base canonique est donnée par
$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}.$$
tandis qu'une isométrie indirecte de déterminant -1 est une symétrie orthogonale par rapport à une droite. On rappelle que la matrice de la symétrie orthogonale par rapport à la droite d'angle $\frac{\theta}{2}$ par rapport à l'axe des abscisses est donné dans la base canonique par
$$\begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}$$
Cela se vérifie notamment facilement en passant aux nombres complexes.



Tous les sous-groupes d'indice 2 sont distingués. Il reste donc le cas des sous-groupes d'ordre 2. Les relations ci-dessus montrent qu'aucun n'est distingué sauf celui engendré par $\{-\mathrm{Id}\}$ qui est en fait le centre et le groupe dérivée de $\mathbf{D}_4$ et est même caractéristique (de même que $\langle\rho\rangle$).

5. Finalement terminons par la caractérisation géométrique du groupe $\mathbf{D}_n$. Il est clair que $\mathbf{D}_n$ est contenu dans le groupe des isométries de P_n. Montrons alors que le cardinal de ce groupe d'isométries est $2n$ pour conclure. Puisqu'une isométrie préserve les distances, on constate immédiatement que l'image par une isométrie qui préserve P_n d'un sommet est un autre sommet (en considérant la distance d'un point de P_n à l'origine, qui est maximale uniquement pour les sommets). On en déduit que l'image du sommet A ne peut être qu'un autre sommet, ce qui laisse n choix. Mais alors l'image d'un sommet adjacent de A, disons B, toujours pour des raisons de conservation de la distance doit être adjacent à l'image de B, ce qui laisse 2 possibilités. On constate qu'on a donc au plus $2n$ choix, l'image de l'arête AB déterminant complètement l'isométrie. Comme on a en a déjà $2n$, on les a bien toutes!

► **Compléments . –** Pour un entier $n > 0$, le groupe diédral $\mathbf{D}_n$ est le sous-groupe des isométries du plan engendré par σ et par la rotation ρ de centre O et d'angle $\frac{2\pi}{n}$. On montre alors que $\mathbf{D}_n$ contient $2n$ éléments et correspond au groupe des isométries du plan préservant le polygone régulier P_n du plan à n côtés de sommet les racines n-ièmes de l'unité. Tout ce qu'on a fait se généralise en effet parfaitement au cas général. On constate de même que $\sigma\rho\sigma = \rho^{-1}$ et cette relation entraîne que tout élément de $\mathbf{D}_n$ est de la forme $\sigma^\ell\rho^k$ pour $\ell, k \in \mathbf{N}$. Comme σ est d'ordre 2 et ρ d'ordre n, on obtient que $\mathbf{D}_n$ est d'ordre $2n$ et que

$$D_n = \{\mathrm{Id}, \rho, \dots, \rho^{n-1}, \sigma, \sigma\rho, \dots, \sigma\rho^{n-1}\}.$$

On peut montrer que

$$Z(\mathbf{D}_n) = \begin{cases} \mathbf{D}_n \text{ si } n \in \{1,2\} \\ \{\mathrm{Id}\} \text{ si } n \text{ impair et } n \geqslant 3 \\ \{\mathrm{Id}, \rho^{\frac{n}{2}} = -\mathrm{Id}\} \text{ sinon} \end{cases} \quad \text{et} \quad D(\mathbf{D}_n) = \begin{cases} \{\mathrm{Id}\} \text{ si } n \in \{1,2\} \\ \langle\rho\rangle \text{ si } n \text{ impair et } n \geqslant 3 \\ \langle\rho^2\rangle \text{ sinon.} \end{cases}$$

Dans le cas pair, $\mathbf{D}_n/Z(\mathbf{D}_n) \cong \mathbf{D}_{n/2}$ et $\mathbf{D}_n^{\mathrm{ab}} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ si n est pair et $\cong \mathbf{Z}/2\mathbf{Z}$ si n est impair. On verra que $\mathbf{D}_n = \langle\rho\rangle \rtimes \langle\sigma\rangle \cong \mathbf{Z}/n\mathbf{Z} \rtimes_\varphi \mathbf{Z}/2\mathbf{Z}$ avec $\varphi(1)$ donné par $\overline{m} \mapsto -\overline{m}$. On a $\mathbf{D}_2 \cong \mathbf{Z}/2\mathbf{Z}$ et $\mathbf{D}_3 \cong \mathfrak{S}_3$. Le groupe $\mathbf{D}_n$ est résoluble et nilpotent si, et seulement si, son ordre est une puissance de 2. Les classes de conjugaison sont $\{\mathrm{Id}\}$, $\{-\mathrm{Id}\}$, $\{\rho^k, \rho^{-k}\}$ pour $k \in \{1, \dots, \frac{n}{2} - 1\}$, $\{\sigma, \sigma\rho^2, \dots, \sigma\rho^{n-2}\}$ et $\{\sigma\rho, \sigma\rho^3, \dots, \sigma\rho^{n-1}\}$ si n est pair tandis que si n est impair, on obtient $\{\mathrm{Id}\}$, $\{\rho^k, \rho^{-k}\}$ pour $k \in \{1, \dots, \frac{n-1}{2}\}$ et $\{\sigma, \sigma\rho, \dots, \sigma\rho^{n-1}\}$. Enfin, pour tous diviseurs positifs d et d' de n et $k \in \{0, 1, \dots, \frac{n}{d'} - 1\}$, on pose

$$H_h = \langle\rho^{\frac{n}{d}}\rangle \cong \mathbf{Z}/d\mathbf{Z} \quad \text{et} \quad H_{d',k} = \langle\rho^{\frac{n}{d'}}, \sigma\rho^k\rangle \cong \mathbf{D}_{d'}.$$

Alors tout sous-groupe de $\mathbf{D}_n$ est égal à un sous-groupe H_d pour un unique diviseur d de n ou à un sous-groupe $H_{d',k}$ pour un unique diviseur d' et un unique k. Lorsque n est pair, les sous-groupes distingués sont les H_d pour $d \mid n$ et $\mathbf{D}_n$ et si n est impair les H_d pour $d \mid n$ et $\mathbf{D}_n$ ainsi que $H_{\frac{n}{2},0}$ et $H_{\frac{n}{2},1}$. Il s'agit d'un exemple de groupe donné par générateurs et relations. Ces groupes seront très important dans le cours de Géométrie au second semestre.

Exercice 6 — Groupes de type fini. Soit G un groupe admettant une partie génératrice finie. Montrer que G est fini ou dénombrable. Est-il vrai réciproquement que tout groupe dénombrable admet une partie génératrice finie ?

Solution. Soit S une partie génératrice de G. Notons T l'ensemble des éléments de G qui sont dans S ou dont l'inverse est dans S. Pour tout $r \in \mathbf{N}$, notons G_r l'ensemble des éléments g de G de la forme

$$g = x_1 x_2 \cdots x_r,$$

avec $x_i \in T$ pour tout i (avec la convention habituelle que le produit vide est le neutre de G). Alors, le fait que S engendre G dit que G est la réunion des G_r pour $r \in \mathbf{N}$. Chaque G_r est fini (car T est fini, et le cardinal de G_r est au plus celui de T^r), donc G est (au plus) dénombrable comme union dénombrable d'ensembles finis.

La réciproque est fausse, même pour les groupes abéliens. Par exemple, $(\mathbf{Q}, +)$ n'est pas engendré par une partie finie (par l'absurde si on a une partie génératrice finie $p_1/q_1, \dots, p_n/q_n$, alors tout élément de $\mathbf{Q}$ aurait un dénominateur sous forme réduite qui divise $q_1 \cdots q_n$ mais ce n'est pas le cas de $1/(1 + q_1 \cdots q_n)$ par exemple). De même pour $\mathbf{Z}^{(\mathbf{N})}$ (qui admet une famile libre infinie).

► **Remarque . –** Noter que la forme d'un élément de G, par définition du fait que S engendre G donne immédiatement une application f surjective[21] de $E = \left\{(x_1, \dots, x_r) \in S \cup S^{-1} \ : \ r \in \mathbf{N}\right\}$ (qui est dénombrable par des arguments similaires). L'axiome du choix garantit alors l'existence d'une section $s : G \to E$ telle que $f \circ s = \mathrm{Id}_G$. Ainsi, s est injective et arrive dans un ensemble dénombrable donc G est dénombrable.

Exercice 7 — Quaternions et groupes d'ordre 8. On note H l'ensemble des matrices de $\mathcal{M}_2(\mathbf{C})$ de la forme

$$M_{a,b} := \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}.$$

On pose $H^* = H - \{0\}$.

1. Montrer que H^* est un sous-groupe non commutatif de $\mathrm{GL}_2(\mathbf{C})$.
2. On note $\mathbf{1}$ la matrice identité, et on pose $I := M_{i,0}$, $J = M_{0,1}$, $K = M_{0,i}$. Soit $\mathbf{H}_8 = \{\pm\mathbf{1}, \pm I, \pm J, \pm K\}$. Montrer que $\mathbf{H}_8$ est un sous-groupe non commutatif de cardinal 8 de H^*.
   Indication : On observera que $IJ = K = -JI$, avec des relations analogues par permutations circulaires de I, J, K.
3. Montrer que le centre et le sous-groupe dérivé de $\mathbf{H}_8$ sont tous deux égaux à $\{\pm 1\}$.
4. Montrer que l'abélianisé de $\mathbf{H}_8$ est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$.
5. Est-ce qu'un groupe dont tous les sous-groupes sont distingués est nécessairement abélien ?

Solution.

1. On a que $\det(M_{a,b}) = |a|^2 + |b|^2 \neq 0$ dès que $M_{a,b} \neq \mathbf{0}$ (ce qui est équivalent à $(a, b) \neq (0, 0)$) donc $H \subseteq \mathrm{GL}_2(\mathbf{C})$ et contient l'identité. On calcule également le produit $M_{a,b}M_{c,d} = M_{ac-b\bar{d},ad+b\bar{c}}$ ce qui permet de conclure à la stabilité par produit et enfin $M_{a,b}^{-1} = M_{\frac{\bar{a}}{|a|^2+|b|^2},-\frac{b}{|a|^2+|b|^2}}$ ce qui permet de montrer la stabilité par passage à l'inverse. Il n'est pas commutatif car $M_{i,0}M_{0,1} \neq M_{0,1}M_{i,0}$.
2. On vérifie par le calcul que $I^2 = J^2 = K^2 = IJK = -1$ et que $IJ = -JI = K$, $KI = -IK = J$ et $JK = -KJ = I$ de sorte qu'on obtient bien un groupe de cardinal 8 de table

	1	I	J	K	-1	-I	-J	-K
1	1	I	J	K	-1	-I	-J	-K
I	I	-1	K	-J	-I	1	-K	J
J	J	-K	-1	I	-J	K	1	-I
K	K	J	-I	-1	-K	-J	I	1
-1	-1	-I	-J	-K	1	I	J	K
-I	-I	1	-K	J	I	-1	K	-J
-J	-J	K	1	-I	J	-K	-1	I
-K	-K	-J	I	1	K	J	-I	-1

   à 5 classes de conjugaisons $\{1\}, \{-1\}, \{\pm I\}, \{\pm J\}$ et $\{\pm K\}$. Il est non commutatif par exemple car $IJ \neq JI$.
3. On voit immédiatement que $Z(\mathbf{H}_8) = \{\pm\mathrm{Id}\}$. Puis on voit que tous les commutateurs sont triviaux sauf $[I, J] = [I, K] = [J, K] = -\mathrm{Id}$ si bien que $D(\mathbf{H}_8) = \langle -\mathrm{Id}\rangle = \{\pm\mathrm{Id}\}$.
4. Notons $H = D(\mathbf{H}_8)$. L'abélianisé $\mathbf{H}_8/H$ est donc d'ordre 4 et on voit que les classes ne sont autres que $H = \{\pm 1\}$, $IH = \{\pm I\}$, $JH = \{\pm J\}$ et $KH = \{\pm K\}$ dont on voit[22] qu'on a $IH^2 = JH^2 = KH^2 = H$. On a donc nécessairement que $\mathbf{H}_8^{\mathrm{ab}} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
   Une autre méthode consiste à exploiter le fait que $H = D(\mathbf{H}_8) = Z(\mathbf{H}_8)$. Ainsi, si $\mathbf{H}_8/H \cong \mathbf{Z}/4\mathbf{Z}$, alors $\mathbf{H}_8/Z(\mathbf{H}_8)$ serait cyclique et d'après le cours, cela entraînerait que $\mathbf{H}_8$ est abélien, ce qui n'est pas le cas ! On a donc nécessairement que $\mathbf{H}_8^{\mathrm{ab}} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

   ► **Compléments. –** Noter que les quaternions fournissent un exemple[23] de groupe G tel que $G/Z(G)$ abélien mais non cyclique et que G est non commutatif ! L'hypothèse de cyclicité ne peut donc pas être affaiblie dans le résultat de votre cours !

21. Qui à un élément de $\left\{(x_1, \dots, x_r) \in S \cup S^{-1} \ : \ r \in \mathbf{N}\right\}$ associe $x_1x_2 \cdots x_r$.
22. Par exemple car $(IH)^2 = IHIH$ et, puisque H est distingué dans $\mathbf{H}_8$, $HI = IH$ et $(IH)^2 = I^2H = -H = H$. On rappelle alors que H est l'élément neutre du groupe quotient $\mathbf{H}_8/H$.
23. Et oui, encore !

5. On voit facilement que les sous-groupes de $\mathbf{H}_8$ sont $\{1\}$, $\mathbf{H}_8$, $\{\pm 1\}$ (d'ordre 2) et $\langle I\rangle = \{\pm 1, \pm I\}$, $\langle J\rangle$ et $\langle K\rangle$ (tous trois cycliques d'ordre 4). Les sous-groupes triviaux sont naturellement distingués tout comme ceux d'ordre 4 (car d'indice 2) et le sous-groupe d'ordre 2 étant égal au centre (ou au sous-groupe dérivé) l'est aussi. Ainsi, on a un exemple de groupe non commutatif dont tous les sous-groupes propres sont distingués et cycliques.

▶ **Compléments. –** Si $\mathbf{H}_8 = N \rtimes H$, alors nécessairement N ou H est d'ordre 2, donc égal à $\{\pm 1\}$. Si c'est H, alors H serait distingué et donc le produit serait direct. Cela impliquerait que H_8 est abélien. On peut donc supposer que $N = \{\pm 1\}$. Mais dans ce cas, $\mathrm{Aut}(N)$ est réduit à un élément et tout morphisme $H \to \mathrm{Aut}(N)$ est trivial et on conclurait de la même manière que le produit semi-direct serait direct et $\mathbf{H}_8$ abélien. Ainsi $\mathbf{H}_8$ n'est pas un produit semi-direct non trivial.
Soit maintenant un groupe G d'ordre 8. Si G a un élément d'ordre 8, alors $G \cong \mathbf{Z}/8\mathbf{Z}$. Si G est d'exposant 2, alors $G \cong (\cong \mathbf{Z}/2\mathbf{Z})^3$. Si maintenant G est d'exposant 4 abélien, on a que $G \cong \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Reste alors à traiter le cas d'exposant 4 non abélien. On a ainsi un élément $r \in G$ d'ordre 4 et on pose $R = \langle r\rangle \cong \mathbf{Z}/4\mathbf{Z}$. Soit alors $s \in G \setminus R$ d'ordre minimal. Si s est d'ordre 2, alors on pose $S = \langle s\rangle$ et $S \cap R = \{e\}$ et G est engendré par R et S et $R \lhd G$ car d'indice 2. On sait alors que $G \cong R \rtimes S \cong \mathbf{Z}/4\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z} \cong D_4$ (on a un seul tel produit semi-direct non abélien à isomorphisme près). Enfin, si s est d'ordre 4 (et que tout élément de $G \setminus R$ est d'ordre 4), renommons r et s par I et J et notons $K = IJ$. On sait que I^2 est d'ordre 2 et c'est le seul élément d'ordre 2 de G. On peut le renommer $I^2 = -1$. De même, on obtient $J^2 = -1$. Mais $K \notin R$ car $J \notin R$ donc K est d'ordre 4 et $K^2 = -1$ est d'ordre 2. On a alors que $Z(G) = \{\pm 1\}$. On sait en effet que $Z(G)$ est un sous-groupe de G de cardinal 2 ou 4 (car G est supposé non abélien et est un 2-groupe). Si le cardinal de $Z(G)$ était 4, alors il s'agit d'un sous-groupe distingué d'indice 2 et on aurait $G/Z(G) \cong \mathbf{Z}/2\mathbf{Z}$ cyclique si bien que G serait abélien, ce qui est absurde. On a donc que $Z(G)$ est d'ordre 2, nécessairement engendré par un élément d'ordre 2 et comme -1 est le seul élément de G d'ordre 2, on a le résultat. On a donc 8 éléments distincts de G, à savoir ± 1, $\pm I$, $\pm J$ et $\pm K$ et donc $G = \{\pm 1, \pm I, \pm J, \pm K\}$ avec $I^2 = J^2 = K^2 = -1$ et $K = IJ$. On a par ailleurs que $IJ, IK, JK \notin Z(G)$ et comme $JI \notin R$ car $J \notin R$ et $I \in R$, on a $JI \in \{J, K, -J, -K\}$ car $R = \{\pm 1, \pm I\}$. On a alors clairement $JI \neq \pm J$ et $JI \neq IJ$ sinon I et J commuteraient et donc I commuterait à K et ainsi $I \in Z(G)$. D'où $JI = -IJ = -K$ et de même on montre que $KI = -IK = J$ et $JK = -KJ = I$ et on retrouve la table de multiplication des quaternions donc $G \cong \mathbf{H}_8$.

Exercice 8. On considère le groupe $G = \mathfrak{A}_4$. Soit $D(G)$ son sous-groupe dérivé. Soit V_4 le sous-groupe de G constitué de l'identité et des doubles transpositions.

1. Montrer que $V_4 \lhd G$, puis que $D(G) \subseteq V_4$. *Indication : On observera que G/V_4 est de cardinal 3.*

2. Montrer que $D(G) \neq \{1\}$ et que G ne possède pas de sous-groupe distingué de cardinal 2. En déduire que $D(G) = V_4$.

3. Montrer que si H est un sous-groupe d'indice 2 d'un groupe fini A, alors $H \lhd A$.
Indication : Regarder les classes à gauche et à droite suivant G.

4. Soit H un sous-groupe de $G = \mathfrak{A}_4$. Montrer que si H est d'indice 2, alors $D(G) \subseteq H$ et aboutir à une contradiction.
Indication : On considérera G/H.
Ainsi G (qui est de cardinal 12) n'a pas de sous-groupe de cardinal 6.

5. Montrer au contraire que pour tout $d \in \mathbf{N}^*$ tel que d divise 24, le groupe $\mathfrak{S}_4$ possède un sous-groupe de cardinal d.

Solution.

1. Si l'on conjugue la double transposition $(a, b)(c, d)$ par une permutation σ, on obtient $(\sigma(a), \sigma(b))(\sigma(c), \sigma(d))$, ce qui montre que V_4 est distingué dans $\mathfrak{S}_4$, et donc a fortiori dans $\mathfrak{A}_4$. Ensuite, comme G/V_4 est de cardinal $12/4 = 3$, il est cyclique de cardinal 3 (car 3 est premier) et en particulier abélien, ce qui montre que $D(G) \subset V_4$.

2. On voit facilement que G n'est pas abélien, donc $D(G) \neq \{1\}$. D'autre part un sous-groupe H de G de cardinal 2 est composé de l'identité et d'une double transposition $\tau = (a, b)(c, d)$. Si l'on conjugue τ par $\sigma \in G$, on obtient $(\sigma(a), \sigma(b))(\sigma(c), \sigma(d))$, qui ne reste pas dans H si on choisit par exemple $\sigma \in G$ telle que $\sigma(a) = a$ et $\sigma(b) = c$, ce qui est toujours possible.
On a vu que $D(G) \subset V_4$, donc le cardinal de $D(G)$ divise 4, mais on a aussi vu que ce ne peut être ni 1 ni 2, donc c'est 4 et $D(G) = V_4$.

3. Soit $a \notin H$. Comme le cardinal de l'ensemble G/H des classes à gauche est 2, cet ensemble est composé de H et de la classe aH, qui est le complémentaire de H dans A. De même l'ensemble $H \setminus G$ des classes à droite est composé de H et de Ha, qui est aussi le complémentaire de H dans A. Ainsi $aH = Ha$, et ceci reste vrai quand $a \in H$. Finalement $aHa^{-1} = H$ pour tout $a \in A$, autrement dit $H \lhd A$.

4. D'après **4.**, on a $H \lhd G$. Alors, le groupe G/H est abélien puisque de cardinal 2, ce qui montre que $H \supset D(G)$. Mais d'après c), le groupe $D(G)$ est de cardinal 4 alors que H est de cardinal 6, ce qui contredit le théorème de Lagrange.

5. C'est clair pour $d = 1$ et $d = 24$. Pour $d = 2$, on prend le groupe engendré par une transposition, pour $d = 3$ celui engendré par un 3-cycle et pour $d = 4$ celui engendré par un 4-cycle. Pour $d = 6$, le sous-groupe des permutations laissant fixe 1 est isomorphe à $\mathfrak{S}_3$, il est donc de cardinal 6. Pour $d = 12$, on prend le sous-groupe $\mathfrak{A}_4$. Reste le cas $d = 8$, auquel cas on a un sous-groupe isomorphe au groupe diédral $\mathbf{D}_4$, par exemple celui engendré par un 4-cycle et une transposition.

Exercice 9 — Groupe des automorphismes.

1. Soient p un nombre premier et $n \in \mathbf{N}$. Établir que $\mathtt{Aut}\left((\mathbf{Z}/p\mathbf{Z})^n\right)$ est isomorphe à $\mathrm{GL}_n\left(\mathbf{Z}/p\mathbf{Z}\right)$. Pour quelles valeurs de n ce groupe est-il commutatif ?

2. On suppose que $n \geqslant 2$. Montrer que ce groupe contient un sous-groupe distingué mais non caractéristique.
3. On considère dans cette question le cas $p = n = 2$. Montrer que $\mathtt{Aut}\left(\left(\mathbf{Z}/2\mathbf{Z}\right)^2\right)$ est isomorphe à $\mathfrak{S}_3$.

Solution.

1. Voir le corrigé du partiel de l'an dernier, ici, exercice 2.
2. Voir le corrigé du partiel de l'an dernier, ici, exercice 2.
3. On sait que le cardinal de $\mathsf{GL}_n\left(\mathbf{Z}/p\mathbf{Z}\right)$ est[24] 6 et est non abélien. On sait alors qu'un tel groupe est isomorphe à $\mathfrak{S}_3$. On renvoie eu premier DM de M1 MF pour une autre approche !

Exercice 10 — Groupes d'exposant 2.

1. Soit G un groupe tel que $g^2 = 1$ pour tout $g \in G$. Montrer que G est abélien et donner des exemples de tels groupes finis et infinis.
2. Montrer que si G est fini, il existe un entier n tel que G est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^n$.

Solution.

1. Pour tous $g, h \in G$, on a $(gh)^2 = 1$ soit $ghgh = 1$ et en multipliant à droite par hg il vient $hg^2hgh = hg$ soit $h^2gh = hg$ soit $gh = hg$ et G est abélien. On verra en question suivante que les groupes finis d'exposant 2 sont tous de la forme $(\mathbf{Z}/2\mathbf{Z})^n$ pour un certain entier n. Un exemple de tel groupe infini est $\prod_{i\in I} \mathbf{Z}/2\mathbf{Z}$ avec I infini, par exemple $(\mathbf{Z}/2\mathbf{Z})^{\mathbb{N}}$ l'ensemble des suites à valeurs dans $\mathbf{Z}/2\mathbf{Z}$.
2. - *Méthode 1 :* Puisque G est fini, il admet une partie génératrice minimale[25], disons $\{g_1, \ldots, g_n\}$. On a alors par définition d'une partie génératrice et en utilisant le fait que G est abélien dont tout élément distinct du neutre est son propre inverse par la question précédente, que
$$G = \{g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n} \ : \ \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \in \{0, 1\}\}.$$
Cela donne envie de poser
$$f : \left\{ \begin{array}{ccc} (\mathbf{Z}/2\mathbf{Z})^n & \longrightarrow & G \\ (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) & \longmapsto & g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n}. \end{array} \right.$$
On a aisément qu'il s'agit d'un morphisme et par ce qui rpécède, il est surjectif. Reste à voir qu'il est injectif pour conclure ! Si ce n'est pas le cas, il existe un élément non trivial $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) \neq (0, 0, \ldots, 0)$ dans le noyau, autrement dit tel que
$$g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n} = 1.$$
Sans perte de généralités, on peut supposer que $\varepsilon_1 \neq 0$ et donc $\varepsilon_1 = 1$. On a donc
$$g_1 g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n} = 1 \quad \text{soit} \quad g_1 = g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n}$$
et $\{g_2, \ldots, g_n\}$ est une partie génératrice de G, contredisant la minimalité de $\{g_1, g_2, \ldots, g_n\}$. Cela démontre l'injectivité et donc f est un isomorphisme qui permet de conclure !
- *Méthode 2 :* On considère $(G, +)$ muni d'une loi additive[26] d'exposant 2, autrement dit tel que pour tout $g \in G$, $2g = 0$. On a alors que $\mathbf{Z}/2\mathbf{Z}$ est un corps et on vérifie que G est muni d'une structure de $\mathbf{Z}/2\mathbf{Z}$-espace vectoriel muni de la loi $+$ et de la loi externe suivante
$$\forall \overline{k} \in \mathbf{Z}/2\mathbf{Z}, \quad \forall g \in G, \quad \overline{k} \cdot g = kg$$
qui est bien définie car si $\overline{k} = \overline{k'}$, alors il existe un entier ℓ tel que $k' = k + 2\ell$ si bien que
$$k'g = kg + 2\ell g = 0 \quad \text{car} \quad 2\ell g = \ell(2g) = 0.$$
On vérifie alors que $(G, +, \cdot)$ est un $\mathbf{Z}/2\mathbf{Z}$-espace vectoriel. Comme G est une famille génératrice finie, il est de dimension finie. On sait donc que si $n = \dim_{\mathbf{Z}/2\mathbf{Z}}(G) = n$, alors[27] $G \cong (\mathbf{Z}/2\mathbf{Z})^n$, en tant que $\mathbf{Z}/2\mathbf{Z}$-espaces vectoriels. Mais, un isomorphisme de $\mathbf{Z}/2\mathbf{Z}$-espaces vectoriels est en particulier un isomorphisme des groupes additifs sous-jacents si bien qu'on $G \cong (\mathbf{Z}/2\mathbf{Z})^n$ en tant que groupes, et on retrouve bien le résultat !

► **Compléments . –** On peut se demander pour quels entiers e, un groupe d'exposant[28] e est-il nécessairement commutatif. Clairement $e = 1$ ou 2 convient d'après **1** et ce sont les seuls. Si $e \geqslant 3$ divisible par 4, alors $\mathbf{Z}/e\mathbf{e} \times \mathbf{H}_8$ est d'exposant e et non commutatif. Si maintenant $4 \nmid e$, alors e admet un facteur premier impair et $\mathbf{Z}/e\mathbf{Z} \times U(p)$ avec $U(p)$ le sous-groupe de $\mathsf{GL}_p(\mathbf{F}_p)$ formé des matrices triangulaires supérieures avec des 1 sur la diagonale est d'exposant e car pour toute matrice $M \in U(p)$, $(M - I_p)^p = 0$ et comme on est en caractéristique p, $M^p = I_p$.

24. Car une telle matrice est donnée par le choix d'une première colonne non nulle (ce qui laisse $4 - 1 = 3$ choix) et d'une seconde colonne non colinéaire à la première (ce qui laisse $4 - 2 = 2$ choix).
25. En effet, G (qui est fini) engendre G donc le cardinal des familles génératrices est une partie non vide de $\mathbf{N}$ qui admet donc un plus petit élément.
26. On prend cette convention pour coller à la définition usuelle d'un espace vectoriel. De plus, on a établi qu'un groupe d'exposant 2 est commutatif et on note usuellement une loi commutative $+$.
27. Noter qu'une base étant une famille génératrice minimale, on fait en fait la même chose que dans la première méthode !
28. On dit qu'un groupe G est d'exposant e si pour tout $g \in G$, $g^e = 1$.

Exercice 11 — Exposant d'un groupe. On définit *l'exposant* d'un groupe abélien fini G et on note $\exp(G)$, comme le plus petit entier $n \geqslant 1$ tel que $g^n = 1$ pour tout $g \in G$.

1. Soient x et y deux éléments de G d'ordres respectifs $\omega(x)$ et $\omega(y)$ premiers entre eux. Montrer que xy est d'ordre $\omega(x)\omega(y)$.
2. A-t-on sans hypothèse que l'ordre de xy est donné par $\mathrm{ppcm}(\omega(x), \omega(y))$?
3. Montrer qu'il existe $z \in G$ tel que z soit d'ordre $\exp(G)$.
4. Retrouver alors qu'un sous-groupe fini du groupe multiplicatif d'un corps est cyclique.

Solution.

1. Notons r l'ordre de xy. Puisque G est abélien, on a $(xy)^{nm} = (x^m)^n (y^n)^m = 1$ donc $r \mid mn$. En outre, $1 = (xy)^{rm} = y^{rm}$ donc $n \mid rm$ et donc $n \mid r$ par coprimalité. De même, $m \mid r$ et par coprimalité $nm \mid r$ et $r = nm$.
2. Non, on peut par exemple prendre un élément $x \in G$ d'ordre au moins 2 et $y = x^{-1}$.
3. Posons $M = \mathrm{ppcm}(\omega(x) \ : \ x \in G)$. Par le théorème de Lagrange, $x^M = 1$ pour tout $x \in G$ et $\exp(G) \leqslant M$. Montrons que cette borne est atteinte. Soient $p_1, \dots, p_k$ premiers et $a_1, \dots, a_k$ des entiers strictement positifs tels que $M = \prod_{i=1}^{k} p_i^{a_i}$. Pour tout $i \in \{1, \dots, k\}$, il existe un élément $x_i \in G$ d'ordre $p_i^{a_i}$. En effet, par définition de M, il existe $y_i \in G$ d'ordre $p_i^{a_i} q$ avec $p_i \nmid q$ et $x_i = y^q$ convient. Ainsi, $x = \prod_{i=1}^{k} x_i$ convient et est d'ordre M d'après **1**.
4. Soit G le groupe multiplicatif, de cardinal n, d'un corps k. On veut montrer l'existence d'un élément d'ordre n dans G. On sait par **3.** qu'il existe un élément $g_0 \in G$ d'ordre $\exp(G)$ et que $\exp(G) \leqslant n$ par Lagrange. Par ailleurs, $x^{\exp(G)} = 1$ pour tout $x \in G$. Or, dans un corps, le nombre de racines comptées avec multiplicité d'un polynôme est majoré par son degré de sorte que $n \leqslant \exp(G)$ et finalement g_0 est d'ordre n et G est cyclique.

Exercice 12.

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 distingués d'ordre p^i pour tout $i \in \{0, \dots, n\}$.

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 $x \in G \smallsetminus Z(G)$. 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[29] $\mathbf{H}_8$ 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.

Exercice 13. Soient p un nombre premier et $K = \mathbf{F}_p$. On considère le groupe linéaire $\mathrm{GL}_n(K)$ et son sous-groupe $\mathrm{SL}_n(K)$.

1. Montrer que le centre de $\mathrm{GL}_n(K)$ (resp. de $\mathrm{SL}_n(K)$) est constitué des matrices scalaires de ce groupe.
2. On note $\mathrm{PGL}_n(K)$ (resp. $\mathrm{PSL}_n(K)$) le quotient de $\mathrm{GL}_n(K)$ (resp. $\mathrm{SL}_n(K)$) par son centre. Calculer les cardinaux de $\mathrm{SL}_n(K)$, $\mathrm{PGL}_n(K)$ et $\mathrm{PSL}_n(K)$.

Solution.

29. 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.

1. 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 $(x, e_1, ..., e_{n-1})$ 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.

2. On a que le cardinal de $\mathsf{GL}_n(K)$ est

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

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

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

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

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 $Z(\mathrm{SL}_n(K)) = Z(\mathrm{GL}_n(K)) \cap \mathrm{SL}_n(K) = \{\lambda I_n \ : \ \lambda^n = 1\}$. 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,

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

Exercice 14. Soit $n \geqslant 5$. Trouver tous les morphismes de groupes de $\mathfrak{S}_n$ dans $(\mathbf{Z}/12\mathbf{Z}, +)$. Que se passe-t-il si on remplace $\mathbf{Z}/12\mathbf{Z}$ par un groupe abélien quelconque ? Et si on prend $n = 4$?

Solution. L'observation importante est que commme $\mathbf{Z}/12\mathbf{Z}$ est abélien, le noyau d'un tel morphisme contient le sous-groupe dérivé de $\mathfrak{S}_n$ (en effet l'image de tout commutateur est triviale). Comme ce sous-groupe est $\mathfrak{A}_n$, un tel morphisme est trivial, ou bien se factorise en un morphisme injectif $\mathfrak{S}_n/\mathfrak{A}_n \simeq \{\pm 1\} \to \mathbf{Z}/12\mathbf{Z}$, l'isomorphisme étant induit par la signature. Ainsi, le seul morphisme non trivial est celui obtenu en composant la signature avec le morphisme envoyant 1 sur $\bar{0}$ et -1 sur $\bar{6}$. Ceci s'applique encore à $n = 4$. Si on remplace $\mathbf{Z}/12\mathbf{Z}$ par un groupe abélien A, les morphismes non triviaux sont obtenus en composant la signature avec le morphisme envoyant 1 sur le neutre de A et -1 sur un élément arbitraire d'ordre 2 de A.

2 Actions de groupes, théorèmes de Sylow et simplicité

Exercice 1 — Groupe symétrique, le retour.

1. Soit G un groupe fini. Rappeler pourquoi il existe $n \in \mathbf{N}$ et un homomorphisme injectif de G dans $\mathfrak{S}_n$.
   En déduire qu'il existe $n \in \mathbf{N}$ et un homomorphisme injectif de G dans $\mathfrak{A}_n$ et qu'il existe $n \in \mathbf{N}$ et un homomorphisme injectif de G dans $\mathsf{GL}_n(k)$ pour tout corps k.
2. Montrer qu'un sous-groupe H d'indice n dans $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$.
   Indication : On pourra penser à restreindre l'action de G sur G/H à H.

Solution.

1. Faire agir G sur lui-même par translation à gauche donne lieu à un morphisme $G \to \mathfrak{S}(G) \cong \mathfrak{S}_n$ avec $n = \#G$ défini par $g \mapsto (h \mapsto gh)$. Il suffit alors de montrer l'injectivité qui découle de la liberté de l'action. En effet, soit $g \in G$ tel que pour tout $h \in G$, $gh = h$, alors $g = e$.
   Pour obtenir un morphisme dans un $\mathfrak{A}_k$, on part du morphisme de Cayley $G \to \mathfrak{S}_n$ et on va voir qu'on peut plonger naturellement $\mathfrak{S}_n$ dans $\mathfrak{S}_{n+2}$. On dispose en effet d'un morphisme injectif naturel $\iota : \mathfrak{S}_n \to \mathfrak{S}_{n+2}$ obtenu en prolongeant une bijection σ de $\{1, \dots, n\}$ en une permutation de $\{1, \dots, n+2\}$ par $\sigma(n+1) = n+1$ et $\sigma(n+2) = n+2$. On peut alors définir une application

$$\psi : \left\{ \begin{array}{ccc} \mathfrak{S}_n & \longrightarrow & \mathfrak{A}_{n+2} \\ \sigma & \longmapsto & \left\{ \begin{array}{l} \iota(\sigma) \text{ si } \sigma \in \mathfrak{A}_n \\ \iota(\sigma) \circ (n+1\ n+2) \text{ sinon.} \end{array} \right. \end{array} \right.$$

   L'application est clairement bien définie et on vérifie aisément qu'il s'agit d'un morphisme de groupes injectif (car $i(\sigma)$ pour $\sigma \in \mathfrak{S}_n$ et $(n+1\ n+2)$ sont à support disjoint et commutent donc) et finalement G se plonge dans $\mathfrak{A}_{n+2}$.
   Pour finir, on procède de même en plongeant $\mathfrak{S}_n$ dans $\mathsf{GL}_n(k)$ via

$$\varphi : \left\{ \begin{array}{ccc} \mathfrak{S}_n & \longrightarrow & \mathsf{GL}_n(k) \\ \sigma & \longmapsto & P_\sigma \end{array} \right.$$

   où P_σ est la matrice de permutation associée à σ.
2. Supposons pour commencer que $n \geqslant 5$. On note $G = \mathfrak{S}_n$ et soit H un sous-groupe d'indice n. Notons $X = G/H$ l'ensemble quotient de cardinal n. On dispose de l'action naturelle de G sur X qui induit un morphisme de groupe $\psi : G \to \mathfrak{S}(X) \cong \mathfrak{S}_n$. Montrons qu'il s'agit d'un isomorphisme. Son noyau est un sous-groupe distingué de G, donc égal à $\{1\}, \mathfrak{A}_n$ ou $\mathfrak{S}_n$. Mais on voit que [30]

$$\mathsf{Ker}(\psi) = \bigcap_{a \in G} aHa^{-1} \subseteq H.$$

   Or, $\#H = (n-1)!$ et $(n-1)! < n!/2$ (car $2 < n$) si bien que nécessairement $\mathsf{Ker}(\psi) = \{\mathsf{Id}\}$ et par cardinalité, ψ est un isomorphisme. On peut alors restreindre cette action au sous-groupe H et le groupe H est alors clairement un point fixe pour cette action restreinte. Cela donne lieu à une action de H sur $X \smallsetminus \{H\}$ et ainsi à un morphisme $\varphi : H \to \mathfrak{S}(X \smallsetminus \{H\}) \cong \mathfrak{S}_{n-1}$. Ce morphisme est injectif (car ψ l'est) et donc un isomorphisme par égalité des cardinaux.
   Les cas $n = 2, 3$ sont immédiats et pour $n = 4$, on utilise le fait qu'un sous-groupe d'indice 4 est de cardinal 6 donc abélien ou isomorphe à $\mathfrak{S}_3$. Mais si ce groupe était abélien, alors on aurait un élément d'ordre 6, ce qui n'est pas le cas.

Exercice 2 — Actions de groupes.

1. Soient G un groupe fini et p le plus petit facteur premier de $|G|$. On suppose qu'il existe un sous-groupe $H \lhd G$ d'ordre p. Montrer que H est dans le centre de G.
2. On fait opérer le groupe multiplicatif $G = (\mathbf{Z}/n\mathbf{Z})^\times$ sur l'ensemble $X = \mathbf{Z}/n\mathbf{Z}$ par $a \cdot x = ax$. Décrire les orbites et les stabilisateurs de chacun des éléments de X dans le cas $n = 8$. Écrire l'équation aux classes dans le cas général.
3. Soit E un ensemble muni d'une action $\cdot$ d'un groupe fini G. On note

$$E_G = \{x \in E \ : \ \forall g \in G,\ g \cdot x = x\}.$$

   Si l'on suppose que $E_G = \varnothing$, que $|G| = 15$ et $|E| = 17$, quel est alors le nombre d'orbites et le cardinal de chacune d'entre elles ?
   Si $|G| = 33$ et que $|E| = 19$, établir que $E_G \neq \varnothing$.
4. Soit $H \lhd G$ un sous-groupe distingué d'un groupe G qui agit transitivement sur un ensemble X. Montrer que les orbites de l'action de H (induite par l'action de G) sur X ont toutes même cardinal.
5. Soit une action d'un groupe G sur un ensemble X. Montrer que tous les éléments d'une même orbite ont même stabilisateur si, et seulement si, ce stabilisateur est un sous-groupe distingué de G.

30. De manière générale, le noyau est l'intersection des stabilisateurs.

6. Soit G un groupe de cardinal pq avec p, q deux nombres premiers distincts. On suppose que G opère sur un ensemble X de cardinal $n = pq - p - q$. Montrer qu'il existe au moins un point fixe par cette action.

7. Soit E un espace vectoriel de dimension finie n sur un corps K. On fait opérer le groupe linéaire $G := \mathrm{GL}(E)$ sur l'ensemble des sous-espaces vectoriels de E par : $g.F := g(F)$ pour tout $g \in G$ et tout sous-espace F de E. Quelles sont les orbites pour cette action ?

Solution.

1. Puisque $H \lhd G$, G opère par conjugaison sur H. Cela donne lieu à un morphisme $f : G \to \mathfrak{S}(H)$. On a que pour tout $g \in G$, $f(g) : H \mapsto H$ est donnée par $f(g)(h) = ghg^{-1}$ est en réalité un automorphisme de H si bien que cette action donne lieu à un morphisme $f : G \to \mathtt{Aut}(H)$. Le fait que $H \subseteq Z(G)$ est équivalent au fait que $\mathrm{Ker}(f) = G$. Or, H est d'ordre p premier donc cylcique et isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On a donc que

$$\mathtt{Aut}(H) \cong \mathtt{Aut}\left(\mathbb{Z}/p\mathbb{Z}\right) \cong \left(\mathbb{Z}/p\mathbb{Z}\right)^{\times} \cong \left(\mathbb{Z}/(p-1)\mathbb{Z}\right).$$

Si $\mathrm{Ker}(f) \neq G$, le premier théorème d'isomorphisme fournit que $\#G/\mathrm{Ker}(f) \neq 1$ et divise $\#\mathtt{Aut}(H) = p - 1$, ce qui est absurde car p est le plus petit diviseur premier de $\#G$. On a donc le résultat.

2. Dans le cas $n = 8$, il est clair que l'orbite de $\overline{0}$ est $\{\overline{0}\}$, l'orbite de $\overline{1}$ est $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\} = (\mathbf{Z}/8\mathbf{Z})^{\times}$. On vérifie que l'orbite de $\overline{2}$ est $\{\overline{2}, \overline{6}\}$ et celle de $\overline{4}$ est $\{\overline{4}\}$.
Dans le cas général, montrons que l'on a une orbite pour chaque diviseur d de n de cardinal $\varphi(d)$, avec φ la fonction indicatrice d'Euler. Soient $d \mid n$ et $x \in \mathbf{Z}/n\mathbf{Z}$ d'ordre d (qui existe d'après le cours et on sait qu'alors x est de la forme $\overline{k\frac{n}{d}}$ avec $k \in \{0, \ldots, d-1\}$ premier à d). On a alors qu'un inversible u vérifie $ux = x$ si, et seulement si, $u \equiv 1 \mod d$ soit si, et seulement si, u est dans le noyau du morphisme surjectif (ce qui sera établi dans l'exercice 2, question 3 de la section 3) $(\mathbf{Z}/n\mathbf{Z})^{\times} \mapsto (\mathbf{Z}/d\mathbf{Z})^{\times}$ qui envoie la classe de t modulo n sur sa classe modulo d. On en déduit que ce noyau est de cardinal $\frac{\varphi(n)}{\varphi(d)}$ et par conséquent, on a obtenu le cardinal du stabilisateur de x et son orbite est donc de cardinal $\varphi(d)$. Or, il est clair que si u est inversible, x et ux ont même ordre donc l'orbite de x contient tous les éléments d'ordre d. Comme il y en a $\varphi(d)$, l'orbite d'un élément contient exactement tous les éléments d'ordre d. Finalement, il vient par l'équation aux classes

$$\varphi(n) = \sum_{d \mid n} \varphi(d).$$

3. L'équation aux classes fournit

$$|E| = |E_G| + \sum_{\substack{\omega \in \Omega \\ |\omega| > 1}} \frac{|G|}{|\mathrm{Stab}_\omega|} = \sum_{\substack{\omega \in \Omega \\ |\omega| > 1}} \frac{15}{|\mathrm{Stab}_\omega|}.$$

On a alors que $|\mathrm{Stab}_\omega| \neq 15$ car sinon cela fournit une orbite de cardinal un, ce qui est exclu. On a donc $|\mathrm{Stab}_\omega| \in \{1, 3, 5\}$, et si on note n_k le nombre d'orbites de cardinal k, on a

$$17 = 3n_3 + 5n_5 + 15n_{15}.$$

On a donc $n_{15} = 0$ ou 1. Mais si $n_{15} = 1$, $2 = 3n_3 + 5n_5$ ce qui est impossible donc $n_{15} = 0$ et $17 = 3n_3 + 5n_5$. On a donc $n_5 \leqslant 3$ et en testant toutes les possibilités, on constate qu'il n'y a qu'une solution, $n_3 = 4$ et $n_5 = 1$.
On procède de même dans le second cas en supposant par l'absurde que $|E_G| = 0$. L'équation aux classes fournit alors, avec les mêmes notations que ci-dessus,

$$19 = 3n_3 + 11n_{11} + 33n_{33}.$$

Il vient tout de suite $n_{33} = 0$ puis $19 = 3n_3 + 11n_{11}$ si bien que $n_{11} \leqslant 1$. Mais si $n_{11} = 1$ alors $3n_3 = 8$ ce qui est absurde. On en déduit que $n_{11} = 0$ et $19 = 3n_3$, ce qui fournit là encore une contradiction. Dans tous les cas, on aboutit à une contradiction et donc $|E_G| \neq 0$ et $E_G \neq \varnothing$.

4. Soit $g \in G$ et $x \in X$. On obtient facilement par double inclusion (voir l'exercice 11) que $\mathrm{Stab}_G(g \cdot x) = g\mathrm{Stab}_G(x)g^{-1}$. Soient $x_0 \in X$ et $x \in X$. Par transitivité de l'action de G sur X, il existe $g \in G$ tel que $x = g \cdot x_0$. On vérifie alors (puisque $H \lhd G$) que $\mathrm{Stab}_H(g \cdot x) = g\mathrm{Stab}_H(x)g^{-1}$, ce qui permet de conclure.

5. Cela découle là encore immédiatement du fait que $\mathrm{Stab}_G(g \cdot x) = g\mathrm{Stab}_G(x)g^{-1}$.

6. L'équation aux classes fournit avec les mêmes notations qu'en question **3.** et en supposant par l'absurde qu'on n'a aucun point fixe

$$pq - p - q = n_p p + n_q q + n_{pq} pq.$$

Il vient tout de suite que $n_{pq} = 0$ et $pq - p - q = n_p p + n_q q$. On a alors $n_q \neq 0$ car sinon $pq - p - q = n_p p$ et modulo p, $q \equiv 0 \,(\mathrm{mod}\, p)$ ce qui est absurde. De même, $n_p \neq 0$. On a donc $n_p, n_q \geqslant 1$ et donc

$$pq - p - q = n_p p + n_q q \quad \text{soit} \quad pq = (n_p + 1)p + (n_q + 1)q.$$

On a alors que $p \mid (n_q+1)q$ et comme p est premier avec q, il vient que $n_q+1 = pk$ pour un entier naturel non nul k et de même $n_p+1 = q\ell$ pour un entier naturel non nul ℓ. On en déduit que

$$pq = pqk + pq\ell \quad \text{soit} \quad k+\ell = 1.$$

Il vient que nécessairement $k=0$ ou $\ell = 0$ ce qui est absurde et permet de conclure !

7. On constate que l'action envoie un sous-espace vectoriel de dimension k sur un sous-espace vectoriel de même dimension car g est un isomorphisme. Montrons que réciproquement deux espaces vectoriels F_1 et F_2 de dimension k pour k fixé dans $\{1,\dots,n\}$ sont dans la même orbite. Il suffit de considérer une base de F_1, disons $(e_1,\dots,e_k)$ et la compléter en une base $(e_1,\dots,e_k,e_{k+1},\dots,e_n)$ de E et de même de considérer une base de F_1, disons $(f_1,\dots,f_k)$ et la compléter en une base $(f_1,\dots,f_k,f_{k+1},\dots,f_n)$ de E. L'application linéaire u qui envoie e_i sur f_i est bien un isomorphisme tel que $u(F_1) = F_2$. On a donc $n+1$ orbites qui correspondent aux sous-espaces vectoriels de E de dimension fixée $k \in \{0,\dots,n\}$.

Exercice 3 — Lemme de Cauchy. Soit G un groupe fini et p un nombre premier divisant le cardinal de G. En utilisant une action convenable de $\mathbf{Z}/p\mathbf{Z}$ sur l'ensemble

$$X = \{(g_1,\dots,g_p) \in G^p \ : \ g_1g_2\cdots g_p = 1\},$$

établir que G admet un élément d'ordre p (sans utiliser les théorèmes de Sylow !).

Solution. On comprendra ici les indices d'un élément de X modulo p. On considère alors l'action de $H = \mathbf{Z}/p\mathbf{Z}$ sur X définie par

$$\forall k \in H, \quad \forall (g_1,\dots,g_p) \in X, \quad k\cdot(g_1,\dots,g_p) = (g_{k+1},\dots,g_{k+p}).$$

On a alors bien que pour tout $k \in H$ et $(g_1,\dots,g_p) \in X$, $k\cdot(g_1,\dots,g_p) \in X$. On sait que $g_1\cdots g_p = 1$ mais alors $g_2\cdots g_p = g_1^{-1}$ et donc $g_2\cdots g_pg_1 = 1$ et par récurrence $g_{k+1}\cdots g_{k+p} = 1$ et il est alors clair qu'on a ainsi bien défini une action de H sur X. L'équation aux classes fournit alors

$$\#X = \#X^H + \sum_{\omega\in\Omega'} \#\omega$$

avec $X^H = \{\mathbf{g} \in X \ : \ \#\omega(\mathbf{g}) = 1\}$ et Ω' l'ensemble des orbites de cardinal > 1. Or, H est de cardinal p premier donc on voit aisément (puisque $\omega \neq 1$) que $H_{\mathbf{g}}$ est le groupe trivial pour tout $\mathbf{g}$ et que $\#\omega = \#H = p$. Or, $\#X = (\#G)^{p-1}$ donc $p \mid \#X$ et on en déduit donc que $p \mid \#X^H$. Pour conclure, on remarque que $X^H \neq \varnothing$ puisque $(1,\dots,1) \in X^H$ et finalement il existe un élément de X^H différent de $(1,\dots,1)$. Un tel élément est de la forme $(g,\dots,g)$ pour un certain $g \in G \smallsetminus \{1\}$. Par définition de X, on a alors $g^p = 1$ et $g \neq 1$ donc on a bien trouvé un élément d'ordre p.

Exercice 4. 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 $n!$ et $[H:K] \mid (n-1)!$.
Indication : On pourra considérer l'action de G sur G/H.

2. **Application 1** : Montrer que si H est d'indice 2 dans G, alors H est distingué dans G. Le démontrer également de façon plus élémentaire.

3. **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.

4. **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.

5. On suppose que G est fini. Montrer que G n'est pas la réunion des conjugués gHg^{-1} de H.

6. Montrer que **2.** reste vrai si G est infini.

7. Est-ce que **2.** reste vrai si on ne suppose plus que $[G:H]$ est fini ?

8. 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.

9. 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 $h : G \to \mathfrak{S}(G/H) \cong \mathfrak{S}_n$. Montrons que le noyau de H convient. Attention ici qu'on n'a pas supposé G fini et donc $[G : \mathsf{Ker}(h)]$ n'est pas donné par $\#G/\#\mathsf{Ker}(h)$. Le théorème de factorisation fournit un morphisme injectif $\tilde{h} : G/\mathsf{Ker}(h) \to \mathfrak{S}(G/H) \cong \mathfrak{S}_m$. On peut ainsi identifier $G/\mathsf{Ker}(h)$ à un sous-groupe de $\mathfrak{S}_m$ et en déduire par Lagrange que $[G : \mathsf{Ker}(h)] \mid m!$.
Soit $g \in \mathsf{Ker}(h)$. On a alors pour tout $a \in G$, $gaH = aH$ qui implique immédiatement que $g \in H$. On peut aussi utiliser le résultat rappelé dans le complément en bas de page 5 qui stipule que le noyau du morphisme $h : G \to \mathfrak{S}(X)$ associé à une action du groupe G sur un ensemble X est donné par

$$\mathsf{Ker}(h) = \bigcap_{x\in X} \mathsf{Stab}_G(x).$$

Or, ici on obtient immédiatement par double inclusion que $\mathrm{Stab}_G(aH) = aHa^{-1}$ de sorte que

$$\mathrm{Ker}(h) = \bigcap_{a\in G} aHa^{-1} \subseteq H.$$

On restreint alors 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 $G/H \smallsetminus \{H\}$ de même noyau que h. De manière plus générale, si un groupe G agit sur X et que l'on dispose d'un élément $x_0 \in X$ appartenant à l'intersection des fixateurs pour $g \in G$, autrement dit tel que pour tout $g \in G$, $g \cdot x_0 = x_0$, alors l'action de G sur X induit par restriction une action de G sur $X \smallsetminus \{x_0\}$. En effet, si $x \in X \smallsetminus \{x_0\}$, alors pour tout $g \in G$, $g \cdot x \in X \smallsetminus \{x_0\}$ car sinon $g.x = x_0$ et donc en faisant agir g^{-1}, $x = g^{-1} \cdot x_0$ mais $g^{-1} \cdot x_0 = x_0$, ce qui fournit une contradiction ! On a alors que l'action de G sur X fournit un morphisme $h : G \to \mathfrak{S}(X)$ et celle restreinte à $X \smallsetminus \{x_0\}$ un morphisme $h_2 : G \to \mathfrak{S}(X \smallsetminus \{x_0\})$ et

$$\mathrm{Ker}(h) = \bigcap_{x\in X} \mathrm{Stab}_G(x) = \bigcap_{x\in X\smallsetminus\{x_0\}} \mathrm{Stab}_G(x)$$

car par définition, $\mathrm{Stab}_G(x_0) = G$. Or,

$$\mathrm{Ker}(h_2) = \bigcap_{x\in X\smallsetminus\{x_0\}} \mathrm{Stab}_G(x) \quad \text{de sorte que} \quad \mathrm{Ker}(h) = \mathrm{Ker}(h_2).$$

Le même raisonnement que ci-dessus permet alors de conclure que $K = \mathrm{Ker}(h)$ convient.

▶ **Remarque . –** On ne peut pas utiliser ici le troisième théorème d'isomorphisme car 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 $[H : \mathrm{Ker}(h)] \mid (m-1)!$.

2. On a $m = 2$ et la question **4.** fournit alors que $[H : \mathrm{Ker}(h)] = 1$ soit $H = \mathrm{Ker}(h)$. Ainsi $H \lhd G$. On donne une démonstration plus élémentaire dans l'exercice 8 mais celle-ci a l'avantage de se généraliser comme on va le voir en question **7.**

3. 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 $H \lhd G$. Noter que l'indice d'un sous-groupe H d'un p-groupe est une puissance de p et que dès que l'indice est supérieur à p le raisonnement tombe en défaut. Il est en réalité faux comme en témoigne l'exemple du groupe $\mathbf{D}_4$ qui est un 2-groupe dont certains sous-groupes d'ordre 2 (et donc d'indice 4) ne sont pas distingués comme on a pu le voir lors de l'exercice **2.**

4. 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. Idem, le raisonnement et le résultat tombent en défaut dès qu'on autorise des indices qui ne sont pas le plus petit facteur premier du cardinal de G, comme par exemple un sous-groupe d'ordre 3 (engendré par un 3-cycle) dans $\mathfrak{S}_4$.

5. On a clairement que [31]

$$\bigcup_{g\in G} gHg^{-1} = \bigcup_{\overline{g}\in G/H} gHg^{-1}.$$

31. Noter qu'alors, puisque gHg^{-1} est un sous-groupe de G, si H est d'indice 2, cela entraînerait que G est la réunion de deux sous-groupes, aucun n'étant inclus dans l'autre, ce qui est impossible ! On a un résltat similaire pour les espaces vectoriels. Attention en revanche que ce résultat ne se généralise pas à strictement plus de deux groupes ou espace vectoriels car par exemple

$$\mathfrak{S}_3 = \mathfrak{A}_3 \cup \langle(12)\rangle \cup \langle(13)\rangle \cup \langle(23)\rangle \quad \text{ou} \quad \mathbf{F}_2^2 = \mathrm{Vect}(1,0) \cup \mathrm{Vect}(0,1) \cup \mathrm{Vect}(1,1).$$

En revanche, dans le cas d'un espace vectoriel E sur un corps k **infini**, on a bien que

$$E \neq F_1 \cup F_2 \cup \cdots \cup F_n$$

pour tous $F_1, F_2, \ldots, F_n$ des sous-espaces vectoriels stricts de E. En effet, on peut supposer $F_n \not\subseteq F_1 \cup F_2 \cup \cdots \cup F_{n-1}$ et choisir $x \in F_n \smallsetminus F_1 \cup F_2 \cup \cdots \cup F_{n-1}$ et $y \notin F_n$. On a alors que pour tout $\lambda \in k$, $\lambda x + y \notin F_n$ et pour tout $i \leqslant n-1$, il existe au plus un $\lambda \in k$ tel que $\lambda x + y \in F_i$, ce qui vient contredire le caractère infini du corps k. En effet, si on dispose de $\lambda \neq \mu$ tels que $\lambda x + y$ et $\mu x + y$ sont dans F_i, alors $(\lambda - \mu)x \in F_i$ ce qui est absurde !

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)

$$\begin{aligned}\#\left(\bigcup_{g\in G} gHg^{-1}\smallsetminus\{e\}\right) &= \#\left(\bigcup_{\overline{g}\in G/H} gHg^{-1}\smallsetminus\{e\}\right)\\ &\leqslant \sum_{\overline{g}\in G/H}\#\left(gHg^{-1}\smallsetminus\{e\}\right)\\ &\leqslant \sum_{\overline{g}\in G/H}\#\left(H\smallsetminus\{e\}\right)\leqslant \#(G/H)(\#H-1) = \#G\left(1-\frac{1}{\#H}\right) < \#G-1\end{aligned}$$

car $H\neq G$ si bien que

$$\#\left(\bigcup_{g\in G} gHg^{-1}\smallsetminus\{e\}\right) < \#(G\smallsetminus\{e\}) \quad \text{et} \quad \bigcup_{g\in G} gHg^{-1}\neq G.$$

6. 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 (pusique contenant des bijections qui envoient H sur n'importe quel autre classe à gauche aH avec $a\in G\smallsetminus H$) donc $\varphi(H)$ est un sous-groupe strict du groupe fini $\varphi(G)$ et la question précédente entraîne alors que

$$\bigcup_{g\in G}\varphi(g)\varphi(H)\varphi(g)^{-1}\neq\varphi(G).$$

Ainsi nécessairement

$$\bigcup_{g\in G} gHg^{-1}\neq G.$$

7. Le résultat devient alors faux en général. On pose $G=\mathsf{GL}_n(\mathbf{C})$ 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[32] G. Pour voir que l'indice est infini (autrement que par l'absurde en utilisant la question précédente), on peut par exemple utiliser le fait que toute matrice[33] 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 sous-groupe H d'indice fini non trivial, disons d'indice $r\geqslant 2$. On sait (comme en question **1.**) qu'on peut trouver un sous-groupe K distingué de $GL_n(\mathbf{C})$ tel que $K\subseteq H$. Le fait que H soit d'indice fini implique que K est d'indice fini[34], disons d'indice $m\geqslant 2$ (car $m\geqslant r$ puisque $K\subseteq H$). Pour toute matrice $M\in GL_n(\mathbf{C})$, il existe B telle que $M=B^m$ et ainsi la classe de M dans le **groupe** quotient $GL_n(\mathbf{C})/K$ est triviale si bien que ce dernier quotient est nécessairement trivial et $K=GL_n(\mathbf{C})$. Cela impliquerait que $H=GL_n(\mathbf{C})$, ce qui est exclu puisqu'on a supposé $r\geqslant 2$. Ainsi, on a qu'un seul sous-groupe d'indice fini dans $GL_n(\mathbf{C})$, c'est lui-même, d'indice 1. Puisque $T_n(\mathbf{C})\neq GL_n(\mathbf{C})$, on en déduit qu'il est nécessairement d'indice infini.

8. On choisit $x_0\in X$ et on note $H=\mathsf{Stab}_G(x_0)$. 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 $\mathsf{Stab}_G(x)=gHg^{-1}$ donc par construction $g_0\notin\mathsf{Stab}_G(x)$, ce qui signifie que $g_0\cdot x\neq x$ ce qui conclut la preuve.
Noter que par conséquent, pour une action transitive, tous les stabilisateurs sont conjugués ! Et ici, on cherchait en réalité un élément de

$$\bigcap_{x\in X}\overline{\mathsf{Stab}_G(x)}$$

où $\overline{E}$ représente le complémentaire de l'ensemble E. On cherchait donc un élément de G qui n'appartienne pas à

$$\bigcup_{x\in X}\mathsf{Stab}_G(x)=\bigcup_{g\in X} gHg^{-1} \quad \text{pour} \quad H=\mathsf{Stab}_G(x_0).$$

32. 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. Alors toute rotation étant conjuguée à une rotation d'axe fixé, on a un autre contre-exemple.

33. On dit que le groupe $GL_n(\mathbf{C})$ est *divisible*.

34. En effet, $K=\mathsf{Ker}(h)$ et on peut plonger $GL_n(\mathbf{C})/K$ dans $\mathfrak{S}(GL_n(\mathbf{C})/H)\cong\mathfrak{S}_r$ via l'action de $GL_n(\mathbf{C})$ sur $GL_n(\mathbf{C})/H$ par translation à gauche.

9. 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 $H = \mathfrak{A}_k$ puisque le seul[35] sous-groupe d'indice 2 de $\mathfrak{S}_k$ est le groupe alterné.
Noter qu'on a un sous-groupe d'indice 1, à savoir $\mathfrak{S}_k$ tout entier, et des sous-groupes d'indice k, à savoir[36] les

$$\mathfrak{S}_k(i) = \{\sigma \in \mathfrak{S}_k \ : \ \sigma(i) = i\} \cong \mathfrak{S}_{k-1}$$

pour tout $i \in \{1, \dots, k\}$.

Exercice 5 — Un exercice des olympiades de La Havane 1987. Soit $P_n(k)$ le nombre de permutations de $\{1, \dots, n\}$ qui ont exactement k points fixes. Montrer que $\sum_{k=0}^{n} kP_n(k) = n!$. En déduire le nombre moyen de points fixes d'une permutation aléatoire de $\mathfrak{S}_n$.
Soit G un groupe agissant sur un ensemble X. Généraliser le résultat au nombre moyen de points fixes d'un élément de G.

Solution. Pour une preuve de la formule de Burnside, je vous renvoie ici, page 13. On considère alors l'action de $\mathfrak{S}_n$ sur $\{1, \dots, n\}$ donnée par $\sigma \cdot i = \sigma(i)$. Il s'agit d'une action transitive. On remarque alors que

$$\sum_{k=0}^{n} kP_n(k) = \sum_{k=0}^{n} k \sum_{\substack{\sigma \in \mathfrak{S}_n \\ \#\mathrm{Fix}(\sigma)=k}} = \sum_{k=0}^{n} \sum_{\substack{\sigma \in \mathfrak{S}_n \\ \#\mathrm{Fix}(\sigma)=k}} \#\mathrm{Fix}(\sigma) = \sum_{\sigma \in \mathfrak{S}_n} \#\mathrm{Fix}(\sigma).$$

La formule de Burnside permet alors de conclure que

$$\sum_{k=0}^{n} kP_n(k) = n! \sum_{i=1}^{n} \frac{1}{\#\omega(i)} = n!.$$

On pouvait "redémontrer" Burnside dans ce cas particulier en dénombrant de deux manières l'ensemble

$$A = \{(\sigma, i) \in \mathfrak{S}_n \times \{1, \dots, n\} \ : \ \sigma(i) = i\}.$$

Exercice 6.

1. Combien y a-t-il d'opérations du groupe $\mathbf{Z}/4\mathbf{Z}$ sur l'ensemble $\{1, 2, 3, 4, 5\}$?
2. Soient G et X deux groupes. On dit que G *opère par automorphismes* sur X si on s'est donnée une opération $(g, x) \mapsto g.x$ de G sur X telle que pour tout $g \in G$, l'application $x \mapsto g.x$ soit un automorphisme de X. L'opération de G sur lui-même par translation est-elle une opération par automorphismes ? Même question pour l'opération par conjugaison.
3. On prend $G = (\mathbf{Z}/3\mathbf{Z}, +)$ et $X = (\mathbf{Z}/13\mathbf{Z}, +)$. Combien y a-t-il d'actions de G sur X par automorphismes ? Même question en remplaçant $\mathbf{Z}/13\mathbf{Z}$ par le groupe symétrique $\mathfrak{S}_3$.

Solution.

1. On cherche le nombre de morphismes de $\mathbf{Z}/4\mathbf{Z}$ dans le groupe des permutations $\mathfrak{S}_5$. Se donner un tel morphisme f revient à se donner un élément d'ordre divisant 4 (à savoir $f(\bar{1})$) dans $\mathfrak{S}_5$. Or $\mathfrak{S}_5$ contient un élément d'ordre 1 (l'identité), $C_5^2 = 10$ transpositions, $5.3 = 15$ doubles transpositions (cinq façons de choisir le point fixe, puis trois doubles transpositions avec les quatre éléments restants) et $5.6 = 30$ 4-cycles (cinq façons de choisir le point fixe, et six 4-cycles dans le groupe des permutations des quatre éléments restants). Il y a donc au total $1 + 10 + 15 + 30 = 56$ possibilités.
2. Clairement, oui pour l'opération par conjugaison, non pour l'opération par translation.
3. On sait que le groupe des automorphismes de X est isomorphe au groupe multiplicatif des inversibles de l'anneau $\mathbf{Z}/13\mathbf{Z}$ (en effet si on pose $\varphi_a(x) = ax$, on vérifie immédiatement que $a \mapsto \varphi_a$ est un isomorphisme de $(\mathbf{Z}/13\mathbf{Z})^\times$ sur $\mathrm{Aut}(X)$), lequel est isomorphe au groupe additif $\mathbf{Z}/12\mathbf{Z}$ car 13 est premier. On cherche donc le nombre de morphismes de $\mathbf{Z}/3\mathbf{Z}$ dans $\mathbf{Z}/12\mathbf{Z}$, ou encore le nombre déléments de $\mathbf{Z}/12\mathbf{Z}$ d'ordre divisant 3. Il y a ainsi trois solutions.
   On voit facilement que les seuls automorphismes de $\mathfrak{S}_3$ sont intérieurs (voir un des exercices de la feuille 2 et sinon on utilise le fait que $\mathfrak{S}_3$ est engendré par (12) et (123) donc on a au plus 6 automorphismes et on a six automorphismes intérieurs). Le groupe des automorphismes de $\mathfrak{S}_3$ est donc isomorphe à $\mathfrak{S}_3$ quotienté par son centre (car on a la suite exacte $1 \to Z(G) \to G \xrightarrow{f} \mathrm{Int}(G) \to 1$ avec $f(g) = i_g$ et $i_g(x) = gxg^{-1}$), *i.e.* à $\mathfrak{S}_3$. On est donc ramené à chercher le nombre d'éléments d'ordre 1 ou 3 dans $\mathfrak{S}_3$, et il y a trois solutions.

35. 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.

36. On peut même établir que ce sont les seuls en utilisant des arguments similaires à ceux du complément à la fin de l'exercice 1!

Exercice 7. Combien y a-t-il de colliers différents formés de 9 perles dont 4 bleues, 3 blanches et 2 rouges ?

Solution. On représente un collier par un cercle du plan euclidien orienté de centre l'origine et de rayon 1 muni de neuf points $A_1, \dots, A_9$ à intervalles réguliers. On choisit de dire que deux colliers sont équivalents si, et seulement si, on peut obtenir l'un à partir de l'autre en effectuant une rotation ou en le retournant. Autrement dit, l'ensemble X de tous les colliers possibles à 9 perles dont 4 bleues, 3 blanches et 2 rouges est muni d'une action du groupe diédral D_9 engendré par la rotation de centre l'origine et d'angle $\frac{2\pi}{9}$ et la symétrie axiale σ par rapport à l'axe des abscisses (OA_1). On cherche alors le nombre d'orbites N pour cette action et la formule de Burnside fournit

$$N = \frac{1}{18} \sum_{g \in D_9} \#\mathsf{Fix}(g).$$

Reste alors à calculer $\mathsf{Fix}(g)$ pour tout $g \in D_9$. Si $g = \mathsf{Id}$, on a $\mathsf{Fix}(g) = X$ et un calcul simple fournit $\#X = \binom{9}{4} \times \binom{5}{3} = 1260$. Si $g \in \{\rho, \rho^2, \rho^4, \rho^5, \rho^7, \rho^8\}$, alors le sous-groupe de G engendré par g est égale à $\langle \rho \rangle$ et un élément de $\mathsf{Fix}(g)$ a toutes ses perles de même couleurs si bien que $\mathsf{Fix}(g) = \varnothing$. Si maintenant $g = \rho^3$ ou ρ^6, dans un collier fixe par g, le nombre de perles d'une couleur donnée doit être un multiple de 3 donc à nouveau $\mathsf{Fix}(g) = \varnothing$. Si maintenant g est une symétrie, par exemple $g = \sigma$ (les autres cas étant similaires), l'axe de g ne contient qu'une seule perle (ici A_1) et donc toutes les autres perles vont par paires de couleurs. Ainsi nécessairement A_1 (la perle passant par l'axe de symétrie) est blanche et se donner un collier fixe revient à choisir la couleur de A_2, A_3, A_4, A_5 avec 2 bleues, 1 blanche et 1 rouge. On a ainsi $\#\mathsf{Fix}(g) = \binom{4}{2} \times \binom{2}{1} = 12$. Finalement, on obtient qu'on a

$$N = \frac{1}{18}(1260 + 9 \times 12) = 76$$

tels colliers.

Exercice 8. Soit G un groupe fini non trivial agissant sur un ensemble fini X. On suppose que pour tout $g \neq e \in G$, il existe un unique $x \in X$ tel que $g \cdot x = x$. On souhaite montrer que X admet un point fixe sous G (nécessairement unique).

1. On pose
$$Y = \{x \in X \ : \ \mathsf{Stab}_G(x) \neq \{e\}\}.$$
Montrer que Y est stable par G.
2. On note $n = \#Y/G$ et $y_1, \dots, y_n$ un système de représentants de Y/G. Pour tout $i \in \{1, \dots, n\}$, on note m_i le cardinal de $\mathsf{Stab}_G(y_i)$. En considérant l'ensemble
$$Z = \{(g, x) \in G \smallsetminus \{e\} \times X \ : \ g \cdot x = x\},$$
montrer que
$$1 - \frac{1}{\#G} = \sum_{i=1}^{n} \left(1 - \frac{1}{m_i}\right).$$
3. En déduire que $n = 1$ et conclure.

Solution.

1. Soit $x \in Y$. On sait alors qu'il existe $g \in G \smallsetminus \{e\}$ tel que $g \cdot x = x$. Pour montrer la stabilité par G, on fixe $g' \in G$ et on doit montrer que $g' \cdot x \in Y$. Mais alors $(g'gg'^{-1}) \cdot (g' \cdot x) = g' \cdot x$ et $g'gg'^{-1} \in \mathsf{Stab}_G(g' \cdot x)$. Noter qu'en réalité, $\mathsf{Stab}_G(g' \cdot x) = g'\mathsf{Stab}_G(x)g'^{-1}$. Cela permet de conclure.
2. On peut donc restreindre l'action de G sur X en une action de G sur Y. de la même façon qu'on démontre la formule de Burnside, il vient
$$\#Z = \sum_{g \in G \smallsetminus \{e\}} \#\{x \in X \ : \ g \cdot x = x\} = \#G - 1$$
par hypothèse. Par ailleurs, on a
$$\#Z = \sum_{x \in X} (\#\mathsf{Stab}_G(x) - 1) = \sum_{i=1}^{n} \sum_{x \sim y_i} (m_i - 1) = \sum_{i=1}^{n} \#\omega(y_i)\,(m_i - 1) = \#G \sum_{i=1}^{n} \left(1 - \frac{1}{m_i}\right)$$
ce qui permet de conclure ! On a utilisé ici que le cardinal du stabilisateur est constant sur une orbite et que le cardinal de l'orbite de y_i est donné par $\frac{\#G}{m_i}$.
3. On sait que pour tout $i \in \{1, \dots, n\}$, puisque $y_i \in Y$, $m_i \geqslant 2$ de sorte que $1 - \frac{1}{m_i} \geqslant \frac{1}{2}$. On a donc
$$\frac{n}{2} \leqslant \sum_{i=1}^{n} \left(1 - \frac{1}{m_i}\right) = 1 - \frac{1}{\#G} < 1.$$
Il s'ensuit que $n < 2$ et donc $n = 1$ et $m_1 = \#G$ de sorte que $\mathsf{Stab}_G(y_1) = G$. Finalement, on a obtenu $y_1 \in X$ tel que pour tout $g \in G$, $g \cdot y_1 = y_1$, à savoir un point fixe pour G.

Exercice 9 — Un groupe d'ordre 56 n'est pas simple.
Soit G un groupe d'ordre 56.

1. Montrer que G a un ou huit 7-Sylow.
2. On suppose que G possède huit 7-Sylow. Montrer que deux 7-Sylow distincts sont d'intersection triviale. En déduire le nombre déléments d'ordre 7 dans G puis le nombre de 2-Sylow.
3. Conclure que G n'est pas simple.

Solution.

1. Cela découle des théorèmes de Sylow. On note n_7 le nombre de 7-Sylow. On sait alors que $n_7 \mid 8$ (donc $n_7 \in \{1,2,4,8\}$) et $n_7 \equiv 1 \pmod 9$. Cela élimine 2 et 4 et $n_7 \in \{1,8\}$.
2. Puisque le cardinal d'un 7-Sylow est 7 qui est premier, un 7-Sylow est cyclique engendré par tout élément non trivial. Si on a donc $x \neq e \in S_7 \cap S'7$ avec S_7, S_7' deux 7-Sylow disctints, alors $\langle x \rangle = S_7 = S_7'$ ce qui est absurde. On a donc $S_7 \cap S_7' = \{e\}$. Comme tout élément d'ordre 7 est dans un 7-Sylow par les théorèmes de Sylow, on voit qu'on obtient si $n_7 = 8$, $8 \times 6 = 48$ éléments d'ordre 7 (car tout élément non trivial d'un 7-Sylow est d'ordre 7, que ce sont les seuls éléments d'ordre 7 et que l'on n'a pas de redondance puisque $S_7 \cap S_7' = \{e\}$) dans G. Or, on sait qu'on a au moins un 2-Sylow de cardinal 8 qui fournit des éléments d'ordre une puissance de 2 et donc que l'on n'a pas encore comptés. On obtient ainsi $48 + 8 = 56$ éléments. On ne peut alors pas avoir de second 2-Sylow qui apporterait au moins un élément supplémentaire alors que $\#G = 56$. On en déduit que si $n_7 = 8$, alors $n_2 = 1$.
3. Soit $n_7 = 1$ et G possède un unique 7-Sylow distingué soit $n_7 = 8$ et $n_2 = 1$ et G possède un unique 2-Sylow distingué. Dans tous les cas, G possède un sous-groupe distingué non trivial et n'est donc jamais simple !

Exercice 10. 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[37], 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[38] $\#Z \in \{18, 36, 45, 90\}$. 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[39]. 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 11. Soient p et q deux nombres premiers distincts.

1. Soit G un groupe simple non abélien 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.

37. 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.

38. 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.

39. 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.

3. Montrer qu'un groupe d'ordre p^2q ou p^3q n'est pas simple. Classifier les groupes d'ordre p^2q.

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 $\#G \mid n_p!$.

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 [40].

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 $\psi(\mathbf{Z}/q\mathbf{Z})$ et $\varphi(\mathbf{Z}/q\mathbf{Z})$ 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

40. 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.

ont les mêmes valeurs propres [41] (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 [42] à $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ et est d'ordre p, ce qui est absurde. On a donc les cas suivants :

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 [43] $zx = x^{-1}z$ 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 [44] $(\mathbf{Z}/p\mathbf{Z})^2$, 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 $(\mathbf{Z}/p\mathbf{Z})^2 \rtimes \mathbf{Z}/q\mathbf{Z}$;

41. 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).

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

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

44. 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 $(\mathbf{Z}/p\mathbf{Z})^2$.

- 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.

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[45] $30 = 2 \times 3 \times 5$ 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 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
Et leur ordre se comptent, s'il le faut, un par un :

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

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. Soit $n \geqslant 1$. Montrer qu'il n'existe qu'un nombre fini de classes d'isomorphismes de groupes finis admettant exactement n classes de conjugaison.

Solution. Soit G un tel groupe. On considère l'action de G sur lui-même par conjugaison. Par hypothèse, on suppose qu'on a n orbites. On note $g_1, \dots, g_n$ un ensemble de représentants dans G et on notera $m_i = \#\mathrm{Stab}_G(g_i)$. L'équation aux classes fournit alors

$$1 = \sum_{i=1}^{n} \frac{1}{m_i}. \qquad (*)$$

Par ailleurs, il est clair que les m_i déterminent le cardinal de G (en effet, le plus grand des m_i vaut $\#G$ car le stabilisateur de 1 est G tout entier), il suffit alors de montrer que l'équation $(*)$ possède un nombre fini de solutions $m_i \in \mathbf{N}^*$.
Pour cela considérons l'équation

$$\sum_{i=1}^{n} \frac{1}{m_i} = A$$

pour $A \in \mathbf{Q}$ et notons $N(n, A)$ son nombre de solutions (éventuellement infini). Si $(m_1, \dots, m_n)$ est solution, on considère m_i le minimum des m_j. On a alors $\frac{1}{A} < m_i \leqslant \frac{n}{A}$ et $(m_j)_{j \neq i}$ est solution de

$$\sum_{\substack{j=1 \\ j \neq i}}^{n} \frac{1}{m_j} = A - \frac{1}{m_i}.$$

Il s'ensuit que

$$N(n, A) \leqslant \sum_{\frac{1}{A} < m \leqslant \frac{n}{A}} N\left(n-1, A - \frac{1}{m}\right).$$

Comme $N(1, A) \leqslant 1$ pour tout rationnel A, une récurrence immédiate assure que $N(n, A)$ est fini pour tout A rationnel.

3 Produit semi-direct

Exercice 1 — Produit semi-direct. Soient H et N deux groupes et soient φ et $\psi : H \to \mathrm{Aut}(N)$ des morphismes de groupes. 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. En déduire qu'il existe, à isomorphisme près, un unique produit semi-direct non trivial $(\mathbf{Z}/p\mathbf{Z})^2 \rtimes \mathbf{Z}/p\mathbf{Z}$, où p est un nombre premier impair.
5. Montrer que le centre de ce dernier groupe est isomorphe à $\mathbf{Z}/p\mathbf{Z}$.
6. Soit G un groupe d'ordre p^3 non cyclique et 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 $\langle x \rangle \cong \mathbf{Z}/p^2\mathbf{Z}$.
7. Décrire les classes d'isomorphismes de groupes de cardinal p^3 pour p premier impair.
Indication : On pourra raisonner suivant l'ordre maximal d'un élément du groupe.

Solution. Le produit semi-direct est un outil important de la classification des groupes finis à isomorphisme près (comme vous l'avez vu dans le cours pour les groupes d'ordre pq et comme on le verra avec ceux d'ordre p^3 dans cet exercice)! une idée de base dans la classification des groupes finis est de considérer G un groupe fini et tant que le groupe n'est pas simple, de prendre un sous-groupe H normal de G non trivial (distinct de $\{e\}$ et de G) et de considérer G comme une extension des deux groupes de cardinal strictement inférieur H et G/H, $1 \to H \to G \to G/H \to 1$. Si l'on sait classifier ces extensions et retrouver G à partir de H et G/H, on peut itérer le procédé pour étudier H et G/H. Ce procédé finit par s'arrêter lorsqu'on atteint des groupes finis simples. La classifications des groupes finis repose donc sur deux problèmes, celui de classifier les groupes finis simples et celui de classifier les extensions de groupes. Comme mentionné dans les compléments en fin d'exercice 11, on sait classifier tous les groupes finis simples (à isomorphisme près) mais malheureusement on ne sait pas classifier les extensions. Le produit semi-direct est une réponse partielle à ce problème de classification des extensions puisque vous avez vu dans le cours qu'il correspond au cas des extensions scindées. Dans ce cas, on sait reconstruire (à isomorphisme près) G comme le produit semi-direct de H par G/H. Un des problèmes avec le produit semi-direct est qu'il dépend du morphisme $\varphi : H \to \mathrm{Aut}(N)$ sous-jacent et il est alors intéressant d'avoir des critères pour déterminer pour deux tels morphismes φ et ψ quand les produits semi-directs correspondant sont isomorphes. Cela permettra en particulier d'en déduire qu'à isomorphisme près, le produit semi-direct non trivial $\mathbf{Z}_q\mathbf{Z} \rtimes \mathbf{Z}_p\mathbf{Z}$ pour p et q deux nombres premiers distincts tels que $p \mid q-1$ est unique (à isomorphisme prés).

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 $m \mid n$ (car il s'agit de groupes cycliques engendrés respectivement par $\varphi(h)$ et $\psi(h)$ si h est un générateur de H et alors puisque h est d'ordre n et que φ et ψ sont des morphismes de groupes, $\varphi(h)^n = \psi(h)^n = e$ et donc sont d'ordre divisant n). Il existe donc d premier à m tel que $\varphi(1) = d\psi(1)$ dans $\mathbf{Z}/m\mathbf{Z}$ (car dans $\mathbf{Z}/m\mathbf{Z}$, les générateurs sont les inversibles et $\varphi(1)$ et $\psi(1)$ sont deux générateurs de $\mathbf{Z}/m\mathbf{Z}$). L'application $(\mathbf{Z}/n\mathbf{Z})^\times \to (\mathbf{Z}/m\mathbf{Z})^\times$ qui à $\overline{k}$ associe $\overline{k}$ étant surjective (on l'admet pour l'instant et on le justifiera ci-dessous), il existe $d' \in (\mathbf{Z}/n\mathbf{Z})^\times$ qui s'envoie sur d (autrement dit, $d' \equiv d \mod m$). La multiplication par d' est alors un automorphisme de $\mathbf{Z}/n\mathbf{Z}$ (car on rappelle que $\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) \cong (\mathbf{Z}/n\mathbf{Z})^\times$ où tout automorphisme est de la forme $x \mapsto \ell x$ avec[46] $\ell \in (\mathbf{Z}/n\mathbf{Z})^\times$) qui vérifie $\varphi = \psi \circ \alpha$. En effet, pour tout $x \in \mathbf{Z}/n\mathbf{Z}$, on a (il suffit de vérifier que φ et $\psi \circ \alpha$ coïncident en $\overline{1}$ qui est un générateur de $\mathbf{Z}/n\mathbf{Z}$)

$$\psi \circ \alpha(\overline{1}) = \psi(d') = d'\psi(\overline{1})$$

car on a morphisme additif. Mais on arrive dans $\psi(H) = \varphi(H) = \mathbf{Z}/m\mathbf{Z}$. Ainsi, $d'x = dx$ car $d' \equiv d \mod m$ et $\psi \circ \alpha(\overline{1}) = \varphi(\overline{1})$. On conclut alors par **1.**

Une autre façon de voir les choses peut être de conserver les notations multiplicatives. On note $n = \#H$ et on pose h un générateur de H. On sait alors que $\psi(h)$ et $\varphi(h)$ engendrent le même groupe cyclique d'ordre $m \mid n$. On sait alors que $\psi(h) \in \langle \varphi(h) \rangle$ de sorte qu'il existe k entier tel que $\psi(h) = \varphi(h)^k$. Or, $\psi(h)$ a le même ordre que $\varphi(h)$ si bien qu'on a que k est premier à l'ordre[47] de $\varphi(H) = \psi(H)$, à savoir m. On constate alors que $\psi(h) = \varphi(h^k)$ et on a envie de poser

$$f : \left\{ \begin{array}{ccc} N \rtimes_\psi H & \longrightarrow & N \rtimes_\varphi H \\ (n,h) & \longmapsto & \left(n, h^k\right). \end{array} \right.$$

Le problème est que $h \mapsto h^k$ n'est pas un automorphisme de H (ce qui n'arrive que lorsque k est premier à l'ordre de H ce qui assure que h^k soit un générateur de H) car il n'y a aucune raison que k soit premier à n (l'ordre de H) s'il est premier à un diviseur m de n (penser à $k = 2$, $n = 12$ et $m = 3$). Une solution est alors de trouver k' premier à n de sorte que

$$f : \left\{ \begin{array}{ccc} N \rtimes_\psi H & \longrightarrow & N \rtimes_\varphi H \\ (n,h) & \longmapsto & \left(n, h^{k'}\right). \end{array} \right.$$

soit une bijection. Pour que cela reste un morphisme, on a besoin que $\psi(h) = \varphi(h)^{k'}$, ce qui est assuré dès que $k' \equiv k \mod m$. on cherche donc à nouveau à établir que l'application $(\mathbf{Z}/n\mathbf{Z})^\times \to (\mathbf{Z}/m\mathbf{Z})^\times$ qui à $\overline{k}$ associe[48] $\overline{k}$ est surjective lorsque $m \nmid n$. Démontrons donc cette surjectivité. Pour faire cela proprement, on écrit

$$m = \prod_{i=1}^{r} p_i^{\beta_i} \quad \text{et} \quad n = \prod_{i=1}^{r} p_i^{\alpha_i} \prod_{j=1}^{s} q_j^{\gamma_j}$$

pour des nombres premiers distincts $p_1, \dots, p_r, q_1, \dots, q_j$ et des entiers strictement positifs $\beta_i \leqslant \alpha_i$ et γ_j. Le théorème chinois garantit alors que

$$(\mathbf{Z}/n\mathbf{Z})^\times \cong \prod_{i=1}^{r} (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times \prod_{j=1}^{s} \left(\mathbf{Z}/q_j^{\gamma_j}\mathbf{Z}\right)^\times \quad \text{et} \quad (\mathbf{Z}/m\mathbf{Z})^\times \cong \prod_{i=1}^{r} \left(\mathbf{Z}/p_i^{\beta_i}\mathbf{Z}\right)^\times.$$

L'isomorphisme étant donné, si on dispose pour tout i de l'inverse p_i' de $\frac{n}{p_i^{\alpha_i}}$ modulo $p_i^{\alpha_i}$ (qui existe car ces deux entiers sont premiers entre eux et que l'on peut calculer par l'algorithme de Bézout étendu) et de même de l'inverse q_j' de $\frac{n}{q_j^{\gamma_j}}$ modulo $q_j^{\gamma_j}$ par

$$\left\{ \begin{array}{ccc} (\mathbf{Z}/n\mathbf{Z})^\times & \longrightarrow & \displaystyle\prod_{i=1}^{r} (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times \prod_{j=1}^{s} \left(\mathbf{Z}/q_j^{\gamma_j}\mathbf{Z}\right)^\times \\ \overline{x}^n & \longmapsto & \left(\overline{x}^{p_1^{\alpha_1}}, \dots, \overline{x}^{p_r^{\alpha_r}}, \overline{x}^{q_1^{\gamma_1}}, \dots, \overline{x}^{q_s^{\gamma_s}}\right) \end{array} \right.$$

de réciproque

$$\left\{ \begin{array}{ccc} \displaystyle\prod_{i=1}^{r} (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times \prod_{j=1}^{s} \left(\mathbf{Z}/q_j^{\gamma_j}\mathbf{Z}\right)^\times & \longrightarrow & (\mathbf{Z}/n\mathbf{Z})^\times \\ \left(\overline{x_1}^{p_1^{\alpha_1}}, \dots, \overline{x_r}^{p_r^{\alpha_r}}, \overline{y_1}^{q_1^{\gamma_1}}, \dots, \overline{y_s}^{q_s^{\gamma_s}}\right) & \longmapsto & \overline{\sum_{i=1}^{r} x_i p_i' \frac{n}{p_i^{\alpha_i}} + \sum_{j=1}^{s} y_j q_j' \frac{n}{q_j^{\gamma_j}}}^n \end{array} \right.$$

46. En effet, un automorphisme f de $\mathbf{Z}/n\mathbf{Z}$ cyclique est déterminé par l'image de la classe de 1 qui est nécessairement un inversible, disons $f(\overline{1}) = s$. En effet, pour un tel automorphisme f (donc un morphisme additif), on a

$$\forall k \in \mathbf{Z}n\mathbf{Z}, \forall x \in \mathbf{Z}/n\mathbf{Z} \quad f(kx) = kf(x)$$

et donc f est la mutliplication par s.Par ailleurs, puisqu'il existe g inverse de f tel que $g(f(\overline{1})) = \overline{1}$. On a donc $\overline{1} = g(s) = g(s \times \overline{1}) = sg(\overline{1})$ et $g(\overline{1})$ est l'inverse de s. Réciproquement, la multiplication par un élément inversible est immédiatement un automorphisme.

47. En effet, m est l'ordre de $\psi(h)$ si bien que pour tout $p \mid m$, $\psi(h)^{m/p} = \varphi(h)^{\frac{m}{p}k} \neq e$ si bien que $p \nmid k$.

48. Noter dans un premier temps que cette application est bien définie car si k est premier à n, il l'est avec m car $m \mid n$.

et de même pour $(\mathbf{Z}/n\mathbf{Z})^\times$. Ainsi, à travers ces isomorphismes, l'application $(\mathbf{Z}/n\mathbf{Z})^\times \to (\mathbf{Z}/m\mathbf{Z})^\times$ devient

$$\begin{cases} \prod_{i=1}^{r} (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times \prod_{j=1}^{s} (\mathbf{Z}/q_j^{\gamma_j}\mathbf{Z})^\times & \longrightarrow & \prod_{i=1}^{r} \left(\mathbf{Z}/p_i^{\beta_i}\mathbf{Z}\right)^\times \\ \left(\overline{x_1}^{p_1^{\alpha_1}}, \dots, \overline{x_r}^{p_r^{\alpha_r}}, \overline{y_1}^{q_1^{\gamma_1}}, \dots, \overline{y_s}^{q_s^{\gamma_s}}\right) & \longmapsto & \left(\overline{x_1 p_1' \frac{n}{p_1^{\alpha_1}}}^{p_1^{\beta_1}}, \dots, \overline{x_r p_r' \frac{n}{p_r^{\alpha_r}}}^{p_r^{\beta_r}}\right) = \left(\overline{x_1}^{p_1^{\beta_1}}, \dots, \overline{x_r}^{p_r^{\beta_r}}\right). \end{cases}$$

Il suffit donc de démontrer la surjectivité de cette application ci-dessus. On considère donc un élément $\left(\overline{x_1}^{p_1^{\beta_1}}, \dots, \overline{x_r}^{p_r^{\beta_r}}\right)$ dans $\prod_{i=1}^{r} \left(\mathbf{Z}/p_i^{\beta_i}\mathbf{Z}\right)^\times$. Cela implique en particulier que x_i est premier à p_i et donc en particulier que $x_i \in (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times$ (c'est l'avantage de s'être ramené à des puissances de nombres premiers!) et ainsi un antécédent est donné par $\left(\overline{x_1}^{p_1^{\alpha_1}}, \dots, \overline{x_r}^{p_r^{\alpha_r}}, \overline{1}^{q_1^{\gamma_1}}, \dots, \overline{1}^{q_s^{\gamma_s}}\right)$ et on a gagné! Pour vous faire un peu mieux une idée de ce qu'il se passe, on peut traiter le cas de $n = 24$ et $m = 4$ de sorte que l'application $(\mathbf{Z}/24\mathbf{Z})^\times \to (\mathbf{Z}/4\mathbf{Z})^\times$ de sorte que l'application correspondante (via le théorème chinois) devient

$$\begin{cases} (\mathbf{Z}/8\mathbf{Z})^\times \times (\mathbf{Z}/3\mathbf{Z})^\times & \longrightarrow & (\mathbf{Z}/4\mathbf{Z})^\times \\ \left(\overline{x}^8, \overline{y}^3\right) & \longmapsto & \overline{x}^4. \end{cases}$$

On peut alors relever $3 \in (\mathbf{Z}/4\mathbf{Z})^\times$ par $\left(\overline{3}^8, \overline{1}^3\right) \in (\mathbf{Z}/8\mathbf{Z})^\times$. Pour savoir à quel élément cela correspond pour notre problème de départ (à savoir dans $(\mathbf{Z}/24\mathbf{Z})^\times$), on sait que $3 \times 3 - 8 = 1$ de sorte que l'isomorphisme $(\mathbf{Z}/8\mathbf{Z})^\times \times (\mathbf{Z}/3\mathbf{Z})^\times \to (\mathbf{Z}/24\mathbf{Z})^\times$ est donné par $\left(\overline{x}^8, \overline{y}^3\right) \mapsto \overline{9x - 8y}^{24}$ et un antécédent de 3 (qui n'est pas premier à 24) est alors donné par $9 \times 3 - 8 = 19$ qui est bien inversible modulo 24 (car premier à 24) et vérifie que $19 \equiv 3 \mod 4$. On ne pouvait pas raisonner de même avec m et $\frac{n}{m}$ car ces deux entiers ne sont pas nécessairement premiers entre eux.

► **Complément. –** Si N est abélien et qu'il existe un isomorphisme $f : N \rtimes_\psi H \to N \rtimes_\varphi H$ tel que $f(N) = N$, on peut alors montrer qu'il existe $u \in \mathrm{Aut}(N)$ et $\alpha \in \mathrm{Aut}(H)$ tels que

$$\forall h \in H, \quad \varphi \circ \alpha(h) = u \circ \psi(h) \circ u^{-1}.$$

L'application $u = f_{|N}$ est un automorphisme de N et f induit un isomorphisme[49] $\tilde{f} : N \rtimes_\psi H/N \cong H \to N \rtimes_\varphi H/N \cong H$ 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

$$u \circ \psi(h) \circ u^{-1}(n) = f(1,h)f(f^{-1}(n),1)f(1,h^{-1}) = f(1,h)(n,1)f(1,h^{-1}).$$

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**. Cela fournit une sorte de réciproque partielle aux questions **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

49. On a un morphisme $N \rtimes H \to H$ 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 $(1,\alpha(h))$.

classes d'isomorphismes de produits semi-directs avec le groupe cyclique infini[50] $\mathbf{Z}$. Une application de cette question **3.** consiste à établir que pour p et q deux nombres premiers distincts avec $p \mid q-1$, alors on a un unique produit semi-direct non trivial $\mathbf{Z}/q\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}$. En effet, si l'on se donne deux morphismes non triviaux $\varphi, \psi : \mathbf{Z}/p\mathbf{Z} \to \text{Aut}\left(\mathbf{Z}/q\mathbf{Z}\right) \cong \left(\mathbf{Z}/q\mathbf{Z}\right)^\times \cong \mathbf{Z}/(q-1)\mathbf{Z}$, alors on applique **3.** avec $H = \mathbf{Z}/p\mathbf{Z}$ cyclique. Le fait que les morphismes soient non triviaux implique que $\varphi(H)$ et $\psi(H)$ sont des sous-groupes d'ordre p du groupe cyclique $\mathbf{Z}/(q-1)\mathbf{Z}$. Or, un tel groupe admet un unique sous-groupe d'ordre p d'après le cours donc $\varphi(H) = \psi(H)$.

4. On rappelle que $\#\text{GL}_2(\mathbf{F}_p) = (p^2-1)(p^2-p) = p(p-1)^2(p+1)$ donc les p-Sylow de $\text{GL}_2(\mathbf{F}_p)$ sont d'ordre p et tous conjugués[51]. Un produit semi-direct non trivial $\left(\mathbf{Z}/p\mathbf{Z}\right)^2 \rtimes \mathbf{Z}/p\mathbf{Z}$ est la donnée d'un morphisme $\varphi : \mathbf{Z}/p\mathbf{Z} \to \text{Aut}\left(\left(\mathbf{Z}/p\mathbf{Z}\right)^2\right)$ non trivial. Or, dans $\left(\mathbf{Z}/p\mathbf{Z}\right)^2$, tous les éléments vérifient $g^p = e$ et un raisonnement identique à celui de l'exercice permet de munir $\left(\mathbf{Z}/p\mathbf{Z}\right)^2$ d'une structure d'espace vectoriel sur le corps $\mathbf{Z}/p\mathbf{Z}$ tel que tout automorphisme de groupe corresponde à un isomorphisme d'espace vectoriel. Il s'ensuit que $\text{Aut}\left(\left(\mathbf{Z}/p\mathbf{Z}\right)^2\right) \cong \text{GL}_2\left(\mathbf{Z}/p\mathbf{Z}\right)$. Par simplicité de $\mathbf{Z}/p\mathbf{Z}$, un tel morphisme est injectif et les images de ψ et φ (qui sont des sous-groupes d'ordre p de $\text{GL}_2\left(\mathbf{Z}/p\mathbf{Z}\right)$) sont des p-Sylow et par conséquent conjugués par une matrice $P \in \text{GL}_2(\mathbf{F}_p)$. Notons que

$$\psi^{(P)} : \left\{ \begin{array}{ccc} \mathbf{F}_p & \longrightarrow & \varphi(\mathbf{F}_p) \\ x & \longmapsto & P^{-1}\psi(x)P \end{array} \right.$$

est un isomorphisme. Dès lors[52], $\varphi^{-1} \circ \psi^{(P)}$ 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 que $\psi = P\varphi^k P^{-1}$ où $\varphi^k(x) = \varphi(kx)$. Les questions **1.** et **2.** permettent alors de conclure que $\left(\mathbf{Z}/p\mathbf{Z}\right)^2 \rtimes_\varphi \mathbf{Z}/p\mathbf{Z} \cong \left(\mathbf{Z}/p\mathbf{Z}\right)^2 \rtimes_\psi \mathbf{Z}/p\mathbf{Z}$. On a donc obtenu l'unicité. Quant à l'existence, comme $\text{Aut}\left(\left(\mathbf{Z}/p\mathbf{Z}\right)^2\right) \cong \text{GL}_2(\mathbf{F}_p)$, l'existence d'un tel produit semi-direct non trivial qui correspond à un morphisme non trivial $\mathbf{Z}/p\mathbf{Z} \to \text{GL}_2(\mathbf{F}_p)$ permet de conclure (il suffit de considérer l'inclusion d'un p-Sylow, qui sera isomorphe à $\mathbf{Z}/p\mathbf{Z}$).

5. On a affaire à un p-groupe dont le centre est non trivial. Ainsi, le centre de $\left(\mathbf{Z}/p\mathbf{Z}\right)^2 \rtimes \mathbf{Z}/p\mathbf{Z}$ 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 $\mathbf{Z}/p\mathbf{Z}$.

6. Le sous-groupe $\langle x \rangle$ est d'indice p donc l'exercice 5 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 $y \in G \smallsetminus \langle x \rangle$. 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 $y^p = x^{pk}$ (car $y^p = x^\ell$ et $y^{p^2} = x^{p\ell} = e$) donc $p \mid \ell$ et $\ell = pk$). 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 $z \in G \smallsetminus \langle x \rangle$ 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. Si l'on suppose dans un premier temps que $r \not\equiv 1$ modulo p, alors $S \equiv 1$ modulo p, auquel cas l'équation admet immédiatement une solution n_0 puisque S est alors inversible modulo p^2. Sinon, $r \equiv 1$ modulo p et 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 donc $S \equiv p$ modulo p^2 et on voit qu'on peut à nouveau trouver une solution n_0 car la condition devient $p \mid k + n\frac{S}{p}$ avec $\frac{S}{p}$ inversible modulo p. On a donc $z = yx^{n_0} \in G \smallsetminus \langle x \rangle$ est d'ordre p. On a donc par propriété du produit semi-direct[53] que $G = \langle x \rangle \rtimes \langle z \rangle \cong \mathbf{Z}/p^2\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}$.

---

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

51. 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 sait que cela est équivalent (si elle est distincte de l'identité) 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

$$\left\{ \begin{array}{l} ad - bc = 1 \\ a + d = 2. \end{array} \right.$$

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 $\text{GL}_2(\mathbf{F}_p)$.

52. On utilise ici le fait que $\varphi : \mathbf{F}_p \to \varphi(\mathbf{F}_p)$ est un isomorphisme.

53. En effet, $\langle x \rangle \cap \langle z \rangle = \{e\}$. Sinon, il existe un élément non trivial de $\langle x \rangle$ appartenant à $\langle z \rangle$. Mais puisque $\langle x \rangle$ est d'ordre p, tout élément non trivial est de la forme x^k

7. 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 $\psi : \mathbf{Z}/p\mathbf{Z} \to \mathsf{Aut}(\mathbf{Z}/p^2\mathbf{Z}) \cong \mathbf{Z}/p(p-1)\mathbf{Z}$. Le groupe cyclique $\mathbf{Z}/p(p-1)\mathbf{Z}$ admet un unique sous-groupe d'ordre p donc on conclut à l'unicité comme dans le cas des groupes d'ordre pq en utilisant la question **3.** Cela 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 [54]) est distingué (car d'indice p) et isomorphe à $(\mathbf{Z}/p\mathbf{Z})^2$ et tout élément du complémentaire est d'ordre p, le critère du cours assure alors 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 2. Soit p un nombre premier impair.

1. Déterminer les p-Sylow de $\mathsf{GL}_2(\mathbf{F}_p)$.

2. Soient φ et ψ des morphismes non triviaux de $\mathbf{F}_p$ dans $\mathsf{GL}_2(\mathbf{F}_p)$. 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 $P \in \mathsf{GL}_2(\mathbf{F}_p)$ 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 $\#\mathsf{GL}_2(\mathbf{F}_p) = (p^2-1)(p^2-p) = p(p-1)^2(p+1)$ donc les p-Sylow de $\mathsf{GL}_2(\mathbf{F}_p)$ 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 $\mathsf{GL}_2(\mathbf{F}_p)$.

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 $P \in \mathsf{GL}_2(\mathbf{F}_p)$. 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, $\varphi^{(P)} \circ \psi$ 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.

avec k premier à p (que l'on peut choisir entre 1 et $p-1$). On a alors par Bézout, deux entiers u et v tels que $ku + pv = 1$ et puisque $x^k \in \langle z \rangle$, il existe ℓ tel que $x^k = x^\ell$. On élève alors à la puissance u de sorte que $x^{ku} = z^{\ell u}$ mais $x^{ku} = x^{1-pv} = x$ car $x^p = 1$. On aurait donc $x = x^{ku} = z^{\ell u} \in \langle z \rangle$, ce qui est exclu ! Noter que l'on a utilisé de façon cruciale le fait que $\langle x \rangle$ était d'ordre premier. Par exemple, dans le groupe $\mathbf{D}_4$, $\langle \rho \rangle \cap \langle -\mathsf{Id} \rangle = \langle -\mathsf{Id} \rangle \neq \{e\}$.

54. On peut en effet 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). Pour ce faire, 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.

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 qui correspond à un morphisme non trivial $\mathbf{Z}/p\mathbf{Z} \to \mathrm{GL}_2(\mathbf{F}_p)$ et la question **2.** combinée à l'exercice 8 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 $y \in G \smallsetminus \langle x\rangle$. 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 $z \in G \smallsetminus \langle x\rangle$ d'ordre p. Cherchons z sous la forme $z = yx^n$. Ainsi $z^p = (yx^n)^p = yx^nyx^n\cdots yx^n$ 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

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

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 $z = yx^{n_0} \in G \smallsetminus \langle x\rangle$ 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 :

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

4 Pour celles et ceux qui veulent aller plus loin...

Exercice 1.

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 : $\mathbf{Z}/11\mathbf{Z}$;
   - 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 2 — 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. 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. Le corrigé de cette question sera disponible après le DM I.

2. Le corrigé de cette question sera disponible après le DM I.

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 $\sigma_2, \ldots, \sigma_k \in \mathfrak{S}_n(i)$. 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 $k \in \{1, \ldots, n\}$, 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. (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 $g_1, \ldots, g_m$ une famille génératrice de G. Alors $\pi(g_1), \ldots, \pi(g_m)$ engendrent $G/\Phi(G)$ donc[55] $m \geqslant \dim_{\mathbf{F}_p}(G/\Phi(G))$. 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 $\Phi(\mathbf{Z}/p\mathbf{Z}) = \{0\}$.

55. Le r de la question précédente.

Exercice 3. 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[56] $n \geqslant 4$ puisque tout automorphisme de $\mathfrak{S}_n$ avec $n \leqslant 3$ est intérieur[57]. Le groupe $\mathfrak{S}_n$ est engendré par les transpositions[58] $\tau_i = (1i)$ 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 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 $n = 6$.

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

57. 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.

58. 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 $(ij) = (1i)(1j)(1i)$.

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[59] 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 $\mathrm{Aut}(\mathfrak{S}_6)$. 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.

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