Feuille TD 1 – Correction – Groupes

Exercice 1 — 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 [1] 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 $\mathfrak{A}_4$.
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.

Solution.

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 [2] 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 :

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

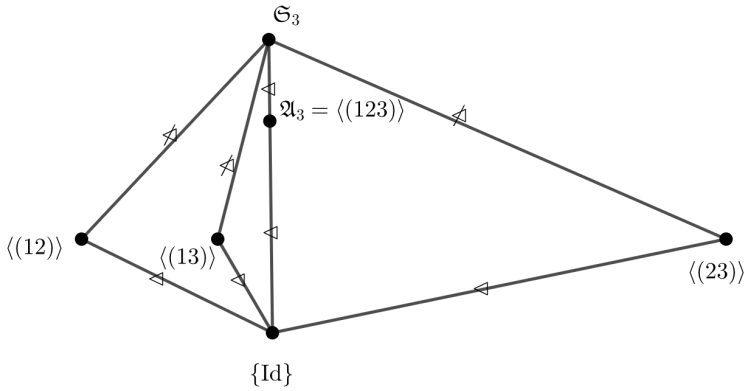
On obtient par le théorème de Lagrange que $g(n) \mid n!$ et g est croissante puisque toute permutation de $\mathfrak{S}_n$ peut être vue comme une permutation de $\mathfrak{S}_k$ pour $k \geqslant n$. On a par exemple

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 [3] a démontré [4] en 1903 l'équivalent

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

2. On obtient facilement le treillis suivant [5]



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 $\langle(ab)\rangle = \{\mathrm{Id}, (ab)\}$ 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 $\langle(abc)\rangle = \{\mathrm{Id}, (abc), (acb)\}$ si bien qu'on a un unique sous-groupe d'ordre 3, à savoir

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

1. 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 $H_2 \subseteq H_1$.
2. 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.
3. On appelle d'ailleurs classiquement cette fonction g la fonction de Landau.
4. En utilisant des résultats d'arithmétique notamment sur la répartition des nombres premiers.
5. Cela se révélera utile quand on verra la théorie de Galois mais aussi dans le cours de géométrie du second semestre quand on classifiera les revêtements galoisiens.! Un treillis est un objet mathématique qui a une définition précise comme ensemble ordonné avec certaines bonnes propriétés qu'on ne précisera pas ici !

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 [6] dans $\mathfrak{S}_3$.
Passons à $\mathfrak{A}_4$. On sait que

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

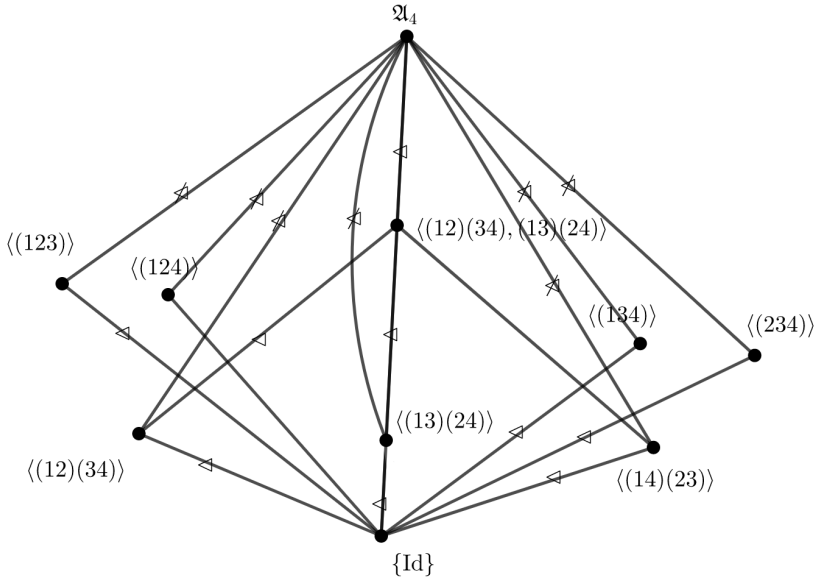
De plus, $\#\mathfrak{A}_4 = 12$ donc les sous-groupes non triviaux sont d'ordre 6, 4, 3 ou 2. Or, on sait qu'un sous-groupe d'ordre 6 [7] est soit cyclique soit isomorphe à $\mathfrak{S}_3$. Ici la seule option serait $\mathfrak{S}_3$ car on n'a pas d'élément d'ordre 6 mais dans $\mathfrak{S}_3$ aucune paire d'éléments d'ordre 2 ne commutent tandis qu'ici tous les éléments d'ordre 2 commutent [8]

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

Pour les groupes d'ordre 4, on a deux possibilités [9] $\mathbf{Z}/4\mathbf{Z}$ 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 :



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 [10], 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 [11] du fait que

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

6. On pouvait le déduire sans calcul des théorèmes de Sylow, puisque ces sous-groupes d'ordre 2 sont les 2-Sylow de $\mathfrak{S}_3$.

7. Soit G d'ordre 6. Si G est abélien, G admet nécessairement un élément d'ordre 2 et un élément d'ordre 3 (par exemple par le lemme de Cauchy ou bien en raisonnant par l'absurde et en aboutissant à une contradiction sur le cardinal si tous les éléments distincts de l'identité sont d'ordre 2 ou d'ordre 3 ou bien en utilisant les théorèmes de Sylow). Le produit de ces deux éléments est alors d'ordre 6 (le groupe est abélien et les ordres sont premiers entre eux) et donc $G \cong \mathbf{Z}/6\mathbf{Z} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$. Si maintenant G n'est pas commutatif, de la même façon G admet un élément σ d'ordre 3 et un élément τ d'ordre 2 qui ne commutent pas (sinon G serait abélien) et qui engendrent G. Les éléments de G sont donc Id, $\sigma, \sigma^2, \tau, \tau\sigma, \sigma\tau$. On ne peut pas avoir $\tau\sigma\tau = \sigma$ car sinon G est abélien, ni Id ni τ ni $\tau\sigma$ ni $\tau\sigma^2$ donc $\tau\sigma\tau = \sigma^2$ et on peut en déduire la table de multiplication de G qui est la même que celle de $\mathfrak{S}_3$ si bien que $G \cong \mathfrak{S}_3$.

8. Une autre méthode est donnée dans l'exercice 8.

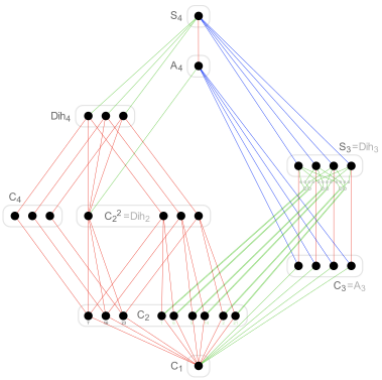
9. Soit G d'ordre 4. Par le théorème de Lagrange, un élément non trivial de G est d'ordre 2 ou 4. Si on a un élément d'ordre 4, alors G est cyclique, isomorphe à $\mathbf{Z}/4\mathbf{Z}$. Sinon, tous les éléments non triviaux sont d'ordre 2 et on peut soit utiliser l'exercice 3 soit raisonner à la main. On dispose dans G de e et de x d'ordre 2. Pour obtenir 4 éléments, on doit avoir également un élément $y \neq x$ d'ordre 2 et comme G est un groupe, on a aussi xy. Comme on e 4 éléments, on a tous les éléments de G. Mais $yx \in G$ et cet élément est distinct de e, de x et de y donc $yx = xy$ et G est commutatif. On obtient alors la table de multiplication de G et on reconnaît le groupe $(\mathbf{Z}/2\mathbf{Z})^2$. On rappelle par ailleurs que grâce au théorème de Lagrange, tout groupe d'ordre p premier est cyclique (et donc abélien) siomorphe à $\mathbf{Z}/p\mathbf{Z}$.

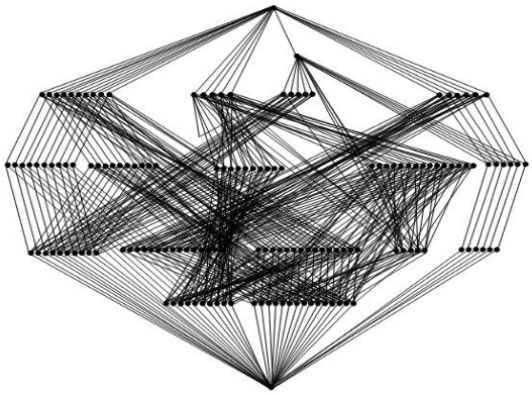
10. On peut là encore le voir grâce aux théorèmes de Sylow avec les 3-Sylows de $\mathfrak{A}_4$.

11. Plus généralement, c'est aussi une conséquence de la question suivante.

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 et pas moins de 156 sous-groupes dans le cas de $\mathfrak{S}_5$:





► **Compléments . –** On a ainsi la classification à isomorphisme près des groupes d'ordre $\leqslant 11$ (sauf le cas d'ordre 8 qui découlera de l'exercice 7).

- 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 $G \cong \mathbf{Z}/p\mathbf{Z}$. Cela résout les cas $2, 3, 5, 7, 11$;
- Si G est d'ordre 4, on a vu 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) ;
- Si G est d'ordre 6, on a vu que $G \cong \mathbf{Z}/6\mathbf{Z}$ si G contient un élément d'ordre 6 (ou deux éléments d'ordre 2 et 3 respectivement qui commutent) et sinon [12] $G \cong \mathfrak{S}_3$ et G est engendré par un élément d'ordre 2 τ et un élément d'ordre 3 σ tels que $\tau\sigma\tau = \sigma^2$;
- Si G est d'ordre $9 = 3^2$, le cours garantit 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 garantit que G est abélien et isomorphe à $\mathbf{Z}/10\mathbf{Z} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$.

Pour aller plus loin, je vous renvoie aux feuilles de TD des annés précédentes, on peut classifier les groupes d'ordre p^2q avec p et q deux nombres premiers disctincts 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 ! On remarquera donc qu'il y a quelque chose qui semble se passer pour les groupes d'ordre 8 ou 12 (on a plus de travail et plus de classes d'isomorphismes). On peut aussi classifier [13] (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 [14] $2^{10} = 1024$. En fait, on conjecture que presque tous les groupes finis sont des 2-groupes dans le sens où

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

et même

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

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

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

12. 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.

13. Voir les feuilles de TD de l'an dernier.

14. Voir Besche, Eick et O'Brien, *The groups of order at most 2000*.

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 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 $\lambda_1, \lambda_2, \dots, \lambda_r$. Par exemple, dans $\mathfrak{S}_4$, la classe de conjugaison des doubles transpositions [15] 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 $Z_{\mathfrak{A}_n}(\sigma) \subseteq Z_{\mathfrak{S}_n}(\sigma)$ strictement et il existe $\mu \in \mathfrak{S}_n \smallsetminus \mathfrak{A}_n$ tel que $\mu\sigma\mu^{-1} = \sigma$. Alors, le groupe alterné étant d'indice 2, il existe $\tau \in \mathfrak{S}_n \smallsetminus \mathfrak{A}_n$ tel que $\mathfrak{S}_n = \mathfrak{A}_n \sqcup \mathfrak{A}_n\tau$ et $\mu = \mu'\tau$ si bien que

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

sont deux bijections qui montrent que $Z_{\mathfrak{S}_n}(\sigma) = Z_{\mathfrak{A}_n}(\sigma) \sqcup \left\{\mu \in \mathfrak{S}_n \smallsetminus \mathfrak{A}_n \ : \ \mu\sigma\mu^{-1} = \sigma\right\}$ avec

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

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, on choisit i et j apparaissant successivement dans un même cycle dans la décomposition de σ et on voit que $(i\ j)\sigma(i\ j)$ est conjugué à σ dans $\mathfrak{S}_n$ mais pas dans $\mathfrak{A}_n$. 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 $Z_{\mathfrak{S}_n}(\sigma) = Z_{\mathfrak{A}_n}(\sigma)$. Alternativement, si σ comporte deux cycles $c = (a_1, \dots, a_k)$ et $c' = (a'_1, \dots, a'_k)$ 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 $Z_{\mathfrak{S}_n}(\sigma) = Z_{\mathfrak{A}_n}(\sigma)$.

Montrons pour finir que tout sous-groupe H de $\mathfrak{S}_n$ d'indice n est isomorphe à $\mathfrak{S}_{n-1}$.
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 [16]

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

15. C'est aussi un exercice intéressant de les dénombrer et on obtient que le cardinal correspondant à une partition $\boldsymbol{\lambda}$ vaut

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

où $a_j(\boldsymbol{\lambda})$ désigne le nombre de λ_k égaux à i. On fait 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.

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

Or, $\#H = (n-1)!$ et $(n-1)! < n!/2$ (car $2 < n$) si bien que nécessairement $\mathrm{Ker}(\psi) = \{\mathrm{Id}\}$ 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 — 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 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.

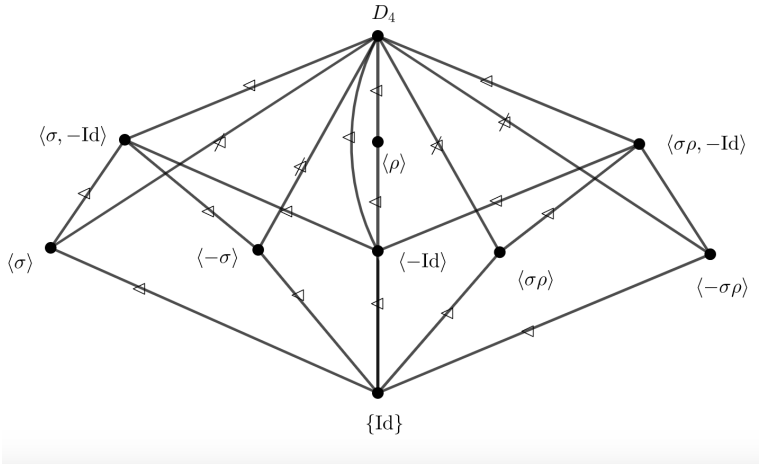
1. Calculer l'ordre de σ et de ρ. Décrire l'isométrie $\sigma\rho\sigma^{-1}$.
2. Montrer que $\mathbf{D}_4$ contient 8 éléments ; caractériser ces éléments géométriquement.
3. Déterminer les classes de conjugaison dans $\mathbf{D}_4$.
4. Donner le treillis des sous-groupes de $\mathbf{D}_4$, en précisant les sous-groupes distingués.

Solution.

1. On vérifie aisément [17] 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 [18] : 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

17. Soit géométriquement soit via les matrices.

18. 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 $\langle\rho\rangle$).

► **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

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

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 ets 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.
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!

Exercice 3 — 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.
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.

2. - *Méthode 1 :* Puisque G est fini, il admet une partie génératrice minimale[19], disons $\{g_1, \dots, g_n\}$. 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
$$G = \{g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n} \ : \ \varepsilon_1, \varepsilon_2, \dots, \varepsilon_n \in \{0,1\}\}.$$
Cela donne envie de poser
$$f : \left\{ \begin{array}{ccc} (\mathbf{Z}/2\mathbf{Z})^n & \longrightarrow & G \\ (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) & \longmapsto & g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n}. \end{array} \right.$$
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 $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) \neq (0, 0, \dots, 0)$ 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 $\{g_2, \dots, g_n\}$ est une partie génératrice de G, contredisant la minimalité de $\{g_1, g_2, \dots, g_n\}$. Cela démontre l'injectivité et donc f est un isomorphisme qui permet de conclure !
- *Méthode 2 :* On considère $(G, +)$ muni d'une loi additive[20] 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[21] $G \cong (\mathbf{Z}/2\mathbf{Z})^n$, 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[22] 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 $\mathrm{GL}_p(\mathbf{F}_p)$ 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, $M^p = I_p$.

Exercice 4 — 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).

19. 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.
20. 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 $+$.
21. Noter qu'une base étant une famille génératrice minimale, on fait en fait la même chose que dans la première méthode !
22. On dit qu'un groupe G est d'exposant e si pour tout $g \in G$, $g^e = 1$.

► **Remarque . –** Noter que la forme d'un élément de G, par définition du fait que S engendre G donne immédiatement une application f surjective[23] de $E = \{(x_1, \dots, x_r) \in S \cup S^{-1} \ : \ r \in \mathbf{N}\}$ (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 5. Soient G un groupe et H un sous-groupe de G d'indice fini m. On note G/H l'ensemble[24] des classes à gauche de G modulo H. Pour $g \in G$, on note $h_g : G/H \to G/H$ l'application $aH \mapsto gaH$.

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

Solution.

1. Il est clair que h_g est injective car si $gaH = ga'H$, alors $a^{-1}a' \in H$ et $aH = a'H$ et de même pour la surjectivité[25] car $h_g(g^{-1}aH) = aH$. On a donc bien une bijection. Le fait qu'on ait un morphisme est clair aussi car $h_g \circ h_{g'} = h_{gg'}$. On fait en réalité ici agir G sur G/H par translation à gauche.
2. Attention ici qu'on n'a pas supposé G fini et donc $[G : \mathrm{Ker}(h)]$ n'est pas donné par $\#G/\#\mathrm{Ker}(h)$. Le théorème de factorisation fournit un morphisme injectif $\tilde{h} : G/\mathrm{Ker}(h) \to \mathfrak{S}(G/H) \cong \mathfrak{S}_m$. On peut ainsi identifier $G/\mathrm{Ker}(h)$ à un sous-groupe de $\mathfrak{S}_m$ et en déduire par Lagrange que $[G : \mathrm{Ker}(h)] \mid m!$.
3. Soit $g \in \mathrm{Ker}(h)$. On a alors pour tout $a \in G$, $gaH = aH$ qui implique immédiatement que $g \in H$. On peut aussi utiliser le résultat rappelé dans le complément page 4 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
$$\mathrm{Ker}(h) = \bigcap_{x \in X} \mathrm{Stab}_G(x).$$
Or, ici on obtient immédiatement par double inclusion que $\mathrm{Stab}_G(aH) = aHa^{-1}$ de sorte que
$$\mathrm{Ker}(h) = \bigcap_{a \in G} aHa^{-1} \subseteq H.$$
4. On considère de façon analogue $h_2 : H \to \mathfrak{S}(G/H \setminus \{H\})$ définie pour $g \in H$ par
$$h_2(g) : \begin{array}{ccc} G/H \setminus \{H\} & \longrightarrow & G/H \setminus \{H\} \\ aH & \longmapsto & gaH. \end{array}$$
On vérifie de même qu'il s'agit bien d'une bijection bien définie et que h_2 est un morphisme de groupes de même noyau que h. Le même raisonnement qu'en question **2.** fournit alors la conclusion souhaitée $[H : \mathrm{Ker}(h)] \mid (m-1)!$ car $\mathfrak{S}(G/H \setminus \{H\}) \cong \mathfrak{S}_{m-1}$. En fait, on a restreint l'action précédente en une action de H sur G/H et utilisé le fait que puisque H est un point fixe de G/H pour cette action, cela donne lieu à une action de H sur $G/H \setminus \{H\}$ de même noyau que h. 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 $X \setminus \{x_0\}$. En effet, si $x \in X \setminus \{x_0\}$, alors pour tout $g \in G$, $g \cdot x \in X \setminus \{x_0\}$ car sinon $g.x = x_0$ et donc en faisant agir g^{-1}, $x = g^{-1} \cdot x_0$ mais $g^{-1} \cdot x_0$, 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 $X \setminus \{x_0\}$ un morphisme $h_2 : G \to \mathfrak{S}(X \setminus \{x_0\})$ et
$$\mathrm{Ker}(h) = \bigcap_{x \in X} \mathrm{Stab}_G(x) = \bigcap_{x \in X \setminus \{x_0\}} \mathrm{Stab}_G(x)$$
car par définition, $\mathrm{Stab}_G(x_0) = G$. Or,
$$\mathrm{Ker}(h_2) = \bigcap_{x \in X \setminus \{x_0\}} \mathrm{Stab}_G(x) \quad \text{de sorte que} \quad \mathrm{Ker}(h) = \mathrm{Ker}(h_2).$$

23. Qui à un élément de $\{(x_1, \dots, x_r) \in S \cup S^{-1} \ : \ r \in \mathbf{N}\}$ associe $x_1 x_2 \cdots x_r$.
24. Qui n'est pas un groupe en général.
25. On pouvait aussi conclure par cardinalité ou exhiber l'inverse de h_g donné par $h_{g^{-1}}$.

▶ **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) $f : G/\mathsf{Ker}(h) \to G/H$ qui à $g\mathsf{Ker}(h)$ associe gH est bien définie et passe au quotient pour la relation donnée par le groupe $H/\mathsf{Ker}(h)$ 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** $G/\mathsf{Ker}(h) \cong G/H \times H/\mathsf{Ker}(h)$ obtenue, on peut alors dire que $[G : \mathsf{Ker}(h)] = [G : H] \times [H : \mathsf{Ker}(h)]$ et donc $[G : H] \times [H : \mathsf{Ker}(h)] = m \times [H : \mathsf{Ker}(h)] \mid m!$ et finalement $[H : \mathsf{Ker}(h)] \mid (m-1)!$.

5. On a $m = 2$ et la question **4.** fournit alors que $[H : \mathsf{Ker}(h)] = 1$ soit $H = \mathsf{Ker}(h)$. 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.**
6. On a donc que G et H sont finis de cardinal une puissance de p. Par **4.**, on a donc $\#H \mid (p-1)!\#\mathsf{Ker}(h)$. Mais $\#H$ est premier avec $(p-1)!$ donc $\#H \mid \#\mathsf{Ker}(h)$ et la question **3.** permet alors de conclure à nouveau à l'égalité $H = \mathsf{Ker}(h)$. 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.**
7. De même, $\#H \mid (m-1)!\#\mathsf{Ker}(h)$ 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 $\mathfrak{S}_4$.

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

Solution.

1. Faisant agir G sur G/H, on obtient un morphisme $f : G \to \mathfrak{S}(G/H) \cong \mathfrak{S}_n$ dont le noyau convient exactement de la même manière que dans l'exercice **5.**
2. On a clairement que[26]
$$\bigcup_{g \in G} gHg^{-1} = \bigcup_{\overline{g} \in G/H} gHg^{-1}.$$

26. 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
$$\mathfrak{S}_3 = \mathfrak{A}_3 \cup \langle (12) \rangle \cup \langle (13) \rangle \cup \langle (23) \rangle \quad \text{ou} \quad \mathbf{F}_2^2 = \mathsf{Vect}(1,0) \cup \mathsf{Vect}(0,1) \cup \mathsf{Vect}(1,1).$$
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 $x \in F_n \setminus F_1 \cup F_2 \cup \cdots \cup F_{n-1}$ 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 $\lambda x + y \in F_i$, ce qui vient contredire le caractère infini du corps k.

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

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

3. On dispose toujours de l'action de G sur G/H qui fournit un morphisme $\varphi : G\to\mathfrak{S}(G/H)$ avec $\mathfrak{S}(G/H)$ un groupe fini. On note alors K le sous-groupe de $\mathfrak{S}(G/H)$ des bijections fixant H et on a alors que $\varphi(H)$ est un sous-groupe de K. Par ailleurs, la transitivité de l'action garantit que $\varphi(G)$ n'est pas contenu dans K (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

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

4. 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[27] 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[28] 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[29], 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.

5. 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

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

27. 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.
28. On dit que le groupe $GL_n(\mathbf{C})$ est *divisible*.
29. 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.

6. Par **1.**, H contient un sous-groupe distingué K de $\mathfrak{S}_k$ d'indice divisant $[\mathfrak{S}_k : H]!$. Comme H n'est pas d'indice 1, ce groupe ne peut pas être $\mathfrak{S}_k$ tout entier sinon $H = \mathfrak{S}_k$ serait d'indice 1. Ce sous-groupe est donc (puisque $k \geqslant 5$) soit le groupe trivial soit le groupe alterné. Supposons qu'il s'agisse du groupe trivial. On a alors que $k!$ divise $[\mathfrak{S}_k : H]! \in \{2!, \dots, (k-1)!\}$ ce qui est absurde donc $K = \mathfrak{A}_k$ et $K \subseteq H$ donc $[G : H] \leqslant [G : K]$ si bien que $[G : H] = 2$ et $H = \mathfrak{A}_k$ puisque le seul[30] 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[31] 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 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 $M_{a,b} = M_{\frac{\bar{a}}{|a|^2+|b|^2},-\frac{b}{|a|^2+|b|^2}}$ 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[32] 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 $\mathbf{H}_8^{\mathrm{ab}} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

30. 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.

31. 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!

32. 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 $\mathbf{H}_8/H$.

▶ **Compléments. –** Noter que les quaternions fournissent un exemple[33] 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 !

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 $s \in G \smallsetminus R$ 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 $G \smallsetminus R$ 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.

33. Et oui, encore !

Exercice 9. Soient p un nombre premier et G un p-groupe fini. Soit $(A,+)$ un groupe abélien avec $A \neq \{0\}$. On suppose donnée une action de G sur A par automorphismes, c'est-à-dire que pour tout $g \in G$, la bijection $x \mapsto g \cdot x$ de A dans A est un automorphisme du groupe abélien A. On suppose de plus que A est *de torsion p-primaire, i.e.* pour tout $x \in A$, il existe $m \in \mathbf{N}$ tel que $p^m x = 0$.

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

Solution.

1. L'hypothèse est que tout élément est d'ordre une puissance de p. Le théorème de structure des groupes abéliens finis garantit que
$$G \cong \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_r\mathbf{Z}$$
avec $d_1 \mid \cdots \mid d_r$. Si maintenant un des d_i possède un autre facteur premier que p, disons q, alors on sait que G va contenir un élément d'ordre q ce qui est absurde. D'où, tous les d_i sont des puissances de p et G est un p-groupe.
On peut aussi raisonner par l'absurde. Supposons qu'il existe un nombre premier $q \neq p$ divisant le cardinal de A. On sait alors qu'il existe q-Sylow S de A. On considère alors un élément $x \in S$ distinct de l'élément neutre. Puisque $x \in S$ et que S est un q-groupe, l'ordre de x est une puissance de q. Mais, l'hypothèse qu'il existe un entier m tel que $p^m x = 0$ (puisque $x \in A$) implique que l'ordre de x est une puissance de p, ce qui est absurde ! On en déduit bien que A est un p-groupe.
2. Noter que puisque l'action est par automorphismes, $\mathrm{Fix}(g)$ est alors un sous-groupe de A pour tout $g \in G$ et on cherche un élément de $\bigcap_{g \in G} \mathrm{Fix}(g)$. L'équation aux classes fournit
$$\#A = \#A^G + \sum_{\omega \in \Omega'} \frac{\#G}{\#\mathrm{Stab}_G(\omega)} \quad \text{avec} \quad A^G = \{x \in A \ : \ \forall g \in G,\ g \cdot x = x\} = \bigcap_{g \in G} \mathrm{Fix}(g) = \text{réunion des orbites de cardinal 1}$$
et puisque $\frac{\#G}{\#\mathrm{Stab}_G(\omega)}$ est une puissance de p car pour $\omega \in \Omega'$ (qui correspond aux orbites de cardinal > 1), la stabilisateur est un sous-groupe strict et G est un p-groupe. Par ailleurs, $p \mid \#A$ si bien que $p \mid \#A^G$. Mais $\#A^G \neq 0$ car $0 \in A^G$ (car on agit par automorphisme) et par conséquent $\#A^G \geqslant p$ et on a le résultat.
3. On peut utiliser le théorème de structure des groupes abéliens de type fini couplé au fait que tout élément de A est de torsion. On peut aussi utiliser que par définition et puisqu'on travaille dans un cadre commutatif
$$B = \left\{ \sum_{g \in G} n_g (g \cdot a) \ : \ \forall g \in G,\ n_g \in \mathbf{Z} \right\}.$$
Mais puisque chacun des $g \cdot a$ est d'ordre fini, il suffit de se restreindre à un nombre fini de n_g.
4. On applique simplement le résultat de **2.** à B (sur lequel l'action de G se restreint[34]) et il existe $x \neq 0$ dans $B \subseteq A$ tel que pour tout $g \in G$, $g \cdot x = x$.

Exercice 10. Montrer que tout groupe d'ordre 255 est cyclique.

Solution. Soit G d'ordre $255 = 3 \times 5 \times 17$. On sait par les théorèmes de Sylow que le nombre n_3 de 3-Sylow vaut 1 ou 85 (car il divise 85 et est congru à 1 modulo 3), celui n_5 des 5-Sylow vaut 1 ou 51 et on a un unique 17-Sylow, que l'on notera S_{17}. On ne peut pas avoir $n_3 = 85$ et

34. En effet, B a été choisi de sorte à être de type fini et stable sous l'action de G. C'est une méthode usuelle pour passer de l'hypothèse fini à infini et il s'agit en fait du plus petit sous-groupe stable sous l'action de G et contenant a. Pour voir que B est stable sous l'action de g, on écrit un élément quelconque b de B sous la forme
$$b = \sum_{g \in G} n_g (g \cdot a) \qquad n_g \in \mathbf{Z}$$
de sorte que pour tout $g' \in G$,
$$g' \cdot b = \sum_{g \in G} n_g g' \cdot (g \cdot a).$$
On a ici utilisé le fait que l'action est lieu par automorphisme (ce qui signifie que $\cdot$ est $\mathbf{Z}$-linéaire dans le cas commutatif) et que la somme est finie car G est fini. On utilise ici que le côté morphisme uniquement (mais le côté automorphisme vient du fait que le morphisme sous-jacent $A \to A$ issu de l'action est une bijection). On a alors
$$g' \cdot b = \sum_{g \in G} n_g \left((g'g) \cdot a\right) \quad \text{soit} \quad g' \cdot b = \sum_{g'' \in G} n_{g'^{-1}g''} \left(g'' \cdot a\right) \in B$$
en effectuant le changement de variable bijectif $G \to G$ donné par $g'' = g'g$.

$n_5 = 51$ car sinon on obtiendrait au moins[35] $85 \times 2 + 51 \times 4 = 374$ éléments dans G. On a donc $n_3 = 1$ ou $n_5 = 1$. Supposons $n_3 = 1$ (l'autre cas se traitant de façon complètement analogue) et S_3 l'unique 3-Sylow. Notons alors S_5 un 5-Sylow quelconque. On a alors

a) $S_3S_{17} \cong S_3 \times S_{17} \lhd G$ car $S_3 \lhd G$ et $S_{17} \lhd G$ (en appliquant le critère du cours);

b) $S_3S_{17} \cap S_5 = \{e\}$ (pour des raisons de cardinalité);

c) $S_3S_5S_{17} = G$ (idem pour des raisons de cardinalité car il contient 3×17 éléments distincts dans S_3S_{17} et tous les gs pour $g \in S_3S_{17}$ et $s \in S_5$ qui sont tous distincts).

On a donc $G = S_3S_{17} \rtimes S_5$ associé à un morphisme $\varphi : S_5 \to \mathrm{Aut}(S_3S_{17})$. On a alors[36] $\mathrm{Aut}(S_3S_{17}) \cong \mathrm{Aut}(\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/17\mathbf{Z}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/16\mathbf{Z}$ donc le morphisme φ est nécessairement trivial (on n'a aucun élément d'ordre 5 à l'arrivée) et le produit direct. Par le lemme chinois, on obtient donc que

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

► **Complément. –** On pourrait être tenté de se passer du cours sur le produit semi-direct en établissant que le morphisme

$$f : \left\{ \begin{array}{ccc} S_5 \times S_3 \times S_{17} & \longrightarrow & G \\ (s_5, s_3, s_{17}) & \longmapsto & s_5s_3s_{17} \end{array} \right.$$

est un isomorphisme mais cela revient à redémontrer des propriétés établies dans le cours sur le produit semi-direct justement ! En effet, pour établir qu'il s'agit d'un morphisme, il s'agit de montrer que pour tous $(s_5, s_3, s_{17}), (s'_5, s'_3, s'_{17}) \in S_5 \times S_3 \times S_{17}$, alors

$$s_5s_3s_{17}s'_5s'_3s'_{17} = s_5s'_5s_3s'_3s_{17}s'_{17}.$$

Puisque $S_{17} \lhd G$, on sait que $S_3S_{17} = S_{17}S_3$ et $s'_3s'_{17} = (s'_3s'_{17}{s'_3}^{-1})s'_3$. Mais comme S_3 est aussi distingué, on a

$$s'_3s'_{17}{s'_3}^{-1}{s'_{17}}^{-1} \in S_{17} \cap S_3 = \{e\} \quad \text{si bien que} \quad s'_3s'_{17}{s'_3}^{-1} = s'_{17}.$$

En d'autres termes, S_3 et S_{17} commutent. On a donc

$$s_5s_3s_{17}s'_5s'_3s'_{17} = s_5s_3s_{17}s'_5s'_{17}s'_3.$$

Pour pouvoir continuer, on aurait besoin de savoir que S_5 commute avec S_3 et S_{17} mais cela n'est pas évident *a priori* (en tout cas par des arguments de comptage). Si on parvient à le démontrer alors on obtient un morphisme injectif en utilisant les intersections triviales et surjectif en utilisant le fait que $S_3S_5S_{17} = G$ et on peut donc conclure. Une façon de la faire est de considérer G/S_{17} qui est un groupe d'ordre $15 = 3 \times 5$ avec $3 \nmid 5 - 1 = 4$ donc $G/S_{17} \cong \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$ contient un unique sous-groupe normal K d'ordre 5. En consiérant alors la surjection canonique $\pi : G \to G/S_{17}$, il vient que $C = \pi^{-1}(K)$ est un sous-groupe distingué de G contenant S_{17}. Par les théorèmes d'isomorphisme, $\#C = \#K \times \#S_{17} = 85 = 5 \times 17$ avec $5 \nmid 17$ donc d'après le cours, un tel groupe est cyclique possédant donc un unique 5-Sylow C_5 (qui est aussi un 5-Sylow de G par cardinalité). Montrons que C_5 est distingué. Soit $g \in G$. On a alors

$$gC_5g^{-1} \subseteq gCg^{-1} = C \quad \text{car} \quad C \lhd G.$$

Ainsi, gC_5g^{-1} est un 5-Sylow de C qui n'en possède qu'un seul, à savoir C_5 donc $gC_5g^{-1} = C_5$ et on a gagné. En réalité, de manière plus générale, si un groupe G possède pour tout $p \mid \#G$ un unique p-Sylow, alors il est produit direct de ses p-Sylow et est nilpotent en raisonnant comme ci-dessus ou comme dans l'exercice 13. Noter qu'on peut établir qu'un groupe d'ordre pq avec $p \nmid q - 1$ si $p < q$ sont deux nombres premiers distincts sans recourir au produit semi-direct par des arguments de cardinalité ! En effet, un tel groupe possède un unique p-Sylow et un unique q-Sylow et alors on a au plus $1 + p - 1 + q - 1 = p + q - 1$ éléments d'ordre $1, p$ ou q. Or, $p + q - 1 < pq$ car $p+q-1 < 2q-1 \leqslant 2q < pq$ dès que $p > 2$. Si maintenant $p = 2$, il vient $p+q-1 = q-1 < 2q$. Dans tous les cas, il existe nécessairement un élément d'ordre pq et le groupe est cyclique ! Noter que cela implique que G est produit de ses p-Sylow (ou plus simplement abélien) et donc nilpotent.

35. En effet, il est clair qu'en considérant l'ordre d'un élément g de l'intersection d'un 3-Sylow et d'un 5-Sylow, que cet ordre doit divisier 3 et 5 et est donc égal à 1 si bien qu'un 3-Sylow et un 5-Sylow sont disjoints mais aussi que puisque les 3-Sylow (et les 5-Sylow) sont cycliques d'ordre premier (et ainsi tout éléme,t non trivial en est un générateur), que l'intersection de deux 3-Sylow (et de deux 5-Sylow) distincts est trivial.

36. En effet, on a par ce qui précède et le théorème chinois que $S_3S_{17} \cong S_3 \times S_{17} \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \cong \mathbf{Z}/51\mathbf{Z}$. Or, deux groupes isomorphes ont des groupes d'automorphismes isomorphes donc $\mathrm{Aut}(S_3S_{17}) \cong \mathrm{Aut}(\mathbf{Z}/51\mathbf{Z})$. Le cours garantit alors que $\mathrm{Aut}(\mathbf{Z}/51\mathbf{Z}) \cong (\mathbf{Z}/51\mathbf{Z})^\times$ et le théorème chinois fournit à nouveau $(\mathbf{Z}/51\mathbf{Z})^\times \cong (\mathbf{Z}/3\mathbf{Z})^\times \times (\mathbf{Z}/17\mathbf{Z})^\times$. Pour finir, on sait alors par le cours que $(\mathbf{Z}/3\mathbf{Z})^\times \cong \mathbf{Z}/2\mathbf{Z}$ et $(\mathbf{Z}/17\mathbf{Z})^\times \cong \mathbf{Z}/16\mathbf{Z}$. **Attention** qu'en général, pour deux groupes G_1 et G_2, on a $\mathrm{Aut}(G_1 \times G_2) \ncong \mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2)$ comme on peut le voir avec $G_1 = G_2 = \mathbf{Z}/2\mathbf{Z}$ pour lesquels on a $\mathrm{Aut}(G_1 \times G_2) \cong \mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z})$ tandis que $\mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2) = \{\mathrm{Id}\}$. En revanche, si le cardinal de G_1 et celui de G_2 sont premiers entre eux, alors on a bien $\mathrm{Aut}(G_1 \times G_2) \cong \mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2)$. En effet, $\mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2) \to \mathrm{Aut}(G_1 \times G_2)$ défini par $(\varphi_1, \varphi_2) \mapsto [(g_1, g_2) \mapsto (\varphi_1(g_1), \varphi_2(g_2))]$ est toujours un morphisme injectif et **dans le cas où les ordres sont premiers entre eux**, $\varphi \mapsto ([g_1 \mapsto \varphi(g_1, 1)], [g_2 \mapsto \varphi(1, g_2)])$ est un morphisme réciproque. Noter qu'en général il ne s'agit pas d'un morphisme comme en témoigne le contre-exemple ci-dessus (car il existe des isomorphismes de $\mathbf{F}_2^2$ qui ne stabilisent pas chacun des facteurs $\mathbf{F}_2$). Mais dans le cas où les ordres sont premiers entre eux, on obtient bien un morphisme car les sous-groupes $G_1 \times \{1\}$ et $\{1\} \times G_2$ sont caractéristiques (donc stables par tout automorphisme). Pour le voir, on peut dire que l'image de $G_1 \times \{1\}$ par un automorphisme φ de $G_1 \times G_2$ a même cardinal que G_1 et donc s'il contenait un élément de la forme $(g_1, g_2) \in G_1 \times G_2$ avec $g_2 \neq 1$. Mais, on peut alors si on note o_1 l'ordre de g_1, obtenir que $(g_1^{o_1}, g_2^{o_1}) = (1, g_2^{o_1}) \in \varphi(G_1 \times \{1\})$. Mais puisque $o_1 \mid \#G_1$ qui est premier à $\#G_2$, alors $g_2^{o_1} \neq 1$. Ainsi, on a obtenu un élément de la forme $(1, g'_2) \in \varphi(G_1 \times \{1\})$ avec $g'_2 \neq 1$ mais cela implique que $\varphi(G_1 \times \{1\}) \cap (\{1\} \times G_2)$ est non trivial, ce qui est absurde puisqu'ils ont des cardinaux premiers antre eux.

Exercice 11 — Groupes résolubles.

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

Solution.
La terminologie provient de la théorie de Galois. Le groupe de Galois du corps de décomposition d'un polynôme P à coeeficients dans $\mathbf{Q}$ est résoluble si, et seulement si, les racines de P sont exprimables par radicaux. Le fait que le groupe $\mathfrak{S}_n$ ne soit plus résoluble dès que $n \geqslant 5$ explique pourquoi à partir du degré 5, il n'existe plus de méthode de résolution par radicaux (contrairement aux degrés 2, 3 et 4).

1. On utilise le fait que G est résoluble si, et seulement s'il existe un entier n tel que $D^n(G) = \{e\}$. On constate alors que si $H \leqslant G$, pour tout n, $D^n(H) \leqslant D^n(G)$ donc H est résoluble. Soit maintenant $H \lhd G$ et considérons le groupe quotient G/H. On a alors le morphisme surjectif canonique $\pi : G \to G/H$ et par surjectivité, $D^n(G/H) = \pi(D^n(G))$ pour tout n, ce qui permet de conclure. On voit alors que de façon plus générale si $f : G \to H$ est un morphisme de groupes surjectif avec G résoluble, alors H est résoluble [37].

   ▶ **Remarque. –** On pouvait évidemment utiliser l'autre définition du cours. Si on se donne
   $$G_0 = \{e\} \leqslant G_1 \leqslant \cdots \leqslant G_n = G$$
   comme dans le cours, alors les $H \cap G_i$ fonctionnent ! En effet, si $G_i \lhd G_{i+1}$, alors $G_i \cap H \lhd G_{i+1} \cap H$ et si G_{i+1}/G_i est abélien, alors $G_{i+1} \cap H/G_i \cap H$ aussi. En effet, soit $g, g' \in G_{i+1} \cap H$. On sait puisque G_{i+1}/G_i est abélien qu'il existe $g_i \in G_i$ tel que $gg' = g'gg_i$. Or, ici, $gg', g'g \in G_{i+1} \cap H$ donc $g_i \in H$ et $g_i \in G_i \cap H$ si bien que dans $G_{i+1} \cap H/G_i \cap H$, on a bien $\overline{gg'} = \overline{g'g}$.
   De même, dans le cas du quotient,
   $$\{e\} = G_0H/H \leqslant G_1H/H \leqslant \cdots \leqslant G_nH/H = G/H$$
   convient. En effet, on a bien $G_iH/H \lhd G_{i+1}H/H$ si [38] $G_i \lhd G_{i+1}$ et $(G_{i+1}H/H)/(G_iH/H) \cong G_{i+1}H/G_iH$ abélien via les théorèmes d'isomoprhisme ! Atttneion au fait que l'on ne peut pas simplifier par H (prendre par exemple $H = G$ pour s'en convaincre). En revanche, puisque H est dans le noyau de la projection canonique $G_{i+1}H \to G_{i+1}H/G_iH$, on peut supposer que deux éléments de $G_{i+1}H/G_iH$ proviennent de deux éléments de G_{i+1}. On considère donc $g, g' \in G_{i+1}$ et alors $gg' = g'gg_i$ avec $g_i \in G_i \subseteq G_iH$ de sorte que dans $G_{i+1}H/G_iH$, $\overline{gg'} = \overline{g'g}$.
   On obtient par la même occasion des informations sur la classe de résolubilité, à savoir sur le plus petit indice n tel que $D^n(G) = \{e\}$.
2. Soit $1 \to N \to G \to H \to 1$ une suite exacte avec H et N deux groupes résolubles et montrons que G est résoluble. On sait alors que l'application $p : G \to H$ est surjective donc comme en **1.**, il s'ensuit qu'il existe un entier n tel que $\{e\} = D^n(H) = p(D^n(G))$ si bien que $D^n(G) \subseteq \mathrm{Ker}(p) = \mathrm{Im}(i) = i(N) \cong N$ où $i : N \to G$ est injective. Ainsi, il existe un entier [39] m tel que $D^m(i(N)) = \{e\}$ et alors $D^{n+m}(G) = \{e\}$ et G est résoluble.

   ▶ **Remarque. –** Idem, on pouvait composer une suite de composition pour $i(N)$
   $$G_0 = \{e\} \leqslant G_1 \leqslant \cdots \leqslant G_m = i(N)$$
   avec une suite de composition de $H \cong G/N$ (via les théorèmes d'isomorphisme)
   $$G'_m = \{\overline{e}\} = N/N \leqslant G'_{m+1} = G_{m+1}/N \leqslant \cdots \leqslant G'_{m+n} = G/N$$
   avec G_i pour $i \in \{m+1, \ldots, m+n\}$ des sous-groupes contenant N et tels que $G_i \lhd G_{i+1}$ et $G'_{i+1}/G'_i \cong G_{i+1}/G_i$ abéliens pour obtenir une suite de composition qui convient pour G
   $$G_0 = \{e\} \leqslant G_1 \leqslant \cdots \leqslant G_m = i(N) \leqslant G_{m+1} \leqslant \cdots \leqslant G_{m+n} = G.$$

37. Si $f : G_1 \to G_2$ est un morphisme de groupes, on a pour tout entier n, $f(D^n(G_1)) \subseteq D^n(G_2)$ avec égalité si f est surjectif.
38. En effet, $H \lhd G$ et $G_i \lhd G_{i+1}$. Ainsi, pour tout $x \in G_iH$ (donc $x = g_ih_1$ avec $g_i \in G_i$ et $h_1 \in H$) et $\in G_{i+1}H$ (donc $y = g_{i+1}h_2$ avec $g_{i+1} \in G_{i+1}$ et $h_2 \in H$), on a
$$yxy^{-1} = g_{i+1}h_2g_ih_1h_2^{-1}g_{i+1}^{-1}.$$
Or, $H \lhd G$ donc $H \lhd G_i$ et $H \lhd G_{i+1}$ donc $h_2g_i = g_ih'_2$ pour $h'_2 \in H$ et $h'_2h_1h_2^{-1}g_{i+1}^{-1} = g_{i+1}^{-1}h$ pour $h \in H$ si bien que
$$yxy^{-1} = g_{i+1}g_ig_{i+1}^{-1}h \in G_iH \quad \text{car} \quad g_{i+1}g_ig_{i+1}^{-1} \in G_i \quad \text{car} \quad G_i \lhd G_{i+1}.$$

39. Un groupe isomorphe à un groupe résoluble étant bien évidemment lui-même résoluble (car ils ont le même groupe dérivé ou en prenant l'image d'une suite de composition par un isomorphisme) !

3. Un groupe nilpotent est résoluble mais la réciproque est fausse comme en témoigne l'exemple du groupe $\mathfrak{S}_3$ (on aurait aussi pu prendre $\mathfrak{A}_4$ ou $\mathfrak{S}_4$). Une preuve est donnée page 32 du polycopié de cours, on pouvait aussi utiliser le fait (pour $G = \mathfrak{S}_3$ par exemple) que $D(G) = \mathfrak{A}_3$ qui est abélien donc $D^2(G) = \{e\}$ pour obtenir la résolubilité et le fait qu'un groupe est nilpotent si, et seulement s'il existe un entier n tel que $C^n(G) = \{e\}$ où $C^0(G) = G$ et $C^{n+1}(G)$ est le groupe engendré par les commutateurs $ghg^{-1}h^{-1}$ avec $g \in G$ et $h \in C^n(G)$ (la preuve étant analogue à celle dans le cas résoluble, voir l'exercice 13). On a dans notre cas, $C^1(G) = D(G) = \mathfrak{A}_3$ et $C^2(G)$ est alors un sous-groupe non trivial de $C^1(G) = \mathfrak{A}_3$ car $\mathfrak{A}_3$ n'est pas central dans G si bien que nécessairement $C^2(G) = \mathfrak{A}_3$ et par récurrence immédiate, $C^n(G) = \mathfrak{A}_3 \neq \{e\}$. On pouvait aussi utiliser que les seuls sous-groupes distingués de $\mathfrak{S}_3$ sont $\{\mathrm{Id}\}$, $\mathfrak{A}_3$ et $\mathfrak{S}_3$ et donc cela ne peut donner lieu qu'aux suites de compositions de groupes normaux $\{\mathrm{Id}\} \lhd \mathfrak{S}_3$ mais $\mathfrak{S}_3$ est non abélien ou $\{\mathrm{Id}\} \lhd \mathfrak{A}_3 \lhd \mathfrak{S}_3$ où on a bien $\mathfrak{S}_3/\mathfrak{A}_3$ abélien mais $\mathfrak{A}_3$ non inclus dans $Z(\mathfrak{S}_3) = \{\mathrm{Id}\}$.

4. On peut utiliser le fait qu'on sait qu'un tel groupe est non simple (par exemple en reprenant la preuve de la non simplicité de G d'ordre pq qui établit que si $p < q$, alors G possède un seul q-Sylow qui est donc distingué). Il existe donc $H \lhd G$. On peut supposer sans perte de généralité que H est de cardinal p donc abélien et ainsi G/H est de cardinal q donc abélien et la suite $\{e\} \subseteq H \subseteq G$ montre que G est résoluble.
Reste à traiter le cas de $p = q$ mais on sait qu'un groupe d'ordre p^2 est abélien (voir le cours) donc résoluble. De manière générale, on sait qu'un p-groupe est nilpotent et donc résoluble [40].

5. On a le résultat d'après ce qui précède si $p = q = r$. Si deux des nombres premiers sont égaux, on est ramené à la question suivante, on supposera donc que $p < q < r$. On a alors que $n_r \in \{1, pq\}$ et $n_q \in \{1, r, pr\}$. Supposons que $n_r, n_q \neq 1$. Alors G admet exactement $pq(r-1)$ éléments d'ordre r et au moins $r(q-1)$ éléments d'ordre q. cela fournit que

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

Mais on remarque que

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

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

6. Supposons que $q < p$. On a alors que le nombre n_p de p-Sylow vaut 1 et donc on obtient un unique p-Sylow H d'ordre p^2 donc abélien donc résoluble tel que G/H soit d'ordre q donc cyclique donc résoluble et par **2.**, G est résoluble.
Si maintenant $p < q$. On a alors que $n_q \in \{1, p^2\}$ et $n_p \in \{1, q\}$. Si $n_p \neq 1$ et $n_q \neq 1$, alors on a au moins

$$1 + p^2(q-1) + p^2 - 1 + 1 = \#G + 1$$

éléments dans G (l'identité, puis $q-1$ éléments d'ordre q dans les p^2 q-Sylow et enfin $p^2 - 1$ éléments d'ordre divisant p dans un des p-Sylow plus un autre tel élément au moins dans un second p-Sylow). On a donc une contradiction et donc soit $n_p = 1$ soit $n_q = 1$ et on obtient que le q-Sylow ou le p-Sylow est distingué et on conclut comme dans le premier cas !

► **Compléments. –** On peut montrer de même qu'un groupe d'ordre $p^\alpha q$ avec $p > q$ (car $n_p = 1$ et un p-groupe est résoluble et le quotient abélien aussi), d'ordre [41] $p^\alpha q^\beta$ avec $p^\alpha < q + 1$ (car $n_q = 1$ et des p-groupes sont résolubles).
On peut alors déduire de tout cela que tout groupe d'ordre < 60 est résoluble. Pour l'ordre 60, on sait que $\mathfrak{A}_5$ est simple non abélien et par conséquent non résoluble.
Je rappelle qu'un groupe simple est résoluble si, et seulement s'il est commutatif (car $D(G) \lhd G$ et $D(G) \neq \{e\}$ donc $D(G) = G$) et cela a alors lieu si, et seulement si, c'est un groupe d'ordre premier. Pour la culture, je mentionne le théorème de Feit-Thompson (qui est très profond et difficile mais qui a joué un rôle majeur dans la classification des groupes finis simples) conjecturé par Burnside en 1911 démontré en 1963 et qui stipule que tout groupe d'ordre impair est résoluble. Il s'agissait d'une des pistes pour classifier à isomorphisme près les groupes finis. On utilise les sous-groupes distingués non triviaux pour réaliser G comme extension de deux sous-groupes de cardinal strictement inférieurs. Ce procédé donne finalement lieu à des groupes simples que l'on sait aujourd'hui classifier (un tel groupe est soit alterné, soit cyclique, soit de type Lie soit un des 26 groupes simples sporadiques). Le problème est alors que l'on ne sait pas classifier les extensions de groupes ! On a enfin le résultat suivant (sorte de réciproque partielle du théorème de Lagrange), à savoir le théorème de Hall : G est résoluble si, et seulement si, pour tout $d \mid n = \#G$ tel que pgcd $\left(d, \frac{n}{d}\right) = 1$, G possède un sous-groupe d'ordre d. Noter que si d est une puissance d'un nombre

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

$$G'_n = Z(G)/Z(G) \subseteq G'_{n+1} = G_{n+1}/Z(G) \subseteq \cdots \subseteq G'_{n+m} = G/Z(G)$$

avec $G'_i \lhd G/Z(G)$ donc $G_i \lhd G$ et $G'_{i+1}/G'_i \cong G_{i+1}/G_i \leqslant Z(G/G_i) \cong Z(G'/G'_i)$. On a alors que

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = Z(G) \subseteq G_{n+1} \subseteq \cdots \subseteq G_{n+m} = G$$

montre que G est nilpotent.

41. En réalité, on dispose du théorème de Burnside qui fournit que tout groupe d'ordre $p^n q^m$ est résoluble dont une démonstration passe par la théorie des représentations.

premier, l'hypothèse de résolubilité est inutile car le résultat découle des théorèmes de Sylow. En général, elle est nécessaire! On pourra en effet remarquer que $\mathfrak{A}_5$ ne contient pas de sous-groupes d'ordre 15 ou 20. On dispose par ailleurs d'une réciproque de ce résultat : un groupe G possédant au moins un sous-groupe d'ordre d pour chaque d diviseur de n tel que pgcd $\left(d, \frac{n}{d}\right) = 1$, alors G est résoluble. Cela implique immédiatement le théorème de Burnside!
On a également que le produit direct de deux groupes résolubles l'est puisque $D(G_1 \times G_2) \cong D(G_1) \times G_2$.
Pour finir, établissons l'équivalence pour un groupe G **fini**[42] on a l'équivalence entre G résoluble et l'existence d'une suite de composition

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

avec $G_{i+1} \triangleleft G_i$ et G_{i+1}/G_i cyclique d'ordre premier. Il est en particulier clair que cette dernière propriété (puisque cyclique implique abélien) implique toujours résoluble. Établissons alors la réciproque dans le cas G fini. Commençons par montrer par récurrence sur le cardinal, que si H est un groupe abélien fini, alors une telle suite de compositions aux quotients cycliques d'ordre premier existe. Si H est simple, comme H est supposé abélien, il est cyclique d'ordre premier et alors $\{e\} \leqslant H$ convient! Sinon, on peut trouver un sous-groupe strict $N \triangleleft H$ d'ordre maximal. On considère alors la projection canonique $\pi : H \to H/N$. On en déduit que H/N est simple car sinon, il contiendrait un sous-groupe normal $K \triangleleft H/N$ et $\pi^{-1}(K)$ serait un sous-groupe distingué de H distinct de $\{e\}$ et de H (car π est surjective). Par ailleurs, comme il s'agit d'un quotient d'un groupe abélien, H/N est abélien et comme on a vu qu'il est simple, il est cyclique d'ordre premier. On peut donc commencer notre suite de composition par $H_n = H \geqslant H_{n-1} = N$ où $\#N < \#N$. L'hypothèse de récurrence appliqueée à N fournit $H_0 = \{e\} \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} = N$ à quotients cycliques d'ordre premiers. La suite $H_0 = \{e\} \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} = N \leqslant H_n = H$ convient alors. Pour conclure, si G est résoluble, on dispose d'une suite $\{e\} = G_0 \leqslant G_1 \leqslant \cdots G_n = G$ avec $G_{i+1} \triangleleft G_i$ et G_{i+1}/G_i abéliens. Pour tout $i \in \{0, \ldots, n-1\}$, on peut donc trouver une suite de composition

$$G_0' = \{\overline{e}\} \triangleleft G_1' = G_{i,1}/G_i \triangleleft G_2' = G_{i,2}/G_i \triangleleft \cdots \triangleleft G_{r_i}' = G_{i+1}/G_i$$

avec les $G_{i,j}'$ pour $j \in \{1, \ldots, r_i\}$ des sous-groupes contenant G_i vérifiant $G_{i,j} \triangleleft G_{i,j+1}$ et tels que G_{i+1}'/G_i' cyclique d'ordre premier. Par ailleurs, par les théorèmes d'isomorphisme, il vient que

$$G_{j+1}'/G_j' = (G_{i+1,j}/G_i)/(G_{i,j}/G_i) \cong G_{i+1,j}/G_{i,j} \quad \text{qui est donc cyclique d'ordre premier.}$$

Ainsi, la suite de composition convient (autrement dit est à quotients cycliques d'ordre premier)

$$\{e\} = G_0 \leqslant G_{0,1} \triangleleft \cdots \triangleleft G_{0,r_0} = G_1 \triangleleft G_{1,1} \triangleleft \cdots \triangleleft G_{1,r_1} = G_2 \triangleleft \cdots \triangleleft G_n = G.$$

Noter qu'on ne peut pas imposer le fait que les G_i soient distingués dans G mais seulement dans G_{i+1}. Si on rajoute cette condition, on parle de groupe *hyper-résoluble* qui est une notion strictement plus forte. par exemple, en utilisant le fait que les seuls sous-groupes distingués de $\mathfrak{S}_4$ sont $\{\mathrm{Id}\}$, V_4 (engendré par les doubles transpositions), $\mathfrak{A}_4$ et $\mathfrak{S}_4$, une telle suite à quotients cycliques d'ordre premier est impossible avec la condition que les $G_i \triangleleft \mathfrak{S}_4$ tandis que la suite $\{e\} \leqslant \langle (12) \rangle \leqslant V_4 \leqslant \mathfrak{A}_4 \leqslant \mathfrak{S}_4$ est en revanche bien à quotients abéliens mais $\langle (12) \rangle \not\triangleleft \mathfrak{S}_4$.

Exercice 12 — 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,

42. Noter que cette hypothèse n'est essentielle ici.

$1 \to H \to G \to G/H \to 1$. 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[43] $\ell \in (\mathbf{Z}/n\mathbf{Z})^\times$) 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[44] de $\varphi(H) = \psi(H)$, à savoir m. On constate alors que $\psi(h) = \varphi(h^k)$ et on a envie de poser

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

43. 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.

44. 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 $p \nmid k$.

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

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

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[45] $\overline{k}$ 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

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

de réciproque

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

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

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

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.

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

▶ **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[46] $\tilde{f} : N \rtimes_\psi H/N \cong H \to N \rtimes_\varphi H/N \cong H$ 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 classes d'isomorphismes de produits semi-directs avec le groupe cyclique infini[47] $\mathbf{Z}$. 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 $\varphi, \psi : \mathbf{Z}/p\mathbf{Z} \to \mathrm{Aut}\,(\mathbf{Z}/q\mathbf{Z}) \cong (\mathbf{Z}/q\mathbf{Z})^\times \cong \mathbf{Z}/(q-1)\mathbf{Z}$, 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 $\#\mathrm{GL}_2(\mathbf{F}_p) = (p^2-1)(p^2-p) = p(p-1)^2(p+1)$ donc les p-Sylow de $\mathrm{GL}_2(\mathbf{F}_p)$ sont d'ordre p et tous conjugués[48]. Un produit semi-direct non trivial $(\mathbf{Z}/p\mathbf{Z})^2 \rtimes \mathbf{Z}/p\mathbf{Z}$ est la donnée d'un morphisme $\varphi : \mathbf{Z}/p\mathbf{Z} \to \mathrm{Aut}\left((\mathbf{Z}/p\mathbf{Z})^2\right)$ non trivial. Or, dans $(\mathbf{Z}/p\mathbf{Z})^2$, tous les éléments vérifient $g^p = e$ et un raisonnement identique à celui de l'exercice permet de munir $(\mathbf{Z}/p\mathbf{Z})^2$ 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 $\mathrm{Aut}\left((\mathbf{Z}/p\mathbf{Z})^2\right) \cong \mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$. Par simplicité de $\mathbf{Z}/p\mathbf{Z}$, un tel morphisme est injectif et les images de ψ et

46. 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 $(1,\alpha(h))$.

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

48. 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

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

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

φ (qui sont des sous-groupes d'ordre p de $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$) sont des p-Sylow et par conséquent conjugués par une matrice $P \in \mathrm{GL}_2(\mathbf{F}_p)$. 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[49], $\varphi^{-1} \circ \psi^{(P)}$ 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 $(\mathbf{Z}/p\mathbf{Z})^2 \rtimes_\varphi \mathbf{Z}/p\mathbf{Z} \cong (\mathbf{Z}/p\mathbf{Z})^2 \rtimes_\psi \mathbf{Z}/p\mathbf{Z}$. On a donc obtenu l'unicité. Quant à l'existence, comme $\mathrm{Aut}\left((\mathbf{Z}/p\mathbf{Z})^2\right) \cong \mathrm{GL}_2(\mathbf{F}_p)$, l'existence d'un tel produit semi-direct non trivial qui correspond à un morphisme non trivial $\mathbf{Z}/p\mathbf{Z} \to \mathrm{GL}_2(\mathbf{F}_p)$ 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 $(\mathbf{Z}/p\mathbf{Z})^2 \rtimes \mathbf{Z}/p\mathbf{Z}$ 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 $\mathbf{Z}/p\mathbf{Z}$.

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 $y \in G \setminus \langle x \rangle$. On a alors que $y^p \in \langle x \rangle$ car $\overline{y^p} = \langle x \rangle$ dans le quotient et $y^{p^2} = e$ car y ne peut pas être d'ordre p^3, G étant non cyclique. Il existe donc $k \in \mathbf{Z}$ tel que $y^p = x^{pk}$ (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 $z \in G \setminus \langle x \rangle$ d'ordre p. Cherchons z sous la forme $z = yx^n$. Ainsi $z^p = (yx^n)^p = yx^n yx^n \cdots yx^n$ et par une récurrence immédiate, il vient

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

L'élément z est donc d'ordre p si, et seulement si, $p^2 \mid pk+n(r^{p-1}+\cdots+r+1)$ où l'inconnue est n. Notons $S := r^{p-1}+\cdots+r+1$. On a alors $(r-1)S = r^p - 1$ qui est congru à $r-1$ modulo p. 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 $z = yx^{n_0} \in G \setminus \langle x \rangle$ est d'ordre p. On a donc par propriété du produit semi-direct[50] que $G = \langle x \rangle \rtimes \langle z \rangle \cong \mathbf{Z}/p^2\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}$.

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 $\psi : \mathbf{Z}/p\mathbf{Z} \to \mathrm{Aut}(\mathbf{Z}/p^2\mathbf{Z}) \cong \mathbf{Z}/p(p-1)\mathbf{Z}$. Le groupe cyclique $\mathbf{Z}/p(p-1)\mathbf{Z}$ admet un unique sous-groupe d'ordre p donc 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[51]) 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 13 — Groupes nilpotents.

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.

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

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

50. 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 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 $\mathbf{D}_4$, $\langle \rho \rangle \cap \langle -\mathrm{Id} \rangle = \langle -\mathrm{Id} \rangle \neq \{e\}$.

51. On peut en effet montrer qu'un p-groupe d'ordre p^n possède des sous-groupes d'ordre p^i pour tout $i \in \{0, \ldots, n\}$ (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.

2. Montrer que le centre d'un groupe nilpotent est non trivial.
3. Montrer que si G est nilpotent et que H est un sous-groupe de G, alors H est nilpotent.
4. Montrer que si $H \lhd G$ et que G est nilpotent, alors G/H est nilpotent.
5. On suppose H et G/H nilpotents. Le groupe G est-il nilpotent ?
6. Soient p, q, r trois nombres premiers. Montrer que tout groupe d'ordre pqr est résoluble. Un tel groupe est-il nilpotent ?
7. On suppose G fini. Montrer que G est nilpotent si, et seulement si, tout sous-groupe maximal de G est distingué et si, et seulement si, G est produit direct de ses p-Sylow pour tout nombre premier p divisant $\#G$.

Solution.
On commence par donner un critère dans le cas des groupes nilpotents correspondant à celui du $D^n(G) = \{e\}$ pour les groupes résolubles. Soient G un groupe fini, $N \lhd G$, $H \leqslant G$ et $\pi : G \to G/N$ la surjection canonique. On a alors que $\pi(H) \leqslant Z(G/N)$ si, et seulement si, $[H, G] \leqslant N$ où, pour $H_1, H_2 \leqslant G$, on note $[H_1, H_2]$ le sous-groupe de G engendré par les commutateurs de la forme $h_1 h_2 h_1^{-1} h_2^{-1}$ avec $h_1 \in H_1$ et $h_2 \in H_2$. en effet, la condition que $\pi(H) \leqslant Z(G/N)$ équivaut à $[\pi(H), G/N] = \{\overline{e}\}$. On a clairement que $[\pi(H), G/N] = [\pi(H), \pi(G)] = \pi([H, G])$ par surjectivité du morphisme de groupes π. Ainsi, on a immédiatement que $[\pi(H), G/N] = \{\overline{e}\}$ si, et seulement si, $[H, G] \leqslant N$.
On définit alors *la suite centrale descendante* associée à G par $C^1(G) = [G, G]$ et $C^{n+1}(G) = [G, C^n(G)]$ pour $n \in \mathbf{N}^\times$. En déduire que G est nilpotent si, et seulement si, il existe $n_0 \in \mathbf{N}^\times$ tel que $C^{n_0}(G) = \{e\}$. Le groupe G est alors nilpotent si, et seulement si, il existe $n_0 \in \mathbf{N}^\times$ tel que $C^{n_0}(G) = \{e\}$. Si G est nilpotent, il existe une suite de groupes

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

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

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

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

1. C'est du cours et évident à partir des définitions ou des caractérisations en termes de D^n et C^n. La réciproque est fausse comme on l'a vu dans l'exercice 11 question **3.**
2. Soit G un groupe nilpotent. Il existe $n \geqslant 0$ maximal tel que $C^n(G) \neq \{e\}$. On a alors $C^{n+1}(G) = \{e\}$ soit $[G, C^n(G)] = \{e\}$. Cela signifie que le sous-groupe non trivial $C^n(G)$ est contenu dans $Z(G)$ qui est donc non trivial. On pouvait aussi considérer le premier terme distinct de G_0 de la suite de composition $G_0 = \{e\} \lhd G_1$ qui vérifie aisni $G_1 \cong G_1/G_0 \leqslant Z(G/G_0) \cong Z(G)$.
   Plus généralement, si $N \neq \{e\} \lhd G$, alors $N \cap Z(G) \neq \{e\}$ (si l'on ne suppose plus N normal, le résultat tombe en défaut comme on le voit avec $\mathbf{D}_4$ et N d'ordre 2 dans $\mathbf{D}_4$ non contenu dans le sous-groupe cyclique d'ordre 4). En posant dans notre cas $N_i = N \cap C^i(G)$, on a une suite d'extensions
   $$N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_n = \{e\}$$
   où on vérifie que $[G, N_i] \subseteq N_{i+1}$. Choisissons alors l'entier k maximal tel que $N_k \neq \{e\}$. On a $N_k \leqslant N$ et $[G, N_k] \subseteq N_{k+1} = \{e\}$ donc $N_k \subseteq Z(G)$. Il faut penser aux groupes nilpotents comme des sortes de généralisation des p-groupes (dont vous avez vu dans le cours qu'ils sont nilpotents et dont on a v que le centre est aussi non trivial !).
3. Une récurrence simple assure que pour tout $n \geqslant 0$, $C^n(H) \subseteq C^n(G)$, ce qui entraîne immédiatement le résultat. On a également que l'image d'un groupe nilpotent par un morphisme de groupes (car $f(C^n(G)) \subseteq C^n(f(G))$ avec égalité si le morphisme est surjectif) est nilpotent en raisonnant comme dans le cas résoluble.
4. On raisonne comme dans le cas résoluble en établissant que $\pi(C^n(G)) = C^n(G/H)$.
5. C'est faux comme on peut le voir avec $G = \mathfrak{S}_3$, $H = \mathfrak{A}_3$ et $G/H = \{\pm 1\} \cong \mathbf{Z}/2\mathbf{Z}$. On a alors H et G/H abéliens donc nilpotents mais G non nilpotent. Ce qui fait que la preuve dans le cas résoluble ne fonctionne pas ici est que la propriété de la définition des groupes résolubles est relative dans le sens où elle ne dépend que de la relation de G_i à G_{i+1} tandis qu'ici, dans le cas nilpotent, elle dépend de la relation de G_i à G_{i+1} mais aussi à G ! En particulier, on a en général $C^n(C^m(G)) \neq C^{n+m}(G)$ et $C^n(C^m(G))$ est plus petit que $C^{n+m}(G)$. En effet, par exemple $C^1(C^n(G)) = [C^n(G), C^n(G)]$ tandis que $C^{n+1}(G) = [G, C^n(G)]$.
   On a en revanche le résultat plus faible suivant : si $H \leqslant G$ est un sous-groupe central (donc en particulier nilpotent), alors G/H nilpotent implique G nilpotent. En effet, on a l'existence d'un n tel que $C^n(G/H) = \{e\}$ donc $\pi(C^n(G)) = \{e\}$ soit $C^n(G) \leqslant H$ et donc $C^n(G)$ est central et $C^{n+1}(G) = \{e\}$.
6. On a déjà traité la résolubilité. On sait que tout p-groupe est nilpotent donc si $p = q = r$, on obtient donc un groupe nilpotent.
   Si maintenant (sans perte de généralité), $p = q \neq r$, un tel groupe n'est pas nécessairement nilpotent comme en témoigne l'exemple de $\mathfrak{S}_3 \times \mathbf{Z}/2\mathbf{Z}$ (qui s'il était nilpotent entraînerait que $\mathfrak{S}_3$ est nilpotent).
   Supposons pour finir que $p < q < r$. Un tel groupe n'est pas non plus nécessairement nilpotent comme en témoigne l'exemple de $\mathfrak{S}_3 \times \mathbf{Z}/5\mathbf{Z}$ (qui s'il était nilpotent entraînerait que $\mathfrak{S}_3$ est nilpotent comme quotient par le sous-groupe distingué $\mathbf{Z}/5\mathbf{Z}$).

7. Supposons dans un premier temps que G est produit direct de ses p-Sylow. On a alors que chacun des p-Sylow est nilpotent en tant que p-groupe et on peut vérifier qu'un produit direct de groupes nilpotents est nilpotent (tout se passe composante par composante et $C^n(G_1 \times G_2) \cong C^n(G_1) \times C^n(G_2)$), ainsi G est nilpotent.

Réciproquement, supposons que G est nilpotent. Soit $M \leqslant G$ un sous-groupe maximal (qui existe car on a un nombre fini de sous-groupes stricts de G). Puisqu'il existe un n_0 tel que $C^{n_0}(G) = \{e\}$, il existe un entier minimal n tel que $C^n(G) \leqslant M$ et par minimalité de n, il existe $g \in C^{n-1}(G) \setminus M$. Alors, on a $[g, M] \subseteq [C^{n-1}(G), G] = C^n(G) \subseteq M$ ce qui assure que $gMg^{-1} \subseteq M$ et[52] $g \in N_G(M) \setminus M$ (en tenant le même raisonnement avec g^{-1}). Par conséquent, $N_G(M)$ est un sous-groupe de G contenant M, distinct de M donc égal à G par maximalité. On a donc $N_G(M) = G$ et M est distingué dans G. On a donc que tout sous-groupe maximal est distingué. Soit S un p-Sylow de G. Supposons que $N_G(S) \neq G$. Alors $N_G(S)$ est contenu dans un sous-groupe maximal M de G. Par hypothèse, M est distingué dans G donc pour tout $g \in G$, $gSg^{-1} \subseteq gMg^{-1} = M$ donc S et gSg^{-1} sont deux p-Sylow de M, donc conjugués dans M. Il existe ainsi $m \in M$ tel que $gSg^{-1} = mSm^{-1}$ donc $m^{-1}g \in N_G(S) \subseteq M$ donc $g \in M$ ce qui implique que $M = G$, ce qui est absurde par définition d'un sous-groupe maximal. Ainsi $N_G(S) = S$ et S est distingué et l'unique p-Sylow de G.

Considérons alors l'application $\varphi : \prod_{p|\#G} S_p \to G$ défini par le produit dans G et où S_p désigne l'unique p-Sylow. Comme les p-Sylow ont des cardinaux premiers entre eux, on voit que les éléments d'un sous-groupe de Sylow commutent avec ceux d'un autre. En effet, soit $x \in S_p$ et $y \in S_q$ distincts de e, alors $xyx^{-1}y^{-1} \in S_q$ (car $xyx^{-1} \in S_q \lhd G$) et de même $xyx^{-1}y^{-1} \in S_p$ (car $yx^{-1}y^{-1} \in S_p \lhd G$) et ainsi, $xyx^{-1}y^{-1} \in S_p \cap S_q = \{e\}$ et $xy = yx$. Cela entraîne qu'on a un morphisme de groupes et ce dernier est clairement injectif (car par commutativité et le fait que les ordres soient premiers entre eux, l'ordre d'un élément $s_1 \cdots s_r$ est le ppcm des ordre des s_i donc un élément du noyau est nécessairement trivial). On en déduit le résultat par cardinalité. On aurait pu utiliser une généralisation (ou itérer comme dans l'esprit de l'exercice 10) de la Remarque 3.8 page 25 du polycopié en remarquant que les intersections sont deux à deux triviales, que chaque sous-groupe est distingué et que le produit des cardinaux est égal au cardinal de G.

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

52. On rappelle que le normalisateur d'un sous-groupe M de G est le plus grand sous-groupe de G dans lequel M est distingué, à savoir $N_G(M) = \left\{g \in G : gMg^{-1} = M\right\}$. Il s'agit du stabilisateur de M pour l'action de G sur l'ensemble de ses sous-groupes par conjugaison.