Feuille TD 1 – Correction partielle – 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 $\mathfrak{A}_4$.
   Soient G un groupe et $K \subseteq H$ deux sous-groupes de G. On suppose que $K \lhd H$ et que $H \lhd G$. A-t-on $K \lhd G$? Démontrer que si K est caractéristique dans H et que H est caractéristique dans G, alors K est caractéristique dans G.
3. Une *partition d'un entier* n est une suite $0 < \lambda_1 \leqslant \lambda_2 \leqslant \cdots \leqslant \lambda_r$ d'entiers tels que $\sum_{i=1}^{r} \lambda_i = n$. Montrer que les classes de conjugaison de $\mathfrak{S}_n$ sont en bijection avec les partitions de n.

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 :

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

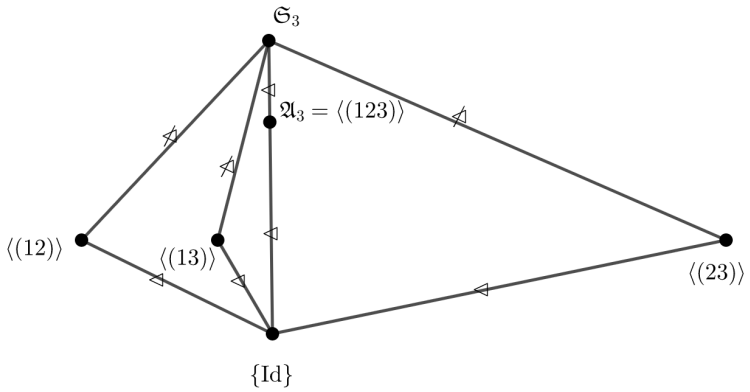
   On obtient par le théorème de Lagrange que $g(n) \mid n!$ et g est croissante puisque toute permutation de $\mathfrak{S}_n$ peut être vue comme une permutation de $\mathfrak{S}_k$ pour $k \geqslant n$. On a par exemple

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]



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!

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

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

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

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

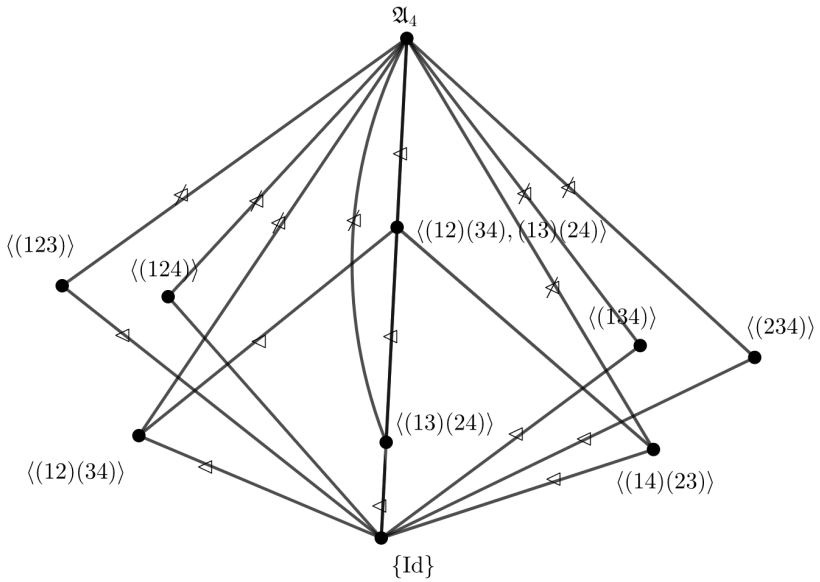
De plus, $\#\mathfrak{A}_4 = 12$ donc les sous-groupes non triviaux sont d'ordre 6, 4, 3 ou 2. Or, on sait qu'un sous-groupe d'ordre 6 est soit cyclique soit isomorphe à $\mathfrak{S}_3$. Ici la seule option serait $\mathfrak{S}_3$ car on n'a pas d'élément d'ordre 6 mais dans $\mathfrak{S}_3$ aucune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

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

Pour les groupes d'ordre 4, on a deux possibilités $\mathbf{Z}/4\mathbf{Z}$ 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 [8], 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 [9] du fait que

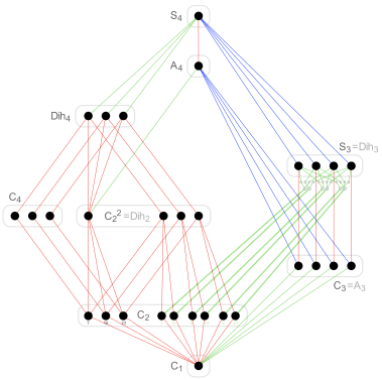
$$(ab)(cd)(abc)(ab)(cd) = (adb) \quad \text{et} \quad (abc)(ab)(cd)(acb) = (ad)(bc) \quad \text{si} \quad \{a, b, c, d\} = \{1, 2, 3, 4\}$$

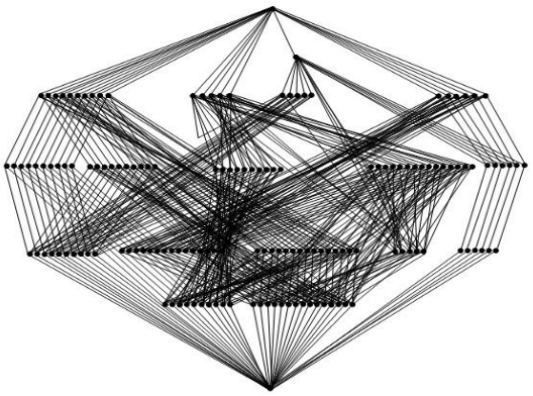
Reste à traiter le cas du groupe de Klein qui est distingué dans $\mathfrak{A}_4$. Cela découle de la question suivante ou des théorèmes de Sylow mais peut se voir aussi à la main grâce aux calculs précédents. En particulier, on a montré que $\mathfrak{A}_4$ est engendré par une double transposition

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. Une autre méthode est donnée dans l'exercice 8.
8. On peut là encore le voir grâce aux théorèmes de Sylow avec les 3-Sylows de $\mathfrak{A}_4$.
9. Plus généralement, c'est aussi une conséquence de la question suivante.

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 $\mathfrak{S}_5$:





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

▶ **Compléments . –** On a en fait la classification à isomorphisme près des groupes d'ordre $\leqslant 11$.

- Le seul groupe d'ordre 1 est le groupe trivial ;
- Si G est d'ordre p avec p premier alors nécessairement tout élément $g \in G$ distinct de l'identité est d'ordre p et engendre G si bien que [10] $G \cong \mathbf{Z}/p\mathbf{Z}$. Cela résout les cas $2, 3, 5, 7, 11$;
- Si G est d'ordre 4, on a que $G \cong \mathbf{Z}/4\mathbf{Z}$ si G contient un élément d'ordre 4 et sinon $G \cong (\mathbf{Z}/2\mathbf{Z})^2$ et G est engendré par toute paire d'éléments d'ordre 2 (qui commutent). En effet, l'ordre d'un élément non trivial de G divise 4 par Lagrange et vaut donc 2 ou 4. Si on a un élément d'ordre 4, alors G est cyclique et $G \cong \mathbf{Z}/4\mathbf{Z}$. Sinon, tout élément non trivial est d'ordre 2 et on peut faire appel à l'exercice 11 ou raisonner à la main. On doit avoir (puisque G est d'ordre 4) au moins un élément d'ordre 2, que nous pouvons appeler x. Puisque $x^2 = e$, $x^{-1} = x$ et donc on doit nécessairement avoir dans G un autre élément $y \neq x$ d'ordre 2. On a ainsi
$$\{e, x, y, xy\} \subseteq G \quad \text{et donc} \quad G = \{e, x, y, xy\}.$$
Noter qu'ici on a utilisé que $xy \neq e, x, y$. On en déduit que $yx \in G$ et $yx \neq e, x, y$ donc $yx = xy$ et cela permet d'écrire la table de G. On reconnaît celle de $(\mathbf{Z}/2\mathbf{Z})^2$ si bien que $G \cong (\mathbf{Z}/2\mathbf{Z})^2$.
- Si G est d'ordre 6, on a que $G \cong \mathbf{Z}/6\mathbf{Z}$ si [11] 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 τ d'ordre 2 et un élément σ d'ordre 3 tels que $\tau\sigma\tau = \sigma^2$. En effet, l'ordre d'un élément non trivial de G vaut (par Lagrange) 2, 3 ou 6. Si on a un élément d'ordre 6, alors G est cyclique et $G \cong \mathbf{Z}/6\mathbf{Z}$. On peut donc supposer que tout élément non trivial est d'ordre 2 ou 3. On va montrer qu'il existe un élément d'ordre 2 et un élément d'ordre 3. En effet, si tous les éléments sont d'ordre 2, il vient qu'alors G est abélien [13] et contient au moins deux éléments d'ordre 2 distincts qui commutent. Le sous-groupe engendré par ces deux éléments est alors isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$

10. En effet, pour $x \in G \smallsetminus \{e\}$, $G = \{e, x, x^2, \ldots, x^{p-1}\}$. On pose alors l'application
$$\varphi : \left\{ \begin{array}{ccc} \mathbf{Z}/p\mathbf{Z} & \longrightarrow & G \\ \overline{k} & \longmapsto & x^k. \end{array} \right.$$
On vérifie comme toujours qu'une application définie sur un quotient est bien définie. Soient pour cela $\overline{k} = \overline{k'}$ pour $k, k' \in \mathbf{Z}$. Par définition, on a $k = k' + p\ell$ pour un certain entier ℓ. On a alors
$$x^k = x^{k'+p\ell} = x^{k'}\,(x^p)^\ell = x^{k'}$$
puisque $x^p = e$. L'application est donc bien définie et surjective vue la description de G plus haut. Comme $\#G = \#(\mathbf{Z}/p\mathbf{Z}) = p$, on a une bijection. Par ailleurs, il s'agit d'un morphisme de groupes puisque pour tous $\overline{k}, \overline{k'}$ dans $\mathbf{Z}/p\mathbf{Z}$ (attention ici que la loi de groupe sur $\mathbf{Z}/p\mathbf{Z}$ est **additive** tandis que celle sur G est **multiplicative**),
$$f\left(\overline{k} + \overline{k'}\right) = f\left(\overline{k+k'}\right) = x^{k+k'} = x^k x^{k'} = f\left(\overline{k}\right) f\left(\overline{k'}\right).$$
On a donc bien un isomorphisme et le résultat !

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

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

donc d'ordre 4, ce qui contredit le théorème de Lagrange. De même, si l'on avait que des éléments d'ordre 3, alors on disposerait d'au moins deux éléments x, y avec $y \neq x, x^2$ d'ordre 3 et

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

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

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

et où tous ces éléments sont deux à deux distincts. Alors, $\sigma\tau \in G$ et comme $\sigma\tau \neq \tau\sigma$, sinon le produit fournit un élément d'ordre [14] 6, on a nécessairement que $\tau\sigma\tau = \sigma^2$. Cela permet de dresser la table de multiplication du groupe G et on reconnaît celle de $\mathfrak{S}_3$ si bien que $G \cong \mathfrak{S}_3$.

- Si G est d'ordre 8, les exercices sur le groupe diédral et les quaternions ainsi le cours sur les produits semi-directs garantira que G est isomorphe soit à $(\mathbf{Z}/2\mathbf{Z})^3$, soit à $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, soit à $\mathbf{Z}/8\mathbf{Z}$, soit au groupe diédral $\mathbf{D}_4$ soit au groupe des quaternions $\mathbf{H}_8$.
- Si G est d'ordre $9 = 3^2$, le cours garantira que G est abélien et donc le théorème de structure des groupes abéliens de type fini garantit que $G \cong \mathbf{Z}/9\mathbf{Z}$ ou $G \cong (\mathbf{Z}/3\mathbf{Z})^2$;
- Si G est d'ordre $10 = 2 \times 5$ avec $2 \mid 5 - 1$, le cours sur le produit semi-direct garantira que G est soit abélien et isomorphe à $\mathbf{Z}/10\mathbf{Z} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$ soit isomorphe à l'unique produit semi-direct non trivial $\mathbf{Z}/2\mathbf{Z} \rtimes \mathbf{Z}/5\mathbf{Z}$ (qui est en fait isomorphe au groupe diédral [15] $\mathbf{D}_5$).

Pour aller plus loin, je vous renvoie aux feuilles de TD des annés précédentes [16] pour le cours d'Algèbre M1 MF, on peut classifier les groupes d'ordre p^2q avec p et q deux nombres premiers distincts ce qui traite le cas de 12 (qui peut également se traiter "à la main"), 13 est premier, 14 et 15 sont alors couverts par le cours sur le produit semi-direct ! On remarquera donc qu'il y a quelque chose qui semble se passer pour les groupes d'ordre 8 ou 12 (on a plus de travail et plus de classes d'isomorphismes). On peut aussi classifier [17] (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 [18] $2^{10} = 1024$. 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

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

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 $\lambda_1, \lambda_2, \ldots, \lambda_r$. Par exemple, dans $\mathfrak{S}_4$, la classe de conjugaison des doubles transpositions [19] correspond à la partition $2 + 2 = 4$ et un 3-cycles à $3 + 1 = 4$.

14. En effet, $(\sigma\tau)^6 = \sigma^6\tau^6$ car G est abélien si $\sigma\tau = \tau\sigma$. Mais comme $\tau^2 = \sigma^3 = e$, on a $(\tau\sigma)^6 = e$. L'ordre de $\tau\sigma$ (qui est différent de e) vaut donc 2, 3 ou 6 mais $(\tau\sigma)^2 = \tau^2\sigma^2$ (toujours par caractère abélien de G) et donc $(\tau\sigma)^2 = \sigma^2 \neq e$ car $\tau^2 = e$ et σ est d'ordre 3. De même, $(\tau\sigma)^3 = \tau \neq e$ et l'ordre de $\tau\sigma$ est bien 6.
15. Voir l'exercice 3.
16. Disponibles sur la page web de David Harari.
17. Voir à nouveau les feuilles de TD de l'an dernier.
18. Voir Besche, Eick et O'Brien, *The groups of order at most 2000*.
19. C'est aussi un exercice intéressant de les dénombrer et on obtient que le cardinal correspondant à une partition $\boldsymbol{\lambda}$ vaut

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

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

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

avec

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

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

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

est une bijection qui montre que $Z_{\mathfrak{S}_n}(\sigma) = Z_{\mathfrak{A}_n}(\sigma) \sqcup \left\{\mu \in \mathfrak{S}_n \smallsetminus \mathfrak{A}_n \ : \ \mu\sigma\mu^{-1} = \sigma\right\}$ 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, σ commute avec le sous-groupe engendré par les cycles apparaissant dans sa décomposition en produit de cycles à supports disjoints. En effet, si τ commute à σ, comme la conjugaison préserve le type de décomposition en produit de cycles à supports disjoints et que tous les cycles apparaissant dans celle de σ sont de longueur différente, cela implique que τ commute à chacun de ces cycles individuellement. Fixons à présent la décomposition en cycle de $\sigma = c_1c_2\cdots c_r$. On utilise alors que si c est un cycle de longueur ℓ, alors le centralisateur de c est donné par

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

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

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

et donc $Z_{\mathfrak{S}_n}(\sigma) \subsetneq Z_{\mathfrak{A}_n}(\sigma)$ strictement. Alternativement, si σ comporte deux cycles $c = (a_1,\dots,a_k)$ 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 $Z_{\mathfrak{S}_n}(\sigma) \subsetneq Z_{\mathfrak{A}_n}(\sigma)$ strictement.

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 [20]

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

où $a_i(\boldsymbol{\lambda})$ 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.

20. 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 $X \setminus \{H\}$ et ainsi à un morphisme $\varphi : H \to \mathfrak{S}(X \setminus \{H\}) \cong \mathfrak{S}_{n-1}$. 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.

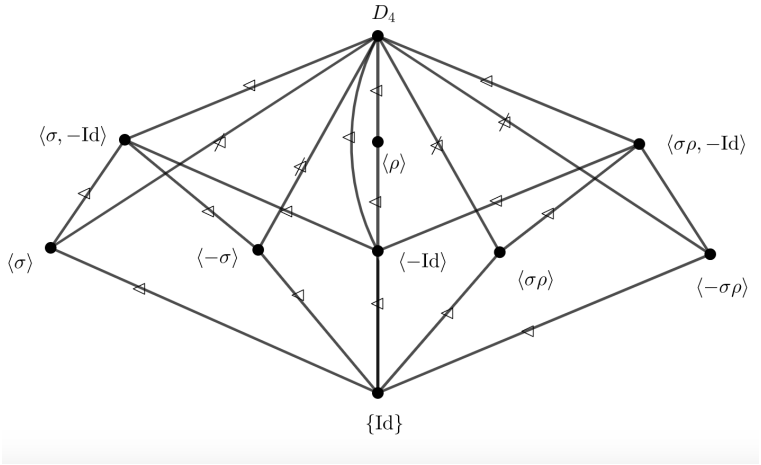
Exercice 2 — Groupe diédral. On considère les deux transformations suivantes du plan euclidien : la rotation ρ de centre O et d'angle $\frac{\pi}{2}$, et la symétrie σ par rapport à l'axe des abscisses. Le groupe *diédral* $\mathbf{D}_4$ est le sous-groupe des isométries du plan engendré par ρ et σ.

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[21] 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[22] : 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

21. Soit géométriquement soit via les matrices.
22. 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

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

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

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

Alors tout sous-groupe de $\mathbf{D}_n$ est égal à un sous-groupe H_d pour un unique diviseur d de n ou à un sous-groupe $H_{d',k}$ pour un unique diviseur d' et un unique k. Lorsque n est pair, les sous-groupes distingués sont les H_d pour $d \mid n$ et $\mathbf{D}_n$ et si n est impair les H_d pour $d \mid n$ et $\mathbf{D}_n$ ainsi que $H_{\frac{n}{2},0}$ et $H_{\frac{n}{2},1}$. Il s'agit d'un exemple de groupe donné par générateurs et relations. Ces groupes seront très important dans le cours de Géométrie au second semestre.
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 — Quaternions et groupes d'ordre 8. On note H l'ensemble des matrices de $\mathcal{M}_2(\mathbf{C})$ de la forme

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

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

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

Solution.

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

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

   à 5 classes de conjugaisons $\{1\}, \{-1\}, \{\pm I\}, \{\pm J\}$ et $\{\pm K\}$. Il est non commutatif par exemple car $IJ \neq JI$.
3. On voit immédiatement que $Z(\mathbf{H}_8) = \{\pm \mathrm{Id}\}$. Puis on voit que tous les commutateurs sont triviaux sauf $[I,J] = [I,K] = [J,K] = -\mathrm{Id}$ si bien que $D(\mathbf{H}_8) = \langle -\mathrm{Id}\rangle = \{\pm\mathrm{Id}\}$.
4. Notons $H = D(\mathbf{H}_8)$. L'abélianisé $\mathbf{H}_8/H$ est donc d'ordre 4 et on voit que les classes ne sont autres que $H = \{\pm 1\}$, $IH = \{\pm I\}$, $JH = \{\pm J\}$ et $KH = \{\pm K\}$ dont on voit[23] 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 façon de voir les choses est de considérer la projection canonique $\pi : \mathbf{H}_8 \to \mathbf{H}_8/H$. On a alors que $\pi(I)^2 = \pi(I^2) = \pi(-1) = \pi(1)$ puisque $-1 \in H = \mathrm{Ker}(\pi)$. On a donc que $\pi(I) \neq \pi(1)$ car $I \notin H$ est d'ordre 2. On obtient de même que tous les éléments non triviaux sont d'ordre 2 dans $\mathbf{H}_8/H$ (on utilise ici la surjectivité de π).
   Une autre méthode consiste à exploiter le fait que $H = D(\mathbf{H}_8) = Z(\mathbf{H}_8)$. Ainsi, si $\mathbf{H}_8/H \cong \mathbf{Z}/4\mathbf{Z}$, alors $\mathbf{H}_8/Z(\mathbf{H}_8)$ serait cyclique et d'après le cours, cela entraînerait que $\mathbf{H}_8$ est abélien, ce qui n'est pas le cas ! On a donc nécessairement que $\mathbf{H}_8^{\mathrm{ab}} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

   ▶ **Compléments.** – Noter que les quaternions fournissent un exemple[24] 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 $s \in G \setminus R$ d'ordre minimal. Si s est d'ordre 2, alors on pose $S = \langle s\rangle$ et $S \cap R = \{e\}$ et G est engendré par R et S et $R \lhd G$ car d'indice 2. On sait alors que $G \cong R \rtimes S \cong \mathbf{Z}/4\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z} \cong D_4$ (on a un seul tel produit semi-direct non abélien à isomorphisme près). Enfin, si s est d'ordre 4 (et que tout élément de $G \setminus R$ est d'ordre 4), renommons r et s par I et J et notons $K = IJ$. On sait que I^2 est d'ordre 2 et c'est le seul élément d'ordre 2 de G. On

23. 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 $\mathbf{H}_8/H$.
24. Et oui, encore !

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 $G \cong \mathbf{H}_8$.