Exercices Algèbre - Groupes I

Exercice 1 — Groupe symétrique I. Soit $\mathfrak{S}_n$ le groupe symétrique d'indice n.

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 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. Soit G un groupe fini. Rappeler pourquoi il existe $n \in \mathbf{N}$ et un homomorphisme injectif de G dans $\mathfrak{S}_n$.
   En déduire qu'il existe $n \in \mathbf{N}$ et un homomorphisme injectif de G dans $\mathfrak{A}_n$ et qu'il existe $n \in \mathbf{N}$ et un homomorphisme injectif de G dans $\mathrm{GL}_n(k)$ pour tout corps k.
4. Une *partition de 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. Que dire des classes de conjugaison dans $\mathfrak{A}_n$?
5. Montrer qu'un sous-groupe H d'indice n dans $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$ (on pourra penser à restreindre l'action de G sur G/H à H).

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 [1] ou encore en utilisant le théorème de Lagrange et le fait que $\mathfrak{S}_3$ n'est pas cyclique car non abélien. Bref, on trouve 3 pour chacun des deux 3-cycles. De même, pour $\mathfrak{S}_4$, on trouve 4 atteint pour les six 4-cycles. Pour $\mathfrak{S}_5$, on obtient 6 pour chacun des 20 produits d'une transposition et d'un 3-cycle à supports disjoints. De manière générale, on voit que l'ordre maximal dans $\mathfrak{S}_n$ est donné par

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

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

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

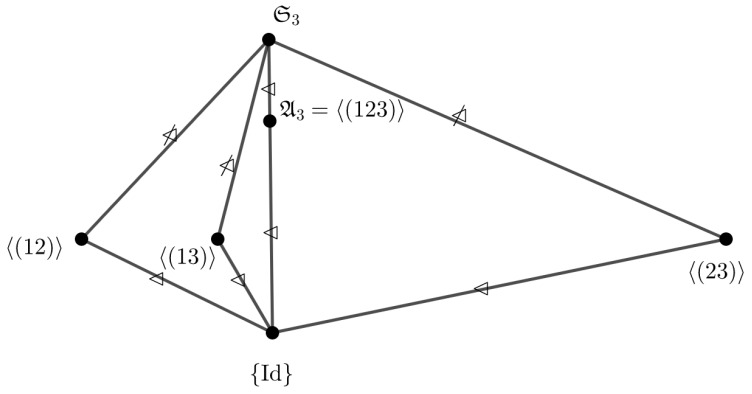
   On obtient par le théorème de Lagrange que $g(n) \mid n!$ et g est croissante. On a par exemple

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

   Landau a démontré [2] en 1909 l'équivalent

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

2. On obtient facilement le treillis suivant [3]



1. 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.
2. En utilisant des résultats d'arithmétique notamment sur la répartition des nombres premiers.
3. 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[4] dans $\mathfrak{S}_3$.
Passons à $\mathfrak{A}_4$. On sait que

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

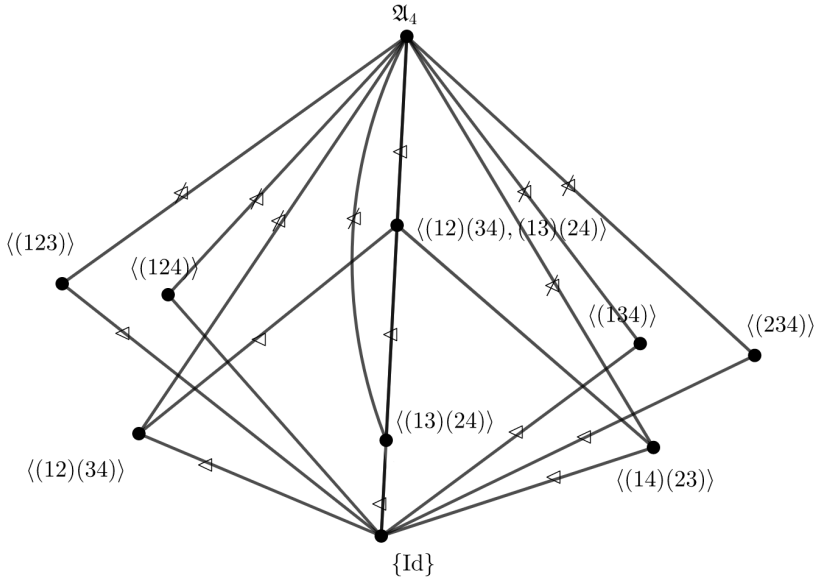
De plus, $\#\mathfrak{A}_4 = 12$ donc les sous-groupes non triviaux sont d'ordre 6, 4, 3 ou 2. Or, on sait qu'un sous-groupe d'ordre 6[5] est soit cyclique soit isomorphe à $\mathfrak{S}_3$. ici la seule option serait $\mathfrak{S}_3$ car on n'a pas d'élément d'ordre 6 mais dans $\mathfrak{S}_3$ aucune paire d'éléments d'ordre 2 ne commutent tandis qu'ici tous les éléments d'ordre 2 commutent

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

Pour les groupes d'ordre 4, on a deux possibilités[6] $\mathbf{Z}/4\mathbf{Z}$ 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 :



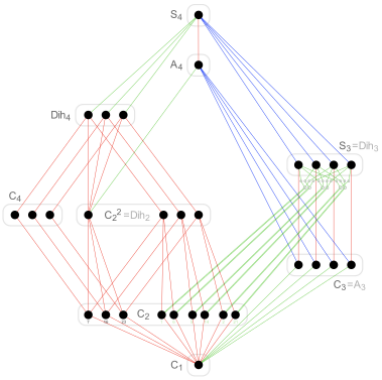
Le groupe trivial est toujours distingué, les sous-groupes d'ordre 2 sont d'indice 2 dans le groupe de Klein donc distingué dans celui-ci. Par ailleurs[7], les sous-groupes d'ordre 3 sont tous conjugués et donc non distingués et de même pour les sous-groupes d'ordre 2. On peut le voir à la main[8] du fait que

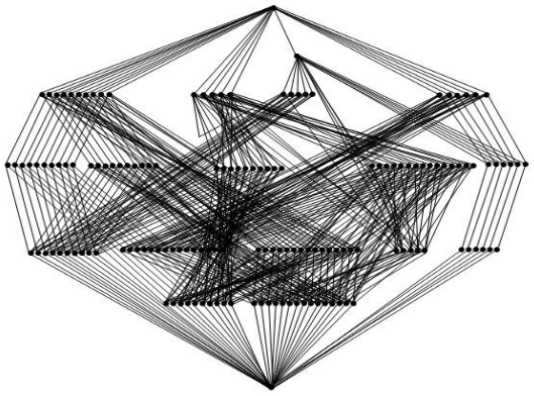
$$(ab)(cd)(abc)(ab)(cd) = (adb) \quad \text{et} \quad (abc)(ab)(cd)(acb) = (ad)(bc) \quad \text{si} \quad \{a, b, c, d\} = \{1, 2, 3, 4\}$$

4. On pouvait le déduire sans calcul des théorèmes de Sylow, puisque ces sous-groupes d'ordre 2 sont les 2-Sylow de $\mathfrak{S}_3$.
5. Voir exercice 5.
6. Idem voir exercice 5.
7. On peut là encore le voir grâce aux théorèmes de Sylow avec les 3-Sylows de $\mathfrak{A}_4$.
8. 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 :





3. Faire agir G sur lui-même par translation à gauche donne lieu à un morphisme $G \longrightarrow \mathfrak{S}(G) \cong \mathfrak{S}_n$ avec $n = \#G$ défini par $g \mapsto (h \mapsto gh)$. Il suffit alors de montrer l'injectivité qui découle de la liberté de l'action. En effet, soit $g \in G$ tel que pour tout $h \in G$, $gh = h$, alors $g = e$.

Pour obtenir un morphisme dans un $\mathfrak{A}_k$, on part du morphisme de Cayley $G \longrightarrow \mathfrak{S}_n$ et on va voir qu'on peut plonger naturellement $\mathfrak{S}_n$ dans $\mathfrak{S}_{n+2}$. On dispose en effet d'un morphisme injectif naturel $\iota : \mathfrak{S}_n \longrightarrow \mathfrak{S}_{n+2}$ obtenu en prolongeant une bijection σ de $\{1,\dots,n\}$ en une permutation de $\{1,\dots,n+2\}$ par $\sigma(n+1) = n+1$ et $\sigma(n+2) = n+2$. On peut alors définir une application

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

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

Pour finir, on procède de même en plongeant $\mathfrak{S}_n$ dans $\mathrm{GL}_n(k)$ via

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

où P_σ est la matrice de permutation associée à σ.

4. 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 $c = (a_1,\dots,a_k)$ un k-cycle de $\mathfrak{S}_n$. Alors pour tout $\sigma \in \mathfrak{S}_n$, on a

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

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 $\lambda_1, \lambda_2, \dots, \lambda_r$. Par exemple, dans $\mathfrak{S}_4$, la classe de conjugaison des doubles transpositions[9] correspond à la partition $2+2=4$ et un 3-cycles à $3+1=4$.

9. 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.

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 $\sigma \in \mathfrak{A}_n$

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

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 $\mu \in \mathfrak{S}_n \setminus \mathfrak{A}_n$ tel que $\mu\sigma\mu^{-1} = \sigma$. Alors, le groupe alterné étant d'indice 2, il existe $\tau \in \mathfrak{S}_n$ tel que $\mathfrak{S}_n = \mathfrak{A}_n \sqcup \mathfrak{A}_n\tau$ et $\mu = \mu'\tau$ si bien que

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

sont deux bijections qui montrent que $Z_{\mathfrak{S}_n}(\sigma) = Z_{\mathfrak{A}_n}(\sigma) \sqcup Z_{\mathfrak{A}_n}(\tau\sigma\tau^{-1})$ avec $\#Z_{\mathfrak{A}_n}(\sigma) = \#Z_{\mathfrak{A}_n}(\tau\sigma\tau^{-1})$. 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 $Z_{\mathfrak{S}_n}(\sigma) = Z_{\mathfrak{A}_n}(\sigma)$.

5. 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 [10]

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

Or, $\#H = (n-1)!$ et $(n-1)! < n!/2$ (car $2 < n$) si bien que nécessairement $\mathrm{Ker}(\psi) = \{\mathrm{Id}\}$ 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* 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 D_4 contient 8 éléments ; caractériser ces éléments géométriquement.

3. Déterminer les classes de conjugaison dans D_4.

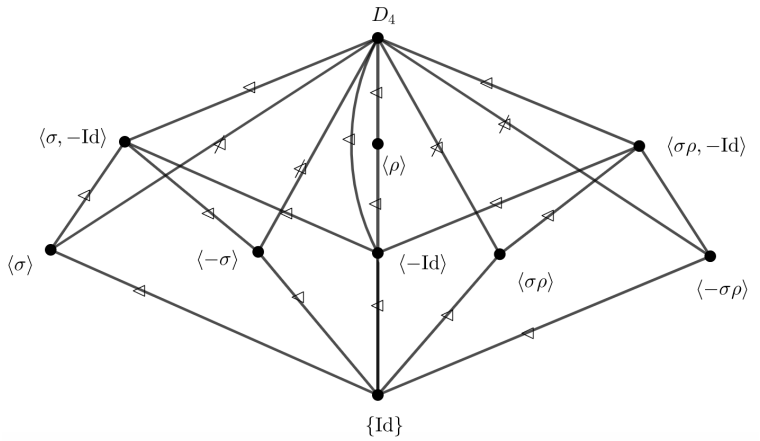
4. Donner le treillis des sous-groupes de D_4, en précisant les sous-groupes distingués.

5. Pour un entier $n > 0$, le groupe diédral D_n est le sous-groupe des isométries du plan engendré par σ et par la rotation ρ' de centre O et d'angle $\frac{2\pi}{n}$. Montrer que D_n contient $2n$ éléments et correspond au groupe des isométries du plan préservant le polygone régulier du plan à n côtés de sommet les racines n-ièmes de l'unité.

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

Solution.

1. On vérifie aisément 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 D_4 contient au moins 8 éléments distincts : 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 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 $r_1, \ldots, r_s \in \{0, \ldots, 3\}$ 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 $\{\rho^2\}$. La relation $\sigma\rho\sigma^{-1}$ montre que la classe de conjugaison de ρ est donnée par $\{\rho, \rho^3\}$ (le conjugué d'une rotation est une rotation). Enfin, la relation $\sigma\rho\sigma = \rho^3$ fournit que $\rho\sigma\rho^{-1} = \sigma\rho^2$ 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 D_4), $\sigma\rho$ 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



   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 D_4 et est même caractéristique (de même que $\langle\rho\rangle$).
5. Tout ce qu'on a fait se généralise bien au cas général. On constate de même que $\sigma\rho\sigma = \rho^{-1}$ et cette relation entraîne que tout élément de 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 D_n est d'ordre $2n$ et que
   $$D_n = \{\mathrm{Id}, \rho, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \ldots, \sigma\rho^{n-1}\}.$$
   On peut montrer que
   $$Z(D_n) = \begin{cases} D_n \text{ si } n \in \{1, 2\} \\ \{\mathrm{Id}\} \text{ si } n \text{ impair et } n \geqslant 3 \\ \{\mathrm{Id}, \rho^{\frac{n}{2}} = -\mathrm{Id}\} \text{ sinon} \end{cases} \quad \text{et} \quad D(D_n) = \langle[\sigma, \rho]\rangle\langle\rho^2\rangle (= \langle\rho\rangle \text{ si } n \text{ impair}).$$

Dans le cas pair, $D_n/Z(D_n) \cong D_{n/2}$ et $D_n^{\text{ab}} \cong \mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$ si n est pair et $\cong \mathbf{Z}/2\mathbf{Z}$ si n ets impair. On verra que $D_n = \langle\rho\rangle\rtimes\langle\sigma\rangle \cong \mathbf{Z}/n\mathbf{Z}\rtimes_\varphi \mathbf{Z}/2\mathbf{Z}$ avec $\varphi(1)$ donné par $\overline{m} \mapsto -\overline{m}$. On a $D_2 \cong \mathbf{Z}/2\mathbf{Z}$ et $D_3 \cong \mathfrak{S}_3$. Le groupe D_n est résoluble et nilpotent si, et seulement si, son ordre est une puissance de 2. Les classes de conjugaison sont $\{\text{Id}\}$, $\{-\text{Id}\}$, $\{\rho^k, \rho^{-k}\}$ pour $k \in \left\{1, \dots, \frac{n}{2}-1\right\}$, $\{\sigma, \sigma\rho^2, \dots, \sigma\rho^{n-2}\}$ et $\{\sigma\rho, \sigma\rho^3, \dots, \sigma\rho^{n-1}\}$ si n est pair tandis que si n est impair, on obtient $\{\text{Id}\}$, $\{\rho^k, \rho^{-k}\}$ pour $k \in \left\{1, \dots, \frac{n-1}{2}\right\}$ et $\{\sigma, \sigma\rho, \dots, \sigma\rho^{n-1}\}$. Enfin, pour tous diviseurs positifs d et d' de n et $k \in \left\{0, 1, \dots, \frac{n}{d'}-1\right\}$, on pose

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

Alors tout sous-groupe de 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 D_n et si n est impair les H_d pour $d \mid n$ et D_n ainsi que $H_{\frac{n}{2},0}$ et $H_{\frac{n}{2},1}$.
Finalement terminons par la caractérisation géométrique du groupe D_n. Il est clair que 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. Il n'y a que deux isométries envoyant l'arête AB sur l'arête CD, une rotation et la composée de cette rotation avec la symétrie d'axe la médiatrice du segment $[CD]$. L'image de l'arête AB détermine complètement l'isométrie et comme on a n arêtes, on obtient bien $2n$ isométries.

Exercice 3. Soient G un groupe et H un sous-groupe de G d'indice fini m. On note G/H l'ensemble des classes de G modulo H (ceci n'est pas un groupe en général). Pour $g \in G$, on note $h_g : G/H \to G/H$ l'application $aH \mapsto gaH$.

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

Solution.

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

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

On vérifie de même qu'il s'agit bien d'une bijection bien définie et que h_2 est un morphisme de groupes de même noyau que h. Le même raisonnement qu'en question **2.** fournit alors la conclusion souhaitée $[H : \text{Ker}(h)] \mid (m-1)!$ car $\mathfrak{S}(G/H \setminus \{H\}) \cong \mathfrak{S}_{m-1}$. En fait, on a restreint l'action précédente en une action de H sur G/H et utilisé le fait que puisque H est un point fixe de G/H pour cette action, cela donne lieu à une action de H sur $G/H \setminus \{H\}$ de même noyau que h.
Noter qu'en TD, l'un d'entre vous a suggéré d'utiliser le troisième théorème d'isomorphisme. Je rappelle que ce théorème garantit que si $N \lhd G$ et $H \lhd G$ avec $N \leqslant H$, alors $H/N \lhd G/N$ et l'application $f : G/N \to G/H$ qui à gN associe gH est bien définie de noyau H/N et passe au quotient pour donner un isomorphisme $(G/N)/(H/N) \cong G/H$. L'hypothèse que les deux groupes sont distingués est importante sinon G/H ou G/N n'a pas de structure de groupe et H/N n'est pas nécessairement distingué dans G/N. Par ailleurs, comme vous le verrez dans le cours, le fait qu'on ait un isomorphisme $G/H \cong N$ **n'implique pas** que $G \cong H \times N$ et en particulier ici on n'a pas nécessairement $G/N \cong G/H \times H/N$ (penser par exemple à $G = \mathbf{H}_8$, $H = Z(\mathbf{H}_8) \cong \mathbf{Z}/2\mathbf{Z}$ et $N = G/H \cong (\mathbf{Z}/2\mathbf{Z})^2$. En revanche, on a bien dans tous les cas une **bijection** entre G/N et $G/H \times H/N$. Cela est évident par cardinalité si G est fini mais ici ce n'est pas dans les hypothèses et il faut alors remarquer que l'application ensembliste surjective (l'ensemble d'arrivée n'étant pas nécessairement un groupe) $f : G/\text{Ker}(h) \to G/H$ qui à $g\text{Ker}(h)$ associe gH est bien définie et passe au quotient pour la relation donnée par le groupe $H/\text{Ker}(h)$ 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** $G/\text{Ker}(h) \cong G/H \times H/\text{Ker}(h)$ obtenue, on peut alors dire que $[G : \text{Ker}(h)] = [G : H] \times [H : \text{Ker}(h)]$ et donc $[G : H] \times [H : \text{Ker}(h)] = m \times [H : \text{Ker}(h)] \mid m!$ et finalement $[H : \text{Ker}(h)] \mid (m-1)!$.

5. On a $m = 2$ et la question **4.** fournit alors que $[H : \mathrm{Ker}(h)] = 1$ soit $H = \mathrm{Ker}(h)$. Ainsi $H \lhd G$.
6. On a donc que G et H sont finis de cardinal une puissance de p. Par **4.**, on a donc $\#H \mid (p-1)!\#\mathrm{Ker}(h)$. Mais $\#H$ est premier avec $(p-1)!$ donc $\#H \mid \#\mathrm{Ker}(h)$ et la question **3.** permet alors de conclure à nouveau à l'égalité $H = \mathrm{Ker}(h)$. Ainsi $H \lhd G$.
7. De même, $\#H \mid (m-1)!\#\mathrm{Ker}(h)$ et $\#H = \#G/m$ ne contient que des facteurs premiers $\geqslant m$ et donc $\#H$ est premier avec $(m-1)!$ et on conclut comme en question précédente.

Exercice 4 — 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 1 la matrice identité, et on pose $I := M_{i,0}$, $J = M_{0,1}$, $K = M_{0,i}$. Soit $\mathbf{H}_8 = \{\pm 1, \pm I, \pm J, \pm K\}$. Montrer que $\mathbf{H}_8$ est un sous-groupe non commutatif de cardinal 8 de H^* (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. Justifier que $\mathbf{H}_8$ n'est pas un produit semi-direct et déterminer, à isomorphisme près, tous les groupes d'ordre 8.
6. Est-ce qu'un groupe dont tous les sous-groupes sont distingués est nécessairement abélien ?

Solution.

1. On calcule le produit $M_{a,b}M_{c,d} = M_{ac-b\bar{d},ad+b\bar{c}}$ ce qui permet de conclure.
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 $\{\pm K\}$.
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 $D(\mathbf{H}_8) = \{\pm \mathrm{Id}\}$.
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 qu'on a $IH^2 = JH^2 = KH^2 = H$. On a donc nécessairement que $\mathbf{H}_8^{\mathrm{ab}} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
5. 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 $G \setminus R$ sont 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 $G/Z(G) \cong \mathbf{Z}/2\mathbf{Z}$ 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 $G \cong \mathbf{H}_8$.

6. 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.

Exercice 5. Faire la liste, à isomorphisme près, des groupes de cardinal $\leqslant 7$.

Solution.

1. Le seul groupe d'ordre 1 est le groupe trivial ;
2. 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 et 7.
3. 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 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). Le produit de ces deux éléments est alors d'ordre 6 (le groupe est abélien) 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 $\mathrm{Id}, \sigma, \sigma^2, \tau, \tau\sigma, \sigma\tau$. 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 $G \cong \mathfrak{S}_3$;
4. Le cas des groupes d'ordre 8 a été traité dans l'exercice précédent.

On remarque donc qu'il y a quelque chose qui semble se passer pour les groupes d'ordre 8 (on a plus de travail et plus de classes d'isomorphismes). On va classifier (à isomorphisme près) les groupes de cardinal $\leqslant 15$ dans le TD suivant et 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 (14). En fait, on peut voir que plus l'ordre du groupe possède de facteurs premiers, 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 ce nombre de facteurs premiers 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 [11] $2^{10} = 1024$. 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

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

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

Solution.

1. Faisant agir G sur G/H, on obtient un morphisme $f : G \to \mathfrak{S}(G/H) \cong \mathfrak{S}_n$ dont le noyau convient.
2. On a clairement que
$$\bigcup_{g\in G} gHg^{-1} = \bigcup_{\overline{g}\in G/H} gHg^{-1}$$

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

où gHg^{-1} ne dépend que de la classe de g dans G/H car $(gh)H(gh)^{-1} = gHg^{-1}$. Il vient par conséquent que (bien faire attention ici que e appartient à chacun des conjugués)

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

car $H\neq G$ si bien que

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

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

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

Cela entraîne alors nécessairement que

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

4. Le résultat devient alors faux en général. On pose $G=\mathrm{GL}_n(\mathbf{C})$ et $H=T_n(\mathbf{C})\cap G$ le sous-groupe des matrices triangulaires supérieures inversibles. On sait alors que toute matrice de G est trigonalisable, autrement dit conjuguée à une matrice de $T_n(\mathbf{C})$ de sorte que

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

mais H est d'indice infini dans[12] G. Pour voir que l'indice est infini, on peut par exemple utiliser le fait que toute matrice M de $GL_n(\mathbf{C})$ s'écrit sous la forme $M=\exp(N)=\left(\exp\left(\frac{N}{n}\right)\right)^n$ et donc toute matrice de $GL_n(\mathbf{C})$ est une puissance n-ième pour tout entier naturel n. Supposons alors que $GL_n(\mathbf{C})$ possède un quotient fini, disons d'ordre r. Pour toute matrice $M\in GL_n(\mathbb{C})$, il existe B telle que $M=B^r$ et ainsi la classe de M est triviale si bien qu'un tel quotient est nécessairement trivial. Puisque $T_n(\mathbf{C})\neq GL_n(\mathbf{C})$, on en déduit qu'il est d'indice infini.

5. On choisit $x_0\in X$ et on note $H=\mathrm{Stab}_G(x_0)$. On a alors que H est un sous-groupe de G différent de G (sinon $X=\{x_0\}$ par transitivité). On peut donc trouver $g_0\in G$, $g_0\notin\bigcup_{g\in G} gHg^{-1}$. Soit alors $x\in X$. On sait qu'il existe $g\in G$ tel que $x=g\cdot x_0$ et alors $\mathrm{Stab}_G(x)=gHg^{-1}$ donc par construction $g_0\notin\mathrm{Stab}_G(x)$, ce qui signifie que $g_0\cdot x\neq x$ ce qui conclut la preuve.

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

Exercice 7.

1. Soit G un groupe tel que $G/Z(G)$ est cyclique. Rappeler pourquoi G est abélien. Le résultat tient-il toujours si l'on suppose seulement que $G/Z(G)$ est abélien ?

2. Justifier que la probabilité que deux éléments d'un groupe non abélien commutent est $\leqslant\frac{5}{8}$.

3. Montrer qu'un p-groupe d'ordre p^n possède des sous-groupes d'ordre p^i pour tout $i\in\{0,\dots,n\}$ (on peut même imposer la condition que ces sous-groupes soient distingués comme dans l'exercice 6 du Perrin).

4. Soient p un nombre premier et P un p-Sylow de G. Montrer que $P\cdot Z(G)$ est un sous-groupe de G, et que $(P\cdot Z(G))/Z(G)$ est un p-Sylow de $G/Z(G)$.

5. Montrer que ceci induit une bijection entre les p-Sylow de G et les p-Sylow de $G/Z(G)$.

12. 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.

Solution.

1. On note $\overline{a}$ un générateur de $G/Z(G)$. Tout élément de G est alors de la forme $a^m z$ avec $m \in \mathbf{N}$ et $z \in Z(G)$ ce qui permet de conclure. Le résultat tombe en défaut si l'on suppose seulement abélien comme on le voit avec le contre-exemple des quaternions.

2. En effet, si G est non abélien, alors par l'exercice 7, $G/Z(G)$ ne peut pas être cyclique est est donc de cardinal au moins 4. Si l'on note $z = \#Z(G)$ et $n = \#G$, alors $n \geqslant 4z$. Si maintenant $x \in Z(G)$, pour tout $y \in G$, x et y commutent. Soit alors $x \in G \setminus Z(G)$. Les éléments y qui commutent avec x sont les éléments du centralisateur de x pour l'action par conjugaison. On obtient alors un sous-groupe strict car x n'est pas central, de cardinal $\leqslant \frac{n}{2}$. On obtient finalement que le nombre de paires $(x, y) \in G^2$ qui commutent vérifie
$$\leqslant zn + (n-z)\frac{n}{2} = \frac{nz}{2} + \frac{n^2}{2} \leqslant \frac{n^2}{8} + \frac{n^2}{2} = \frac{5}{8}n^2.$$
Il reste à diviser par $\#G^2 = n^2$ pour obtenir que la probabilité est bien $\leqslant \frac{5}{8}$. Noter que cette probabilité est optimale et est notamment pour les groupes [13] $\mathbf{H}_8$ et $\mathbf{D}_4$.

3. On raisonne par récurrence sur n. Pour $n = 0$, c'est évident. Supposons la propriété connue pour les groupes d'ordre p^n et soit G un groupe d'ordre p^{n+1}. Si $i = 0$, il n'y a rien à faire et on peut supposer que $i \geqslant 1$. On sait que $Z(G)$ est non trivial et en tant que p-groupe, il admet un élément d'ordre p donc un sous-groupe Z d'ordre p. Comme Z est central, il est distingué et on note $\pi : G \to G/Z$ la surjection canonique. Par hypothèse, G/Z est de cardinal p^n et possède donc un sous-groupe H' de cardinal p^{i-1}. Il est alors clair que $H = \pi^{-1}(H')$ est un sous-groupe de G de cardinal p^i ce qui conclut la preuve.

4. Par le théorème d'isomorphisme, on a que $PZ(G)/Z(G) \cong P/(P \cap Z(G))$ et est un sous-groupe de $G/Z(G)$ qui s'identifie à $\pi(P)$ où $\pi : G \to G/Z(G)$ est la surjection canonique. Ce qui suit est à rapprocher du théorème 2.13 et serait valable en remplaçant $Z(G)$ par n'importe quel sous-groupe H distingué dans G. Commençons par établir que $P \cap Z(G)$ est un p-Sylow de $Z(G)$. Le groupe P est un p-Sylow de $PZ(G)$ car contenu dans $PZ(G)$ et un p-groupe de cardinal maximal. On note alors $\#P = p^n$ et $\#PZ(G) = p^n s$ avec $p \nmid s$. On écrit alors $\#Z(G) = p^m r$ avec $p \nmid r$, $m \leqslant n$ et $r \mid s$. Par le théorème d'isomorphisme, on a $\#(P \cap Z(G)) = \#P\#Z(G)/\#PZ(G) = p^m \frac{r}{s}$. Mais $P \cap Z(G)$ est un p-groupe donc $s = r$ et $P \cap Z(G)$ est un p-Sylow de $Z(G)$. Posons alors $\#G = p^n t$ avec $p \nmid t$ et $s \mid t$. On a alors $\#(G/Z(G)) = p^{n-m}\frac{t}{s}$. Or, $PZ(G)/Z(G)$ est d'ordre p^{n-m}, il s'agit donc d'un p-Sylow de $G/Z(G)$.

5. On considère alors l'application bien définie f des p-Sylow de G dans les p-Sylow de $G/Z(G)$ qui à P associe $PZ(G)/Z(G)$ et vérifions qu'il s'agit bien d'une bijection. Définissons pour ce faire la bijection réciproque.
Soit à présent S un p-Sylow de $G/Z(G)$. On pose alors $H = \pi^{-1}(S)$. On remarque que $G/H \to \tilde{G}/S$ est une bijection [14] avec $\tilde{G} = G/Z(G)$ si bien que si l'indice de S dans $\tilde{G}$ est premier à p, il en est de même de celui [15] de H dans G. Ainsi un p-Sylow de H est un p-Sylow de G. Soit alors P un p-Sylow de H (et donc de G). Par ailleurs, par définition de H, on a $Z(G) \lhd H$ et ainsi le sous-groupe $PZ(G) \leqslant H$. On a aussi d'après **4.** que $\pi(P) = PZ(G)/Z(G)$ est un p-Sylow de $\tilde{G}$ inclus dans S, donc égal à S. Ainsi $\pi(P) = S = \pi(H)$ et on en déduit que $H \leqslant PZ(G)$ et donc que $H = PZ(G)$. Enfin, P est unique. En effet, si P' est un autre p-Sylow de H, alors il existe $g \in H$ tel que $P' = gPg^{-1}$. Mais on vient de voir que $H = PZ(G)$ de sorte que $g = g_1 g_2$ avec $g_1 \in P$ et $g_2 \in Z(G)$ si bien que
$$P' = gPg^{-1} = P' = g_1 g_2 P g_2^{-1} g_1^{-1} = g_1 P g_1^{-1} = P$$
car g_2 commute à tout élément de G et $g_1 \in P$. Finalement, on définit g de l'ensemble des p-Sylow de $\tilde{G} = G/Z(G)$ vers celui des p-Sylow de G qui à tout p-Sylow S de $\tilde{G}$ associe l'unique p-Sylow P de G tel que $\pi^{-1}(S) = PZ(G)$. Cette application est bien définie et est bien la réciproque de f. On pouvait aussi bien sûr utiliser ce qui précède pour démontrer que f est injective et surjective.

Exercice 8 — Exposant d'un groupe. On définit *l'exposant* d'un groupe abélien fini G et on note $\exp(G)$, comme le plus petit entier $n \geqslant 1$ tel que $g^n = 1$ pour tout $g \in G$.

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

Solution.

1. Notons r l'ordre de xy. Puisque G est abélien, on a $(xy)^{nm} = (x^m)^n (y^n)^m = 1$ donc $r \mid mn$. En outre, $1 = (xy)^{rm} = y^{rm}$ donc $n \mid rm$ et donc $n \mid r$ par coprimalité. De même, $m \mid r$ et par coprimalité $nm \mid r$ et $r = nm$.
2. Non, on peut par exemple prendre un élément $x \in G$ d'ordre au moins 2 et $y = x^{-1}$.

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

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

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

3. Posons $M = \text{ppcm}(\omega(x) \ : \ x \in G)$. Par le théorème de Lagrange, $x^M = 1$ pour tout $x \in G$ et $\exp(G) \leqslant M$. Montrons que cette borne est atteinte. Soient $p_1, \dots, p_k$ premiers et $a_1, \dots, a_k$ des entiers strictement positifs tels que $M = \prod_{i=1}^{k} p_i^{a_i}$. Pour tout $i \in \{1, \dots, k\}$, il existe un élément $x_i \in G$ d'ordre $p_i^{a_i}$. En effet, par définition de M, il existe $y_i \in G$ d'ordre $p_i^{a_i} q$ avec $p_i \nmid q$ et $x_i = y^q$ convient. Ainsi, $x = \prod_{i=1}^{k} x_i$ convient et est d'ordre M d'après **1**.

4. Soit G le groupe multiplicatif, de cardinal n, d'un corps k. On veut montrer l'existence d'un élément d'ordre n dans G. On sait par **3.** qu'il existe un élément $g_0 \in G$ d'ordre $\exp(G)$ et que $\exp(G) \leqslant n$ par Lagrange. Par ailleurs, $x^{\exp(G)} = 1$ pour tout $x \in G$. Or, dans un corps, le nombre de racines comptées avec multiplicité d'un polynôme est majoré par son degré de sorte que $n \leqslant \exp(G)$ et finalement g_0 est d'ordre n et G est cyclique.

Exercice 9.

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. Pour quels entiers e, un groupe d'exposant e est-il nécessairement commutatif ?

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.

2. Clairement $e = 1$ ou 2 convient d'après **1** et ce sont les seuls. Si $e \geqslant 3$ divisible par 4, alors $\mathbf{Z}/e\mathbf{Z} \times \mathbf{H}_8$ 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 $\text{GL}_p(\mathbf{F}_p)$ 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 10. Soit $P_n(k)$ le nombre de permutations de $\{1, \dots, n\}$ qui ont exactement k points fixes. Montrer que $\sum_{k=0}^{n} k P_n(k) = n!$ (cette dernière question était un exercice des olympiades de La Havane en 1987...).

Solution. On considère alors l'action de $\mathfrak{S}_n$ sur $\{1, \dots, n\}$ donnée par $\sigma \cdot i = \sigma(i)$. Il s'agit d'une action transitive. On remarque alors que

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

La formule de Burnside permet alors de conclure que

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

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

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

Exercice 11. Soient p un nombre premier et G un p-groupe fini. Soit $(A, +)$ un groupe abélien avec $A \neq \{0\}$. On suppose donnée une action de G sur A par automorphismes, c'est-à-dire que pour tout $g \in G$, la bijection $x \mapsto g \cdot x$ de A dans A est un automorphisme du groupe abélien A. On suppose de plus que A est *de torsion p-primaire*, *i.e.* pour tout $x \in A$, il existe $m \in \mathbf{N}$ tel que $p^m x = 0$.

1. Montrer que si A est fini, son cardinal est une puissance de p (on pourra utiliser la classification des groupes abéliens finis, ou encore le théorème de Sylow).

2. On suppose que A est fini. Montrer qu'il existe $x \neq 0$ dans A tel que pour tout $g \in G$, on ait $g \cdot x = x$.

3. On ne suppose plus A fini. Soit $a \neq 0$ dans A. Montrer que le sous-groupe B de A engendré par $\{g \cdot a, g \in G\}$ est fini.

4. En déduire que le résultat de **2.** vaut encore sans l'hypothèse A fini.

Solution.

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

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

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 en disant que tout élément de G engendre un p-groupe et appartient donc à un p-Sylow mais puisque A est abélien, on a un unique p-Sylow et celui-ci contient A, il lui est donc égal.

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

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

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

3. On peut utiliser le théorème de structure des groupes abéliens de type fini couplé au fait que tout élément de A est de torsion.

4. On applique simplement le résultat de **2.** à B et il existe $x \neq 0$ dans $B \subseteq A$ tel que pour tout $g \in G$, $g \cdot x = x$.

Exercice 12.

1. Combien y a-t-il d'opérations du groupe $\mathbf{Z}/4\mathbf{Z}$ sur l'ensemble $\{1, 2, 3, 4, 5\}$?

2. Soient G et X deux groupes. On dit que G *opère par automorphismes* sur X si on s'est donnée une opération $(g, x) \mapsto g.x$ de G sur X telle que pour tout $g \in G$, l'application $x \mapsto g.x$ soit un automorphisme de X. L'opération de G sur lui-même par translation est-elle une opération par automorphismes ? Même question pour l'opération par conjugaison.

3. On prend $G = (\mathbf{Z}/3\mathbf{Z}, +)$ et $X = (\mathbf{Z}/13\mathbf{Z}, +)$. Combien y a-t-il d'actions de G sur X par automorphismes ? Même question en remplaçant $\mathbf{Z}/13\mathbf{Z}$ par le groupe symétrique $\mathfrak{S}_3$.

Solution.

1. On cherche le nombre de morphismes de $\mathbf{Z}/4\mathbf{Z}$ dans le groupe des permutations $\mathfrak{S}_5$. Se donner un tel morphisme f revient à se donner un élément d'ordre divisant 4 (à savoir $f(\bar{1})$) dans $\mathfrak{S}_5$. Or $\mathfrak{S}_5$ contient un élément d'ordre 1 (l'identité), $C_5^2 = 10$ transpositions, $5.3 = 15$ doubles transpositions (cinq façons de choisir le point fixe, puis trois doubles transpositions avec les quatre éléments restants) et $5.6 = 30$ 4-cycles (cinq façons de choisir le point fixe, et six 4-cycles dans le groupe des permutations des quatre éléments restants). Il y a donc au total $1 + 10 + 15 + 30 = 56$ possibilités.

2. Clairement, oui pour l'opération par conjugaison, non pour l'opération par translation.

3. On sait que le groupe des automorphismes de X est isomorphe au groupe multiplicatif des inversibles de l'anneau $\mathbf{Z}/13\mathbf{Z}$ (en effet si on pose $\varphi_a(x) = ax$, on vérifie immédiatement que $a \mapsto \varphi_a$ est un isomorphisme de $(\mathbf{Z}/13\mathbf{Z})^\times$ sur $\mathrm{Aut}(X)$), lequel est isomorphe au groupe additif $\mathbf{Z}/12\mathbf{Z}$ car 13 est premier. On cherche donc le nombre de morphismes de $\mathbf{Z}/3\mathbf{Z}$ dans $\mathbf{Z}/12\mathbf{Z}$, ou encore le nombre déléments de $\mathbf{Z}/12\mathbf{Z}$ d'ordre divisant 3. Il y a ainsi trois solutions.

On voit facilement que les seuls automorphismes de $\mathfrak{S}_3$ sont intérieurs (voir un des exercices de la feuille 2 et sinon on utilise le fait que $\mathfrak{S}_3$ est engendré par (12) et (123) donc on a au plus 6 automorphismes et on a six automorphismes intérieurs). Le groupe des automorphismes de $\mathfrak{S}_3$ est donc isomorphe à $\mathfrak{S}_3$ quotienté par son centre (car on a la suite exacte $1 \to Z(G) \to G \xrightarrow{f} \mathrm{Int}(G) \to 1$ avec $f(g) = i_g$ et $i_g(x) = gxg^{-1}$), *i.e.* à $\mathfrak{S}_3$. On est donc ramené à chercher le nombre d'éléments d'ordre 1 ou 3 dans $\mathfrak{S}_3$, et il y a trois solutions.

Exercice 13. Soit G un groupe. Soit $x_0 \in G$. On appelle *centralisateur* de x_0 l'ensemble G_{x_0} des éléments x de G vérifiant $xx_0 = x_0x$.

1. Montrer que G_{x_0} est un sous-groupe de G. Est-il toujours distingué ?

2. On suppose G fini. Soit C la classe de conjugaison de x_0. Trouver une relation entre $\#G$, $\#C$, et $\#G_{x_0}$.

Solution.

1. Il est immédiat que G_{x_0} est un sous-groupe de G, mais il n'est pas toujours distingué : par exemple, dans $\mathfrak{S}_3$, le centralisateur d'une transposition τ est le sous-groupe $\{\mathrm{id}, \tau\}$, lequel n'est pas distingué.

2. Le groupe G opère par conjugaison sur lui-même. Par définition C est l'orbite de x_0 et G_{x_0} son stabilisateur, d'où

$$\#G = \#C.\#G_{x_0}.$$

Exercice 14. 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 $D(G) \subset V_4$ (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.

3. En déduire que $D(G) = V_4$.

4. Montrer que si H est un sous-groupe d'indice 2 d'un groupe fini A, alors $H \lhd A$ (regarder les classes à gauche et à droite suivant G).

5. Soit H un sous-groupe de $G = \mathfrak{A}_4$. Montrer que si H est d'indice 2, alors $D(G) \subset H$ (on considérera G/H) et aboutir à une contradiction en utilisant **3**. Ainsi G (qui est de cardinal 12) n'a pas de sous-groupe de cardinal 6.

6. Montrer au contraire que pour tout $d \in \mathbf{N}^\times$ 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.
3. 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 $D(G) = V_4$.
4. 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 $H \lhd A$.
5. 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.
6. 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 D_4, par exemple celui engendré par un 4-cycle et une transposition.

Exercice 15. Soit $n \geqslant 5$. Trouver tous les morphismes de groupes de $\mathfrak{S}_n$ dans $(\mathbf{Z}/12\mathbf{Z}, +)$. Que se passe-t-il si on remplace $\mathbf{Z}/12\mathbf{Z}$ par un groupe abélien quelconque ? Et si on prend $n = 4$?

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

Exercice 16. 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 $p_1/q_1, \ldots, p_n/q_n$, 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).

Exercice 17. Soit G un groupe fini agissant sur un ensemble fini X. Calculer le nombre moyen de points fixes d'un élément de G. Que dire en particulier si l'action est transitive ? De la moyenne du nombre de points fixes d'une permutation aléatoire ?

Solution. Par la formule de Burnside, on voit que le nombre moyen de point fixe vaut

$$\frac{1}{\#G} \sum_{g \in G} \#\mathrm{Fix}(g) = \sum_{x \in X} \frac{1}{\#\omega(x)} = \#\Omega$$

où Ω est l'ensemble des orbites. Dans le cas d'une action transitive, on voit donc que ce nombre moyen est de 1 et dans le cas du groupe symétrique et de son action naturelle sur $\{1, \ldots, n\}$ (qui est transitive), on trouve 1 point fixe en moyenne.

Exercice 18 — Lemme de Cauchy. Soit G un groupe fini et p un nombre premier divisant le cardinal de G. En utilisant une action convenable de $\mathbf{Z}/p\mathbf{Z}$ sur l'ensemble

$$X = \left\{(g_1, \ldots, g_p) \in G^p \ : \ g_1 g_2 \cdots g_p = 1\right\},$$

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

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

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

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

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

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

Exercice 19. Combien y a-t-il de colliers différents formés de 9 perles dont 4 bleues, 3 blanches et 2 rouges ?

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

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

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

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

tels colliers.

Exercice 20. Soit $n \geqslant 1$. Montrer qu'il n'existe qu'un nombre fini de classes d'isomorphismes de groupes finis admettant exactement n classes de conjugaison.

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

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

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

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

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

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

Il s'ensuit que

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

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