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. Si l'article vous intéresse (et que vous lisez l'allemand), je peux vous transmettre l'article ! Vous trouverez une version en français ici.
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 :

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.

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

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

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 $G \to \mathfrak{S}(G) \cong \mathfrak{S}_n$ avec $n = \#G$ défini par $g \mapsto (h \mapsto gh)$. Il suffit alors de montrer l'injectivité qui découle de la liberté de l'action. En effet, soit $g \in G$ tel que pour tout $h \in G$, $gh = h$,

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.

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

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

L'application est clairement bien définie et on vérifie aisément qu'il s'agit d'un morphisme de groupes injectif (car $i(\sigma)$ pour $\sigma \in \mathfrak{S}_n$ et $(n+1 \ n+2)$ sont à support disjoint et commutent donc) et finalement G se plonge dans $\mathfrak{A}_{n+2}$.
Pour finir, on procède de même en plongeant $\mathfrak{S}_n$ dans $\mathrm{GL}_n(k)$ 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 $3+1=4$.
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 $Z_{\mathfrak{A}_n}(\sigma) \subseteq Z_{\mathfrak{S}_n}(\sigma)$ 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 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

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

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.

et donc $\mathrm{Cl}_{\mathfrak{S}_n}(\sigma) = \mathrm{Cl}_{\mathfrak{A}_n}(\sigma)$. 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 $\mathrm{Cl}_{\mathfrak{S}_n}(\sigma) = \mathrm{Cl}_{\mathfrak{A}_n}(\sigma)$.

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.

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 $\langle\rho\rangle$).

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 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. Est-ce qu'un groupe dont tous les sous-groupes sont distingués est nécessairement abélien ?

Solution.

1. On calcule le produit $M_{a,b}M_{c,d} = M_{ac-b\overline{d},ad+b\overline{c}}$ 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. 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 4. 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 5 — 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.

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

Solution.

1. Notons r l'ordre de xy. Puisque G est abélien, on a $(xy)^{nm} = (x^m)^n (y^n)^m = 1$ donc $r \mid mn$. En outre, $1 = (xy)^{rm} = y^{rm}$ donc $n \mid rm$ et donc $n \mid r$ par coprimalité. De même, $m \mid r$ et par coprimalité $nm \mid r$ et $r = nm$.
2. Non, on peut par exemple prendre un élément $x \in G$ d'ordre au moins 2 et $y = x^{-1}$.
3. Posons $M = \text{ppcm}(\omega(x) \ : \ x \in G)$. 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 6.

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.

   On peut alors établir que, si G est fini, alors $G \cong (\mathbf{Z}/2\mathbf{Z})^r$ pour un certain entier r. En effet, on peut choisir $x_1, \dots, x_r$ un système minimal de générateurs de G. On vérifie alors que l'application

   $$\varphi : \left\{ \begin{array}{ccc} (\mathbf{Z}/2\mathbf{Z})^r & \longrightarrow & G \\ (\alpha_1, \dots, \alpha_r) & \longmapsto & x_1^{\alpha_1} \cdots x_r^{\alpha_r} \end{array} \right.$$

   est bien définie et est un morphisme de groupes surjectif par définition d'un système de générateur et injectif car ce système de générateur a été choisi minimal. Il s'agit par conséquent d'un isormophisme.
2. Clairement $e = 1$ ou 2 convient d'après **1** et ce sont les seuls. Si $e \geqslant 3$ divisible par 4, alors $\mathbf{Z}/(e/4)\mathbf{Z} \times \mathbf{H}_8$ est d'exposant e et non commutatif. Si maintenant $4 \nmid e$, alors e admet un facteur premier impair et $\mathbf{Z}/(e/p)\mathbf{Z} \times U(p)$ avec $U(p)$ le sous-groupe de $\mathrm{GL}_p(\mathbf{F}_p)$ formé des matrices triangulaires supérieures avec des 1 sur la diagonale est d'exposant e car pour toute matrice $M \in U(p)$, $(M - I_p)^p = 0$ et comme on est en caractéristique p, $M^p = I_p$.

Exercice 7. 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 8. 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 9. 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).