Correction & Exercices Supplémentaires TD THéorie des GRoupes

Antoine Dequay, TD de Christophe Dupont

10 décembre 2024

Notions importantes abordées dans ce module (**B.A.-BA.**) : action de groupe, classe, groupe, groupe quotient, groupe résoluble, groupe simple, morphisme, ordre, produit direct, produit semi-direct, sous-groupe, sous-groupe normal/distingué, théorème de Lagrange, théorème d'isomorphisme, théorèmes de Sylow, $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^*$ (groupe multiplicatif des inversibles de $\mathbb{Z}/n\mathbb{Z}$), $\mathfrak{S}_n$ (groupe symétrique), $\mathfrak{A}_n$ (groupe alterné), D_n (groupe diédral), U_n (groupe des racines $n^{\text{ème}}$ de l'unité), V (groupe de Klein), Q_8 (groupe des quaternions), GL_n (groupe linéaire), SL_n (groupe spécial linéaire), ...

Les remarques en violet ne sont pas indispensables à la compréhension des corrections, mais peuvent donner des pistes pour aller plus loin, prendre un autre point de vue ou prendre de l'avance sur le cours.

Table des matières

0 Exercices Supplémentaires THGR

0.1 Feuille 1

Exercice 0.1. Soit G un groupe qui possède exactement deux sous-groupes distincts de G et $\{1\}$.

1. Montrer que tout élément de G est d'ordre fini. En déduire que G est d'ordre fini.
2. Montrer que G est cyclique.
3. Montrer que G est d'ordre pq ou p^3 avec $p \neq q$ deux nombres premiers.

Démonstration.

1. Montrons que tout élément de G est d'ordre fini. Soit $x \in G$. Supposons par l'absurde que x soit d'ordre infini. Alors le sous-groupe de G engendré par x est infini et isomorphe à $\mathbb{Z}$. Or $\mathbb{Z}$ possède une infinité de sous-groupes (les $n\mathbb{Z}$), donc G possède aussi une infinité de sous-groupes, ce qui est absurde. Donc x est d'ordre fini.

   Montrons maintenant que G est d'ordre fini. Supposons par l'absurde que G soit infini. Soit $x \neq 1$, on note $H = \langle x \rangle$. Alors H est fini, donc il n'est pas égal à G. Soit $y \notin H$. Alors $K = \langle y \rangle$ est un sous-groupe fini de G différent de G, H et $\{1\}$. Comme G est infini, on peut trouver un élément $z \notin H \cup K$. Le sous-groupe engendré par z est alors différent de G, H, K et $\{1\}$. Or c'est absurde car G possède exactement deux sous-groupes distincts de G et $\{1\}$. Donc G est fini.
2. Soit $x \neq 1$ un élément de G. On note H le sous-groupe engendré par x. On sait que $H \neq \{1\}$. Si $H = G$ alors on aura prouvé que G est cyclique. Sinon $H \neq G$ et il existe $y \in G \backslash H$. On note K le sous-groupe engendré par y. Comme précédemment $K \neq \{1\}$. De plus $K \neq H$. Si $K = G$ alors G est cyclique. Supposons que $K \neq G$. Alors il existe $z \notin H \cup K$. Le sous-groupe engendré par z n'est ni $\{1\}$, ni H ni K. C'est donc nécessairement G. Donc G est cyclique.
3. Comme G est un groupe cyclique, il est donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$ pour un certain entier $n > 1$. Or le groupe $\mathbb{Z}/n\mathbb{Z}$ possède un sous-groupe d'ordre d pour tout d diviseur de n. Puisque le groupe G possède exactement deux sous-groupes distincts de G et 1, alors G est d'ordre pq ou p^3 avec $p \neq q$ deux nombres premiers.

□

Exercice 0.2. Soient G et G' deux groupes. Soit morphisme de groupe $f : G \to G'$.

(a) On dit que f est un monomorphisme si pour tout groupe Γ, la propriété suivante est vérifiée : pour tous morphismes de groupes $u, v : \Gamma \to G$, si $f \circ u = f \circ v$ alors $u = v$.

(b) On dit que f est un épimorphisme si pour tout groupe Γ, la propriété suivante est vérifiée : pour tous morphismes de groupes $u, v : G' \to \Gamma$, si $u \circ f = v \circ f$ alors $u = v$.

Montrer les résultats suivant :

1. f est un morphisme injectif si et seulement si f est un monomorphisme.
2. f est un morphisme surjectif si et seulement si f est un épimorphisme. *Indication : Pour le sens réciproque, on pourra considérer l'ensemble : $E = G'/f(G) \cup \{\infty\}$ et $\Gamma = \mathfrak{S}_E$.*

Démonstration.

1. Supposons que f soit injective, soient alors Γ un groupe et $u, v : \Gamma \to G$ deux morphismes de groupes tels que $f \circ u = f \circ v$. Soit $x \in \Gamma$, alors par hypothèse $f(u(x)) = f(v(x))$, donc $u(x) = v(x)$ car f est injective. Donc $u = v$ et f est un monomorphisme.

   Réciproquement, si f est un monomorphisme, prenons $x, y \in G$ tels que $f(x) = f(y)$ et considérons les morphismes de groupes $u : \mathbb{Z} \to G, n \mapsto x^n$ et $v : \mathbb{Z} \to G, n \mapsto y^n$. Alors il est clair que $f \circ u = f \circ v$, donc $u = v$ puisque f est un monomorphisme. En particulier, cela implique que $x = y$ et donc f est injective.
2. Supposons que f soit surjective, et soit un groupe Γ ainsi que $u, v : G' \to \Gamma$ deux morphismes de groupes tels que $u \circ f = v \circ f$. Soit $z \in G'$, alors comme f est surjective, il existe $x \in G$ tel que $f(x) = z$. Alors $u(z) = u(f(x)) = v(f(x)) = v(z)$, donc $u = v$.

Réciproquement, supposons que f soit un épimorphisme. Supposons par l'absurde que f ne soit pas surjective, alors $f(G) = H \neq G'$. On pose $E = G'/f(G) \cup \{\infty\}$ l'ensemble quotient de G' par $f(G)$ union un point. Pour $g \in G'$ on définit

$$\begin{array}{rccc} \sigma_g \colon & E & \to & E \\ & x'H & \mapsto & gx'G \\ & \infty & \mapsto & \infty \end{array}$$

Soit τ la transposition de E qui échange H et ∞. Alors soit $u \colon G' \to E, g \mapsto \sigma_g$ et $v \colon G' \to E, g \mapsto \tau \circ \sigma_g \circ \tau$. On vérifie que $u \circ f = v \circ f$. Puisque f est un épimorphisme alors cela implique que $u = v$. Soit $z \notin H$, alors $\sigma_z(\infty) = \infty$ et

$$\tau \circ \sigma_z \circ \tau(\infty) = \tau(\sigma_z(H)) = \tau(zH) = zH$$

Ce qui est absurde.

□

Exercice 0.3. On montre ici que le groupe $G := \mathrm{SL}_2(\mathbb{Z})$ est engendré par deux matrices :

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Pour cela, on introduit le demi-plan de Poincaré $\mathbb{H} := \{z \in \mathbb{C} \mid \Im(z) > 0\}$ et on note $\Gamma := \langle S, T \rangle$ le sous-groupe de G engendré par S et T.

1. Montrer que la formule
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z := \frac{az+b}{cz+d}$$
définit bien une action de $\mathrm{SL}_2(\mathbb{R})$ sur $\mathbb{H}$. Quel est le noyau de cette action ?
2. Exprimer l'action de S, T, ST et TS sur $\mathbb{H}$ et préciser l'ordre de ces transformations.
3. On note $\mathcal{D}$ la partie de $\mathbb{H}$ suivante :
$$\mathcal{D} := \left\{ z \in \mathbb{H} \mid |\Re(z)| \leqslant \frac{1}{2} \text{ et } |z| \geqslant 1 \right\}.$$
Faire un dessin. Montrer que pour $z \in \mathbb{H}$ il existe $\boldsymbol{g} \in \boldsymbol{\Gamma}$ tel que $g \cdot z \in \mathcal{D}$.
4. Soient $z \in \mathcal{D}$ et $g \in G \backslash \{Id\}$. Montrer que si $g \cdot z \in \mathcal{D}$ alors z est sur le bord de $\mathcal{D}$ et préciser la valeur de g (suivant la position de z).
5. Calculer les stabilisateurs de l'action de G pour un point de $\mathcal{D}$ (on traitera soigneusement les cas $z = \imath$, $z = j$ et $z = -\bar{j}$).
6. Soit $z_0 = 2i$. Pour $g \in G$, on considère $z := g \cdot z_0$. D'après la question 3, il existe un élément $\gamma \in \Gamma$ tel que $\gamma \cdot z \in \mathcal{D}$. En utilisant la question précédente, montrer que $g = \gamma^{-1}$ et conclure.

Démonstration.

1. On vérifie dans un premier temps que $\dfrac{az+b}{cz+d} \in \mathbb{H}$ (on multiplie par le conjugué du dénominateur en haut et en bas) :
$$\Im\left((az+b)(c\bar{z}+d)\right) = \Im(ac|z|^2 + adz + bc\bar{z} + bd) = (ad-bc)\Im(z).$$
Comme $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, on a $ad - bc = 1$ et finalement $\dfrac{az+b}{cz+d} \in \mathbb{H}$, car $z \in \mathbb{H}$.

On vérifie par ailleurs que $I_2 \cdot z = z$ et que :

$$\begin{aligned}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \cdot z \right) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \frac{a'z + b'}{c'z + d'} \\ &= \frac{a\frac{a'z+b'}{c'z+d'} + b}{c\frac{a'z+b'}{c'z+d'} + d} \\ &= \frac{(aa' + bc')z + (ab' + bd')}{(ca' + dc')z + (cb' + dd')} \\ &= \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} \cdot z \\ &= \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \right) \cdot z.\end{aligned}$$

Donc la formule donnée définit bien une action.

On cherche à calculer le noyau de l'action vue comme application de $\mathrm{SL}_2(\mathbb{Z})$ dans $\mathfrak{S}_{\mathbb{H}}$. On cherche donc les éléments de $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ tels que pour tout $z \in \mathbb{H}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{c\bar{z} + d} = z.$$

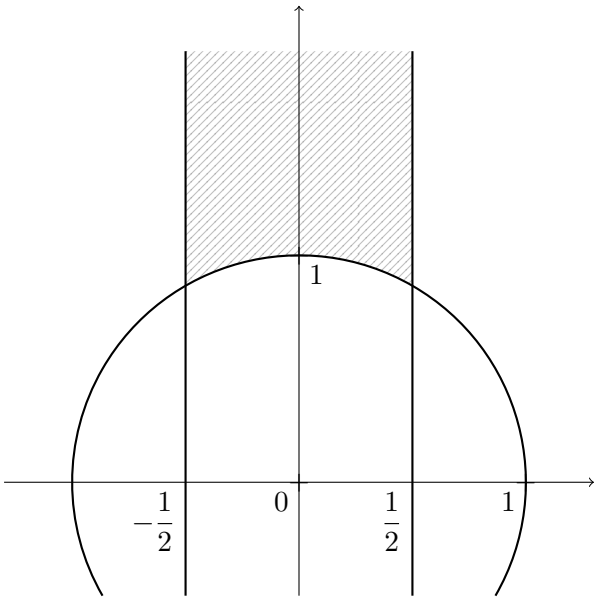
On trouve le système : $\begin{cases} a = d \\ b = c = 0 \end{cases}$, donc le noyau de l'action est $\mathbb{Z} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

2. On a :

$$\begin{aligned} S \cdot z &= \frac{-1}{z} \\ T \cdot z &= z + 1 \\ ST \cdot z &= \frac{-1}{z+1} \\ TS \cdot z &= \frac{z-1}{z} \end{aligned}$$

De plus (à chaque fois, les puissance plus petites agissent non trivialement) :
— $S^2 = -I_2$ agit trivialement donc l'ordre de la transformation est 2,
— $T^n \cdot z = z + n$, donc son ordre est infini,
— $(ST)^3 = -I_2$, donc son ordre est 3,
— $(TS)^3 = -I_2$, donc son ordre est 3.

3. On a la figure suivante :



On commence par remarquer que $\Im(g\cdot z)=\dfrac{\Im(z)}{|cz+d|^2}$ avec $g=\begin{pmatrix}a&b\\c&d\end{pmatrix}$. Puisque c et d sont des entiers, on peut choisir g tel que $\Im(g\cdot z)$ soit maximale (En effet, on cherche à minimiser $|cz+d|$. Voir ci-dessous pourquoi on choisit un tel g).

On va maintenant"recentrer" le point. Par la question 2, on voit que, pour $z\in\mathbb{H}$, si on pose $k=\left\lfloor \Re(g\cdot z)+\dfrac{1}{2}\right\rfloor$, on a $\Re(T^{-k}\cdot g\cdot z)=\Re(g\cdot z)-k\in[-1/2,1/2]$.

Assurons-nous que ce point n'est pas dans le disque unité ouvert. Si c'est le cas, alors $\left|S\cdot T^{-k}\cdot g\cdot z\right|>1$. Mais alors, on voit que $\Im(S\cdot T^{-k}\cdot g\cdot z)>\Im(T^{-k}\cdot g\cdot z)=\Im(g\cdot z)$, ce qui est absurde par définition de g. Donc $T^{-k}\cdot g\cdot z\in\mathcal{D}$.

Il reste à vérifier que $g\in\Gamma$. C'est bien le cas, car par la formule $\Im(g\cdot z)=\dfrac{\Im(z)}{|cz+d|^2}$, pour maximiser $\Im(g\cdot z)$, on doit prendre $(c,d)\in\{(0,1),(1,0)\}$, et donc on peut prendre $g\in\{Id_2,S\}\subset\Gamma$ respectivement.

4. On pose $g=\begin{pmatrix}a&b\\c&d\end{pmatrix}$. On a vu que $\Im(g\cdot z)=\dfrac{\Im(z)}{|cz+d|^2}$. Quitte à considérer $\widetilde{(z,g)}=(g\cdot z,g^{-1})$, on peut supposer que $\Im(g\cdot z)\geqslant\Im(z)$ (i.e $|cz+d|^2\leqslant 1$). Nécessairement, on $|c|<2$: on va distinguer plusieurs cas :
   - Si $c=0$, alors $d=\pm1$ et l'action de g est la translation par $\pm b$. Comme $\Re(z)$ et $\Re(g\cdot z)$ sont dans $[-1/2,1/2]$, il vient $b=0$ et $g=\pm I_2$ ou $b=\pm1$ (et $g=\pm T$) et $\Re(z),\Re(g\cdot z)\in\{-1/2,1/2\}$,
   - Si $c=1$, alors $|z+d|\leqslant 1$ donc $d=0$ sauf si $z=j$ (respectivement $z=-\bar{j}$), et dans ce cas, $d\in\{0,1\}$ (resp. $d\in\{0,-1\}$).
     - Le cas $d=0$ donne $b=1$ et $|z|\leqslant 1$, donc $|z|=1$. Il vient alors $g\cdot z=a+\dfrac{1}{z}$, et comme précédemment, il vient $a=0$, sauf si $\Re(z)=\pm1/2$. Dans ce cas, $z=j$ ou $z=-\bar{j}$, et alors $a\in\{0,-1\}$ ou $a\in\{0,1\}$.
     - Si $z=j$ et $d=1$, alors $a-b=1$ et $g\cdot j=\dfrac{aj+a-1}{j+1}=\dfrac{a\bar{j}+1}{\bar{j}}=a+j$ donc $a\in\{0,1\}$.
     - De même pour le cas $z=-\bar{j}$.
   - Si $c=-1$, le raisonnement est similaire au cas $c=1$ en inversant les signes de a,b,c et d.

   Dans tous les cas, z est bien sur le bord de $\mathcal{D}$.
5. Par ce qui précède, si $g\neq\pm I_2$ est dans le stabilisateur de $z\in\mathcal{D}$, z est sur le bord de $\mathcal{D}$. Par contraposée, tout élément qui n'est pas sur le bord de $\mathcal{D}$ possède un stabilisateur trivial.
   - Par ce qui précède, si $z\in\mathcal{D}$ est tel que que $z\neq j,-\bar{j}$ et $\Re(z)=\pm1/2$, alors $g\cdot z\in\mathcal{D}$ si et seulement l'action est une translation. En particulier g ne stabilise pas D, donc le stabilisateur de z est réduit à l'identité.
   - Si $|z|=1$ et $g\cdot z\in\mathcal{D}$, on a de nouveau $c=1$ et $d=0$, donc si on suppose $z\notin\{j,-\bar{j}\}$, alors $g\cdot z=-1/z$.

     Le seul z stabilisé par un tel g est $z=\imath$. Donc $\mathrm{Stab}(i)=\{I_2,S\}$.
   - Il ne reste qu'à traiter le cas où $z=\rho$ ou $z=-\bar{\rho}$. Dans ces cas, (à l'aide la discussion précédente, et en testant les divers cas) on montre que $\mathrm{Stab}(j)=\langle ST\rangle$ et $\mathrm{Stab}(\bar{j})=\langle TS\rangle$.
6. On a $(\gamma g)\cdot z_0=\gamma\cdot z\in\mathcal{D}$. Comme $z_0\in\mathcal{D}$ et que z_0 n'est pas sur le bord de $\mathcal{D}$, on a, par la question précédente, $\gamma g=\pm I_2$. Donc $g=\gamma^{-1}\in\Gamma$, et on a $G\subset\Gamma$, d'où $G=\Gamma$.

□

Exercice 0.4 (Groupe libre, théorie de la présentation)**.** Soit X un ensemble. À tout élément x de X, on associe un symbole x^{-1}. Et l'on note X^{-1} l'ensemble des x^{-1} pour x parcourant x. On va construire un ensemble $G(X)$ de la manière suivante : un élément de $G(X)$ est un mot, c'est-à-dire une suite finie d'éléments de $X\cup X^{-1}$ne comprenant aucune séquence de deux termes consécutifs de la forme xx^{-1} ou $x^{-1}x$ pour $x\in X$. On va ajouter une loi de composition interne sur $G(X)$. On multiplie deux éléments (ou mots) de $G(X)$ en les concaténant puis en le réduisant, c'est-à-dire en éliminant les séquences xx^{-1} ou $x^{-1}x$ que l'on rencontre. On va définir l'élément neutre de $G(X)$ comme étant le mot vide.

1. Montrer que $G(X)$ avec la loi ainsi définie est un groupe.
2. Soit $f\colon X \to G$ une application ensembliste, montrez que l'on peut définir un morphisme de groupe $\tilde{f} : G(X) \to G$ qui vérifie $\tilde{f}(x) = f(x)$ pour tout $x \in X$.
3. Soit R un ensemble de relations entre les éléments de X. Construire un groupe sur X (le plus gros possible) dans lequel ces relations sont vérifiées. On note $\langle X \mid R\rangle$ ce groupe (c'est une présentation !).

   Remarque. Ce groupe est caractérisé par la propriété universelle suivante :

   $$\forall H \in Grp, \forall f : X \to H, (\exists! F : G \to H, \forall x \in X, F(x) = f(x))$$
   $$\Leftrightarrow (x_1^{a_1} \dots x_n^{a_n} \in R \Rightarrow f(x_1)^{a_1} \dots f(x_n)^{a_n} = 1).$$

4. Trouver une présentation pour $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathfrak{S}_n$, le groupe modulaire $\mathrm{PSL}_2(\mathbb{Z})$, et le groupe de tresse B_n (comparer à la présentation de $\mathfrak{S}_n$).

Une fois fait, venez parler présentation (absolue) avec moi.

Exercice 0.5 (Groupes topologiques)**.** On va chercher à montrer qu'il existe une infinité de puissances de 2 commençant par un 9.

1. Montrer que tout sous groupe de $\mathbb{R}$ est soit monogène, soit dense. *Indication : pensez aux sous-groupes de $\mathbb{Z}$!*
2. Que se passe-t-il pour un sous-groupe H de la forme $\mathbb{Z} + \alpha\mathbb{Z}$?
3. Application : montrer que $\cos(\mathbb{N})$ est dense dans $[-1, 1]$.
4. Que se passe-t-il pour un sous-groupe H de la forme $\mathbb{Z}^{+*} + \alpha\mathbb{Z}^{-*}$, pour $\alpha \in \mathbb{R}^+\backslash\mathbb{Q}$?
   (a) Montrer que pour tout $\varepsilon \in \mathbb{R}^{+*}$, il existe une infinité de $n \in \mathbb{Z}$ tels qu'il existe $m \in \mathbb{Z}$ vérifiant $0 < n + \alpha m < \varepsilon$.
   (b) Reprendre la question précédente en supposant $n \in \mathbb{N}$, puis conclure. On pourra s'intéresser à $(n + \alpha\mathbb{Z}) \cap \mathbb{R}^{+*}$
5. Conclure.

Une fois fait, venez parler groupes topologiques avec moi.

Exercice 0.6 (Help !)**.** Prouver que $\mathrm{Sp}_g(\mathbb{Z}/n\mathbb{Z})$ est engendré par les matrices $B_g(A) = \begin{pmatrix} A & 0_g \\ 0_g & {}^tA^{-1} \end{pmatrix}$ pour $A \in \mathrm{GL}_g(\mathbb{Z}/n\mathbb{Z})$, $S_g(C) = \begin{pmatrix} 1_g & 0_g \\ C & 1_g \end{pmatrix}$ pour $C \in \mathcal{M}_g(\mathbb{Z}/n\mathbb{Z})$ symétrique et $H_g = \begin{pmatrix} 0_g & 1_g \\ -1_g & 0_g \end{pmatrix}$, où $\mathrm{Sp}_g(\mathbb{Z}/n\mathbb{Z}) \subset \mathcal{M}_{2g}(\mathbb{Z}/n\mathbb{Z})$ est l'ensemble des matrices M vérifiant ${}^tMH_gM = H_g$. Donner un algorithme permettant de décomposer un élément de $\mathrm{Sp}_g(\mathbb{Z}/n\mathbb{Z})$ en produit d'éléments de la forme ci-dessous.

Une fois fait, venez m'aider !

Exercice 0.7 (Topologie algébrique)**.** Plantez n piquets alignés dans le sol, et prenez une corde. Trouvez une façon d'enrouler la corde autour des piquets de sorte à ce que, si vous faites un noeud avec les bouts de la corde, elle soit retenue par ces piquets, mais que si vous enlevez n'importe quel piquet du sol, la corde ne soit plus attachée à rien...

Une fois fait, venez parler groupe fondamental avec moi.

Exercice 0.8 (Décomposition polaire et applications)**.**

1. On va montrer que $\mu : O(n, \mathbb{R}) \times \mathscr{S}_n^{++}(\mathbb{R}) \xrightarrow{\sim} \mathrm{GL}_n(\mathbb{R})$, où $\mathscr{S}_n^{++}(\mathbb{R})$ désigne l'ensemble des matrices symétriques définies positives :
   (a) Pour $M \in \mathrm{GL}_n(\mathbb{R})$, cherchez à construire une (la ?) racine carrée de ${}^tMM$ (pensez à diagonaliser !).
   (b) Explicitez S et O en fonction de M. Qu'avez-vous prouvé sur μ ?

(c) Pour l'injectivité de μ, exprimez S en fonction de S^2 grâce a un polynôme bien choisi, et pensez à la diagonalisation simultanée.

(d) Pour la continuité, on cherche montrer celle de μ^{-1}. On admettra la compacité de $O(n, \mathbb{R})$.

2. Calculer la norme triple (pour la norme $\|.\|_2$) d'une matrice de $\mathrm{GL}_n(\mathbb{R})$.
3. Montrer que tout sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$ qui contient $O(n, \mathbb{R})$ lui est égal.
4. En s'inspirant de la suite convergente (vers 1) $u_{k+1} = \dfrac{u_k + u_k^{-1}}{2}$ pour $u_0 > 0$, donner une méthode numérique permettant d'approcher la décomposition polaire.

Exercice 0.9 (Exponentielle symétrique)**.** Montrer que exp : $\mathscr{S}_n^+(\mathbb{R}) \to \mathscr{S}_n^{++}(\mathbb{R})$ est un homéomorphisme. (On pourra utiliser l'exercice précédent, et au passage comprendre la dénomination de décomposition polaire...)

0.2 Feuille 2 : version difficile

Exercice 0.10. Soit G un groupe qui possède exactement deux sous-groupes distincts de G et $\{1\}$. Montrer que G est d'ordre pq ou p^3 avec $p \neq q$ deux nombres premiers.

Indication : Il se trouve que G est abélien...

Démonstration. Montrons que tout élément de G est d'ordre fini. Soit $x \in G$. Supposons par l'absurde que x soit d'ordre infini. Alors le sous-groupe de G engendré par x est infini et isomorphe à $\mathbb{Z}$. Or $\mathbb{Z}$ possède une infinité de sous-groupes (les $n\mathbb{Z}$), donc G possède aussi une infinité de sous-groupes, ce qui est absurde. Donc x est d'ordre fini.

Montrons maintenant que G est d'ordre fini. Supposons par l'absurde que G soit infini. Soit $x \neq 1$, on note $H = \langle x \rangle$. Alors H est fini, donc il n'est pas égal à G. Soit $y \notin H$. Alors $K = \langle y \rangle$ est un sous-groupe fini de G différent de G, H et $\{1\}$. Comme G est infini, on peut trouver un élément $z \notin H \cup K$. Le sous-groupe engendré par z est alors différent de G, H, K et $\{1\}$. Or c'est absurde car G possède exactement deux sous-groupes distincts de G et $\{1\}$. Donc G est fini.

Montrons que G est cyclique. Soit $x \neq 1$ un élément de G. On note H le sous-groupe engendré par x. On sait que $H \neq \{1\}$. Si $H = G$ alors on aura prouvé que G est cyclique. Sinon $H \neq G$ et il existe $y \in G \backslash H$. On note K le sous-groupe engendré par y. Comme précédemment $K \neq \{1\}$. De plus $K \neq H$. Si $K = G$ alors G est cyclique. Supposons que $K \neq G$. Alors il existe $z \notin H \cup K$. Le sous-groupe engendré par z n'est ni $\{1\}$, ni H ni K. C'est donc nécessairement G. Donc G est cyclique.

Comme G est un groupe cyclique, il est donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$ pour un certain entier $n > 1$. Or le groupe $\mathbb{Z}/n\mathbb{Z}$ possède un sous-groupe d'ordre d pour tout d diviseur de n. Puisque le groupe G possède exactement deux sous-groupes distincts de G et 1, alors G est d'ordre pq ou p^3 avec $p \neq q$ deux nombres premiers. □

Exercice 0.11. Soient G et G' deux groupes. Soit morphisme de groupe $f : G \to G'$.

(a) On dit que f est un monomorphisme si pour tout groupe Γ, la propriété suivante est vérifiée : pour tous morphismes de groupes $u, v : \Gamma \to G$, si $f \circ u = f \circ v$ alors $u = v$.

(b) On dit que f est un épimorphisme si pour tout groupe Γ, la propriété suivante est vérifiée : pour tous morphismes de groupes $u, v : G' \to \Gamma$, si $u \circ f = v \circ f$ alors $u = v$.

Montrer les résultats suivant :

1. f est un morphisme injectif si et seulement si f est un monomorphisme
2. f est un morphisme surjectif si et seulement si f est un épimorphisme

Démonstration.

1. Supposons que f soit injective, soient alors Γ un groupe et $u, v : \Gamma \to G$ deux morphismes de groupes tels que $f \circ u = f \circ v$. Soit $x \in \Gamma$, alors par hypothèse $f(u(x)) = f(v(x))$, donc $u(x) = v(x)$ car f est injective. Donc $u = v$ et f est un monomorphisme.

   Réciproquement, si f est un monomorphisme, prenons $x, y \in G$ tels que $f(x) = f(y)$ et considérons les morphismes de groupes $u : \mathbb{Z} \to G, n \mapsto x^n$ et $v : \mathbb{Z} \to G, n \mapsto y^n$. Alors il est clair que $f \circ u = f \circ v$, donc $u = v$ puisque f est un monomorphisme. En particulier, cela implique que $x = y$ et donc f est injective.

2. Supposons que f soit surjective, et soit un groupe Γ ainsi que $u, v : G' \to \Gamma$ deux morphismes de groupes tels que $u \circ f = v \circ f$. Soit $z \in G'$, alors comme f est surjective, il existe $x \in G$ tel que $f(x) = z$. Alors $u(z) = u(f(x)) = v(f(x)) = v(z)$, donc $u = v$.

   Réciproquement, supposons que f soit un épimorphisme. Supposons par l'absurde que f ne soit pas surjective, alors $f(G) = H \neq G'$. On pose $E = G'/f(G) \cup \{\infty\}$ l'ensemble quotient de G' par $f(G)$ union un point. Pour $g \in G'$ on définit

$$\begin{array}{rccc} \sigma_g : & E & \to & E \\ & x'H & \mapsto & gx'G \\ & \infty & \mapsto & \infty \end{array}$$

Soit τ la transposition de E qui échange H et ∞. Alors soit $u\colon G' \to E, g \mapsto \sigma_g$ et $v\colon G' \to E, g \mapsto \tau \circ \sigma_g \circ \tau$. On vérifie que $u \circ f = v \circ f$. Puisque f est un épimorphisme alors cela implique que $u = v$. Soit $z \notin H$, alors $\sigma_z(\infty) = \infty$ et

$$\tau \circ \sigma_z \circ \tau(\infty) = \tau(\sigma_z(H)) = \tau(zH) = zH$$

Ce qui est absurde.

□

Exercice 0.12. On montre ici que le groupe $G := \mathrm{SL}_2(\mathbb{Z})$ est engendré par deux matrices :

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Pour cela, on introduit le demi-plan de Poincaré $\mathbb{H} := \{z \in \mathbb{C} \mid \Im(z) > 0\}$ et on note $\Gamma := \langle S, T \rangle$ le sous-groupe de G engendré par S et T.

1. Montrer que la formule
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z := \frac{az+b}{cz+d}$$
définit bien une action de $\mathrm{SL}_2(\mathbb{R})$ sur $\mathbb{H}$. Quel est le noyau de cette action ?
2. Exprimer l'action de S, T, ST et TS sur $\mathbb{H}$ et préciser l'ordre de ces transformations.
3. On note $\mathcal{D}$ la partie de $\mathbb{H}$ suivante :
$$\mathcal{D} := \left\{ z \in \mathbb{H} \mid |\Re(z)| \leqslant \frac{1}{2} \text{ et } |z| \geqslant 1 \right\}.$$
Faire un dessin. Montrer que pour $z \in \mathbb{H}$ il existe $\boldsymbol{g \in \Gamma}$ tel que $g \cdot z \in \mathcal{D}$.
4. Soient $z \in \mathcal{D}$ et $g \in G \backslash \{Id\}$. Montrer que si $g \cdot z \in \mathcal{D}$ alors z est sur le bord de $\mathcal{D}$ et préciser la valeur de g (suivant la position de z).
5. Calculer les stabilisateurs de l'action de G pour un point de $\mathcal{D}$ (on traitera soigneusement les cas $z = \imath$, $z = j$ et $z = -\bar{j}$).
6. Soit $z_0 = 2i$. Pour $g \in G$, on considère $z := g \cdot z_0$. D'après la question 3, il existe un élément $\gamma \in \Gamma$ tel que $\gamma \cdot z \in \mathcal{D}$. En utilisant la question précédente, montrer que $g = \gamma^{-1}$ et conclure.

Démonstration.

1. On vérifie dans un premier temps que $\dfrac{az+b}{cz+d} \in \mathbb{H}$ (on multiplie par le conjugué du dénominateur en haut et en bas) :
$$\Im\left((az+b)(c\bar{z}+d)\right) = \Im(ac|z|^2 + adz + bc\bar{z} + bd) = (ad-bc)\Im(z).$$
Comme $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, on a $ad - bc = 1$ et finalement $\dfrac{az+b}{cz+d} \in \mathbb{H}$, car $z \in \mathbb{H}$.
On vérifie par ailleurs que $I_2 \cdot z = z$ et que :
$$\begin{aligned}
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \cdot z \right) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \frac{a'z+b'}{c'z+d'} \\
&= \frac{a\frac{a'z+b'}{c'z+d'} + b}{c\frac{a'z+b'}{c'z+d'} + d} \\
&= \frac{(aa'+bc')z + (ab'+bd')}{(ca'+dc')z + (cb'+dd')} \\
&= \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix} \cdot z \\
&= \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \right) \cdot z.
\end{aligned}$$

Donc la formule donnée définit bien une action.
On cherche à calculer le noyau de l'action vue comme application de $\mathrm{SL}_2(\mathbb{Z})$ dans $\mathfrak{S}_{\mathbb{H}}$. On cherche donc les éléments de $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ tels que pour tout $z \in \mathbb{H}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{c\bar{z}+d} = z.$$

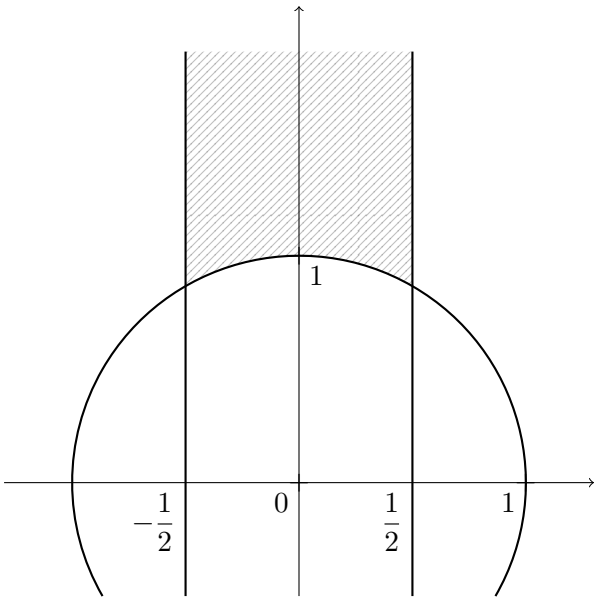
On trouve le système : $\begin{cases} a = d \\ b = c = 0 \end{cases}$, donc le noyau de l'action est $\mathbb{Z}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

2. On a :

$$S \cdot z = \frac{-1}{z}$$
$$T \cdot z = z + 1$$
$$ST \cdot z = \frac{-1}{z+1}$$
$$TS \cdot z = \frac{z-1}{z}$$

De plus (à chaque fois, les puissance plus petites agissent non trivialement) :
— $S^2 = -I_2$ agit trivialement donc l'ordre de la transformation est 2,
— $T^n \cdot z = z + n$, donc son ordre est infini,
— $(ST)^3 = -I_2$, donc son ordre est 3,
— $(TS)^3 = -I_2$, donc son ordre est 3.

3. On a la figure suivante :



On commence par remarquer que $\Im(g \cdot z) = \dfrac{\Im(z)}{|cz+d|^2}$ avec $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Puisque c et d sont des entiers, on peut choisir g tel que $\Im(g \cdot z)$ soit maximale (En effet, on cherche à minimiser $|cz+d|$. Voir ci-dessous pourquoi on choisit un tel g).
On va maintenant"recentrer" le point. Par la question 2, on voit que, pour $z \in \mathbb{H}$, si on pose $k = \left\lfloor \Re(g \cdot z) + \dfrac{1}{2} \right\rfloor$, on a $\Re(T^{-k} \cdot g \cdot z) = \Re(g \cdot z) - k \in [-1/2, 1/2]$.
Assurons-nous que ce point n'est pas dans le disque unité ouvert. Si c'est le cas, alors $\left|S \cdot T^{-k} \cdot g \cdot z\right| > 1$. Mais alors, on voit que $\Im(S \cdot T^{-k} \cdot g \cdot z) > \Im(T^{-k} \cdot g \cdot z) = \Im(g \cdot z)$, ce qui est absurde par définition de g. Donc $T^{-k} \cdot g \cdot z \in \mathcal{D}$.

Il reste à vérifier que $g \in \Gamma$. C'est bien le cas, car par la formule $\Im(g \cdot z) = \dfrac{\Im(z)}{|cz+d|^2}$, pour maximiser $\Im(g \cdot z)$, on doit prendre $(c,d) \in \{(0,1),(1,0)\}$, et donc on peut prendre $g \in \{Id_2, S\} \subset \Gamma$ respectivement.

4. On pose $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On a vu que $\Im(g \cdot z) = \dfrac{\Im(z)}{|cz+d|^2}$. Quitte à considérer $\widetilde{(z,g)} = (g \cdot z, g^{-1})$, on peut supposer que $\Im(g \cdot z) \geqslant \Im(z)$ (i.e $|cz+d|^2 \leqslant 1$). Nécessairement, on $|c| < 2$: on va distinguer plusieurs cas :
   — Si $c = 0$, alors $d = \pm 1$ et l'action de g est la translation par $\pm b$. Comme $\Re(z)$ et $\Re(g \cdot z)$ sont dans $[-1/2, 1/2]$, il vient $b = 0$ et $g = \pm I_2$ ou $b = \pm 1$ (et $g = \pm T$) et $\Re(z), \Re(g \cdot z) \in \{-1/2, 1/2\}$,
   — Si $c = 1$, alors $|z+d| \leqslant 1$ donc $d = 0$ sauf si $z = j$ (respectivement $z = -\bar{j}$), et dans ce cas, $d \in \{0,1\}$ (resp. $d \in \{0,-1\}$).
      — Le cas $d = 0$ donne $b = 1$ et $|z| \leqslant 1$, donc $|z| = 1$. Il vient alors $g \cdot z = a + \dfrac{1}{z}$, et comme précédemment, il vient $a = 0$, sauf si $\Re(z) = \pm 1/2$. Dans ce cas, $z = j$ ou $z = -\bar{j}$, et alors $a \in \{0,-1\}$ ou $a \in \{0,1\}$.
      — Si $z = j$ et $d = 1$, alors $a - b = 1$ et $g \cdot j = \dfrac{aj + a - 1}{j+1} = \dfrac{a\bar{j}+1}{\bar{j}} = a + j$ donc $a \in \{0,1\}$.
      — De même pour le cas $z = -\bar{j}$.
   — Si $c = -1$, le raisonnement est similaire au cas $c = 1$ en inversant les signes de a, b, c et d.

   Dans tous les cas, z est bien sur le bord de $\mathcal{D}$.
5. Par ce qui précède, si $g \neq \pm I_2$ est dans le stabilisateur de $z \in \mathcal{D}$, z est sur le bord de $\mathcal{D}$. Par contraposée, tout élément qui n'est pas sur le bord de $\mathcal{D}$ possède un stabilisateur trivial.
   — Par ce qui précède, si $z \in \mathcal{D}$ est tel que que $z \neq j, -\bar{j}$ et $\Re(z) = \pm 1/2$, alors $g \cdot z \in \mathcal{D}$ si et seulement l'action est une translation. En particulier g ne stabilise pas D, donc le stabilisateur de z est réduit à l'identité.
   — Si $|z| = 1$ et $g \cdot z \in \mathcal{D}$, on a de nouveau $c = 1$ et $d = 0$, donc si on suppose $z \notin \{j, -\bar{j}\}$, alors $g \cdot z = -1/z$.
   Le seul z stabilisé par un tel g est $z = \imath$. Donc $\mathrm{Stab}(i) = \{I_2, S\}$.
   — Il ne reste qu'à traiter le cas où $z = \rho$ ou $z = -\bar{\rho}$. Dans ces cas, (à l'aide la discussion précédente, et en testant les divers cas) on montre que $\mathrm{Stab}(j) = \langle ST \rangle$ et $\mathrm{Stab}(\bar{j}) = \langle TS \rangle$.
6. On a $(\gamma g) \cdot z_0 = \gamma \cdot z \in \mathcal{D}$. Comme $z_0 \in \mathcal{D}$ et que z_0 n'est pas sur le bord de $\mathcal{D}$, on a, par la question précédente, $\gamma g = \pm I_2$. Donc $g = \gamma^{-1} \in \Gamma$, et on a $G \subset \Gamma$, d'où $G = \Gamma$.

□

Exercice 0.13 (Groupe libre, théorie de la présentation)**.** Soit X un ensemble. À tout élément x de X, on associe un symbole x^{-1}. Et l'on note X^{-1} l'ensemble des x^{-1} pour x parcourant x. On va construire un ensemble $G(X)$ de la manière suivante : un élément de $G(X)$ est un mot, c'est-à-dire une suite finie d'éléments de $X \cup X^{-1}$ne comprenant aucune séquence de deux termes consécutifs de la forme xx^{-1} ou $x^{-1}x$ pour $x \in X$. On va ajouter une loi de composition interne sur $G(X)$. On multiplie deux éléments (ou mots) de $G(X)$ en les concaténant puis en le réduisant, c'est-à-dire en éliminant les séquences xx^{-1} ou $x^{-1}x$ que l'on rencontre. On va définir l'élément neutre de $G(X)$ comme étant le mot vide.

1. Montrer que $G(X)$ avec la loi ainsi définie est un groupe.
2. Soit $f \colon X \to G$ une application ensembliste, montrez que l'on peut définir un morphisme de groupe $\tilde{f} : G(X) \to G$ qui vérifie $\tilde{f}(x) = f(x)$ pour tout $x \in X$.
3. Soit R un ensemble de relations entre les éléments de X. Construire un groupe sur X (le plus gros possible) dans lequel ces relations sont vérifiées. On note $\langle X \mid R \rangle$ ce groupe (c'est une présentation !).

   Remarque. Ce groupe est caractérisé par la propriété universelle suivante :

   $$\forall H, \forall f : X \to H, (\exists! F : G \to H, \forall x \in X, F(x) = f(x)) \Leftrightarrow (x_1^{a_1} \dots x_n^{a_n} \in R \Rightarrow f(x_1)^{a_1} \dots f(x_n)^{a_n} = 1).$$

4. Trouver une présentation pour $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathfrak{S}_n$, le groupe modulaire $\mathrm{PSL}_2(\mathbb{Z})$, et le groupe de tresse B_n (comparer à la présentation de $\mathfrak{S}_n$).

Une fois fait, venez parler présentation (absolue) avec moi.

Exercice 0.14 (Groupes topologiques)**.** Montrer qu'il existe une infinité de puissances de 2 commençant par un 9.

Une fois fait, venez parler groupes topologiques avec moi.

Exercice 0.15 (Help !)**.** Prouver que $\mathrm{Sp}_g(\mathbb{Z}/n\mathbb{Z})$ est engendré par les matrices $B_g(A) = \begin{pmatrix} A & 0_g \\ 0_g & {}^tA^{-1} \end{pmatrix}$ pour $A \in \mathrm{GL}_g(\mathbb{Z}/n\mathbb{Z})$, $S_g(C) = \begin{pmatrix} 1_g & 0_g \\ C & 1_g \end{pmatrix}$ pour $C \in \mathcal{M}_g(\mathbb{Z}/n\mathbb{Z})$ symétrique et $H_g = \begin{pmatrix} 0_g & 1_g \\ -1_g & 0_g \end{pmatrix}$, où $\mathrm{Sp}_g(\mathbb{Z}/n\mathbb{Z}) \subset \mathcal{M}_{2g}(\mathbb{Z}/n\mathbb{Z})$ est l'ensemble des matrices M vérifiant ${}^tMH_gM = H_g$. Donner un algorithme permettant de décomposer un élément de $\mathrm{Sp}_g(\mathbb{Z}/n\mathbb{Z})$ en produit d'éléments de la forme ci-dessous.

Une fois fait, venez m'aider !

Exercice 0.16 (Topologie algébrique)**.** Plantez n piquets alignés dans le sol, et prenez une corde. Trouvez une façon d'enrouler la corde autour des piquets de sorte à ce que, si vous faites un noeud avec les bouts de la corde, elle soit retenue par ces piquets, mais que si vous enlevez n'importe quel piquet du sol, la corde ne soit plus attachée à rien...

Une fois fait, venez parler groupe fondamental avec moi.

Exercice 0.17 (Théorème de Frobenius-Zolotarev)**.** On va prouver le théorème suivant : Soient $p \in \mathbb{N}$ premier impair et $n \in \mathbb{N}^*$. Alors on a :

$$\forall u \in \mathrm{GL}_n(\mathbb{F}_p),\ \varepsilon(u) = \left(\frac{\det(u)}{p}\right).$$

On rappelle que :

— $\varepsilon(u)$ est la signature de u, vue comme permutation de $\mathbb{F}_p^n$,

— le symbole de Legendre est désigné par : $\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \equiv 0\,[p] \\ 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p \\ -1 & \text{sinon} \end{cases}$.

1. Soit K un corps et M un groupe abélien. On suppose que $K \neq \mathbb{F}_2$ ou $n \neq 2$. Montrer que tout morphisme de groupes $\varphi : \mathrm{GL}_n(K) \to M$ se factorise par le déterminant.
2. Soit $p \in \mathbb{N}$ premier impair. Le symbole de Legendre est l'unique morphisme de groupes non-trivial de $\mathbb{F}_p^*$ dans $\{\pm 1\}$.

Exercice 0.18 (Décomposition polaire et applications)**.**

1. Montrer que $O(n,\mathbb{R}) \times \mathscr{S}_n^{++}(\mathbb{R}) \xrightarrow{\sim} \mathrm{GL}_n(\mathbb{R})$, où $\mathscr{S}_n^{++}(\mathbb{R})$ désigne l'ensemble des matrices symétriques définies positives.
2. Calculer la norme triple (pour la norme $\|.\|_2$) d'une matrice de $\mathrm{GL}_n(\mathbb{R})$.
3. Montrer que tout sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$ qui contient $O(n,\mathbb{R})$ lui est égal.
4. Donner une méthode numérique permettant d'approcher la décomposition polaire.

Exercice 0.19 (Exponentielle symétrique)**.** Montrer que $\exp : \mathscr{S}_n^+(\mathbb{R}) \to \mathscr{S}_n^{++}(\mathbb{R})$ est un homéomorphisme. (On pourra utiliser l'exercice précédent, et au passage comprendre la dénomination de décomposition polaire...)

Exercice 0.20 (Étude de $O(p,q)$)**.** Montrer que, pour $p, q \neq 0$, on a un homéomorphisme :

$$O(p,q) \cong O(p,\mathbb{R}) \times O(q,\mathbb{R}) \times \mathbb{R}^{pq},$$

où $O(p,q)$ désigne le sous-groupe de $\mathrm{GL}_{p+q}(\mathbb{R})$ formé des isométries de la forme quadratique standard de signature (p,q). (On pourra utiliser l'exercice précédent, et celui d'avant)

0.3 Feuille 3 : TD type agreg

Dans toute la suite, $\mathbb{F}_q$ dénote le corps fini à q éléments. Quelques rappels :
— Pour E un espace vectoriel, l'espace projectif $\mathbb{P}(E)$ est l'espace des droites vectorielles de E.
— Faire opérer un groupe G sur un ensemble E signifie qu'on s'intéresse à un morphisme de groupe $\varphi : G \longrightarrow \mathfrak{S}_E$ (on dit que φ est une action de groupe). On note classiquement :

$$\varphi : \begin{pmatrix} G & \longrightarrow & \mathfrak{S}_E \\ g & \longmapsto & \varphi_g : \begin{pmatrix} E & \xrightarrow{\sim} & E \\ e & \longmapsto & g \cdot e \end{pmatrix} \end{pmatrix}$$

1. Soit $n \in \mathbb{N}$ et E un espace vectoriel sur $\mathbb{F}_q$ de dimension n. Pour tout un entier m avec $0 \leqslant m \leqslant n$, on note X_m l'ensemble des m-uplets $(x_1, \dots, x_m) \in E^m$ formés de m vecteurs linéaires indépendants.
   (a) Calculer $\mathrm{Card}(X_m)$. En déduire $\mathrm{Card}(\mathrm{GL}_n(\mathbb{F}_q))$.
   (b) Quel est le cardinal de l'espace projectif $\mathbb{P}(E)$?
2. Soit $n \geqslant 2$ un entier. Soit $\mu_n(\mathbb{F}_q)$ le groupe des racines n-ièmes de l'unité dans $\mathbb{F}_q$. Montrer que $\mathrm{Card}(\mu_n(\mathbb{F}_q)) = \mathrm{pgcd}(n, q-1)$. En déduire le cardinal de $\mathrm{PSL_n}(\mathbb{F}_q)$.
   Indication : Soit $d = \mathrm{pgcd}(n, q-1)$. Pour $x \in \mathbb{F}_q^*$, montrer que $x^d = 1$ si et seulement si $x \in \mu_n(\mathbb{F}_q)$. Combien de racines possède le polynôme $X^d - 1$ dans $\mathbb{F}_q^*$?
3. Montrer que $\mathrm{GL}_2(\mathbb{F}_2)$ est isomorphe au groupe symétrique $\mathfrak{S}_3$.
   Indication : Faire opérer $\mathrm{GL}_2(\mathbb{F}_2)$ sur $\mathbb{F}_2^2$.
4. Soit $E = \mathbb{F}_3^2$.
   (a) Construire, au moyen des 4 droites vectorielles $D_1, \dots, D_4$ de E un homomorphisme surjectif $\varepsilon : \mathrm{GL}_2(\mathbb{F}_3) \longrightarrow \mathfrak{S}_4$.
   (b) Montrer que ε induit un isomorphisme entre $\mathrm{PSL}_2(\mathbb{F}_3)$ et le groupe alterné $\mathfrak{A}_4$.
   (c) En déduire que $\mathrm{SL}_2(\mathbb{F}_3)$ n'est pas parfait. (Un groupe G est parfait s'il coïncide avec le sous-groupe $[G, G]$ engendré par les commutateurs)
5. Montrer que $\mathrm{PSL}_2(\mathbb{F}_4)$ est isomorphe à $\mathfrak{A}_5$. *Indication : $\mathrm{PSL}_2(\mathbb{F}_4)$ opère sur l'ensemble X des droites vectorielles de $\mathbb{F}_4^2$. Quel est le cardinal de $\mathrm{PSL}_2(\mathbb{F}_4)$?*
6. Montrer que $\mathrm{PGL}_2(\mathbb{F}_5)$ est isomorphe à $\mathfrak{S}_5$ et que $\mathrm{PSL}_2(\mathbb{F}_5)$ est isomorphe à $\mathfrak{A}_5$.
7. Soit $n \in \mathbb{N}$ et E un espace vectoriel sur $\mathbb{F}_q$ de dimension n.
   Pour un entier m avec $0 \leqslant m \leqslant n$, soit $G_{n,m}$ l'ensemble des sous-espaces vectoriels de E de dimension m. Trouver une formule pour $\mathrm{Card}(G_{n,m})$. *Indication : $\mathrm{GL_n}(\mathbb{F}_q)$ opère transitivement sur $G_{n,m}$.*
8. Pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, on munit $M_n(\mathbb{K}) \cong \mathbb{K}^{n^2}$ de la topologie standard.
   (a) Montrer que $\mathrm{GL_n}(\mathbb{Q})$ est dense dans $\mathrm{GL_n}(\mathbb{R})$ et que $\mathrm{SL_n}(\mathbb{Q})$ est dense dans $\mathrm{SL_n}(\mathbb{R})$.
   (b) Montrer que $\mathrm{GL_n}(\mathbb{C})$, $\mathrm{SL_n}(\mathbb{C})$ et $\mathrm{SL_n}(\mathbb{R})$ sont connexes par arcs et que $\mathrm{GL_n}(\mathbb{R})$ n'est pas connexe.
9. Soit $n \geqslant 1$ un entier et $\Gamma = \mathrm{SL_n}(\mathbb{Z})$. Pour un nombre premier p, on considère l'homomorphisme $\varphi_p : \Gamma \longrightarrow \mathrm{SL_n}(\mathbb{Z}/p\mathbb{Z})$ induit par la réduction modulo p.
   (a) Montrer que φ_p est surjectif.
   (b) On note Γ_p le noyau de φ_p. Quel est l'indice de Γ_p dans Γ ?
   (c) On suppose que $p \geqslant 3$. Montrer que Γ_p ne possède pas d'éléments d'ordre fini distinct de l'identité.
   (d) En déduire que Γ ne possède, à isomorphisme près, qu'un nombre fini de sous-groupes finis.
10. Soit $n \geqslant 2$, et soit $a = (a_1, \dots, a_n)^t \in \mathbb{Z}^n$. Montrer que les propriétés suivantes sont équivalentes :
    (a) Il existe une matrice $A \in \mathrm{SL_n}(\mathbb{Z})$ dont la première colonne est a.
    (b) $\mathrm{pgcd}(a_1, \dots, a_n) = 1$.

1 Feuille 1

Exercice 1.1 (**B.A.-BA.**)**.** Soit G un groupe tel que $g^2 = e$ pour tout $g \in G$. Montrer que G est abélien.

Démonstration. Soit $(x, y) \in G^2$. Montrons que $xy = yx$. Par propriété de G, on a : $(xy)^2 = xyxy = e$. Ainsi, $xy = y^{-1}x^{-1}$. Or, pour $g \in G$, on a $g^2 = e$, donc $g = g^{-1}$. Ainsi, il vient bien : $xy = y^{-1}x^{-1} = yx$. □

Exercice 1.2 (**B.A.-BA.**)**.**

1. Soit G un groupe, soient $g \in G$ et $n \geqslant 1$. Montrer que si $g^n = e$, alors l'ordre de g divise n.
2. Soit H un sous-groupe de $\mathbb{Z}$. Montrer qu'il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.
3. La réunion de deux sous-groupes n'est pas toujours un sous-groupe : donner un exemple.
4. Soient H et K deux sous-groupes d'un groupe G. Montrer que $H \cup K$ est un sous-groupe de G si et seulement si $K \subset H$ ou $H \subset K$.

Démonstration.

1. Par définition de l'ordre de g, on peut supposer que $n \geqslant o(g)$. Par division euclidienne de n par $o(g)$, il existe $(q, r) \in \mathbb{N}^* \times [\![1, o(g)[\![$, tel que $n = qo(g) + r$. On a donc :
$$e = g^n = g^{qo(g)+r} = g^{qo(g)}g^r = (g^{o(g)})^q g^r = g^r.$$
Or, $r \in [\![1, o(g)[\![$, donc, par définition de l'ordre, $r = 0$, et $o(g)$ divise bien n.
2. Le résultat est évident si $H = \{0\} = 0\mathbb{Z}$. Sinon, H contient un élément non nul. L'ensemble $H \cap \mathbb{N}^* \subset \mathbb{N}$ est donc non vide et admet un plus petit élément, noté n. On remarque en particulier que n est unique. On a donc $\langle n \rangle = n\mathbb{Z} \subset H$. Réciproquement, si m est dans H, la division euclidienne de m par n donne $m = nq + r$ avec $0 \leqslant r < n$. Comme H est un groupe, $r = m - nq \in H$. Par minimalité de n, $r = 0$, d'où $H = n\mathbb{Z}$.

   Remarque. On remarque, réciproquement, que les $n\mathbb{Z}$ pour $n \in \mathbb{N}$ sont des sous-groupes de $\mathbb{Z}$: on a classifié les sous-groupes de $\mathbb{Z}$!

3. Avec la question précédente, on voit que $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe de $\mathbb{Z}$ puisque 2 et 3 sont dans $2\mathbb{Z} \cup 3\mathbb{Z}$ mais pas $2 + 3 = 5$.
4. Pour le sens réciproque, sans perdre de généralité, on peut supposer que $H \subset K$. Alors $H \cup K = K$ qui est bien un sous groupe de G.
   Pour le sens direct, on prouve la contraposée. Supposons que $K \not\subset H$ et $H \not\subset K$. Alors il existe $h \in H \backslash K$ et $k \in K \backslash H$. En particulier $h, k \in H \cup K$ mais pas $hk \notin H \cup K$. En effet :
$$hk \in H \Longrightarrow h^{-1}hk = k \in H,$$
   car $h^{-1} \in H$, et
$$hk \in K \Longrightarrow hkk^{-1} = h \in K,$$
   car $k^{-1} \in K$.
   Donc $H \cup K$ n'est pas un groupe.

□

Exercice 1.3. Soit G un groupe fini d'ordre pair. Montrer que G contient un élément d'ordre 2.
Indication : on pourra partitionner G en utilisant les sous-ensembles du type $\{g, g^{-1}\}$, où $g \in G$.

Démonstration. Comme G est un groupe, tout élément a un inverse, donc on peut écrire $G = \bigcup_{g\in G}\{g, g^{-1}\}$. Notons H le sous-ensemble de G constitué des éléments d'ordre 1 ou 2. L'ensemble H est non-vide car il contient e. La partition devient : $G = \bigcup_{g\in H}\{g\} \sqcup \bigcup_{g\in G\setminus H}\{g, g^{-1}\}$. On peut alors passer au cardinal, et il vient :

$$\underbrace{\#G}_{2|} = \#H + \# \bigcup_{g\in G\setminus H} \underbrace{\{g, g^{-1}\}}_{2|\#}.$$

Le cardinal de H est donc pair, donc $H\setminus\{e\}$ est non vide, ce qui prouve le résultat. □

Exercice 1.4 (B.A.-BA.). Soient g et h deux éléments d'un groupe G.

(a) Montrer que les éléments g, g^{-1}, hgh^{-1} ont le même ordre.

(b) Montrer que gh et hg ont le même ordre.

(c) Soit n un entier. Exprimer l'ordre de g^n en fonction de celui de g.

(d) On suppose que $gh = hg$, que $\langle g\rangle \cap \langle h\rangle = \{1\}$ et que g et h sont d'ordre fini n et m respectivement. Exprimer l'ordre de gh en fonction de n et de m.

(e) On suppose que $gh = hg$ et que g et h sont d'ordre fini n et m respectivement, avec n et m premiers entre eux. Déduire de (d) que gh est d'ordre mn.

Démonstration.

(a) Soit n l'ordre de g. On note m l'ordre de g^{-1} et k celui de hgh^{-1}. Alors $(g^{-1})^n = (g^n)^{-1} = 1$, donc $m|n$. De même, $g^m = ((g^{-1})^m)^{-1} = 1$, donc $n|m$, d'où : g et g^{-1} ont même ordre.
On a également $(hgh^{-1})^n = hg^nh^{-1} = 1$, donc $k|n$, et $g^k = h^{-1}(hgh^{-1})^k h = 1$, donc $n|k$ et les éléments g et hgh^{-1} ont même ordre.

Remarque. On peut montrer que, pour $\varphi \in \mathrm{Aut}(G)$, $\varphi(g)$ et g ont même ordre. On peut alors appliquer ce résultat pour retrouver les précédents, avec $\varphi : g \mapsto g^{-1}$ (vu comme automorphisme de $\langle g\rangle$, licite car le sous-groupe est abélien) et $\varphi_h : g \mapsto hgh^{-1}$ (qui est un automorphisme intérieur de G) respectivement :
Soit $\varphi \in \mathrm{Aut}(G)$, on note $o(\varphi(g)) = m$. On a $\varphi(g)^n = \varphi(g^n) = 1$, donc $m|n$, et $g^m = \varphi^{-1}(\varphi(g)^m) = 1$, donc $n|m$. Ainsi g et $\varphi(g)$ ont le même ordre.

(b) On note n l'ordre de gh et m l'ordre de hg. Puisque $(gh)^n = 1$ en multipliant à gauche par h et à droite par g on obtient $(hg)^{n+1} = hg$, soit encore $(hg)^n = 1$. Ainsi $m|n$. De la même manière, on montre que $n|m$, ce qui prouve que gh et hg ont le même ordre.

(c) On a $(g^n)^{o(g^n)} = 1$, donc $o(g)|no(g^n)$. Il existe donc $a \in \mathbb{N}^*$ tel que $o(g^n)n = ao(g)$, et il vient $o(g^n)\dfrac{n}{\mathrm{pgcd}(n, o(g))} = a\dfrac{o(g)}{\mathrm{pgcd}(n, o(g))}$.
Comme $\dfrac{n}{\mathrm{pgcd}(n, o(g))}$ et $\dfrac{o(g)}{\mathrm{pgcd}(n, o(g))}$ sont premier entre eux, on en déduit que $\left.\dfrac{o(g)}{\mathrm{pgcd}(n, o(g))}\right| o(g^n)$.
Réciproquement, comme $(g^n)^{\frac{o(g)}{\mathrm{pgcd}(n,o(g))}} = (g^{o(g)})^{\frac{n}{\mathrm{pgcd}(n,o(g))}} = 1$, il vient $o(g^n) \left|\dfrac{o(g)}{\mathrm{pgcd}(n, o(g))}\right.$. Il y a donc bien égalité.

Remarque. Comment avoir l'idée de $\dfrac{o(g)}{\mathrm{pgcd}(, o(g))}$? Si on a déjà l'idée de la solution de la question (d), on peut se dire qu'on cherche à atteindre un multiple de $o(g)$, mais qu'on y arrivera seulement avec des multiples de n. On cherche donc à avoir $n \times o(g^n) = \mathrm{ppcm}(n, o(g))$. Avec la formule $n\times o(g) = \mathrm{pgcd}(n, o(g))\times\mathrm{ppcm}(n, o(g))$, on arrive bien au résultat. On peut le prouver formellement en se plaçant dans $\mathbb{Z}$.

(d) On va montrer que $o(gh) = \text{ppcm}(n, m)$. On remarque que, comme g et h commutent,

$$(gh)^{\text{ppcm}(n,m)} = g^{\text{ppcm}(n,m)} h^{\text{ppcm}(n,m)} = 1.$$

Ainsi $o(gh) | \text{ppcm}(n, m)$.
Soit $k > 0$ tel que $(gh)^k = 1$, en particulier $g^k h^k = 1$ donc $g^k = h^{-k}$. Ainsi $g^k \in \langle g \rangle \cap \langle h \rangle$ et donc $g^k = 1$. De même $h^k = 1$, et il vient $n|k$ et $m|k$ ce qui implique que $\text{ppcm}(n, m)|k$. Finalement on a bien montré que $o(gh) = \text{ppcm}(n, m)$.

(e) On va chercher à montrer que $\langle g \rangle \cap \langle h \rangle = \{1\}$. Ainsi, par la question (d) et comme n et m sont premiers entre eux, on aura bien $o(gh) = \text{ppcm}(n, m) = mn$.
Soient $p, q \in \mathbb{Z}^*$ tels que $g^p = h^q$. Par la question (c), on a alors :

$$o(g^p) = \frac{n}{\text{pgcd}(p, n)} = o(h^q) = \frac{m}{\text{pgcd}(q, m)}.$$

Comme n et m sont premiers entre eux, il vient $\dfrac{n}{\text{pgcd}(p, n)} = \dfrac{m}{\text{pgcd}(q, m)} = 1$, d'où $g^p = h^q = 1$, ce qui prouve le résultat.

□

Exercice 1.5 (B.A.-BA.).

(a) Soit G un groupe. On suppose qu'il existe $g \in G$ d'ordre n tel que $G = \langle g \rangle$. Montrer que G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

(b) Soit $p \geqslant 2$ un nombre premier. Montrer qu'un groupe d'ordre p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
Indication : on pourra admettre le Théorème de Lagrange *qui stipule que si G est un groupe fini, l'ordre d'un sous-groupe de G divise l'ordre de G (ce Théorème sera bientôt démontré en cours).*

Démonstration.

(a) On exhibe l'application : $\varphi : \begin{pmatrix} \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\sim} & G \\ \bar{k} & \longmapsto & g^k \end{pmatrix}$, où k est un représentant de $\bar{k}$ dans $\mathbb{Z}$. Un morphisme de groupe étant entièrement déterminé par l'image d'une partie génératrice du groupe de départ, cela à revient à dire qu'on envoie $1_{\mathbb{Z}/n\mathbb{Z}}$ sur g, un générateur de G. Il faut montrer que φ est un morphisme bien défini bijectif.
— Caractère bien défini : soient $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ et $k_1, k_2 \in \mathbb{Z}^2$ deux représentants de $\bar{k}$. On note $\tilde{k}$ le plus petit représentant positif de $\bar{k}$ dans $\mathbb{Z}$. Avec les divisions euclidiennes $k_1 = q_1 n + \tilde{k}$ et $k_2 = q_2 n + \tilde{k}$, on a (comme g est d'ordre n) : $g^{k_1} = g^{q_1 n + \tilde{k}} = g^{\tilde{k}} = g^{q_2 n + \tilde{k}} = g^{k_2}$.
— Propriété de morphisme : soient $(\bar{p}, \bar{q}) \in (\mathbb{Z}/n\mathbb{Z})^2$ et (p, q) des représentants de $(\bar{p}, \bar{q})$ dans $\mathbb{Z}$, on a : $\varphi(\bar{p} + \bar{q}) = g^{p+q} = g^p g^q = \varphi(\bar{p})\varphi(\bar{q})$.
— Injectivité : soient $(\bar{p}, \bar{q}) \in (\mathbb{Z}/n\mathbb{Z})^2$ et (p, q) des représentants de $(\bar{p}, \bar{q})$ dans $\mathbb{Z}$, on a :

$$\varphi(\bar{p}) = \varphi(\bar{q}) \iff g^p = g^q \iff g^{p-q} = e_G \iff o(g) = n | (p - q) \iff \bar{p} = \bar{q}.$$

— Surjectivité : comme g est d'ordre n, $G = \left\{e_G, g, \ldots, g^{n-1}\right\}$. Or, c'est l'image par φ de $\left\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\right\}$ (dont les éléments sont tous différents).

(b) Soit G un groupe d'ordre p. Par le théorème de Lagrange, tout sous-groupe de G est d'ordre 1 ou p. Comme $p \geqslant 2$, il existe un élément $g \in G \backslash \{e_G\}$. Comme tout sous-groupe de G contient e_G, en particulier, $\#\langle g \rangle > 1$, et $\#\langle g \rangle$ vaut donc p. On a donc $G = \langle g \rangle$, et on peut conclure avec la question précédente.

□

Exercice 1.6 (B.A.-BA.). On montre que tout groupe à 4 éléments est isomorphe soit à $\mathbb{Z}/4\mathbb{Z}$, soit à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Soit G un tel groupe et e, a, b, c ses éléments. Il s'agit d'écrire la table de multiplication du groupe.

(a) Si $a = b^{-1}$, vérifier que G est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

(b) Si $a = a^{-1}$, vérifier que G est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Démonstration. On veut faire la table de la loi de groupe (on nous dit d'utiliser la notation multiplicative). On doit donc avoir le tableau suivant avec sur chaque ligne et chaque colonne les symboles $\{1, a, b, c\}$ (à prouver ! (exo facile)). C'est le principe du sudoku ; la preuve en noir n'utilise pas ce principe, les ajouts en violet passent par cette propriété.

	1	a	b	c
1	1	a	b	c
a	a			
b	b			
c	c			

Par symétrie entre b et c, on a forcément $a = a^{-1}$ ou $a = b^{-1}$. Ce sont les équations obtenues en essayant de mettre un 1 sur la première ligne à compléter.

(a) Si $a = b^{-1}$, alors $b = a^{-1}$ et $c^{-1} = c$. Tous les 1 sont placés sur la grille.

Remarque. Si vous n'êtes pas convaincu, vous pouvez chercher à prouver que l'inverse à droite est toujours l'inverse à gauche dans un groupe quelconque, et même que si on ne définit qu'un neutre à droite et un inverse à droite, alors on a toujours une structure de groupe.
De manière plus imagée, on a trouvé certaines symétries dans le tableau de la loi de groupe ! (attention, tout tableau de loi de groupe n'est pas (entièrement) symétrique, sinon tout groupe serait abélien...).

Cherchons à calculer a^2 :
— $a^2 \neq 1$, car on a supposé $a^{-1} = b \neq a$. Il y a déjà un 1 sur la première ligne.
— Si $a^2 = a$, alors $a = 1$, ce qui est absurde il y a déjà un a sur la première ligne.
— Si $a^2 = b = a^{-1}$, alors $a^3 = 1$, ce qui est absurde, car on aurait, par le théorème de Lagrange, $3|4$. Autre argument qui passe par la propriété du sudoku : si $a^2 = b$, alors $ac = c$, donc $a = 1$, ce qui est absurde.
Ainsi, $a^2 = c$. On en déduit que a est d'ordre 4, et il vient la table suivante :

	1	a	b	c
1	1	a	b	c
a	a	c	1	b
b	b	1	c	a
c	c	b	a	1

On peut encore l'écrire :

	1	a	a^{-1}	a^2
1	1	a	a^{-1}	a^2
a	a	a^2	1	a^{-1}
a^{-1}	a^{-1}	1	a^2	a
a^2	a^2	a^{-1}	a	1

On reconnaît la table du groupe $\mathbb{Z}/4\mathbb{Z}$ (ou utiliser la question 1.5.(a)).

Remarque. Sans passer par une table, on pouvait également chercher à calculer l'ordre de a : Par suppositions successives, ce n'est ni 1, ni 2 (déjà vu). Par le théorème de Lagrange, ce n'est pas 3. C'est donc 4, ce qui permet de conclure directement.

(b) Si $a = a^{-1}$, alors :
— Si $b = c^{-1}$, cela nous ramène au cas précédent (remplacer (a, b, c) par (c, a, b)).
— Si $b = b^{-1}$, alors $c = c^{-1}$. Il ne reste plus qu'à compléter, la règle du sudoku permet de finir !
On cherche à calculer ab.
Si $ab = a$, alors $b = 1$, ce qui est absurde. De même, si $ab = b$, alors $a = 1$, ce qui est absurde.
Si $ab = 1$, alors $a = b^{-1} = b$, ce qui est absurde. Ainsi, $ab = c$. On calcule de la même manière les autres opérations pour obtenir :

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

On reconnaît la table du groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Remarque. On pouvait également résonner comme suit :

— S'il existe un élément d'ordre 4, alors le groupe est cyclique et isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

— Sinon, par le théorème de LAGRANGE, tout élément est d'ordre 1 ou 2. On peut alors montrer que le groupe est abélien (exo 1.1).
Soient $x, y \in G$ distincts et distincts de 1. Ce sont deux éléments d'ordre 2 qui commutent, donc $\langle x, y \rangle$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Ce dernier groupe est d'ordre 4, donc égal à G.

□

2 Feuille 2

Exercice 2.1. Soit G un groupe d'ordre 6. Nous allons montrer que G est isomorphe soit au groupe cyclique $\mathbb{Z}/6\mathbb{Z}$, soit au groupe de permutations $\mathfrak{S}_3$. On admettra que G possède un élément d'ordre 2 noté a et un élément d'ordre 3 noté b (c'est une conséquence du lemme de Cauchy, qui sera démontré dans une feuille de TD consacrée aux actions de groupes).

1. Si G est abélien, montrer que G est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ (utiliser l'exercice 4 de la feuille 1).
2. On suppose que G n'est pas abélien. Montrer que e, a, b, b^2, ab, ba sont deux à deux distincts puis que $ab^2 = ba$. Donner la table de multiplication de G et vérifier que G est isomorphe à $\mathfrak{S}_3$.

Démonstration.

1. On suppose que G est abélien, donc $ab = ba$, et a et b sont d'ordre fini 2 et 3 respectivement, avec 2 et 3 premiers entre eux. Par 1.4.(e), ab est d'ordre 6. Il ne reste plus qu'à conclure avec la question 1.5.(a).
2. Comme les trois éléments ont des ordres différents, on a : $\#\{e, a, b\} = 3$.
   On vérifie :
   — $b^2 \neq e$, car $o(b) = 3$,
   — $b^2 \neq a$, car $(b^2)^2 = b$ et $(b^2)^3 = e$, donc $o(b^2) = 3 \neq 2 = o(a)$,
   — $b^2 \neq b$, sinon $b = e$, ce qui est absurde,
   donc $\#\{e, a, b, b^2\} = 4$.
   On vérifie :
   — $ab \neq e$, sinon $a = b^{-1} = b^2$, ce qui est absurde,
   — $ab \neq a$, sinon $b = e$, ce qui est absurde,
   — $ab \neq b$, sinon $a = e$, ce qui est absurde,
   — $ab \neq b^2$, sinon $a = b$, ce qui est absurde,
   donc $\#\{e, a, b, b^2, ab\} = 5$.
   On vérifie :
   — $ba \neq e$, sinon $a = b^{-1} = b^2$, ce qui est absurde,
   — $ba \neq a$, sinon $b = e$, ce qui est absurde,
   — $ba \neq b$, sinon $a = e$, ce qui est absurde,
   — $ba \neq b^2$, sinon $a = b$, ce qui est absurde,
   — dans la question précédente, on a vu en particulier que : $ab = ba \implies G = \mathbb{Z}/6\mathbb{Z}$ abélien. Ainsi, par contraposé, comme G est supposé non-abélien, on a $ab \neq ba$,
   donc $\#\{e, a, b, b^2, ab, ba\} = 6$.
   Comme G est de cardinal 6, on a décrit tous les éléments de G. Ainsi, $ab^2 \in \{e, a, b, b^2, ab, ba\}$.Comme pour l'exercice 1.6, avec seulement les égalités provenant de l'ordre de a et b et la règle du sudoku, on peut compléter entièrement le tableau. On vérifie que :
   — $ab^2 \neq e$, sinon $a = b^{-2} = b$, ce qui est absurde,
   — $ab^2 \neq a$, sinon $b^2 = e$, ce qui est absurde,
   — $ab^2 \neq b$, sinon $ab = e$, ce qui est absurde,
   — $ab^2 \neq b^2$, sinon $a = e$, ce qui est absurde,
   — $ab^2 \neq ab$, sinon $b = e$, ce qui est absurde.
   Ainsi, il ne reste qu'une possibilité : $ab^2 = ba$. On tire de cette égalité :

$$ab.b = a.b^2 = ba, \quad b.ab = ba.b = a, \quad b.ba = b^2.a = ab,$$

$$ab.ba = b, \quad a.ba = ab.a = b^2, \quad ba.b^2 = ab,$$

$$ba.ba = e, \quad ab.ab = e, \quad b^2.ab = ba$$

   les autres égalités proviennent des ordres de a et b.

	e	a	b	b^2	ab	ba
e	e	a	b	b^2	ab	ba
a	a	e	ab	ba	b	b^2
b	b	ba	b^2	e	a	ab
b^2	b^2	ab	e	b	ba	a
ab	ab	b^2	ba	a	e	b
ba	ba	b	a	ab	b^2	e

	Id	(1 2)	(1 2 3)	(1 3 2)	(2 3)	(1 3)
Id	Id	(1 2)	(1 2 3)	(1 3 2)	(2 3)	(1 3)
(1 2)	(1 2)	Id	(2 3)	(1 3)	(1 2 3)	(1 3 2)
(1 2 3)	(1 2 3)	(1 3)	(1 3 2)	Id	(1 2)	(2 3)
(1 3 2)	(1 3 2)	(2 3)	Id	(1 2 3)	(1 3)	(1 2)
(2 3)	(2 3)	(1 3 2)	(1 3)	(1 2)	Id	(1 2 3)
(1 3)	(1 3)	(1 2 3)	(1 2)	(2 3)	(1 3 2)	Id

On vérifie bien que c'est la table de multiplication de $\mathfrak{S}_3$, avec :

$$(e, a, b, b^2, ab, ba) = (Id, (1\ 2), (1\ 2\ 3), (1\ 3\ 2), (2\ 3), (1\ 3)).$$

Ainsi, G et $\mathfrak{S}_3$ sont bien isomorphes.

□

Exercice 2.2 (**B.A.-BA.**). Soit $n \geqslant 2$. Décider pour chacune des applications suivantes si c'est un morphisme.

1. $f\colon \mathcal{M}_n(\mathbb{R}) \to \mathcal{M}_n(\mathbb{R})$, $a \mapsto a + {}^t a$.
2. $f\colon \mathrm{GL}_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R})$, $a \mapsto {}^t a$.
3. $f\colon \mathrm{GL}_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R})$, $a \mapsto {}^t a^{-1}$.

Démonstration.

1. Soient $A, B \in \mathcal{M}_n(\mathbb{R})$, alors $f(A+B) = (A+B) + (A+B)^t = f(A) + f(B)$, donc l'application f est donc un morphisme de groupe.
   Par ailleurs, le morphisme f n'est pas injectif car son noyau comprend les matrices anti-symétriques, ni surjectif, car son image est incluse dans l'ensemble des matrices symétriques.
2. L'application n'est pas un morphisme de groupe. En effet, si on choisit A et B deux matrices qui ne commutent pas entre elles, $f(A^tB^t) = BA \neq AB = f(A^t)f(B^t)$. Par exemple, dans $\mathrm{GL}_2(\mathbb{R})$, on peut choisir :

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ et } B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \text{ avec } AB = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \text{ et } BA = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

   Les matrices A et B sont bien dans $\mathrm{GL}_n(\mathbb{R})$, car sont d'inverses respectifs A et $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$.
3. C'est un morphisme de groupe. En effet (les deux contravariances s'annulent),

$$f(AB) = {}^t(AB)^{-1} = {}^tA^{-1t}B^{-1} = f(A)f(B)$$

   C'est un isomorphisme car $f^2 = \mathrm{id}$.

□

Exercice 2.3. Soit $\varphi\colon G_1 \to G_2$ un morphisme de groupes.

1. Soit g un élément de G_1 d'ordre fini. Montrer que l'ordre de $\varphi(g)$ divise l'ordre de g.
2. On suppose que G_1 est engendré par l'ensemble de ses éléments d'ordre 2 et que G_2 est fini, d'ordre impair. Montrer que φ est trivial.

Démonstration.

1. On a : $\varphi(g)^{o(g)} = \varphi(g^{o(g)}) = \varphi(1) = 1$. Ainsi : $o(\varphi(g))|o(g)$.

2. Puisque φ est un morphisme de groupe, il est déterminé par l'image d'une partie génératrice de G_1. On s'intéresse donc à l'image par φ des éléments d'ordre 2 de G_1. Soit $g \in G_1$ un élément d'ordre 2.

   D'après la question précédente, $o(\varphi(g))$ divise $o(g)$. Donc $o(\varphi(g)) \in \{1, 2\}$. Or, comme l'ordre d'un élément de G_2 divise l'ordre de G_2, il vient $o(\varphi(g)) = 1$, donc $\varphi(g) = 1$. Finalement le morphisme φ est trivial.

□

Exercice 2.4. Soit φ un morphisme d'un groupe fini $(G, *)$ vers $(\mathbb{C}^*, \times)$. On suppose que φ n'est pas une application constante. Calculer

$$\sum_{x \in G} \varphi(x).$$

Démonstration. Comme φ n'est pas l'application triviale, il existe $y \in G$ tel que $\varphi(y) \neq 1$. On remarque que l'application $G \to G$, $x \mapsto xy$ est une bijection d'inverse $x \mapsto xy^{-1}$. On a alors :

$$\sum_{x \in G} \varphi(x) \left(= \sum_{xy \in G} \varphi(xy) \right) = \sum_{x \in G} \varphi(xy) = \varphi(y) \sum_{x \in G} \varphi(x).$$

Comme $\varphi(y) \neq 1$, il vient : $\sum_{x \in G} \varphi(x) = 0$. □

Exercice 2.5 (B.A.-BA.). Soient G un groupe et H un sous-groupe. Montrer que l'application $gH \mapsto Hg^{-1}$ est une bijection de l'ensemble des classes à gauche sur celui des classes à droites.

Rappel. On définit les *classes à droite* de H dans G comme les classes d'équivalence de la relation $x \sim_R y \Leftrightarrow xy^{-1} \in H$ et les *classes à gauche* comme étant celles de la relation $x \sim_L y \Leftrightarrow y^{-1}x \in H$. L'ensemble des classes à droite est noté $H\backslash G$, et l'ensemble des classes à gauche H/G. Si H est normal (ou distingué), les deux ensembles sont égaux : c'est le groupe quotient.

Démonstration. On commence par s'intéresser aux ensembles de départ et d'arrivée de l'application. Soit $g \in G$, montrons que les classe à gauche de G sont exactement les éléments de la forme gH.

Soit $x \in gH$, alors il existe $h \in H$ tel que $x = gh$, soit encore $g^{-1}x = h \in H$. Donc $x \sim_L g$. Réciproquement, si $x \sim_L g$ alors il existe $h \in H$ tel que $g^{-1}x = h$, soit encore $x = gh \in gH$, ce qui prouve que les classes à gauche sont de la forme gH avec $g \in G$.

La preuve pour les classes à droite est la similaire.

On note f l'application qui envoie gH sur Hg^{-1}. Montrons que f est injective. On a par équivalences successives :

$$Hg^{-1} = Hx^{-1} \iff g^{-1} \sim_R x^{-1} \iff g^{-1}x \in H \iff x \sim_L g \iff gH = xH,$$

ce qui prouve la bijectivité de f. □

Remarque. L'exercice n'est pas utile pour cela, mais il n'est plus très difficile de prouver le théorème de Lagrange, à présent qu'on sait ce qu'est une classe à gauche... (Il suffit voir que $G = \bigcup_{g \in G} gH$, puis de choisir des représentants des classes à gauches et passer au cardinal).

Exercice 2.6. On considère une décomposition d'un entier n de la forme $n = n_1 + \cdots + n_k$ avec $n_i > 0$. Montrer que $\prod_{i=1}^{k} (n_i!)$ divise $n!$. On pourra appliquer le théorème de Lagrange à un sous-groupe bien choisi de S_n.

Démonstration. On pose $n_0 = 0$, et on considère la partition de $[\![1, n]\!]$ donnée par

$$\bigsqcup_{i=0}^{k-1} \left[\!\left[\sum_{j=0}^{i} n_j + 1, \sum_{j=0}^{i+1} n_j \right]\!\right].$$

On considère le sous-groupe H de $\mathfrak{S}_n$ qui stabilise cette partition. Cela revient à chercher les permutations "morceau par morceau", et on a : $H \simeq \prod_{i=1}^{k} \mathfrak{S}_{n_i}$. Donc l'ordre de H vaut $\prod_{i=1}^{k}(n_i!)$, ce qui prouve que $\prod_{i=1}^{k}(n_i!)$ divise $n!$, par le théorème de Lagrange. □

3 Feuille 3

Exercice 3.1 (**B.A.-BA.**)**.** Soient G un groupe et H un sous-groupe normal de G d'indice n.

1. Montrer que $g^n \in H$ pour tout $g \in G$.
2. Cette propriété nécessite la condition de normalité : dans $G = \mathfrak{S}_3$, donner un exemple de sous-groupe (non-normal) H d'indice 3 et d'un élément $g \in S_3$ tel que $g^3 \notin H$.

Démonstration.

1. Soit $g \in G$. Puisque le groupe G/H est d'indice n, l'image de g dans G/H vérifie $\bar{g}^n = 1$ (Lagrange). Cela implique que $g^n \in H$.
2. On prend $G = \mathfrak{S}_3$ et $H = \{\mathrm{id}, (1\ 2)\}$. Le groupe H est un sous-groupe de G d'indice $\frac{6}{2} = 3$, mais $(1\ 3)^3 = (1\ 3)$ n'est pas dans H.

□

Exercice 3.2 (**B.A.-BA.**)**.** Soient K, H deux sous-groupes d'un groupe G.

1. Vérifier que si $K \lhd G$, alors $K \cap H \lhd H$.
2. Montrer que si $K \lhd G$, alors KH est un sous-groupe de G. Déduire de 1. que du plus $K \lhd KH$.
3. Vérifier que si $K < H$ et $K \lhd G$ alors $K \lhd H$.
4. Trouver dans $G = \mathfrak{S}_4$ deux sous-groupes K, H vérifiant $K \lhd H$ et $H \lhd G$ mais tels que K n'est pas normal dans G.

Démonstration.

1. Supposons que $K \lhd G$. En particulier, $K < G$, et on a bien $K \cap H < H$. De plus : $\forall k \in K, \forall g \in G, gkg^{-1} \in K$. En particulier, on a : $\forall k \in K, \forall h \in H, hkh^{-1} \in K$. Comme $H < G$, il vient bien : $\forall k \in K \cap H, \forall h \in H, hkh^{-1} \in K \cap H$. Ainsi, on a bien $K \cap H \lhd H$.
2. Montrons que KH est bien un sous-groupe de G. On a bien $1 \times 1 = 1 \in KH$. Soient $(kh, \tilde{k}\tilde{h}) \in (KH)^2$. Alors :
   — $(kh)^{-1} = \underbrace{h^{-1}k^{-1}\left(h^{-1}\right)^{-1}}_{\in K} h^{-1} \in KH$,
   — $kh\tilde{k}\tilde{h} = \underbrace{k\underbrace{h\tilde{k}\tilde{h}\tilde{h}^{-1}h^{-1}}_{\in K}}_{\in K}\underbrace{h\tilde{h}}_{\in H} \in KH$.
   Donc KH est bien un sous-groupe de G, et par ce qui précède, on a : $K = K \cap KH \lhd KH$.
3. En effet, si $K < H$ et $K \lhd G$, alors : $\forall k \in K, \forall g \in G, gkg^{-1} \in K$. En particulier, comme $K < H < G$, on a bien : $\forall k \in K, \forall h \in H, hkh^{-1} \in K$. Donc $K \lhd H$.
4. On remarque que $K = \{Id, (1\ 2)(3\ 4)\}$ est distingué dans $H = \{Id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ qui est lui-même distingué dans $\mathfrak{S}_4$. Cependant K n'est pas distingué dans $\mathfrak{S}_4$ (conjuguer par $(1\ 3)$ par exemple).

□

Exercice 3.3 (**B.A.-BA.**)**.** Soit G un groupe.

1. Montrer que $Z(G) \lhd G$.
2. Montrer que si le quotient $G/Z(G)$ est monogène, alors G est abélien.
3. Soit G un groupe d'ordre p^2 où p est un nombre premier. On admet que $Z(G)$ n'est pas trivial (on l'établira plus tard dans le cours en considérant l'action du groupe G sur lui-même par conjugaison). Montrer que G est abélien.

Démonstration.

1. Par définition de $Z(G)$, on a, pour tout $z \in Z(G)$ et $g \in G$: $gzg^{-1} = g^{-1}gz = z \in Z(G)$, d'où le résultat.

2. Soit $\bar{a}$ tel que $\langle \bar{a} \rangle = G/Z(G)$ et a un antécédent de $\bar{a}$ par la projection $\pi : G \longrightarrow G/Z(G)$. Soient $x, y \in G$, alors il existe $n, m \in \mathbb{N}$ tels que $\bar{x} = \bar{a}^n$ et $\bar{y} = \bar{a}^m$, soit $x = a^n x'$ et $y = a^m y'$, où $x', y' \in Z(G)$. On a alors :
$$xy = a^n x' a^m y' = a^{n+m} y' x' = yx.$$
Donc finalement, $a \in Z(G)$, donc $\bar{a} = 1$ et $G = Z(G)$.
3. Comme $\#Z(G) > 1$ et divise p^2 (théorème de Lagrange), on a $\#Z(G) \in \{p, p^2\}$. Supposons par l'absurde que $Z(G) = p$. Alors $\#G/Z(G) = p$, donc le groupe quotient est cyclique, et donc, par la question 1, $G = Z(G)$. C'est donc absurde, et on a bien G abélien.

□

Exercice 3.4 (**B.A.-BA.**). Soit G un groupe.

1. Montrer que $D(G) \lhd G$.
2. Soit $N \lhd G$. Montrer que G/N est un groupe abélien si et seulement si $D(G) < N$.
3. On définit $D_0(G) = G$ et $D_{i+1}(G) = D(D_i(G))$ pour tout $i \geqslant 0$. Observer que $D_{i+1}(G) \lhd D_i(G)$ et que $D_i(G)/D_{i+1}(G)$ est abélien.

Démonstration.

1. On rappelle que $D(G) = \left\langle \{[x, y], (x, y) \in G^2\} \right\rangle < G$, où $[x, y] = xyx^{-1}y^{-1}$. Soit $(x, y, g) \in G^3$, on a : $g[x, y]g^{-1} = gxyx^{-1}y^{-1}g^{-1} = gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1} = [gxg^{-1}, gyg^{-1}] \in D(g)$. On a prouvé le résultat sur les générateurs. La conjugaison étant un morphisme, le résultat s'étend sur tout le sous-groupe, ce qui montre bien que $D(G) \lhd G$.

   On pouvait également remarquer que $[\cdot, \cdot]$ est défini uniquement avec des opérations de groupe. Comme la conjugaison par $g \in G$ (notée c_g) est un morphisme, on a donc $c_g([x, y]) = [c_g(x), c_g(y)]$.

   Enfin, on pouvait également prendre $x \in D(G)$, et remarquer que :
$$gxg^{-1} = \underbrace{gxg^{-1}x^{-1}}_{=[g,x] \in D(g)} \underbrace{x}_{\in D(G)} \in D(G).$$

2. On raisonne par équivalences :
$$\begin{aligned} G/N \text{ abélien} &\iff \forall (\bar{x}, \bar{y}) \in (G/N)^2, [\bar{x}, \bar{y}] = e \\ &\iff \forall (x, y) \in G, [x, y] \in N \\ &\iff D(G) < N. \end{aligned}$$

3. On a vu en question 1. que $D_0(G) \lhd D_1(G)$. Pour le prouver dans le cas $i \in \mathbb{N}$, il suffit d'appliquer le résultat de la question 1. à $\tilde{G} = D_i(G)$. En appliquant le résultat de la question 2. à ce même $\tilde{G}$, on obtient bien le caractère abélien des quotients successifs.

□

Remarque. On appelle cette suite la suite dérivée de G. Si elle est stationnaire à $\{e\}$, G est dit résoluble.

Exercice 3.5. Un sous-groupe H d'un groupe G est dit *caractéristique* si $\alpha(H) = H$ pour tout $\alpha \in \mathrm{Aut}(G)$. On note alors $H \blacktriangleleft G$.

1. Montrer que $H \blacktriangleleft G$ implique $H \lhd G$. Montrer que le $Z(G)$ et $D(G)$ sont caractéristiques dans G.
2. Donner un exemple de sous-groupe d'un groupe G qui est normal mais pas caractéristique.
3. Montrer que $K \blacktriangleleft H \blacktriangleleft G$ implique $K \blacktriangleleft G$. En déduire (cf Ex 4) que $D_i(G) \blacktriangleleft G$ pour tout $i \geqslant 0$.
4. Montrer que $K \blacktriangleleft H \lhd G$ implique $K \lhd G$.

Démonstration.

1. — Être un groupe normal est équivalent à être stable par tous les automorphismes intérieur. Or $\mathrm{Int}(G) < \mathrm{Aut}(G)$, donc être caractéristique implique être normal.
   — Soient $x \in Z(G)$, $y \in G$ et $\alpha \in \mathrm{Aut}(G)$. Alors il existe $y' \in G$ tel que $\alpha(y') = y$. On va montrer que $\alpha(Z(G)) \subset Z(G)$ ce qui permettra de conclure sur l'égalité puisque α est un automorphisme (donc bijectif. On ne le précisera plus dans la suite). On a :
   $$\alpha(x)y = \alpha(x)\alpha(y') = \alpha(xy') = \alpha(y'x) = y\alpha(x).$$
   Donc $\alpha(x) \in Z(G)$ ce qui prouve que le centre de G est caractéristique.
   — Soit $\alpha \in \mathrm{Aut}(G)$. On va vérifier que "$\alpha$ d'un commutateur est un commutateur". Comme α est un morphisme de groupe, la linéarité permettra de déduire que $\alpha(\mathcal{D}(G)) \subset \mathcal{D}(G)$.
   $$\alpha(xyx^{-1}y^{-1}) = \alpha(x)\alpha(y)\alpha(x)^{-1}\alpha(y)^{-1}.$$
   Ce qui prouve que $\mathcal{D}(G)$ est un sous-groupe caractéristique de G.
2. On considère le sous-groupe $\{0\} \times \mathbb{Z}/2\mathbb{Z}$ de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. L'automorphisme $\alpha\colon (x, y) \mapsto (y, x)$ ne stabilise pas $\{0\} \times \mathbb{Z}/2\mathbb{Z}$ car $\alpha(\{0\} \times \mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z} \times \{0\}$. Pourtant, le groupe est bien normal dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

   La même idée peut se transposer aux matrices (avec $n \geqslant 2$) dans $(\mathcal{M}_n, +)$ avec comme sous-groupe normal le sous-groupe des matrices triangulaires supérieures, et comme automorphisme particulier la transposition.
3. Soit $\alpha \in \mathrm{Aut}(G)$, puisque $H \blacktriangleleft G$, $\alpha(H) = H$ et donc $\alpha|_H^H \in \mathrm{Aut}(H)$. Or $K \blacktriangleleft H$, donc $\alpha(K) = \alpha|_H^H(K) = K$, ce qui prouve que $K \blacktriangleleft G$.
   Pour montrer que $D_i(G) \blacktriangleleft G$ pour tout $i \geqslant 0$, il suffit de faire une récurrence, l'initialisation se faisant avec la question 1.

   Remarque. Ici, on a utilisé la notation suivante : Pour $f : A \to U$, $B \subset A$ et $V \subset U$ tels que $f(B) \subset U$, on écrit : $f|_B^V : \begin{pmatrix} B & \longrightarrow & V \\ x & \longmapsto & f(x) \end{pmatrix}$.
4. Soit $\alpha \in \mathrm{Int}(G)$, puisque $H \lhd G$, $\alpha(H) = H$ et donc $\alpha|_H^H \in \mathrm{Aut}(H)$. Puisque $K \blacktriangleleft H$, on a $\alpha(K) = \alpha|_H^H(K) = K$, et donc $K \lhd G$.

□

Exercice 3.6. Soit G un groupe non abélien d'ordre 8.

1. Montrer que G contient un élément x d'ordre 4 et que le groupe qu'il engendre est normal dans G.
2. Soit alors $y \in G \backslash \langle x \rangle$; montrer que $y^2 = 1$ ou $y^2 = x^2$.
3. Si $y^2 = 1$, montrer que $yxy = x^{-1}$ et en déduire que G est isomorphe à D_4.
4. Dans le cas restant, écrire la table de G est conclure que G est isomorphe à Q_8.
5. Donner la liste des groupes d'ordre 8 à isomorphisme près.

Démonstration.

1. L'ordre des éléments dans G est compris dans $\{8, 4, 2, 1\}$ par le théorème de Lagrange.
   Le groupe n'étant pas abélien, il n'est pas cyclique, donc il n'y a pas d'élément d'ordre 8.
   De même si tous les éléments de G étaient d'ordre 2, alors le groupe serait abélien. (En effet, dans ce cas, on a pour tout $(x, y) \in G^2$: $(xy)^2 = 1$, donc $xy = y^{-1}x^{-1} = yx$).
   Donc il existe un élément x d'ordre 4.
   Le groupe $\langle x \rangle$ est d'indice $\dfrac{8}{4} = 2$ dans G, donc il est normal. (voir la remarque en fin d'exercice).

2. Par définition de y, son image dans $G/\langle x\rangle$ n'est pas le neutre. Comme $\#G/\langle x\rangle = 2$, il vient $\bar{y}^2 = 1$, donc $y^2 \in \langle x\rangle$.
   Si $y^2 \neq 1$, alors y^2 est d'ordre 2 (par LAGRANGE). Le seul élément d'ordre 2 dans $\langle x\rangle$ est x^2, cela permet de conclure.
3. Si $y^2 = 1$, alors comme $\langle x\rangle$ est normal, on a $yxy \in \langle x\rangle$. De plus yxy est d'ordre 4, donc il vaut soit x, soit x^{-1}.
   Or si $yxy = x$, alors x et y commutent. Comme $G = \langle x\rangle \sqcup y\langle x\rangle$, alors cela impliquerait que G est commutatif, ce qui est absurde. Donc $yxy = x^{-1}$.
   A cause des relations sur ses éléments (qui est une présentation de D_4 [1]), le groupe G s'identifie à un quotient de D_4. Comme G et D_4 ont le même ordre, ils sont bien isomorphes.
4. Les éléments de G sont $\{1, x, y, x^2, x^{-1}, y^{-1}, xy, (xy)^{-1}\}$. Il faut alors utiliser les relations $x^4 = 1$ et $x^2 = y^2$, le caractère normal de $\langle x\rangle$ dans G (qui permet par exemple de calculer yxy^{-1}) pour pouvoir calculer la table du groupe (vu la forme de la question, ne pas hésiter à commencer par calculer la table de Q_8 pour "s'aider" à trouver le résultat).

	1	x	y	x^2	x^{-1}	y^{-1}	xy	$(xy)^{-1}$
1	1	x	y	x^2	x^{-1}	y^{-1}	xy	$(xy)^{-1}$
x	x	x^2	xy	x^{-1}	1	$(xy)^{-1}$	y^{-1}	y
y	y	$(xy)^{-1}$	x^2	y^{-1}	xy	1	x	x^{-1}
x^2	x^2	x^{-1}	y^{-1}	1	x	y	$(xy)^{-1}$	xy
x^{-1}	x^{-1}	1	$(xy)^{-1}$	x	x^2	xy	y	y^{-1}
y^{-1}	y^{-1}	xy	1	y	$(xy)^{-1}$	x^2	x^{-1}	x
xy	xy	y	x^{-1}	$(xy)^{-1}$	y^{-1}	x	x^2	1
$(xy)^{-1}$	$(xy)^{-1}$	y^{-1}	x	xy	y	x^{-1}	1	x^2

   On compare cette table à la table de $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ avec les relations $i^2 = j^2 = k^2 = ijk = -1$ et $ij = k$, $ji = -k$, $ik = -j$, $jk = i$. Comme dit dans H2G2 : toute ressemblance avec le produit vectoriel ne serait fortuite !

	1	i	j	-1	$-i$	$-j$	k	$-k$
1	1	i	j	-1	$-i$	$-j$	k	$-k$
i	i	-1	k	$-i$	1	$-k$	$-j$	j
j	j	$-k$	-1	$-j$	k	1	i	$-i$
-1	-1	$-i$	$-j$	1	i	j	$-k$	k
$-i$	$-i$	1	$-k$	i	-1	k	j	$-j$
$-j$	$-j$	k	1	j	$-k$	-1	$-i$	i
k	k	j	$-i$	$-k$	j	i	-1	1
$-k$	$-k$	$-j$	i	k	$-j$	$-i$	1	-1

5. On a classifié les groupes d'ordre 8 non abéliens. Les groupes abéliens d'ordre 8 sont $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$. [2]

□

Remarque. On cherche à prouver que :

$$\left.\begin{array}{l} H \leqslant G \\ [G : H] = 2 \end{array}\right\} \Longrightarrow H \lhd G$$

Soient $g \in G$ et $h \in H$, montrons que $ghg^{-1} \in H$.
— Si $g \in H$, le résultat est immédiat, car $H \leqslant G$,

1. Pour aller plus loin, voir ici.
2. Voir une version complète ici

— Sinon, on traduit l'hypothèse $[G : H] = 2$. Cela signifie que $\#\{gH, g \in G\} = 2$. On vérifie qu'on peut prendre e et g comme représentants de ces ensembles (vrai car $g \in G \backslash H$). Ainsi, comme les classes d'équivalences forment une partition de G, on peut écrire : $G = H \sqcup gH$. Il suffit donc de montrer que $ghg^{-1} \notin gH$.
On raisonne pour cela par l'absurde : si $ghg^{-1} \in gH$, alors il existe $h_0 \in H$ tel que $ghg^{-1} = gh_0$. Mais alors, il vient $g = h_0^{-1}h \in H$, ce qui est absurde, d'où le résultat.

On pouvait aussi reprendre l'exercice 2.5....

4 Feuille 4

Exercice 4.1 (**B.A.-BA.**).

1. Quel est le dernier chiffe de l'écriture décimale de 3^{2024} ?
2. Soit x un générateur de $\mathbb{Z}/n\mathbb{Z}$ et soit $m \in \{1, \dots, n\}$. Montrer que mx est d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $m = \dfrac{n}{d}k$ où k est premier avec d.
3. Montrer que $\displaystyle\sum_{d|n} \varphi(d) = n$. On pourra regrouper les éléments selon leur ordre dans $\mathbb{Z}/n\mathbb{Z}$.

Démonstration.

1. Pour avoir son dernier chiffre en écriture décimale, on peut chercher à représenter 3^{2024} dans $\mathbb{Z}/10\mathbb{Z}$. On commence par chercher l'ordre de 3 dans $(\mathbb{Z}/10\mathbb{Z})^\times$.
   On constate que 3 est d'ordre 4 modulo 10 (pour la multiplication). De plus $2024 = 4 \times 506 + 0$. Il vient donc $3^{2024} \equiv 3^0\,[10] \equiv 1\,[10]$.
2. Supposons que $o(mx) = d$, alors $(md)x = 0$, donc $o(x) = n|md$. Ainsi $m = \dfrac{n}{d}k$ pour un certain entier k non nul.
   Notons $p = \operatorname{pgcd}(d, k)$, $d = pd'$ et $k = pk'$. Alors $d'mx = \dfrac{n}{pd'}pk'd'x = k'nx = 0$ car $o(x) = n$. Donc $o(mx) = d|d'|d$, donc $d' = d$ et il vient bien $p = 1$.
   Réciproquement, si $m = \dfrac{n}{d}k$ et k premier avec d, alors, on a bien $mdx = nkx = 0$. Donc mx est d'ordre un diviseur de d.
   Comme d est premier avec k, il existe u, v tels que $1 = ku + dv$. On a $o(mx)\dfrac{n}{d}kx = 0$, donc $o(mx)\dfrac{n}{d}kux = 0$. Ainsi :
   $$o(mx)\frac{n}{d}(1 - dv)x = o(mx)\frac{n}{d}x = 0.$$
   Ainsi, comme x est d'ordre n, $o(mx)\dfrac{n}{d}$ est divisible par n. Comme $o(mx)$ est un diviseur de d, on a forcément $d = d'$, ce qui prouve que mx est d'ordre d.
3. On remarque que :
   $$\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d|n} \underbrace{\{x \in \mathbb{Z}/n\mathbb{Z} | o(x) = d\}}_{=:A_d}.$$
   Le groupe $\mathbb{Z}/n\mathbb{Z}$ étant cyclique, on note x un générateur, et pour tout $y \in \mathbb{Z}/n\mathbb{Z}$, il existe un unique $m \in [\![1, n]\!]$ tel que $y = mx$. Par la question précédente, on a :
   $$A_d = \{mx \in \mathbb{Z}/n\mathbb{Z} | o(x) = d, m \in [\![1, n]\!]\} = \left\{mx \in \mathbb{Z}/n\mathbb{Z} \,\middle|\, m \in [\![1, n]\!], m = \frac{n}{d}k, k \in [\![1, d]\!], k \wedge d = 1\right\}$$
   $$= \left\{\frac{n}{d}kx \in \mathbb{Z}/n\mathbb{Z} \,|\, k \in [\![1, d]\!], k \wedge d = 1\right\}.$$
   Par la définition de l'indicatrice d'Euler, $\#A_d = \varphi(d)$ pour d un diviseur de n.
   L'union étant disjointe, il vient bien $\displaystyle\sum_{d|n} \varphi(d) = n$.

□

Les trois prochains exercices sont destinés à montrer les propriétés suivantes.
Ex 4.2 : $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique pour tout nombre premier $p \geqslant 2$.
Ex 4.4 : $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique pour tout nombre premier $p \geqslant 3$ et pour tout entier $\alpha \geqslant 2$.
Ex 4.5 : $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est isomorphe à $(\mathbb{Z}/2^{\alpha-2}\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$ pour tout entier $\alpha \geqslant 3$.

Exercice 4.2. Soit $O = \{d \mid o(x) = d, x \in (\mathbb{Z}/p\mathbb{Z})^\times\}$. On commence par montrer (questions 1. et 2.) qu'il existe un élément d'ordre $r = \operatorname{ppcm}(O)$, en particulier r divise $p - 1$. La question 3. permet de conclure.

1. Redémontrer (cf Feuille 2) que si $o(x) = p$ et $o(y) = q$ avec p, q premiers entre eux, alors $o(xy) = pq$.
2. Notons $\prod_{i=1}^{n} p_i^{m_i}$ la décomposition de r en facteurs premiers. Vérifier qu'il existe $x_i \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $p_i^{m_i}$ divise $o(x_i)$. En déduire qu'il existe $y_i \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $o(y_i) = p_i^{m_i}$. En déduire qu'il existe un élément d'ordre $r = \text{ppcm}(O)$.
3. Soit $E := \left\{x \in (\mathbb{Z}/p\mathbb{Z})^\times, x^r = 1\right\}$. Vérifier que $E = (\mathbb{Z}/p\mathbb{Z})^\times$. Vérifier ensuite que $p - 1 \leqslant r$. En déduire que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p - 1$.

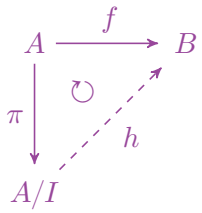
Démonstration.

1. Comme $(xy)^{pq} = 1$, $pq \mid o(xy)$. De plus, si $(xy)^k = 1$, alors $x^k = y^{-k}$, et donc $x^{kp} = 1 = y^{kp}$, en particulier $q \mid kp$, donc $q \mid k$ puisque $p \wedge q = 1$. De même, $p \mid k$, donc $pq \mid k$.
2. Pour $i \in [\![1, n]\!]$, il existe un élément $x_i \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $o(x) = p_i^{m_i} u$ avec u un certain entier premier avec p_i. (En effet, si $p_i^{m_i}$ n'apparaissait dans l'ordre d'aucun $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, il ne pourrait pas apparaître dans $\text{ppcm}(O)$). Ainsi, avec $y_i = x_i^u$, $o(y_i) = p_i^{m_i}$.
   Par la question précédente, l'élément $y = \prod_{i=1}^{n} y_i \in (\mathbb{Z}/p\mathbb{Z})^\times$ est d'ordre r.
3. L'ensemble E est non vide, et on a même $(\mathbb{Z}/p\mathbb{Z})^\times \subset E$, car r est le ppcm des ordres de tous les éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$, donc $E = (\mathbb{Z}/p\mathbb{Z})^\times$.
   Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, l'équation $x^r - 1 = 0$ possède au plus r solutions. Ainsi, $\text{Card}(E) = p - 1 \leqslant r$. Puisque r divise $p - 1$ (par LAGRANGE, d'après la question précédente), il vient $r = p - 1$, et donc $(\mathbb{Z}/p\mathbb{Z})^\times$ possède un élément d'ordre $p - 1$, donc est cyclique.

□

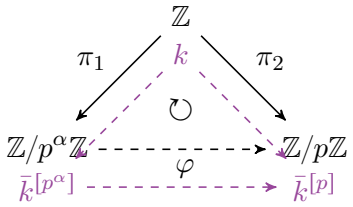
Exercice 4.3. Soit p un nombre premier et soit φ le morphisme d'anneau naturel $\mathbb{Z}/p^\alpha\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$. Vérifier que φ est bien défini et qu'il induit un morphisme de groupes $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ surjectif.

Rappel. En général, on voit cette version de la *Propriété universelle de l'anneau quotient* $(A/I, \pi)$: Pour tout morphisme d'anneau $f : A \longrightarrow B$ tel que $I \subset \text{Ker}(f)$, il existe un unique $h : A/I \longrightarrow B$ qui rende commutatif le diagramme suivant :



Le coeur de la preuve de cette propriété est le fait que $\text{Ker}(\pi) \subset \text{Ker}(f)$. Cela permet de montrer que h est bien défini. La vérification des propriétés est alors "simplement" calculatoire.

Démonstration. Pour prouver que $\varphi : \begin{pmatrix} \mathbb{Z}/p^\alpha\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ \bar{k}^{[p^\alpha]} & \longmapsto & \bar{k}^{[p]} \end{pmatrix}$ est bien défini, on part de la projection $\begin{pmatrix} \mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ k & \longmapsto & \bar{k}^{[p]} \end{pmatrix}$. On remarque que $p^\alpha\mathbb{Z} \subset p\mathbb{Z} = \text{Ker}(f)$. Par la propriété universelle du quotient, φ est donc bien défini, comme factorisation de f par $\mathbb{Z}/p^\alpha\mathbb{Z}$:



Le morphisme φ induit bien un morphisme de groupe $\Phi : (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$: c'est une propriété générale des morphismes d'anneaux[3].

Enfin, le morphisme Φ est bien surjectif, par la construction ci-dessus, et car π_2 l'est. En effet, $(\mathbb{Z}/p\mathbb{Z})^* = \left\{\bar{k}^{[p]}, k \wedge p = 1, k \in [\![1,p]\!]\right\}$, donc $\varphi\left(\pi_1\left(\{k \in [\![1,p]\!], k \wedge p = 1\}\right)\right) = (\mathbb{Z}/p\mathbb{Z})^*$, ce qui prouve que Φ est surjectif. □

Exercice 4.4. Soit $p \geqslant 3$ un nombre premier et soit $\alpha \geqslant 2$.

1. Montrer que pour tout $k \geqslant 0$, il existe un entier λ_k non divisible par p tel que :

$$(1+p)^{p^k} = 1 + \lambda_k p^{k+1}.$$

   En déduire que la classe de $1+p$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}$ est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.
2. Exhiber un élément d'ordre $p-1$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ (utiliser les Exercices 2. et 3.).
3. En déduire que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.

Démonstration.

1. On procède par récurrence sur k. Pour $k=0$, on a $(1+p)^{p^0} = 1+p$, donc $\lambda_0 = 1$. On suppose le résultat vrai pour un certain rang k. Alors :

$$(1+p)^{p^{k+1}} = (1+\lambda_k p^{k+1})^p = 1 + \lambda_{k+1} p^{k+2},$$

   où $\lambda_{k+1} = \lambda_k + \sum_{i=2}^{p} \binom{p}{i} \lambda_k^i p^{(k+1)(i-1)-1} \equiv 1\,[p]$. Cela permet de conclure la récurrence.

   Par ce qui précède, on a : $(1+p)^{p^{\alpha-1}} \equiv 1\,[p^\alpha]$, donc l'ordre de $\overline{1+p}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ divise $p^{\alpha-1}$ (c'est donc une puissance de p). Pour $k \in [\![0, \alpha-2]\!]$, on a $(1+p)^{p^k} = 1 + \lambda_k p^{k+1} \not\equiv 1\,[p^\alpha]$ car p ne divise pas λ_k. Donc $\overline{1+p}$ est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.
2. Par l'exercice 4.2., on sait que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique. On a donc accès à y un générateur, qui est d'ordre $p-1$. Par l'exercice 4.3., comme Φ est surjective, il possède un antécédent x par Φ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. Alors, en considérant $\tilde{x} = x^{\frac{o(x)}{p-1}}$ ($o(x)$ est bien divisible par $p-1$, voir 2.3.1), on a bien $\tilde{x}^{p-1} = 1$.
3. On cherche à construire un élément d'ordre $\#(\mathbb{Z}/p^\alpha\mathbb{Z})^\times = p^{\alpha-1}(p-1)$. Comme $\overline{1+p}$ et $\tilde{x}$ commutent, que $o(\overline{1+p}) = p^{\alpha-1}$, que $o(\tilde{x}) = p-1$ et que $\mathrm{pgcd}(p^{\alpha-1}, p-1) = 1$, $(\overline{1+p})\tilde{x}$ est bien d'ordre voulu.

□

Exercice 4.5. Soit $\alpha \geqslant 3$.

1. Montrer que pour tout $k \geqslant 0$, il existe λ_k impair tel que

$$5^{2^k} = 1 + \lambda_k 2^{k+2}.$$

   En déduire que $\bar{5}$ est d'ordre $2^{\alpha-2}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$.
2. On considère (cf Ex 4.3) le morphisme naturel $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$, celui-ci est surjectif. Montrer que son noyau est d'ordre $2^{\alpha-2}$ et engendré par $\bar{5}$. En déduire que

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \left(\mathbb{Z}/2^{\alpha-2}\mathbb{Z}\right) \times \mathbb{Z}/2\mathbb{Z}.$$

Démonstration.

3. Pour $\varphi : A \longrightarrow B$ et $a \in A^\times$, $\varphi(a \times a^{-1}) = \varphi(1_A) = 1_b = \varphi(a) \times \varphi(a^{-1})$, donc $\varphi(a) \in B^\times$ et $\varphi(a)^{-1} = \varphi(a^{-1})$: φ induit un morphisme de groupes $\tilde{\varphi} : A^\times \longrightarrow B^\times$.

1. On procède par récurrence sur k. Pour $k = 0$ le résultat est clair ($\lambda_0 = 1$). On suppose le résultat vrai pour un certain rang k. Alors :

$$5^{2^{k+1}} = (1 + \lambda_k 2^{k+2})^2 = 1 + \lambda_k 2^{k+3} + \lambda_k^2 2^{2k+4} = 1 + \lambda_{k+1} 2^{k+3},$$

où $\lambda_{k+1} = \lambda_k + \lambda_k^2 2^{k+1} \equiv 1\,[2]$. Cela permet de conclure la récurrence.
Par ce qui précède, on a : $5^{2^{\alpha-2}} \equiv 1\,[2^\alpha]$, donc l'ordre de $\bar{5}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ divise $2^{\alpha-2}$. Pour $k \in [\![0, \alpha-3]\!]$, on a $5^{2^k} = 1 + \lambda_k 2^{k+2} \not\equiv 1\,[2^\alpha]$ car λ_k est impair. Donc $\bar{5}$ est d'ordre $2^{\alpha-2}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$.

2. Notons $\varphi : (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$. Le théorème d'isomorphisme nous assure que le cardinal de son noyau est $\dfrac{2^{\alpha-1} \times (2-1)}{2} = 2^{\alpha-2}$. Comme $\bar{5} \equiv 1\,[4]$, par construction du morphisme de l'exercice 4.3., il est clair que le sous-groupe engendré par $\bar{5}$ est dans le noyau de ce morphisme. Par cardinalité, $\bar{5}$ engendre le noyau.
On a donc $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times / \langle\bar{5}\rangle \simeq (\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$.
Il reste à montrer que :

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \langle\bar{5}\rangle \times (\mathbb{Z}/4\mathbb{Z})^\times.$$

Attention, $A/B \simeq C \implies A \simeq B \times C$ est **faux** en général ! Pensez à $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$...
Pour cela, on utilise le critère d'isomorphisme du produit direct. On pose :
— $H_1 = \mathrm{Ker}(\varphi) = \langle\bar{5}\rangle$,
— $H_2 = \{1, -1\} \subset (\mathbb{Z}/2^\alpha\mathbb{Z})^\times$.
On peut vérifier que :
— Pour tout $(h_1, h_2) \in H_1 \times H_2$, $h_1 h_2 = h_2 h_1$ (évident),
— $H_1 H_2 = (\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ (par cardinalité),
— $H_1 \cap H_2 = \{1\}$.
Ainsi, on a bien $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ isomorphe au produit $H_1 \times H_2 \simeq \left(\mathbb{Z}/2^{\alpha-2}\mathbb{Z}\right) \times \mathbb{Z}/2\mathbb{Z}$.

□

Remarque. Pour une construction "à la main", on pouvait écrire, pour $x \in (\mathbb{Z}/2^\alpha\mathbb{Z})^\times$:
— Si $\varphi(x) = 1 = 3^0$, alors il existe un unique $k_x \in [\![0, 2^{\alpha-2} - 1]\!]$ tel que $x = \overline{5^{k_x}}$,
— Si $\varphi(x) = 3 = 3^1$, alors il existe un unique $k_x \in [\![0, 2^{\alpha-2} - 1]\!]$ tel que $x = \overline{-5^{k_x}}$.
Pour $x \in (\mathbb{Z}/2^\alpha\mathbb{Z})^\times$, il existe donc un unique couple $(u_x, k_x) \in \{0,1\} \times [\![0, 2^{\alpha-2} - 1]\!]$ tel que $x = \overline{(-1)^{u_x} \times 5^{k_x}}$. Ainsi, on peut vérifier que $\begin{pmatrix} (\mathbb{Z}/2^\alpha\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/2^{\alpha-1}\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\ x & \longmapsto & (k_x, u_x) \end{pmatrix}$ est un isomorphisme.

5 Feuille 5

Exercice 5.1 (**B.A.-BA.**)**.** Écrire les décompositions en cycles des permutations suivantes :

1. $(3\,1\,4)(1\,5\,9\,2\,6)(5\,3)$,
2. σ^{-1} avec $\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}$.

Démonstration.

1. La permutation est :
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 6 & 9 & 3 & 1 & 4 & 7 & 8 & 2 \end{pmatrix}$$
la décomposition en cycle disjoint est donc : $\sigma = (1\ 5)(2\ 6\ 4\ 3\ 9)$.
2. Puisque $\sigma = (1\ 2\ 5\ 4\ 3)$, il vient $\sigma^{-1} = (3\ 4\ 5\ 2\ 1)$.

□

Exercice 5.2 (**B.A.-BA.**)**.** Calculer σ^{2024} avec
$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 9 & 8 & 11 & 7 & 3 & 2 & 6 & 12 & 5 & 4 & 1 \end{pmatrix}.$$

Démonstration. On peut écrire σ en cycle disjoints $\sigma = (1\ 10\ 5\ 7\ 2\ 9\ 12)(3\ 8\ 6)(4\ 11)$. Ainsi, σ est décomposée en un 7-cycle, un 3-cycle et une permutation. On a : $2024 = 7 \times 289 + 1 = 674 \times 3 + 2 = 2 \times 1012 + 0$. Ainsi, $\sigma^{2023} = (1\ 10\ 5\ 7\ 2\ 9\ 12)^1(3\ 8\ 6)^2(4\ 11)^0 = (1\ 10\ 5\ 7\ 2\ 9\ 12)(3\ 6\ 8)$. □

Exercice 5.3 (**B.A.-BA.**)**.** Dans $\mathfrak{S}_3$. Donner la liste des éléments en précisant leur classe de conjugaison. Lister les sous-groupes et les sous-groupes normaux.

Démonstration. On sait que $\mathrm{Card}(\mathfrak{S}_3) = 3! = 6$. La liste des éléments, rangés par classe de conjugaison (donc par type), donne :
$$\mathfrak{S}_3 = \{Id\} \cup \{(1\ 2), (1\ 3), (2\ 3)\} \cup \{(1\ 2\ 3), (1\ 3\ 2)\}.$$

On laisse de côté les sous-groupes triviaux $\{Id\}$ et $\mathfrak{S}_3$, qui sont normaux. D'après le théorème de Lagrange, l'ordre d'un sous-groupe non trivial de $\mathfrak{S}_3$ est 2 ou 3.

— Le groupe $\mathfrak{S}_3$ admet 3 sous-groupes d'ordre 2 chacun engendré par une transposition,
— Il existe un unique sous-groupe d'ordre 3, celui engendré par un 3-cycle (l'autre 3-cycle est le carré du premier) : c'est $\mathfrak{A}_3$.

La liste complète des sous-groupes est donc :
$$\{\{Id\}, \{Id, (1\ 2)\}, \{Id, (1\ 3)\}, \{Id, (2\ 3)\}, \{Id, (1\ 2\ 3), (1\ 3\ 2)\}, \mathfrak{S}_3\}.$$

Comme les sous-groupes normaux sont des réunions de classes de conjugaisons, le seul sous-groupe normal non-trivial de $\mathfrak{S}_3$ est $\mathfrak{A}_3 = \{Id, (1\ 2\ 3), (1\ 3\ 2)\}$. □

Exercice 5.4. Même exercice avec $\mathfrak{A}_4$. On constatera que $\mathfrak{A}_4$ ne possède pas de sous-groupes d'ordre 6.

Démonstration. On sait que $\mathrm{Card}(\mathfrak{A}_4) = \dfrac{4!}{2} = 12$. La liste des éléments, rangés par classe de conjugaison (donc a minima par type), donne :
$$\begin{aligned}\mathfrak{A}_4 = &\{Id\} \cup \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \\ &\cup \{(1\ 2\ 3), (1\ 3\ 4), (1\ 4\ 2), (2\ 4\ 3)\} \cup \{(1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 3), (2\ 3\ 4)\}.\end{aligned}$$

Pour trouver les classes de conjugaison des 3-cycles, on peut commencer par en prendre un au hasard, par exemple $(1\ 2\ 3)$. La conjugaison par les double-transpositions permet de récupérer 3 autres 3-cycles. La relation orbite-stabilisateur montre alors que la classe de conjugaison est soit complète, soit égale à $\mathfrak{A}_4$, ce qui est absurde vu les premières classes calculées. Il reste alors 4 éléments, on n'a plus qu'à vérifier qu'ils sont dans la même classe de conjugaison.

On laisse de côté les sous-groupes triviaux, qui sont normaux. D'après le théorème de Lagrange, l'ordre d'un sous-groupe non trivial de $\mathfrak{A}_4$ est 2,3,4 ou 6.

— Le groupe $\mathfrak{A}_4$ admet 3 sous-groupes d'ordre 2, chacun engendré par une double-transposition,
— Tout sous-groupe d'ordre 3 est engendré par un 3-cycle et il en existe 4 (un par élément de $\{1,2,3,4\}$ fixé par le sous-groupe),
— Le groupe engendré par toutes les doubles transpositions est d'ordre 4, et comme un tel sous-groupe ne peut pas contenir d'élément d'ordre 3, il n'y en a pas d'autre (le groupe est isomorphe à V_4)
— Si $\mathfrak{A}_4$ admet un sous-groupe H d'ordre 6, alors H est d'indice 2 et donc distingué dans $\mathfrak{A}_4$. Ainsi, H est la réunion de classes de conjugaison distinctes, ce qui est absurde puisqu'elles sont de cardinal 1,3,4 et 4.

La liste complète des sous-groupes est donc :

$$\{\{Id\}, \{Id, (1\ 2)(3\ 4)\}, \{Id, (1\ 3)(2\ 4)\}, \{Id, (1\ 4)(2\ 3)\},$$
$$\{Id, (1\ 2\ 3), (1\ 3\ 2)\}, \{Id, (1\ 2\ 4), (1\ 4\ 2)\}, \{Id, (1\ 3\ 4), (1\ 4\ 3)\}, \{Id, (2\ 3\ 4), (2\ 4\ 3)\},$$
$$\{Id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}, \mathfrak{A}_4\}.$$

Les sous-groupes normaux sont des réunions de classes de conjugaisons (d'ordre 1, 3, 4 et 4). Par le théorème de Lagrange, les cardinaux possibles pour ces sous-groupes sont 1, 2, 3, 4 et 12. On voit alors que le seul sous-groupe normal non-trivial de $\mathfrak{A}_4$ est $\{Id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ (isomorphe à V_4). □

Remarque. Pour le sous-groupe d'ordre 6, on pouvait aussi procéder ainsi :

Soit H un sous-groupe de $\mathfrak{A}_n$ d'ordre 6. Il est donc distingué car d'indice 2. Il contient donc un élément d'ordre 2 (une double-transposition), noté t et un élément d'ordre 3 (un 3-cycle), noté c.

Alors la conjugaison $c^{-1}tc$ et ctc^{-1} donne deux autres éléments d'ordre 2 distincts, tous contenus dans H. Donc le groupe contenant toutes les double-transpositions, noté V_4, est contenu dans H. Or 4 ne divise pas 6 : c'est absurde d'après le théorème de Lagrange. Il n'y a donc pas de sous-groupe d'ordre 6.

Exercice 5.5. Soit G un groupe fini d'ordre $2m$ avec m impair. Montrer que G admet un sous-groupe H d'indice 2 (en particulier $N \triangleleft G$ et G n'est pas simple). On pourra s'intéresser à l'image de G dans son plongement de Cayley.

Lemme (**B.A.-BA.**). Soit G un groupe d'ordre $2m$ avec m impair, il existe $x \in G$ d'ordre 2.

Démonstration. Par l'absurde, supposons que G ne possède pas d'élément d'ordre 2. On peut alors partitionner G de la manière suivante :

$$G = \{e\} \cup \bigcup_{x \in G\setminus\{e\}} \{x, x^{-1}\}.$$

L'union n'est bien sûr pas disjointe (on peut prendre une famille de représentants pour la rendre disjointe, mais ce n'est pas nécessaire pour la suite), mais les sous-ensembles $\{x, x^{-1}\}$, par hypothèse, sont tous de cardinal 2. Ainsi, G est d'ordre impair, ce qui est absurde. □

Démonstration. On note $\varphi\colon G \hookrightarrow \mathfrak{S}_{2m}$ le plongement de Cayley de G, et on considère le morphisme $\bar{\varphi} = \varepsilon \circ \varphi\colon G \to \mathbb{Z}/2\mathbb{Z}$, où ε désigne la signature. Montrons que $\bar{\varphi}$ est surjectif.

Comme G est d'ordre $2m$, G possède un élément x d'ordre 2. Son image par φ est donc un produit de transpositions disjointes (car seules les transpositions et l'élément neutre sont d'ordre un diviseur de 2 dans $\mathfrak{S}_{2m}$). Comme l'action par translation à gauche est sans point fixe (i.e. pour $x \in G$, si $gx = x$, alors $g = e$), $\varphi(x)$ n'a pas de point fixe (car $x \neq e$), et donc est un produit de m transpositions disjointes. Ainsi, $\bar{\varphi}(x) = 1 \equiv m\,[2]$, et le morphisme $\bar{\varphi}$ est surjectif.

On note $H = \mathrm{Ker}(\bar{\varphi})$ qui est distingué, alors par le premier théorème d'isomorphisme, on a $G/H \simeq \mathbb{Z}/2\mathbb{Z}$. Ainsi, on a bien trouvé un sous-groupe H d'indice 2. □

Exercice 5.6. On se place dans le groupe $\mathfrak{S}_6$.

1. Résoudre l'équation $\sigma^2 = (1\ 2)(3\ 4)$ dans $\mathfrak{S}_6$.
2. En déduire que l'on ne peut pas plonger Q_8 dans $\mathfrak{S}_6$ (indication : dans Q_8, -1 a 6 racines carrées).

Démonstration.

1. Si $\sigma^2 = (1\,2)(3\,4)$, alors σ est d'ordre 4.

   On cherche à obtenir des informations sur le type de σ. On regarde donc les partitions possibles de 6 avec les diviseurs de 4. Comme σ est d'ordre 4, sa décomposition en cycles disjoints possède au moins un 4-cycle, donc il vient uniquement les possibilités : $6 = 4 + 1 + 1 = 4 + 2$.

   On a donc accès uniquement à une transposition (ou pas) et un 4-cycle. Vu le carré de σ, le 4-cycle fait intervenir les entiers $1, 2, 3$ et 4.

   On trouve donc 4 possibilités :$(1\ 3\ 2\ 4)$, $(1\ 4\ 2\ 3)$, et $(1\ 3\ 2\ 4)(5\ 6)$ ou $(1\ 4\ 2\ 3)(5\ 6)$.
2. On suppose qu'il existe un plongement $\varphi\colon Q_8 \hookrightarrow \mathfrak{S}_6$. Montrons que $\varphi(-1)$ est une double-transposition. Puisque -1 possède au moins une racine dans Q_8 et est d'ordre 2 alors $\varphi(-1)$ possède au moins une racine dans $\mathfrak{S}_6$ et est d'ordre 2. Or les transpositions ne possèdent pas de racine dans $\mathfrak{S}_6$ (s'ils en avait une, ce serait un 4-cycle, mais le carré d'un 4-cycle est une double-transposition). De même le produit de 3 transpositions n'ont pas de racines dans $\mathfrak{S}_6$. Ainsi $\varphi(-1)$ est bien une double-transposition.

   Mais -1 possède 6 racines dans Q_8 alors que, d'après la question précédente, quitte à échanger le rôle de 1, 2, 3 et 4, une double-transposition ne possède que 4 racines dans $\mathfrak{S}_6$. Finalement on ne peut pas plonger Q_8 dans $\mathfrak{S}_6$.

□

Remarque. On prouve aussi que l'on ne peut pas plonger Q_8 dans $\mathfrak{S}_7$. En effet, les éléments d'ordre 4 dans $\mathfrak{S}_7$ sont les produits de 4-cycles et de transposition (à supports disjoints). De plus, une double-transposition est la seule à avoir des racines, et elle en possède 8 distinctes. Par exemple si $\sigma^2 = (1\ 2)(3\ 4)$, alors

$$\sigma \in \left\{ \begin{array}{l} (1\ 3\ 2\ 4), (1\ 3\ 2\ 4)(5\ 6), (1\ 3\ 2\ 4)(5\ 7), (1\ 3\ 2\ 4)(6\ 7), \\ (1\ 4\ 2\ 3), (1\ 4\ 2\ 3)(5\ 6), (1\ 4\ 2\ 3)(5\ 7), (1\ 4\ 2\ 3)(6\ 7) \end{array} \right\}.$$

De plus, si $\varphi\colon Q_8 \hookrightarrow \mathfrak{S}_7$ est un plongement alors $\varphi(-1)$ est une double-transposition. Pour plus de simplicité on peut supposer que $\varphi(-1) = (1\ 2)(3\ 4)$, alors $\varphi(i), \varphi(j)$ et $\varphi(k)$ sont dans l'ensemble

$$\left\{ \begin{array}{l} (1\ 3\ 2\ 4), (1\ 3\ 2\ 4)(5\ 6), (1\ 3\ 2\ 4)(5\ 7), (1\ 3\ 2\ 4)(6\ 7), \\ (1\ 4\ 2\ 3), (1\ 4\ 2\ 3)(5\ 6), (1\ 4\ 2\ 3)(5\ 7), (1\ 4\ 2\ 3)(6\ 7) \end{array} \right\}.$$

Mais $(1\ 3\ 2\ 4)(1\ 3\ 2\ 4) = (1\ 2)(3\ 4)$ et $(1\ 3\ 2\ 4)(1\ 4\ 2\ 3) = \mathrm{id}$. Donc on ne peut pas vérifier la relation $\varphi(i)\varphi(j) = \varphi(k)$.

Ainsi, Q_8 ne se plonge pas dans $\mathfrak{S}_7$.

Exercice 5.7. L'objectif est de lister les sous-groupes normaux du groupe diédral D_n. Soient r, s des générateurs de D_n, avec $r^n = 1$, $s^2 = 1$ et $srs = r^{-1}$. On montre que si n est impair, alors les sous-groupes normaux non triviaux de D_n sont les sous-groupes de $\langle r \rangle$. On montre ensuite que si n est pair, la liste des sous-groupes normaux non triviaux de D_n s'enrichit des sous-groupes $\langle r^2, s \rangle$, $\langle r^2, sr \rangle$.

1. Vérifier que $\langle r \rangle$ est normal dans D_n.
2. Montrer que les sous-groupes de $\langle r \rangle$ sont caractéristiques de $\langle r \rangle$. En particulier, les sous-groupes de $\langle r \rangle$ sont normaux dans D_n (cf Exercice 3.5).

   Questions 3-4-5 : cas n est impair, $n = 2k + 1$. Soit N un sous-groupe normal de D_n qui n'est pas un sous-groupe de $\langle r \rangle$. Montrons que $N = D_n$.
3. Montrer qu'il existe $j \in \{0, \dots, n-1\}$ tel que $sr^j \in N$.
4. Montrer que $r^{-2} \in N$. *Indication : On pourra calculer* $r(sr^j)r^{-1}$.

5. En déduire que $r \in N$, puis que $s \in N$ et enfin que $N = D_n$.

   Questions 6-7 : cas n est pair, $n = 2k$. Soit N un sous-groupe normal de D_n qui n'est pas un sous-groupe de $\langle r \rangle$. Comme dans 3. et 4., il existe $j \in \{0, \dots, n-1\}$ tel que $sr^j \in N$ et $r^{-2} \in N$.

6. Si j est pair, observer que $s \in N$. En déduire que, si N n'est pas égal à D_n, alors $N = \langle r^2, s \rangle$.

7. Si j est impair, observer que $sr \in N$. En déduire que, si N n'est pas égal à D_n, alors $N = \langle r^2, sr \rangle$.

Démonstration.

1. Au vu des relations entre générateurs, on a, pour $k \in [\![0, n]\!]$: $sr^k s^{-1} = (srs)^k = r^{-k}$. Ainsi, le sous-groupe est bien stable par conjugaison par un élément de D_n (car stable par conjugaison par ses générateurs, le cas r étant évident).

   Remarque. On pouvait aussi remarquer que $\langle r \rangle$ est d'indice 2 dans D_n, donc normal.

2. Comme $\langle r \rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, l'application suivante est une bijection : $\begin{pmatrix} \{H \leqslant \langle r \rangle\} & \xrightarrow{\sim} & \{d, d \mid n\} \\ H & \longmapsto & \#H \end{pmatrix}$. Comme un automorphisme de $\langle r \rangle$ préserve l'ordre des sous-groupes de $\langle r \rangle$, par la bijection précédente, les sous-groupes de $\langle r \rangle$ sont laissés invariants par automorphisme de $\langle r \rangle$. Ainsi, les sous-groupes de $\langle r \rangle$ sont bien caractéristiques dans $\langle r \rangle$. Par la question précédente et la question 3.5.4., on a bien le résultat souhaité.

3. On cherche à mettre sous une forme réduite les éléments de D_n. De la relation $srs = r^{-1}$, on tire $rs = sr^{-1}$. Ainsi, à partir d'un expression faisant intervenir r et s, on peut se ramener à une expression de la forme $s^a r^b$, avec $(a, b) \in \mathbb{Z}^2$. Vu les ordres des générateurs, on peut décrire exactement les éléments du groupe : $\left\{ r^k, sr^k \mid k \in [\![0, n-1]\!] \right\}$.

   Comme N n'est pas inclus dans $\langle r \rangle$, il possède donc bien un élément de la forme sr^j pour un certain $j \in [\![0, n-1]\!]$.

4. On a :
$$r\left(sr^j\right)r^{-1} = s(srs)r^{j-1} = sr^{j-2} \in N,$$
   d'où :
$$sr^j\left(sr^{j-2}\right)^{-1} = sr^2s = r^{-2} \in N.$$

5. Ainsi, $r = r^{-2k} \in N$, puis $s = sr^j r^{-j} \in N$, donc $D_n = \langle s, r \rangle \leqslant N$, d'où l'égalité.

6. On a bien $s = sr^j\left(r^{-2}\right)^{\frac{j}{2}} \in N$, donc $\langle r^2, s \rangle \leqslant D_n$. Comme ce sous-groupe est d'ordre n, il est d'indice 2 (donc distingué) dans D_n, donc si $N \neq D_n$, on a bien égalité.

7. On a bien $sr = sr^j\left(r^{-2}\right)^{\frac{j-1}{2}} \in N$, donc $\langle r^2, sr \rangle \leqslant D_n$. Comme ce sous groupe est d'ordre n, il est d'indice 2 (donc distingué) dans D_n, donc si $N \neq D_n$, on a bien égalité.

□

6 Feuille 6

Exercice 6.1 (**B.A.-BA.**)**.** Soit G un groupe fini et $H \lhd G$ un sous-groupe d'ordre p, où p le plus petit diviseur premier de $|G|$. Montrer que $H < Z(G)$. On pourra considérer l'action de G sur H par conjugaison.

Démonstration. Comme H est normal dans G, l'action de G sur H par conjugaison $\begin{pmatrix} G \times H & \longrightarrow & H \\ (g,h) & \longmapsto & ghg^{-1} \end{pmatrix}$ est bien définie.

Pour prouver le résultat, il suffit de montrer que pour tout $h \in H \backslash \{e\}$, $\mathrm{Orb}(h) = \{h\}$. En effet, cela implique que pour tout $g \in G$ et $h \in H$, on a $ghg^{-1} = h$, d'où $H < Z(G)$.

Soit $h \in H$, la relation orbite-stabilisateur donne : $\#\mathrm{Stab}(h) = \dfrac{\#G}{\#\mathrm{Orb}(h)}$.

Par définition de l'action, on a $\mathrm{Orb}(h) \subset H$, donc $\#\mathrm{Orb}(h) \leqslant p$. Or p est le plus petit diviseur premier de $\#G$, et $\#\mathrm{Orb}(h) \mid \#G$. On a donc $\#\mathrm{Orb}(h) \in \{1, p\}$.

Si $\#\mathrm{Orb}(h) = p$, alors $\mathrm{Orb}(h) = H$, donc il existe $g \in G$ tel que $ghg^{-1} = e$, et il vient $h = e$, ce qui est absurde, car $\mathrm{Orb}(e) = \{e\}$.

Donc $\#\mathrm{Orb}(h) = 1$ pour tout $h \in H$. Comme $ehe^{-1} = h \in \mathrm{Orb}(h)$, on a bien le résultat attendu. □

Exercice 6.2. L'objectif est de montrer :

Théorème de Cauchy

Soit G un groupe d'ordre n et p un diviseur premier de n. Alors G contient un élément d'ordre p.

Notons $X := \{(g_1, \dots, g_p) \in G^p \mid g_1 g_2 \cdots g_p = 1\}$.

1. Vérifier que le groupe $\mathbb{Z}/p\mathbb{Z}$ agit sur X *via* la formule :
$$\bar{1} \cdot (g_1, \dots, g_p) = (g_p, g_1, \dots, g_{p-1}).$$
2. Décrire explicitement l'ensemble $X^{\mathbb{Z}/p\mathbb{Z}}$ des points fixes de cette action.
3. Calculer le cardinal de X et montrer que $X^{\mathbb{Z}/p\mathbb{Z}}$ n'est pas réduit à un singleton. Conclure.

Démonstration.

1. Vérifions dans un premier temps que si $(g_1, \dots, g_p) \in X$, alors $(g_p, g_1, \dots, g_{p-1}) \in X$:
$$g_p g_1 \cdots g_{p-1} = g_p g_1 \cdots g_{p-1} g_p g_p^{-1} = g_p e g_p^{-1} = e.$$
Si $\bar{k}$ est un élément de $\mathbb{Z}/p\mathbb{Z}$, puisque $\bar{1}$ engendre $\mathbb{Z}/p\mathbb{Z}$, on a (les indices sont pris modulo p) :
$$\bar{k} \cdot (g_1, \dots, g_p) = (g_{1-k}, g_{2-k}, \dots, g_{p-k}).$$
On vérifie alors facilement que $\bar{0} \cdot (g_1, \dots, g_p) = (g_1, \dots, g_p)$ et que $\overline{k+l} \cdot (g_1, \dots, g_p) = \bar{k} \cdot (\bar{l} \cdot (g_1, \dots, g_p))$.
2. Par définition, $X^{\mathbb{Z}/p\mathbb{Z}} = \{(g_1, \dots, g_p) \in X \mid \forall \bar{k} \in \mathbb{Z}/p\mathbb{Z}, \bar{k} \cdot (g_1, \dots, g_p) = (g_1, \dots, g_p)\}$. En particulier, on a $(g_1, \dots, g_p) = (g_p, g_1, \dots, g_{p-1})$, d'où $g_i = g_{i-1}$ pour tout $i \in [\![2, p]\!]$. On en déduit donc que $(g_1, \dots, g_p) = (g, g, \dots, g)$ pour un certain $g \in G$, avec $g^p = e$.
Réciproquement, tout élément de la forme $(g, g, \dots, g)$ avec $o(g) \mid p$ est dans $X^{\mathbb{Z}/p\mathbb{Z}}$, donc, comme p est premier, $X^{\mathbb{Z}/p\mathbb{Z}} = \{(g, \dots, g), g \in G, o(g) = p\} \cup \{(e, \dots, e)\}$.
3. Pour qu'un élément $(g_1, \dots, g_p)$ soit dans X on peut prendre des éléments $g_1, \dots, g_{p-1}$ quelconques dans G, et dans ce cas g_p est uniquement déterminé par $g_p^{-1} = g_1 \cdots g_{p-1}$. Donc $\#X = n^{p-1}$.
L'équation aux classes classes permet d'affirmer que
$$|X| = |X^{\mathbb{Z}/p\mathbb{Z}}| + \sum_{\substack{i=0 \\ \#\mathrm{Orb}(x_i) \neq 1}}^{r} |\mathrm{Orb}(x_i)|,$$

où les $x_i \in X$ sont les représentants des orbites qui partitionnent X. Or $|\mathrm{Orb}(x_i)| = \dfrac{p}{|\mathrm{Stab}(x_i)|}$ d'après la relation orbite-stabilisateur. Comme $|\mathrm{Orb}(x_i)| \neq 1$ et comme p est premier, $|\mathrm{Orb}(x_i)| = p$. Donc $n^{p-1} \equiv |X^{\mathbb{Z}/p\mathbb{Z}}| \,[p] \equiv 0\,[p]$. Puisque $X^{\mathbb{Z}/p\mathbb{Z}}$ contient au moins un élément qui est $(e, \dots, e)$, la congruence nous permet d'affirmer qu'il contient au moins $p-1$ autres éléments dans $X^{\mathbb{Z}/p\mathbb{Z}}$, donc au moins $p-1$ éléments de la forme $(g, \dots, g)$ où $o(g) = p$, par la question précédente (on a accès à un élément d'ordre p, les autres sont ses puissances).

□

Exercice 6.3. Il s'agit d'établir :

Théorème

Soit G un groupe fini et soit p le plus petit diviseur premier de $|G|$. Si H est un sous-groupe de G d'indice p, alors H est distingué dans G.

Le cas $p = 2$, démontré de manière élémentaire en cours, est un cas particulier. Soient G un groupe et H un sous-groupe de G. Soit G/H l'ensemble des classes à gauche modulo H. On considère l'application $G \times G/H \to G/H$ qui à (g, kH) associe gkH.

1. (a) Montrer que cette application définit une action de G sur G/H.
   (b) Soit $k \in G$. Montrer que $Stab_G(kH) = kHk^{-1}$.
   (c) D'après le cours, l'action de G sur G/H induit un morphisme ρ de G dans le groupe des bijections de G/H :
   $$\rho : G \to \mathrm{Bij}(G/H).$$
   Montrer que $\ker(\rho) = \bigcap_{k \in G} kHk^{-1}$.
2. On suppose que $|G|$ est fini et que $|G/H| = p$, où $p \geqslant 2$ est le plus petit diviseur premier de $|G|$. Nous allons montrer que H est distingué dans G.
   (a) Montrer que $|G/ker(\rho)|$ divise $p! = p \times (p-1) \times (p-2) \times \cdots \times 2 \times 1$.
   (b) Montrer que $\ker(\rho) \neq G$. En déduire que $|G/\ker(\rho)| \neq 1$.
   (c) Soit $q \geqslant 2$ un diviseur premier de $|G/\ker(\rho)|$.
   Montrer ensuite que $q = p$ (on pourra utiliser 2.(a)).
   (d) Établir que $|G/\ker(\rho)| = p$.
   (e) A ce stade, on a obtenu $|G/H| = |G/\ker(\rho)|$.
   En déduire que $H = \ker(\rho)$ et conclure.

Remarque. Tiré du CC2 2023.

Démonstration.

1. (a) Notons a (pour *action*) l'application de l'énoncé. Pour clarifier les notations lors de la vérification des axiomes, matérialisons nettement le "point" dans la notation de l'application a, c'est-à-dire que l'on note $a(g, kH) = g \cdot kH$, défini comme étant égal à gkH. Pour vérifier les axiomes, soient g_1, g_2, k dans G. On a :
$$\begin{aligned}(g_1g_2) \cdot kH &= ((g_1g_2)k)H && \text{par définition de } a,\\ &= (g_1(g_2k))H && \text{car la multiplication de } G \text{ est associative},\\ &= g_1 \cdot (g_2kH) && \text{par définition de } a,\\ &= g_1 \cdot (g_2 \cdot kH) && \text{encore par définition de } a.\end{aligned}$$
De plus, comme e est neutre on a $e \cdot kH = (ek)H = kH$. Donc a est une action de G sur G/H.

(b) On peut raisonner par équivalence. Soit $g \in G$:

$$\begin{aligned} g \in Stab_G(kH) &\iff gkH = kH, \\ &\iff k^{-1}gkH = H, \\ &\iff k^{-1}gk \in H, \\ &\iff g \in kHk^{-1}. \end{aligned}$$

Ainsi $Stab_G(kH) = kHk^{-1}$.

(c) Le noyau de ρ est l'ensemble des $g \in G$ tels que $\rho(g) = \mathrm{id}_{G/H}$, c'est-à-dire tels que $gkH = kH$ pour tout $k \in G$, c'est-à-dire tels que $g \in \bigcap_{k\in G} Stab_G(kH)$. Utilisant la question précédente, on en déduit que $\ker(\rho) = \bigcap_{k\in G} kHk^{-1}$.

2. (a) Le morphisme $\rho : G \to \mathrm{Bij}(G/H)$ induit un morphisme injectif $\bar{\rho} : G/\ker(\rho) \hookrightarrow \mathrm{Bij}(G/H)$ qui identifie $G/\ker(\rho)$ à un sous-groupe de $\mathrm{Bij}(G/H)$. Comme G/H est de cardinal p, le groupe $\mathrm{Bij}(G/H)$ est isomorphe au groupe symétrique $\mathfrak{S}_p$ qui est de cardinal $p!$. D'après le théorème de Lagrange, on en déduit que $|G/\ker(\rho)|$ divise $p!$.

(b) D'après la question 1.(c) on a $\ker(\rho) = \bigcap_{k\in G} kHk^{-1}$. Ce sous-groupe est inclus dans tous les kHk^{-1}, en particulier $(k = e)$ il est inclus dans H. C'est un sous-groupe strict de G, puisque $[G : H] = p \geqslant 2$. Donc $\ker(\rho) \neq G$, ou encore $|G/ker(\rho)| \neq 1$.

(c) D'après 2.(a) tous les facteurs premiers de $|G/\ker(\rho)|$ divisent $p!$. Ainsi q divise $p!$ et comme cette factorielle est produit de nombres $\leqslant p$, tous ses facteurs premiers sont $\leqslant p$. En particulier $q \leqslant p$. Par ailleurs, par le théorème de Lagrange, $|G/\ker(\rho)|$ divise $|G|$, donc q est un facteur premier de $|G|$. Comme p est le plus petit d'entre eux, on a $p \leqslant q$. Finalement $q = p$.

(d) Notons $c := |G/\ker(\rho)|$. D'après 2.(b) on a $c \neq 1$, et comme on vient de montrer que le seul facteur premier de c est p, on peut écrire $c = p^a$ avec $a \geqslant 1$. On sait aussi que c divise $p!$ d'après 2.(a). Or la multiplicité de p dans $p!$ est égale à 1 car aucun des nombres $1, 2, \ldots, p-1$ n'est divisible par p. Finalement $c = p$, comme demandé.

(e) On a obtenu $|G/H| = p = |G/\ker(\rho)|$. Par ailleurs, on a l'inclusion $\ker(\rho) \subset H$, déjà utilisée à la question 2.(b). Ceci implique que $p = |G/H| = |G|/|H| \leqslant |G|/|\ker(\rho)| = p$ donc l'inégalité est une égalité, et $H = \ker(\rho)$. Le sous-groupe H est donc le noyau d'un morphisme ; les noyaux sont toujours des sous-groupes distingués, donc H est distingué.

□

7 Feuille 7

Remarque. On a vu (par exemple au CC1) que pour $K, H < G$, si $H \lhd G$, alors $HK = KH$. Ainsi, dans la caractérisation du produit semi-direct, l'hypothèse "$NH = G$" peut être remplacée par "$HN = G$", car on montre toujours que $N \lhd G$. On ne le remarquera plus dans la suite.

Exercice 7.1 (**B.A.-BA.**)**.** Montrer que $\mathfrak{S}_3$ s'écrit comme un produit semi-direct de $\mathbb{Z}/3\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.

Démonstration. On utilise la caractérisation du produit semi-direct. On constate que $\mathbb{Z}/3\mathbb{Z} \simeq \mathfrak{A}_3 \lhd \mathfrak{S}_3$. On peut prendre par exemple $\mathbb{Z}/2\mathbb{Z} \simeq \{\mathrm{id}, (1\ 2)\} < \mathfrak{S}_3$. On vérifie alors que $\mathfrak{A}_3 \cap \{\mathrm{id}, (1\ 2)\} = \{\mathrm{id}\}$ et $\mathfrak{A}_3\{\mathrm{id}, (1\ 2)\} = \mathfrak{S}_3$.

Ainsi, $\mathfrak{S}_3 \simeq \mathfrak{A}_3 \rtimes_\alpha \{\mathrm{id}, (1\ 2)\}$, où $\alpha : \begin{pmatrix} \{\mathrm{id}, (1\ 2)\} & \longrightarrow & \mathrm{Aut}(\mathfrak{A}_3) \\ h & \longmapsto & \begin{pmatrix} \mathfrak{A}_3 & \xrightarrow{\sim} & \mathfrak{A}_3 \\ n & \longmapsto & hnh^{-1} \end{pmatrix} \end{pmatrix}$

Remarque. La définition de α est incluse avec la caractérisation du produit semi-direct !

□

Exercice 7.2 (**B.A.-BA.**)**.** Soit $\mathrm{T}_n(\mathbb{R})$ le groupe des matrices triangulaires supérieures inversibles. Montrer que $\mathrm{T}_n(\mathbb{R})$ est le produit semi-direct de $\mathrm{V}_n(\mathbb{R})$ (matrices triangulaires supérieures avec des 1 sur la diagonale) par $\mathrm{D}_n(\mathbb{R})$ (matrices diagonales inversibles).

Remarque. Le groupe $\mathrm{V}_n(\mathbb{R})$ est aussi noté $\mathrm{U}_n(\mathbb{R})$ (voir ANUM).

Démonstration. On utilise la caractérisation du produit semi-direct. On doit vérifier que :

1. $\mathrm{D}_n(\mathbb{R}) < \mathrm{T}_n(\mathbb{R})$, $\mathrm{D}_n(\mathbb{R}) \cap \mathrm{V}_n(\mathbb{R}) = \{\mathrm{id}\}$ (évidents),
2. $\mathrm{D}_n(\mathbb{R})\mathrm{V}_n(\mathbb{R}) = \mathrm{T}_n(\mathbb{R})$,
3. $\mathrm{V}_n(\mathbb{R}) \lhd \mathrm{T}_n(\mathbb{R})$.

Soit $(M_{i,j})_{(i,j)\in[\![1,n]\!]^2} \in \mathrm{T}_n(\mathbb{R})$, alors, par définition de $\mathrm{T}_n(\mathbb{R})$, pour tout $i \in [\![1,n]\!]$, $(M_{i,i})$ est inversible, donc $\mathrm{Diag}(M_{i,i})_{i\in[\![1,n]\!]} \in D_n(\mathbb{R})$ et $(M_{i,i}^{-1}M_{i,j})_{(i,j)\in[\![1,n]\!]^2} \in V_n(\mathbb{R})$, et il vient :

$$\mathrm{Diag}(M_{i,i})_{i\in[\![1,n]\!]}(M_{i,i}^{-1}M_{i,j})_{(i,j)\in[\![1,n]\!]^2} = (M_{i,j})_{(i,j)\in[\![1,n]\!]^2}.$$

On a donc prouvé l'inclusion "$\supset$". L'autre sens est immédiat, ce qui permet de prouver le point 2.

Pour le point 3., on passe par la caractérisation des sous-groupes distingués comme noyaux de morphismes. On considère le morphisme $f : \begin{pmatrix} \mathrm{T}_n(\mathbb{R}) & \longrightarrow & \mathrm{D}_n(\mathbb{R}) \\ A & \longmapsto & \mathrm{Diag}(a_1, \cdots, a_n) \end{pmatrix}$. On peut vérifier que f est un morphisme de groupes et donc $\mathrm{Ker}(f) = \mathrm{V}_n(\mathbb{R}) \lhd \mathrm{T}_n(\mathbb{R})$.

Ainsi, $\mathrm{T}_n(\mathbb{R})$ est le produit semi-direct de $\mathrm{V}_n(\mathbb{R})$ par $\mathrm{D}_n(\mathbb{R})$. □

Exercice 7.3. Montrer que le groupe Q_8 ne s'écrit pas comme un produit semi-direct non trivial.

Démonstration. Par l'absurde, si Q_8 est un produit semi-direct, alors, par la caractérisation du produit semi-direct, il possède deux sous-groupes Q et N tels que $Q \cap N = \{1\}$.

Or : $\forall Q, N < Q_8$, $Q \neq \{1\} \neq N \implies \{1, -1\} \subset Q \cap N$. Ainsi, Q_8 ne peut pas s'écrire comme un produit semi-direct non trivial. □

Exercice 7.4. Soient H et N deux groupes et $\alpha : H \to \mathrm{Aut}(N)$ un morphisme.

1. (**B.A.-BA.**) Si $\varphi \in \mathrm{Aut}(H)$, on pose $\beta := \alpha \circ \varphi : H \to \mathrm{Aut}(N)$. Montrer que les deux groupes $N \rtimes_\alpha H$ et $N \rtimes_\beta H$ sont isomorphes.
2. (**B.A.-BA.**) Si $u \in \mathrm{Aut}(N)$, on définit $\gamma : H \to \mathrm{Aut}(N)$ par $\gamma(h) = u\alpha(h)u^{-1}$. Montrer que les deux groupes $N \rtimes_\alpha H$ et $N \rtimes_\gamma H$ sont isomorphes.
3. Montrer qu'il existe un unique produit semi-direct non trivial de $\mathfrak{S}_3$ par $\mathbb{Z}/2\mathbb{Z}$.

4. Montrer que les deux groupes $\mathfrak{S}_3 \rtimes \mathbb{Z}/2\mathbb{Z}$ et $\mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$ sont isomorphes.

Démonstration.

1. Soit $\psi : \begin{pmatrix} N \rtimes_\alpha H & \longrightarrow & N \rtimes_\beta H \\ (n,h) & \longmapsto & (n, \varphi^{-1}(h)) \end{pmatrix}$. On vérifie que ψ définit bien un morphisme de groupe :

$$\begin{aligned}\psi((n,h) \cdot_\alpha (n',h')) &= \psi((n\alpha(h)(n'), hh')) = (n\alpha(h)(n'), \varphi^{-1}(hh')) \\ &= (n \underbrace{\alpha(\varphi}_{=\beta}(\varphi^{-1}(h))(n'), \varphi^{-1}(h)\varphi^{-1}(h')) = (n, \varphi^{-1}(h)) \cdot_\beta (n', \varphi^{-1}(h')) \\ &= \psi(n,h) \cdot_\beta \psi(n',h')\end{aligned}$$

   Ce morphisme est clairement bijectif puisque φ est un automorphisme, ce qui conclut.

2. Soit $\psi : \begin{pmatrix} N \rtimes_\alpha H & \longrightarrow & N \rtimes_\gamma H \\ (n,h) & \longmapsto & (u(n), h) \end{pmatrix}$. On vérifie que ψ définit bien un morphisme de groupe :

$$\begin{aligned}\psi((n,h) \cdot_\alpha (n',h')) &= \psi((n\alpha(h)(n'), hh')) = (u(n)u(\alpha(h)(n')), hh') \\ &= (u(n)(\underbrace{u\alpha(h)u^{-1}}_{=\gamma(h)})(u(n')), hh') \\ &= (u(n), h) \cdot_\gamma (u(n'), h') \\ &= \psi(n,h) \cdot_\gamma \psi(n',h')\end{aligned}$$

   Ce morphisme est clairement bijectif puisque u est un automorphisme, ce qui conclut.

3. Se donner un produit semi-direct, c'est se donner un morphisme de groupe :

$$\alpha \colon \mathbb{Z}/2\mathbb{Z} \to \mathfrak{S}_3 .$$

   On sait que $\mathrm{Aut}(\mathfrak{S}_3) = \mathrm{Int}(\mathfrak{S}_3) \simeq \mathfrak{S}_3$, l'isomorphisme étant donné par l'action par conjugaison de $\mathfrak{S}_3$ sur lui-même.
   L'ordre de 1 dans $\mathbb{Z}/2\mathbb{Z}$ est 2, donc son image par α est soit l'identité, soit une transposition.
   L'identité donne le produit direct. Comme toutes les transpositions sont conjuguées dans $\mathfrak{S}_3$, par la question précédente, tous les produits semi-directs non-triviaux sont isomorphes.

4. On se donne un produit semi-direct non-trivial $\mathfrak{S}_3 \rtimes_\alpha \mathbb{Z}/2\mathbb{Z}$, avec $\alpha : \begin{pmatrix} \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathrm{Aut}(\mathfrak{S}_3) = \mathrm{Int}(\mathfrak{S}_3) \\ \overline{1} & \longmapsto & \sigma \mapsto \tau\sigma\tau \end{pmatrix}$, avec τ une transposition. Montrons que c'est un produit direct. On utilise pour cela la caractérisation du produit direct. On doit vérifier :
   — $(\mathfrak{S}_3, 0) := \{(\sigma, 0), \sigma \in \mathfrak{S}_3\} < \mathfrak{S}_3 \rtimes_\alpha \mathbb{Z}/2\mathbb{Z}$,
   — $\{(\mathrm{id}, 0), (\tau, 1)\} < \mathfrak{S}_3 \rtimes_\alpha \mathbb{Z}/2\mathbb{Z}$,
   — Pour tout $h \in \{(\mathrm{id}, 0), (\tau, 1)\}$, $(\sigma, 0) \in (\mathfrak{S}_3, 0)$, $h \cdot_\alpha (\sigma, 0) = (\sigma, 0) \cdot_\alpha h$. En effet, on a :

$$(\sigma, 0) \cdot_\alpha (\tau, 1) = (\tau, 1) \cdot_\alpha (\sigma, 0) = (\sigma\tau, 1),$$

   et

$$(\sigma, 0) \cdot_\alpha (\mathrm{id}, 0) = (\mathrm{id}, 0) \cdot_\alpha (\sigma, 0) = (\sigma, 0),$$

   — $(\mathfrak{S}_3, 0) \cap \{(\mathrm{id}, 0), (\tau, 1)\} = \{(\mathrm{id}, 0)\}$,
   — $(\mathfrak{S}_3, 0)\{(\mathrm{id}, 0), (\tau, 1)\} = \mathfrak{S}_3 \rtimes_\alpha \mathbb{Z}/2\mathbb{Z}$.
   Ainsi, on a : $\mathfrak{S}_3 \rtimes_\alpha \mathbb{Z}/2\mathbb{Z} \simeq (\mathfrak{S}_3, 0)) \times \{(\mathrm{id}, 0), (\tau, 1)\} \simeq \mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$.

□

Exercice 7.5 (B.A.-BA.). Soit G un groupe d'ordre mn avec m et n deux entiers premiers entre eux. On suppose de plus que G admet un unique sous-groupe d'ordre m (noté M) et un unique sous-groupe d'ordre n (noté N). Montrer que G est isomorphe au produit direct $M \times N$.

Démonstration. On utilise la caractérisation du produit direct.

— Le sous-groupe $M \cap N$ est non vide car il contient e. Soit $g \in M \cap N$, alors, par le théorème de Lagrange, $o(g) \mid m \wedge n = 1$, et donc $g = e$. Ainsi, $M \cap N = \{e\}$.
— Comme M est l'unique sous-groupe d'ordre m de G, et que pour tout $g \in G$, gMg^{-1} est un sous-groupe d'ordre m, celui-ci est distingué. Il en est de même pour N. Si $n \in N$ et $m \in M$ alors $nmn^{-1}m^{-1} \in M \cap N = \{e\}$ (reconnaître de 2 façons différentes un produit d'un élément et d'une conjugaison), donc $nm = mn$.
— Enfin, comme N et M sont des sous-groupes distingués, MN est un sous-groupe de G, et on a même $M, N < MN < G$. Ainsi, m et n divisent le cardinal de MN, qui divise celui de G, donc $|MN| = |G|$, d'où $MN = G$.

Donc par caractérisation du produit direct, on a $G \simeq M \times N$. □

Remarque. Les deux caractérisations suivantes du produit direct sont équivalentes :

$$\begin{cases} N, M \lhd G \\ N \cap M = \{e\} \\ MN = G \end{cases} \iff \begin{cases} \forall n \in N, \forall m \in M, nm = mn \\ N \cap M = \{e\} \\ MN = G \end{cases}.$$

En effet :

⇒ : Pour $n \in N$ et $m \in M$, on a, par normalité de N et M : $\underbrace{n}_{\in N}\underbrace{mn^{-1}m^{-1}}_{\in N} = \underbrace{nmn^{-1}}_{\in M}\underbrace{m^{-1}}_{\in M} \in N \cap M = \{e\}$, donc on a bien $nm = mn$.

⇐ : Pour $g \in G$, comme $MN = G$, il existe $nm \in NM$ tel que $nm = g$. Alors il vient :

$$gNg^{-1} = nmNm^{-1}n^{-1} = nNn^{-1} = N \text{ et } gMg^{-1} = nmMm^{-1}n^{-1} = nMn^{-1} = M.$$

Dans les deux cas, on utilise l'hypothèse $\forall n \in N, \forall m \in M, nm = mn$ et le fait que M ou N soit un groupe. On a bien prouvé que M et N sont distingués dans G.

Exercice 7.6.

1. (**B.A.-BA.**) Décrire les structures possibles pour les groupes d'ordre $1225 = 5^2 7^2$ *Indication :* montrer que les Sylow sont distingués et utiliser l'exercice 5. Constater que tous les groupes d'ordre 1225 sont abéliens.
2. Peut-on conclure la même chose pour les groupes d'ordre $441 = 3^2 7^2$?

Démonstration.

1. Soit G un groupe d'ordre 1225. D'après le théorème de Sylow, on a $n_5 \mid 7^2$, donc $n_5 \in \{1, 7, 49\}$. De plus $n_5 \equiv 1 \mod 5$, donc $n_5 = 1$. Il y a un unique 5-Sylow. Comme tous les 5-Sylow sont conjugués entre eux, celui-ci est distingué.

   De même, $n_7 = 1$, et l'unique 7-Sylow est distingué.

   Le groupe G possède un unique sous-groupe N d'ordre 49 et un unique sous-groupe Q d'ordre 25, or $49 \wedge 25 = 1$, donc d'après l'exercice 5, G est le produit direct de N et Q.

   En particulier, G est abélien.
2. Soit G un groupe d'ordre 441. D'après le théorème de Sylow, on a $n_7 \mid 3^2$, donc $n_7 \in \{1, 3, 9\}$. De plus $n_7 \equiv 1 \mod 7$, donc $n_7 = 1$. Ainsi, G possède un unique 7-Sylow, qui est distingué.

   Par contre, les conditions du théorème de Sylow donnent $n_3 \mid 49$ et $n_3 \equiv 1 \mod 3$, donc, "au mieux", on a $n_3 \in \{1, 7, 49\}$.

   En particulier, soit $N = \mathbb{Z}/49\mathbb{Z}$, $H = (\mathbb{Z}/3\mathbb{Z})^2$, et

$$\alpha : \begin{pmatrix} (\mathbb{Z}/3\mathbb{Z})^2 & \longrightarrow & \mathrm{Aut}(\mathbb{Z}/49\mathbb{Z}) \\ (1,0) & \longmapsto & x \mapsto x \\ (0,1) & & x \mapsto 18 * x \end{pmatrix}.$$

On a bien un morphisme de groupes car $18^3 \equiv 1 \mod 49$. De plus, $18^2 \equiv 30 \mod 49$, et on peut vérifier que $N \rtimes_\alpha H$ est non abélien :

$$(1,(0,1)) \cdot_\alpha (1,(0,2)) = (1+\alpha(0,1)(1),(0,0)) = (19,(0,0)),$$

$$(1,(0,2)) \cdot_\alpha (1,(0,1)) = (1+\alpha(0,2)(1),(0,0)) = (31,(0,0))$$

Ce n'est donc pas un produit direct.

□

Exercice 7.7. Soit G un groupe et H un sous-groupe de G.

1. Soit P un p-Sylow de H. Montrer qu'il existe P_1 un p-Sylow de G tel que $P = P_1 \cap H$.
2. On suppose que $H \lhd G$, Montrer que si P_1 est un p-Sylow de G, alors $P_1 \cap H$ est un p-Sylow de H.
3. Soit $G = \mathfrak{A}_5$ et $H = \{\sigma \in \mathfrak{A}_5, \sigma(5) = 5\} < G$ (noter que $H \simeq \mathfrak{A}_4$).
   Montrer que si P_1 est un p-Sylow de G alors $P_1 \cap H$ n'est pas nécessairement un p-Sylow de H. On pourra prendre $p = 2$.

Démonstration.

1. Comme P un p-sous-groupe de G, d'après le premier théorème de Sylow, il existe P_1 un p-Sylow de G tel que $P \subset P_1$. Par ailleurs $P_1 \cap H \supset P \cap H = P$. Comme $P_1 \cap H$ est un p-sous-groupe (car sous-groupe de P_1), il vient $P_1 \cap H = P$.
2. Soit P_1 un p-Sylow de G. Alors $P_1 \cap H$ est un p-sous-groupe de H (car sous-groupe de P_1). Il existe donc un p-Sylow P de H tel que $P_1 \cap H \subset P$. Par la question 1), il existe un p-Sylow P_2 de G tel que $P = P_2 \cap H$. Comme tous les p-Sylow de G sont conjugués, il existe $g \in G$ tel que $P_1 = gP_2g^{-1}$. Comme H est distingué, on a $H = gHg^{-1}$ et donc :

   $$P_1 \cap H = gP_2g^{-1} \cap gHg^{-1} = g(P_2 \cap H)g^{-1} = gPg^{-1}.$$

   Comme gPg^{-1} est un p-Sylow de H, on a bien $P_1 \cap H$ p-Sylow de H.
3. On prend $P = \langle (1\ 2)(3\ 5), (1\ 3)(2\ 5) \rangle$ qui est un 2-Sylow de G. Mais $P \cap H = \{\mathrm{id}\}$ n'est pas 2-Sylow de H.

□

8 Feuille 8 : Structure des groupes simples d'ordre < 60

On montre que tout groupe simple d'ordre < 60 est cyclique d'ordre p premier. Ce problème est assez long, sa correction peut occuper une séance complète de TD.

1. Montrer qu'un groupe d'ordre pq (avec p et q deux entiers premiers distincts) n'est pas simple.
2. Même question pour un groupe d'ordre p^2q (attention au cas $p = 2$ et $q = 3$).
3. De même pour un groupe d'ordre p^2q^2 (attention au cas $p = 2$ et $q = 3$).
4. Idem pour un groupe d'ordre pqr (avec $p > q > r$ trois entiers premiers).
5. Montrer que si $|G| \in \{24, 40, 48, 56\}$ alors G n'est pas simple. *Indication :* Pour $|G| \in \{24, 48\}$, on pourra faire agir G sur l'ensemble de ses 2-Sylow.
6. Conclure.

Démonstration.

1. On suppose $p > q$. D'après le théorème de Sylow, le nombre n_p de p-Sylow divise q et est congru à 1 modulo p. En particulier $n_p \leqslant q < p$, et $n_p \equiv 1\,[p]$. Il vient donc $n_p = 1$. Comme les p-Sylow sont conjugués entre eux et qu'il n'y en a qu'un, on en déduit qu'il est distingué, donc que le groupe n'est pas simple.
2. On va traiter deux cas :
   — Si $p > q$, le même raisonnement qu'à la question précédente permet de conclure.
   — Si $q > p$, alors $n_q \mid p^2$, donc $n_q \in \{1, p, p^2\}$. De plus, $n_q \equiv 1\,[q]$.
      — Si $n_q = 1$, on peut conclure comme à la question précédente.
      — Si $n_q = p$ alors comme $q > p$, il vient $p \equiv 1\,[q]$, ce qui est impossible (car p est premier).
      — Si $n_q = p^2$, alors $p^2 \equiv 1\,[q]$, et donc $p \equiv \pm 1\,[q]$.
      On vient de voir que $p \equiv 1\,[q]$ est impossible, donc $p \equiv -1\,[q]$. Comme $p < q$, on a forcément $p = q - 1$.
      Comme q est premier et que $q > p \geqslant 2$, q est impair, donc p est pair. Le seul cas à traiter est donc le cas $p = 2$ et $q = 3$:
      On sait que $n_3|4$ et $n_3 \equiv 1\,[3]$, donc alors $n_3 \in \{1, 4\}$. Si $n_3 = 1$, on peut conclure comme en question 1. Sinon, le groupe contient quatre 3-Sylow et leur union contient 8 éléments d'ordre 3 (et l'identité). Il ne reste alors de la place que pour un unique 2-Sylow, qui est donc distingué.
3. Par symétrie, on peut supposer sans perte de généralité que $q > p$. On reprends un raisonnement similaire à la question précédente.
   On a $n_q \mid p^2$, donc $n_q \in \{1, p, p^2\}$. De plus, $n_q \equiv 1\,[q]$.
   — Si $n_q = 1$, on peut conclure comme en question 1.
   — Si $n_q = p$ alors comme $q > p$, il vient $p \equiv 1\,[q]$, ce qui est impossible (car p est premier).
   — Si $n_q = p^2$, alors $p^2 \equiv 1\,[q]$, et donc $p \equiv \pm 1\,[q]$.
   On vient de voir que $p \equiv 1\,[q]$ est impossible, donc $p \equiv -1\,[q]$. Comme $p < q$, on a forcément $p = q - 1$.
   Comme q est premier et que $q > p \geqslant 2$, q est impair, donc p est pair. Le seul cas à traiter est donc le cas $p = 2$ et $q = 3$:
   On sait que $n_3|4$ et $n_3 \equiv 1\,[3]$, donc alors $n_3 \in \{1, 4\}$. Si $n_3 = 1$, on peut conclure comme en question 1. Sinon, comme tous les 3-Sylow sont conjugués on peut définir une action de G sur l'ensemble de ses 3-Sylow. On a donc un morphisme de groupe $\varphi\colon G \to \mathfrak{S}_4$.
   Or $\#\,\mathfrak{S}_4 = 24 < 36 = \#G$, donc φ ne peut pas être injectif et son noyau est un sous-groupe distingué non trivial.
4. Par théorème de Sylow, $n_p|qr$, donc $n_p \in \{1, q, r, qr\}$. Or, $n_p \equiv 1\,[p]$ et $p > q > r$, donc $n_p \notin \{q, r\}$. Si $1 \in \{n_p, n_q, n_r\}$, on peut conclure comme en question 1. Sinon, on a $n_p = qr$ p-Sylow d'ordre p premier, donc cycliques, et donc deux-à-deux d'intersection triviale (car ici, tout élément d'un p-Sylow différent du neutre est générateur de celui-ci).

Le groupe G contient donc $qr(p-1)$ éléments d'ordre p. De plus, comme $n_r|pq$ et $n_q|pr$, on a $n_r \geqslant q$ et $n_q \geqslant r$, donc G contient au moins $q(r-1)$ éléments d'ordre r et $r(q-1)$ éléments d'ordre q (car là encore, les r- et q-SYLOW sont cycliques).

Ainsi, en comptant le neutre de G, on a :

$$qr(p-1) + q(r-1) + r(q-1) + 1 \leqslant |G| = pqr,$$

soit encore $q + r \geqslant qr + 1$.

Puisque $2 \leqslant r < q$, on a donc $2q + 1 \leqslant rq + 1 \leqslant q + r < 2q$, ce qui est absurde.

5. (a) Pour $\#G = 24$, si $n_2 = 1$, on peut conclure comme en question 1.

   Sinon, comme $n_2|3$, on a $n_2 = 3$. On fait agir G sur l'ensemble de ses 2-SYLOW. On a donc un morphisme $\varphi\colon G \to \mathfrak{S}_3$. Ce morphisme n'est pas injectif car $\#\mathfrak{S}_3 = 6 < 24 = \#G$. Son noyau est donc un sous-groupe distingué de G non trivial.

   (b) Pour $\#G = 40 = 2^3 \times 5$. Alors $n_5|8$ et $n_5 \equiv 1\,[5]$, ce qui mène à $n_5 = 1$.

   (c) On procède comme pour $\#G = 24$. Pour $\#G = 48 = 2^4 \times 3$, si $n_2 = 1$, on peut conclure comme en question 1.

   Sinon, comme $n_2|3$, on a $n_2 = 3$. On fait agir G sur l'ensemble de ses 2-SYLOW. On a donc un morphisme $\varphi\colon G \to \mathfrak{S}_3$. Ce morphisme n'est pas injectif car $\#\mathfrak{S}_3 = 6 < 48 = \#G$. Son noyau est donc un sous-groupe distingué de G non trivial.

   (d) Pour $\#G = 56 = 7 \times 8$, si $n_7 = 1$, on peut conclure comme en question 1.

   Sinon, $n_7|8$ et $n_7 \equiv 1\,[7]$, donc $n_7 = 8$. Les 7-SYLOW sont d'ordre 7 premier, donc cycliques, et donc deux-à-deux d'intersection triviale (car ici, tout élément d'un 7-SYLOW différent du neutre est générateur de celui-ci).

   Le groupe G contient donc $8(7-1) = 48$ éléments d'ordre 7. Il reste donc $56-48 = 8$ autres éléments, soit exactement assez de place pour un unique 2-SYLOW qui est donc distingué.

   Dans tous les cas, G n'est pas simple.

6. Soit G un groupe d'ordre < 60 non banal (c'est à dire pas un groupe cyclique d'ordre premier).

   Si p est premier et $\alpha > 1$, alors un groupe d'ordre p^α n'est pas simple car son centre n'est pas réduit au neutre (et tout sous-groupe du centre est distingué. Pour le prouver, appliquer la formule aux classes pour l'action par conjugaison de G sur lui-même, ou écrivez le à la main !).

   Vu les questions précédentes, on a le tableau suivant :

	·0	·1	·2	·3	·4	·5	·6	·7	·8	·9
0·	×	×	$\in \mathcal{P}$	$\in \mathcal{P}$	p^α	$\in \mathcal{P}$	pq	$\in \mathcal{P}$	p^α	p^α
1·	pq	$\in \mathcal{P}$	p^2q	$\in \mathcal{P}$	pq	pq	p^α	$\in \mathcal{P}$	p^2q	$\in \mathcal{P}$
2·	p^2q	pq	pq	$\in \mathcal{P}$	24	p^α	pq	p^α	p^2q	$\in \mathcal{P}$
3·	pqr	$\in \mathcal{P}$	p^α	pq	pq	pq	p^2q^2	$\in \mathcal{P}$	pq	pq
4·	40	$\in \mathcal{P}$	pqr	$\in \mathcal{P}$	p^2q	p^2q	pq	$\in \mathcal{P}$	48	p^α
5·	p^2q	pq	p^2q	$\in \mathcal{P}$	**54**	pq	56	pq	pq	$\in \mathcal{P}$

   Il reste donc à traiter le cas $\#G = 54$ à traiter. On a $n_3 \mid 2$ et $n_3 \equiv 1\,[3]$, donc $n_3 = 1$, et on peut conclure comme en question 1.

   On a couvert toutes les possibilités, donc un groupe G d'ordre $|G| < 60$ simple est bien cyclique d'ordre p premier.

□

Remarque. Pourquoi 60 ? A cause de $\mathfrak{A}_5$! (seul groupe simple d'ordre 60 à isomorphisme près)

9 Feuille 9 (Supplémentaire)

Un groupe G est dit résoluble s'il existe une suite finie $G_0, \dots, G_n$ de sous-groupes de G telle que

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_{n-1} \subset G_n = G,$$

avec $G_i \lhd G_{i+1}$ et G_{i+1}/G_i abélien. La suite $(G_i)_i$ est alors appelée suite de résolubilité de G.

Quelques propriétés :
- Les groupes abéliens sont résolubles.
- Tout sous-groupe d'un groupe résoluble est résoluble.
- S'il existe un morphisme surjectif d'un groupe résoluble sur G, alors G est résoluble.
- Si H est résoluble et distingué dans G et que G/H est résoluble, alors G est résoluble.
- Un groupe simple est résoluble si et seulement s'il est commutatif : en effet, il est alors d'ordre premier (donc est cyclique).

Attention, les corrections ci-dessous contiennent sans doute des erreurs (correction datée partiellement relue).

Exercice 9.1. Montrer qu'un groupe G d'ordre $|G| < 60$ est nécessairement résoluble (on pourra utiliser les résultats de la feuille 8).

Démonstration. On va procéder par récurrence.

1. Si $|G| = p^\alpha$. On se référera au résultat de l'exercice 2.
2. Dans le cas général, on procédera par récurrence. Un groupe d'ordre 2 est résoluble. On suppose savoir démontrer que tout groupe d'ordre $2 \leqslant k < n$ est résoluble.

   D'après la feuille 8, tout groupe d'ordre < 60 qui n'est pas un p-groupe n'est pas simple. Soit G un groupe d'ordre $n < 60$. Si c'est un p-groupe, alors il est résoluble, sinon il possède un sous-groupe H distingué non trivial. Alors H est d'ordre $< n$ donc est résoluble par hypothèse de récurrence. De même, G/H est d'ordre $< n$ donc est résoluble par hypothèse de récurrence. Finalement on en déduit que G est résoluble.

   Dans tous les cas, G est résoluble.

□

On peut aussi reprendre la structure de la feuille 8 :

Démonstration. On va montrer que si p et q sont deux nombres premiers alors un groupe d'ordre dans l'ensemble $\{p^\alpha, pq, p^2q, p^2q^2pqr\}$ est toujours résoluble. Pour couvrir l'ensemble des groupes de cardinal inférieur à 60, il restera à prouver que les groupes d'ordre $\{24, 36, 40, 48, 54, 56\}$ sont résolubles.

1. Si $|G| = p^\alpha$. On se référera au résultat de l'exercice 2.
2. Si $|G| = pq$. Sans perdre de généralité, on peut supposer que $p > q$, alors soit S un p-Sylow de G. On a vu (feuille 8, mais c'est corollaire du théorème de Sylow) que S est distingué. De plus $G/S \simeq \mathbb{Z}/q\mathbb{Z}$ est cyclique donc abélien, et S est d'ordre p donc abélien. Ainsi $\{e\} \lhd S \lhd G$, donc G est résoluble.
3. Si $|G| = p^2q$.

   Si $p > q$, alors (feuille 8) l'unique p-Sylow S est distingué et G/S est cyclique donc abélien. De plus S est d'ordre p^2 donc abélien. Ainsi $\{e\} \lhd S \lhd G$, donc G est résoluble.

   Si $q > p$ et $p \neq 2, q \neq 3$, alors (feuille 8) il existe un unique q-Sylow qui est distingué. De plus G/S est d'ordre p^2 donc abélien et S est d'ordre q donc cyclique donc abélien. Ainsi $\{e\} \lhd S \lhd G$, donc G est résoluble.

   Si $p = 2, q = 3$, alors on a vu que soit un 2-Sylow S est unique et donc distingué , c'est c'est le cas pour les 3-Sylow. Dans tous les cas, on peut avoir une suite du type $\{e\} \lhd S \lhd G$ donc G est résoluble.

4. Si $|G| = pqr$ alors (feuille 8), G admet au moins un Sylow distingué H qu'on peut supposer être d'ordre p sans perte de généralité. Alors H est résoluble et G/H est résoluble (car d'ordre qr), donc G est résoluble.
5. Si $|G| = 24$, on fait agir G sur l'ensemble de ses 2-Sylow. On sait que $n_2|3$. Supposons que $n_2 = 3$. Cela donne un morphisme $\varphi\colon G \to \mathfrak{S}_3$. Ce morphisme n'est pas injectif car $3! = 6 < 24$. Comme ce morphisme n'est pas l'identité son noyau est un sous-groupe distingué H de G non trivial. En étudiant les cas selon l'image de φ on trouve que $|H| \in \{4, 8, 12\}$. Dans tous les cas H et G/H sont résolubles, donc G est résoluble.
6. Si $|G| = 36$, comme tous les 3-Sylow sont conjugués on peut définir une action de G sur l'ensemble de ses 3-Sylow. On sait que $n_3|4$ et $n_3 \equiv 1 \mod (3)$, alors $n_3 = 1$ ou 4. Supposons que $n_3 = 4$. Cela induit un morphisme de groupe $\varphi\colon G \to \mathfrak{S}_4$. Or $4! = 24$ et $24 < 36$, donc φ ne peut pas être injectif et son noyau H est un sous-groupe distingué non trivial. En examinant l'image de G les différentes possibilités sont $|H| \in \{18, 12, 9, 6, 3\}$. Dans tous les cas H et G/H sont résolubles sont G est résoluble.
7. Si $|G| = 40$, alors (feuille 8) il n'y a qu'un unique 5-Sylow S qui est donc distingué. De plus G/S est de cardinal 8 donc résoluble, et S est résoluble, donc G est résoluble.
8. Si $|G| = 48$, on fait agir G sur l'ensemble de ses 2-Sylow. On sait que $n_2|3$. Supposons que $n_2 = 3$. Cela donne un morphisme $\varphi\colon G \to \mathfrak{S}_3$. Ce morphisme n'est pas injectif car $3! = 6 < 48$. Comme ce morphisme n'est pas l'identité son noyau est un sous-groupe distingué H de G non trivial. En étudiant les cardinaux, les seules possibilités pour H sont $\{8, 16, 24\}$. Ainsi H est résoluble et G/H est résoluble, donc G est résoluble.
9. Si $|G| = 54 = 3^3 \times 2$, alors $\text{ﻉ}_3 = 1$ donc le 3-Sylow S est distingué d'ordre 9 donc résoluble et G/S est d'ordre 2 donc résoluble. Donc G est résoluble.
10. Si $|G| = 56 = 2^3 \times 3$, alors (c.f feuille 8) soit il possède un 2-Sylow S distingué et alors S et G/S sont résolubles, soit il possède un 7-Sylow S' distingué et alors S' et G/S' sont résolubles. Dans tous les cas, G est résoluble.

□

Exercice 9.2. Montrer qu'un p-groupe est résoluble.

Démonstration. Si $|G| = p^\alpha$. On va procéder par récurrence sur α. Le résultat est évident si $\alpha = 1$. Sinon le centre d'un p-groupe n'est pas réduit au neutre, donc $G/Z(G)$ est d'ordre p^β avec $\beta < \alpha$. Par hypothèse de récurrence, $G/Z(G)$ est résoluble et $Z(G)$ est résoluble, donc G est résoluble. □

Exercice 9.3. Montrer que le sous-groupe $B_n(\mathbb{R}) < \mathrm{GL}_n(\mathbb{R})$ formé des matrices triangulaires supérieures (et inversibles) est résoluble. On pourra considérer le sous-groupe $N < B_n(\mathbb{R})$ des matrices avec des 1 sur la diagonale. On vérifiera que $N \lhd B_n(\mathbb{R})$ et que N et $B_n(\mathbb{R})$ sont résolubles.

Démonstration.

1. Montrons que N est distingué et que $B_n(\mathbb{R})/N$ est résoluble. Par le morphisme

$$\begin{array}{rccc} \varphi\colon & B_n(\mathbb{R}) & \to & (\mathbb{R}^\times)^n \\ & (a_{i,j})_{1\leqslant i,j\leqslant n} & \mapsto & (a_{i,i})_{1\leqslant i\leqslant n} \end{array}$$

   On vérifie que φ est un morphisme de groupe, et que son noyau $\mathrm{Ker}(\varphi) = N$. Puisque le morphisme φ est surjectif, on en déduit du premier théorème d'isomorphisme que $B_n(\mathbb{R})/N$ est isomorphe à $(\mathbb{R}^\times)^n$ qui est résoluble car abélien.
2. Montrons que N est résoluble. L'idée est de montrer qu'à chaque fois qu'on calcule un commutateur, on fait "remonter" la diagonale de 0.

   Pour tout entier $m \geqslant 1$ (tant que ça a du sens), on pose

$$N_m = \{A \in N \mid a_{i,j} = 0 \text{ si } \ 0 < j - i < m\}.$$

   On va voir que $D^m(G) < N_m$.

On considère

$$\begin{array}{rccc}\varphi_{m+1}\colon & N_m & \to & N \\ & (a_{i,j}) & \mapsto & (a'_{i,j})\end{array}$$

où $a'_{i,j} = a_{i,j}$ si $j - i = k$ et $a'_{i,j} = 0$ sinon. Alors φ_{m+1} est un morphisme de groupe. En effet soit $A = (a_{i,j})$ et $B = (b_{i,j})$ deux éléments de N_m. On note $AB = (c_{i,j})$. Alors

$$\begin{aligned} c_{i,i+k} &= \sum_{u=0}^{n} a_{i,u}b_{u,i+k} \\ &= \sum_{u=i+1}^{n} a_{i,u}b_{u,i+k} + b_{i,i+k} \\ &= \sum_{u=i+k}^{n} a_{i,u}b_{u,i+k} + b_{i,i+k} \\ &= a_{i,i+k} + b_{i,i+k} \end{aligned}$$

De plus $\mathrm{Ker}(\varphi_{m+1}) = N_{m+1}$. (Se lit facilement sur l'écriture matricielle). On vient donc de construire une suite de groupe $N = N_1 \geqslant N_2 \geqslant \cdots \geqslant N_m \geqslant \cdots$ telle que $N_{m+1} \lhd N_m$, et on vérifie que N_m/N_{m+1} est abélien (c'est isomorphe à l'image de $\varphi_{m+1}(N_m)$ dont le calcul déjà effectué justifie que c'est un groupe abélien).

Or puisque N_m/N_{m+1} est abélien, on en déduit que $D(N_m) < N_{m+1}$. En particulier $D(G) < N_1$, et par récurrence on montre que $D^m(G) < N_m$.

Finalement comme $N_n = \{\mathrm{id}\}$, on a montré que $D^(n)(G) = \{\mathrm{id}\}$, donc N est résoluble.

Comme N et $B_n(\mathbb{R})/N$ sont résolubles alors $B_n(\mathbb{R})$ est résoluble. □

Exercice 9.4. Décrire les suites dérivées des groupes $\mathfrak{A}_4$, $\mathfrak{S}_4$, Q_8 et D_n.

Démonstration. Pour les groupes $\mathfrak{A}_4$, $\mathfrak{S}_4$, Q_8, on a vu dans l'exercice 1 qu'ils sont résolubles, donc on sait que $D(G) \neq G$ pour $G \in \{\mathfrak{A}_4, \mathfrak{S}_4, Q_8\}$. De plus on sait que $D(G)$ est distingué dans G et $D(G) = \{e\}$ si et seulement si G est abélien.

1. Le seul sous-groupe distingué non trivial de $\mathfrak{A}_4$ est V (engendré par les doubles transpositions), puisque $\mathfrak{A}_4$ est résoluble non abélien, alors $D(\mathfrak{A}_4) = V$. Par contre V est abélien, donc la suite dérivée est $\{e\} \lhd V \lhd \mathfrak{A}_4$.
2. On a vu que $\mathfrak{S}_4/V \simeq \mathfrak{S}_3$ n'est pas abélien, donc la suite dérivée de $\mathfrak{S}_4$ est $\{e\} \lhd V \lhd \mathfrak{A}_4 \lhd \mathfrak{S}_4$.
3. Dans Q_8 on remarque que $[i : j] = -1$. En faisant tous les calculs, on constate que $D(Q_8) = \{1, -1\}$.
4. Soient $\alpha, \beta, \alpha', \beta'$ des entiers. On peut supposer $\alpha \geqslant \alpha'$

$$\begin{aligned} [s^\alpha r^\beta : s^{\alpha'} r^{\beta'}] &= s^\alpha r^\beta s^{\alpha'} r^{\beta'} r^{-\beta} s^{-\alpha} r^{-\beta'} s^{-\alpha'} \\ &= s^{\alpha-\alpha'} s^{\alpha'} r^\beta s^{\alpha'} r^{\beta'-\beta} s^{\alpha-\alpha'} s^{\alpha'} r^{-\beta'} s^{\alpha'} \\ &= s^{\alpha-\alpha'} r^{(-1)^{\alpha'}\beta} r^{\beta'-\beta} s^{\alpha-\alpha'} r^{(-1)^{\alpha'+1}\beta'} \\ &= r^{(-1)^{(\alpha-\alpha')}[(-1)^{\alpha'}\beta+\beta'-\beta]} r^{(-1)^{(\alpha'+1)}\beta'} \\ &= r^{[((-1)^\alpha-(-1)^{(\alpha-\alpha')})\beta+((-1)^{(\alpha-\alpha')}-(-1)^{\alpha'})\beta']} \end{aligned}$$

   Puisque $((-1)^\alpha - (-1)^{(\alpha-\alpha')})$ ne peut valoir que $-2, 0, 2$ alors on a $D(D_n) = \langle r^2 \rangle$.
   • Si n est impair alors $D(D_n) = \langle r \rangle$. On a donc $\{e\} \lhd \langle r \rangle \lhd D_n$.
   • Si n est pair, alors$D(D_n) = \langle r^2 \rangle$. On a donc $\{e\} \lhd \langle r^2 \rangle \lhd D_n$.
5. (méthode 2 pour 4) On sait que $D_n/D(D_n)$ est abélien. Alors $r^{-1}s = sr = rs$ dans $D_n/D(D_n)$ (car abélien). Ceci arrive si et seulement si $r = r^{-1}$ dans $D_n/D(D_n)$, soit encore si et seulement si $r^2 \in D(D_n)$. Donc $\langle r^2 \rangle < D(D_n)$.
   • Si n est impair alors $\langle r^2 \rangle = \langle r \rangle$. De plus $D_n/\langle r \rangle$ est de cardinal 2 donc abélien. Donc $D(D_n) < \langle r \rangle$, soit encore l'égalité : $\langle r \rangle = D(D_n)$. On a donc la suite dérivée $\{e\} \lhd \langle r \rangle \lhd D_n$.
   • Si n est pair, alors$D(D_n) = \langle r^2 \rangle$. En effet $D_n/\langle r \rangle$ est de cardinal 4 donc abélien. On a donc la suite dérivée $\{e\} \lhd \langle r^2 \rangle \lhd D_n$.

□

Exercice 9.5. Donner un exemple de groupes G et H non isomorphes mais pour lesquels $D(G) \simeq D(H)$ et $G/D(G) \simeq H/D(H)$.

Démonstration. On considère $G = D_4$ et $H = Q_8$. D'après l'exercice précédent, $D(D_4) = \langle r^2 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$, et $D(Q_8) = \{-1, 1\} \simeq \mathbb{Z}/2\mathbb{Z}$. De plus $D_4/D(D_4)$ est un groupe d'ordre 4 qui contient au moins deux éléments d'ordre 2, à savoir r et s, c'est donc $V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Par ailleurs $Q_8/D(D_4)$ est un groupe d'ordre 4 qui contient aussi au moins deux éléments d'ordre 2, à savoir i et j, c'est donc $V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

Exercice 9.6. On se place dans le groupe $\mathrm{GL}_2(\mathbb{R})$.

1. Montrer que les matrices de la formes
$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}, \quad \text{avec } (\lambda, \mu) \in \mathbb{R}^2$$
engendrent $\mathrm{SL}_2(\mathbb{R})$.
2. Montrer que les matrices $\begin{pmatrix} 1 & 2\lambda \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ sont conjugués **dans** $\mathrm{SL}_2(\mathbb{R})$. On pourra chercher à conjuguer par une matrice diagonale.
3. Déduire des questions précédentes la suite dérivée de $\mathrm{GL}_2(\mathbb{R})$. Ce groupe est-il résoluble ?

Démonstration.

1. $$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a + \lambda b \\ c & d + \lambda c \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} = \begin{pmatrix} a + \mu b & b \\ c + \mu d & d \end{pmatrix}$$
On part d'une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Si $b = 0$, on multiplie par $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ de sorte que leur produit ait le coefficient en haut à droite non nul.
On peut donc supposer sans perdre de généralité que $b \neq 0$. On pose alors $\mu = \dfrac{1-a}{b}$, alors
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \dfrac{1-a}{b} & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ \dfrac{d-1}{b} & d \end{pmatrix}$$
Puis $\lambda = -b$,
$$\begin{pmatrix} 1 & b \\ \dfrac{d-1}{b} & d \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \dfrac{d-1}{b} & 1 \end{pmatrix}$$
Donc les matrices engendrent bien $\mathrm{SL}_2(\mathbb{R})$.
2. Conjuguons par $P = \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix}$, alors
$$P \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} P^{-1} = \begin{pmatrix} 1 & a^2\lambda \\ 0 & 1 \end{pmatrix}$$
Prendre $a = \sqrt{2}$ convient.

3. On remarque que $D(\mathrm{GL}_2(\mathbb{R})) \subset \mathrm{SL}_2(\mathbb{R})$. De plus avec P comme précédemment et $a = \sqrt{2}$, on a
$$P \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} P^{-1} \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$
De même,
$$P \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} P^{-1} \begin{pmatrix} 1 & 0 \\ -\mu & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}$$
Donc $D(\mathrm{GL}_2(\mathbb{R})) = \mathrm{SL}_2(\mathbb{R})$, et de même $D(\mathrm{SL}_2(\mathbb{R})) = \mathrm{SL}_2(\mathbb{R})$. En particulier, $\mathrm{GL}_2(\mathbb{R})$ n'est pas résoluble.

□

Exercice 9.7. On considère le groupe formé des matrices :
$$G := \left\{ \begin{pmatrix} 1 & f(x) & h(x,y) \\ 0 & 1 & g(y) \\ 0 & 0 & 1 \end{pmatrix} \mid f \in \mathbb{R}[x],\, g \in \mathbb{R}[y],\, h \in \mathbb{R}[x,y] \right\}.$$

1. Montrer que G est un groupe.
2. Calculer le commutateur $[\alpha, \beta]$ de deux éléments α, $\beta \in G$ et montrer que
$$D(G) = \left\{ \begin{pmatrix} 1 & 0 & h(x,y) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid h \in \mathbb{R}[x,y] \right\}.$$
3. Montrer cependant que la matrice
$$\begin{pmatrix} 1 & 0 & x^2+xy+y^2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
n'est pas un commutateur.

Démonstration.

1. On a
$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & c+c'+b'a \\ 0 & 1 & b+b' \\ 0 & 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & c+c'+a'b \\ 0 & 1 & b+b' \\ 0 & 0 & 1 \end{pmatrix}$$
Donc G est stable par la loi du groupe et l'inverse
$$\begin{pmatrix} 1 & -a & ba-c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} \in G$$
Donc G est un groupe.
2. $$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & ba-c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a' & b'a'-c' \\ 0 & 1 & -b' \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & a+a' & c+c'+b'a \\ 0 & 1 & b+b' \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a-a' & -c+-c'+b'a+ba+b'a' \\ 0 & 1 & -b-b' \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & b'a-a'b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Donc un commutateur vérifie $f'(x) = 0, g'(y) = 0$ et $h'(x,y) = f(x)v(y) - u(x)g(y)$. En particulier

$$D(G) = \left\{ \begin{pmatrix} 1 & 0 & h(x,y) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid h \in \mathbb{R}[x,y] \right\}.$$

puisque le produit de plusieurs commutateurs vérifie $f'(x) = g'(y) = 0$ et $h'(x,y) = \sum_i u_i(x)v_i(y)$.

3. Si la matrice
$$\begin{pmatrix} 1 & 0 & x^2+xy+y^2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
est un commutateur, alors $x^2 + xy + y^2 = f(x)v(y) - u(x)g(y)$.
Posons $v(y) = \sum v_i y^i$ et $g(y) = \sum g_i y^i$. Alors, en identifiant les coefficients (en voyant ce polynôme en deux variables comme un polynôme en y à coefficients dans $\mathbb{R}(x)$), on obtient
$$\begin{aligned} x^2 &= v_0 f(x) + u(x) g_0 \\ x &= v_1 f(x) + u(x) g_1 \\ 1 &= v_2 f(x) + u(x) g_2 \end{aligned}$$
Donc les polynômes $1, x, x^2$ qui sont linéaires indépendants dans $\mathbb{R}[x]$, sont combinaisons linéaires de seulement deux polynômes. C'est absurde.
Donc ce n'est pas un commutateur.

□

Exercice 9.8. Soit G un groupe dont on suppose que le centre $Z(G)$ est d'indice fini $[G : Z(G)] = n < +\infty$.

1. Considérons $(g_i)_{i=1\dots n}$ une famille de représentants de $G/Z(G)$. Montrer que tout commutateur est de la forme $[g_i, g_j]$ pour certains indices $1 \leqslant i, j \leqslant n$. Il y a donc au plus n^2 commutateurs.
2. Montrer que pour tout $(x,y) \in G^2$: $[x,y]^{n+1} = [x,y^2] \cdot [yxy^{-1}, y]^{n-1}$.
3. Soit $x \in D(G)$ et écrivons x comme un produit de commutateurs $x = c_1 \cdots c_k$. Montrer que si un commutateur c apparaît au moins $n+1$ fois dans le produit, alors $x = c^{n+1} c'_1 \cdots c'_l$ où les c'_i sont des commutateurs. En déduire (avec la question précédente) que $D(G)$ est fini avec la majoration :
$$|D(G)| \leqslant n^{2n^3}.$$

Démonstration.

1. Soit $[x,y] = xyx^{-1}y^{-1}$ un commutateur. Alors il existe $i, j \in \{1, \cdots, n\}$ et $a, b \in Z(G)$ tels que $x = g_i a$ et $y = g_j b$.
$$[x,y] = g_i a g_j b a^{-1} g_i^{-1} b^{-1} g_j^{-1} = g_i g_j g_i^{-1} g_j^{-1} = [g_i, g_j]$$
car $a, b \in Z(G)$. Il y a donc au plus n^2 commutateurs.
2. On constate que
$$a[x,y]a^{-1} = axyx^{-1}y^{-1}a^{-1} = [axa^{-1}, aya^{-1}]$$
En particulier $y[x,y]^k y^{-1} = [yxy^{-1}, y]^k$. Comme $Z(G)$ est distingué dans G et d'ordre n alors $[x,y]^n = e$ dans le quotient. Donc $[x,y]^n \in Z(G)$.
$$\begin{aligned} [x,y]^{n+1} &= xyx^{-1}[x,y]^n y^{-1} \\ &= xyx^{-1}xyx^{-1}y^{-1}[x,y]^{n-1}y^{-1} \\ &= xy^2x^{-1}y^{-2}y[x,y]^{n-1}y^{-1} \\ &= [x,y^2][yxy^{-1},y]^{n-1} \end{aligned}$$

3. On suppose que c apparaît dans l'écriture de x. Montrons que l'on peut faire "avancer" c dans cette écriture. Or $c_1 c = cc^{-1}c_1 c = cc_1'$ où $c_1' = c^{-1}c_1 c$ est un commutateur. Donc on peut faire avancer n'importe quel c de sorte que x puisse s'écrire sous la forme $x = c^{n+1}c_1' \cdots c_l'$ où les c_i' sont des commutateurs.
   Mais c^{n+1} peut s'écrire comme produit de n commutateurs, et il y a au plus n^2 commutateurs possibles. Donc x est produit d'au plus n^3 commutateurs et il y a au plus n^2 commutateurs. Donc $|D(G)| \leqslant (n^2)^{n^3}$.

□

Exercice 9.9. Dans $\mathrm{GL}_2(\mathbb{R})$, on considère le sous-groupe

$$G := \left\langle x = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle.$$

1. Montrer que G est résoluble (on pourra utiliser l'exercice précédent).
2. Montrer que $xyx^{-1} = y^2$ et en déduire que le sous-groupe engendré par tous les conjugués de y est abélien. On note $\langle\langle y \rangle\rangle$ ce sous-groupe.
3. Le groupe $\langle\langle y \rangle\rangle$ est-il de type fini ?

Démonstration.

1. G est un sous-groupe d'un groupe résoluble (cf exercice précédent) donc est résoluble.
2. On a
$$xy = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}$$
$$y^2 x = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}$$
   Donc $xyx^{-1} = y^2$.
   Le groupe engendré par les commutateurs de y est engendré par$y$, xyx^{-1} et $x^{-1}yx$. Pour montrer que le groupe engendré par les conjugués de y est abélien, il suffit de vérifier que y commute avec xyx^{-1} et $x^{-1}yx$ et que xyx^{-1} et $x^{-1}yx$ commutent entre eux.
$$y \cdot xyx^{-1} = y^3 = xyx^{-1} \cdot y$$
$$y \cdot x^{-1}yx = x^{-1}xyx^{-1}yx = x^{-1}y^2yx = x^{-1}yxx^{-1}y^2x = x^{-1}yx \cdot y$$
$$xyx^{-1} \cdot x^{-1}yx = y^2 \cdot x^{-1}yx = x^{-1}yx \cdot y^2 = x^{-1}yx \cdot xyx^{-1}$$
   Donc $\langle\langle y \rangle\rangle$ est abélien.
3. On remarque que
$$x^{-1}yx = \begin{pmatrix} 2 & 1 \\ 0 & \dfrac{1}{2} \end{pmatrix}$$
   Soit encore
$$x^{-n}yx^n = \begin{pmatrix} 2^n & 1 \\ 0 & \dfrac{1}{2^n} \end{pmatrix}$$
   Comme $x^{-n}yx^n$ n'est pas engendré par $x^{-k}yx^k$, pour $k < n$, alors $\langle\langle y \rangle\rangle$ n'est pas de type fini.

□