Correction & Exercices Supplémentaires TD THéorie des GRoupes

Antoine Dequay, TD de Christophe Dupont

9 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 $z \in \mathbb{H}$:

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

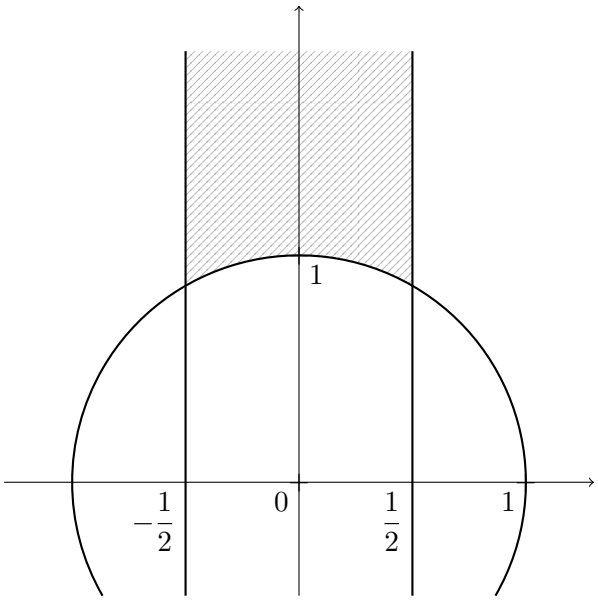
On trouve le système : $\begin{cases} a = d \\ b = c = 0 \end{cases}$, donc le noyau de l'action est $\mathbb{Z} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

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

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 $z \in \mathbb{H}$:

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

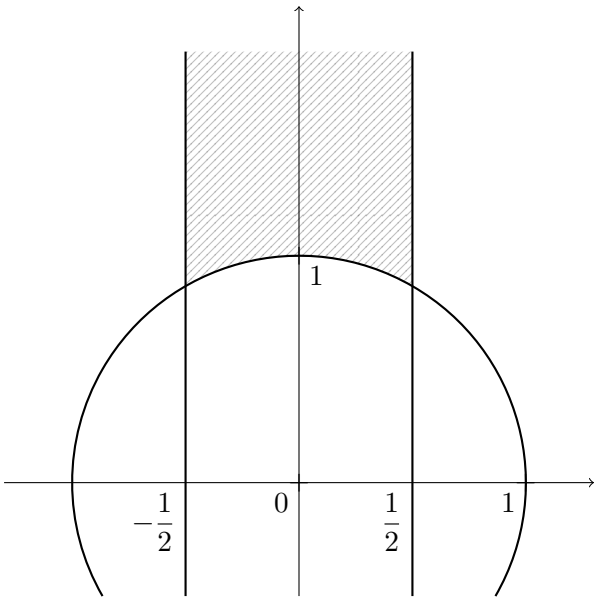
On trouve le système : $\begin{cases} a = d \\ b = c = 0 \end{cases}$, donc le noyau de l'action est $\mathbb{Z}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

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

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) $\mathrm{pgcd}(a_1, \dots, a_n) = 1$.

0.4 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).

Exercice 0.21. Montrer qu'un groupe G d'ordre $|G| < 60$ est nécessairement résoluble (on pourra utiliser les résultats de la feuille 8).

Exercice 0.22. Montrer qu'un p-groupe est résoluble.

Exercice 0.23. 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.

Exercice 0.24. Décrire les suites dérivées des groupes $\mathfrak{A}_4$, $\mathfrak{S}_4$, Q_8 et D_n.

Exercice 0.25. Donner un exemple de groupes G et H non isomorphes mais pour lesquels $D(G) \simeq D(H)$ et $G/D(G) \simeq H/D(H)$.

Exercice 0.26. 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 ?

Exercice 0.27. 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.

Exercice 0.28. 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 :
$$|D(G)| \leqslant n^{2n^3}.$$

Exercice 0.29. 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 ?