UVSQ 2025/2026
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)

Feuille d'exercices numéro 1

1 Petites questions en vrac, pour soi

1.1) Trouver les générateurs de $(\mathbb{Z}/18\mathbb{Z}, +)$ et du groupe des racines 12^{e} de l'unité.

1.2) Donner trois générateurs différents du groupe des racines 2025^{e} complexes de l'unité.

1.3) Combien y a-t-il d'éléments d'ordre 2 dans un groupe cyclique d'ordre n ?

1.4) Trouver tous les sous-groupes de $\mathbb{Z}/20\mathbb{Z}$.

1.5) Compter les homomorphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z}$ et les expliciter.
Se faire la main sur les exemples $\mathbb{Z}/21\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/18\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$.

1.6) Est-il vrai que $\mathbb{U}_m \cap \mathbb{U}_n = \mathbb{U}_{m\wedge n}$? Est-il vrai que le sous-groupe de $\mathbb{C}^\times$ engendré par $\mathbb{U}_m \cup \mathbb{U}_n$ est $\mathbb{U}_{m\vee n}$? Interpréter les résultats obtenus dans le cadre de $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$.

1.7) Trouver tous les homomorphismes de groupes $\mathbb{Q} \to \mathbb{Q}$, $\mathbb{Q} \to \mathbb{Z}$ et $\mathbb{Q} \to \mathbb{Q}^\times$.

1.8) Montrer que le groupe additif quotient $\mathbb{Q}/\mathbb{Z}$ est isomorphe au groupe multiplicatif $\mathbb{U}$ de toutes les racines complexes de l'unité.

1.9) Peut-on trouver un groupe fini d'ordre 168 contenant un sous-groupe d'indice 14 ?

1.10) Quel est l'ordre de $C = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ dans le groupe $\mathrm{GL}(4, \mathbb{C})$?

2 Quelques gammes dans le désordre

2.1) xy et yx sont conjugués

Si G est n'importe quel groupe et si $x, y \in G$, alors xy et yx sont conjugués.

Application : si A et B sont deux matrices carrées inversibles, alors AB et BA sont semblables. Que se passe-t-il si on enlève l'hypothèse d'inversibilité ?

2.2) Transport de l'ordre

Soit $f : G \to G'$ un homomorphisme de groupes. Montrer que si l'ordre de $x \in G$ est fini, alors, l'ordre de $f(x)$ est fini et divise l'ordre de x.

2.3) Sous-groupes et quotients d'un groupe monogène

Tout sous-groupe d'un groupe monogène est monogène. Tout quotient d'un groupe monogène est monogène.

2.4) Ordre d'un produit de deux éléments qui commutent

Soient G un groupe, x et y deux éléments de G qui commutent.

(i) Montrer que si les ordres de x et de y sont premiers entre eux, alors l'ordre de xy est fini, égal au produit des ordres de x et de y.

(ii) On suppose que $\langle x \rangle \cap \langle y \rangle = \{1\}$. Alors, l'ordre de xy est fini, égal au PPCM des ordres de x et de y.

2.5) Transport de système générateur

Soient $f : G \to G'$ un homomorphisme de groupes, et A une partie de G. Est-il vrai que

$$f\left(\langle A \rangle\right) = \langle f(A) \rangle \ ?$$

2.6) Tester la normalité sur un système générateur

(i) Soit G un groupe engendré par une partie A. On suppose que H est un sous-groupe de G tel que $\forall a \in A$, $aHa^{-1} = H$. Le sous-groupe H est-il nécessairement distingué dans G ?

(ii) Soit G un groupe engendré par une partie A. On suppose que H est un sous-groupe de G tel que $\forall a \in A$, $aHa^{-1} \subseteq H$. Le sous-groupe H est-il nécessairement[♫] distingué dans G ?

(iii) Soit G un groupe engendré par une partie A formée d'éléments d'ordres finis. On suppose que H est un sous-groupe de G tel que $\forall a \in A$, $aHa^{-1} \subseteq H$. Le sous-groupe H est-il nécessairement distingué dans G ?

2.7) Combien de générateurs ?

Soit G un groupe fini d'ordre n. Montrer que G a un système générateur de cardinal inférieur ou égal à $\log_2 n$.

2.8) Groupe d'ordre pair ou impair

(i) Montrer qu'un groupe fini d'ordre pair contient toujours un élément d'ordre 2 (on pourra montrer qu'il y a un nombre pair d'éléments dont le carré n'est pas 1).

(ii) Montrer si G est un groupe fini d'ordre impair, tout élément a une racine carrée : $\forall x \in G$, $\exists y \in G$, $x = y^2$.

2.9) Coprimalité de l'ordre et de l'indice

Soient G un groupe et H un sous-groupe distingué de G, d'indice fini.

(i) Soit K un sous-groupe fini de G dont l'ordre est premier avec $[G : H]$. Montrer que $K \subseteq H$.

(ii) Si G et H sont finis et si $|H|$ et $[G : H]$ sont étrangers, alors H est l'unique sous-groupe d'ordre $|H|$ de G.

2.10) Ordre dans un produit

Soient G et H deux groupes, et $(x, y) \in G \times H$. On suppose que x et y sont d'ordres finis m et n respectivement. Montrer que, dans le groupe produit $G \times H$, l'élément (x, y) est d'ordre fini, égal à $\mathrm{PPCM}(m, n)$.

2.11) Produit d'indices

Soient G un groupe, H et K deux sous-groupes de G tels que $H \subseteq K$.

(i) Montrer que $[G : H] = [G : K] \times [K : H]$.

(ii) En déduire que si $[G : H] = [G : K]$ et si cet indice est fini, alors $H = K$.

(iii) Trouver un exemple pour lequel $[G : H] = [G : K]$ et $H \neq K$.

2.12) Groupe opposé

Soit G un groupe. On définit sur G la *loi opposée* par la formule $x \star y = yx$, le dernier produit désignant la loi de G. Montrer que $(G, \star)$ est un groupe, que l'on note G^{op}. Montrer que les groupes G et G^{op} sont isomorphes.

3 Produit de deux sous-groupes

Soient G un groupe, H et K deux sous-groupes de G. On note

$$HK = \{hk,\ h \in H,\ k \in K\}.$$

3.1) Montrer qu'en général, HK n'est pas un sous-groupe de G.

3.2) On suppose que $H \cap K = \{1\}$. Montrer que $\mathrm{Card}\,(HK) = |H| \cdot |K|$.

3.3) Montrer que si $H \triangleleft G$, alors HK est un sous-groupe de G.

3.4) Etudier la réciproque de l'implication du 3.3.

[♫] Voir l'exercice 54.

4 Décimaux modulo les entiers

Vérifier que l'ensemble $\mathbb{D}$ des nombres décimaux est un sous-groupe additif de $\mathbb{R}$. On note

$$S_{10} = \{z \in \mathbb{C},\ \exists n \in \mathbb{N},\ z^{10^n} = 1\}.$$

Montrer que S_{10} est un sous-groupe du groupe multiplicatif $\mathbb{C} \setminus \{0\}$. Les groupes $\mathbb{D}/\mathbb{Z}$ et S_{10} sont-ils isomorphes ? Pour aller plus loin, par quoi peut-on remplacer le groupe des décimaux pour obtenir des énoncés analogues ?

5 Groupes 2-élémentaires

Soit G un groupe dont tous les éléments sont d'ordre 1 ou 2.

5.1) Montrer que G est abélien.

5.2) On note G additivement. On note $\cdot$ la loi de composition externe sur G définie par

$$\begin{array}{ccccc} \mathbb{Z}/2\mathbb{Z} \times G & \longrightarrow & G & & \\ (\varepsilon, g) & \longmapsto & \varepsilon \cdot g & = & \left\{ \begin{array}{ll} 0 & \text{si } \varepsilon = 0 \\ g & \text{si } \varepsilon = 1. \end{array} \right. \end{array}$$

Montrer cette loi de composition externe est bien définie et confère à G une structure de $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel.

5.3) On suppose que G est fini. Montrer qu'il existe $n \in \mathbb{N}$ tel que G soit isomorphe au groupe $(\mathbb{Z}/2\mathbb{Z})^n$.

5.4) Montrer que l'ensemble des parties d'un ensemble, muni de la différence symétrique, est un groupe abélien. Si l'ensemble a un nombre fini n d'éléments, montrer que ce groupe est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$.

6 Sous-groupes d'un groupe à engendrement fini

On dit qu'un groupe est *à engendrement fini* lorsqu'il admet un système générateur fini. Autrement dit, un groupe Γ est à engendrement fini lorsqu'il existe une partie finie de Γ qui engendre Γ.

L'objet de cet exercice est de montrer qu'un sous-groupe d'un groupe à engendrement fini n'est pas nécessairement à engendrement fini.

6.1) Soit G le sous-ensemble de $\mathrm{GL}(2, \mathbb{R})$ défini par

$$G = \left\{ \begin{pmatrix} 2^n & \frac{p}{2^q} \\ 0 & 1 \end{pmatrix},\ (n, p, q) \in \mathbb{Z}^3 \right\}.$$

Montrer que G est un sous-groupe de $\mathrm{GL}(2, \mathbb{R})$.

6.2) Si m et p sont des entiers relatifs, calculer

$$\begin{pmatrix} 2^m & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2^m & 0 \\ 0 & 1 \end{pmatrix}.$$

Montrer soigneusement que le groupe G est engendré par les deux matrices $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

6.3) On note

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{ \frac{p}{2^q},\ (p, q) \in \mathbb{Z}^2 \right\}.$$

Montrer que $\mathbb{Z}\left[\frac{1}{2}\right]$ est un sous-groupe additif de $\mathbb{R}$ qui n'est pas à engendrement fini.

6.4) Soit H le sous-ensemble de G défini par

$$H = \left\{ \begin{pmatrix} 1 & \frac{p}{2^q} \\ 0 & 1 \end{pmatrix},\ (p, q) \in \mathbb{Z}^2 \right\}.$$

Démontrer que H est un sous-groupe de G isomorphe à $\mathbb{Z}\left[\frac{1}{2}\right]$. En déduire que H n'est pas à engendrement fini.

7 Groupes cycliques

Soit n un entier naturel non nul. Faire les preuves des résultats du cours suivants.

7.1) Si $k \in \mathbb{Z}$, alors la classe de k modulo n engendre $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si k et n sont premiers entre eux.

7.2) Si $G = \langle g \rangle$ est un groupe cyclique d'ordre n et si $k \in \mathbb{Z}$, alors $G = \langle g^k \rangle$ si, et seulement si k et n sont premiers entre eux.

7.3) Si $k \in \mathbb{Z}$, le nombre complexe $e^{\frac{2ik\pi}{n}}$ est une racine primitive n^{e} de l'unité si, et seulement si k et n sont premiers entre eux.

7.4) Si $k \in \mathbb{Z}$, alors la classe de k modulo n engendre un sous-groupe d'ordre $\frac{n}{\text{PGCD}(n,k)}$ de $\mathbb{Z}/n\mathbb{Z}$.

7.5) Ecrire la version du résultat précédent pour le groupe des racines n^{e} complexes de l'unité et pour un groupe cyclique d'ordre n abstrait.

7.6) Calculer le nombre de sous-groupes d'un groupe cyclique d'ordre n ; les décrire tous. Calculer le nombre de quotients d'un groupe cyclique d'ordre n ; les décrire tous.

7.7) On note φ la fonction d'Euler. Se rappeler pourquoi $\varphi(mn) = \varphi(m)\varphi(n)$ lorsque m et n sont étrangers et pourquoi $\varphi(p^n) = p^{n-1}(p-1)$ lorsque p est premier et $n \geq 0$. Montrer que pour tout entier naturel non nul n,

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) \tag{1}$$

où le produit porte sur les nombres premiers qui divisent n.

7.8) En utilisant la formule (1), montrer que $m|n \Longrightarrow \varphi(m)|\varphi(n)$.

7.9) En utilisant la formule (1), montrer que si m et n sont des entiers naturels non nul et si d est leur PGCD, alors

$$\varphi(mn)\varphi(d) = \varphi(m)\varphi(n)d.$$

8 Matrices triangulaires unipotentes

8.1) Montrer que l'ensemble

$$\mathcal{U} = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix},\ (a,b,c) \in \mathbb{R}^3 \right\}$$

est un sous-groupe de $\text{SL}(3,\mathbb{R})$ et calculer son centre Z.

8.2) Le groupe Z est-il isomorphe au groupe additif $\mathbb{R}$?

8.3) Montrer que l'application

$$\begin{array}{rccc} f: & \mathcal{U} & \longrightarrow & \mathbb{R}^2 \\ & \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} & \longmapsto & (a,c) \end{array}$$

est un homomorphisme de groupes. En déduire que $\mathcal{U}/Z$ est isomorphe au groupe additif $\mathbb{R}^2$. Le groupe $\mathcal{U}$ est-il isomorphe au groupe additif $\mathbb{R} \times \mathbb{R}^2$?

8.4) Pour tout nombre réel t, on note

$$U(t) = \begin{pmatrix} 1 & t & \frac{t^2}{2} \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix}.$$

Soit $\mathcal{N} = \{U(t),\ t \in \mathbb{R}\}$. Montrer que $\mathcal{N}$ est un sous-groupe de $\mathcal{U}$. Est-il monogène ?

9 Groupes d'exposant fini

9.1 Prélude

(i) Montrer que si $z \in \mathbb{C}$ vérifie $|1+z| = 1+|z|$, alors $z \in \mathbb{R}_+$. En déduire que si a et b sont des nombres complexes non nuls,

$$\Big(|a+b| = |a| + |b|\Big) \Longrightarrow \Big(\frac{a}{b} \in \mathbb{R}_+^*\Big).$$

(ii) Soient $z_1, \ldots, z_n$ des nombres complexes non nuls. Montrer que si $|z_1 + \cdots + z_n| = |z_1| + \cdots + |z_n|$, alors les nombres $\frac{z_k}{z_1}$ sont tous des réels strictement positifs (on pourra procéder par récurrence sur n).

(iii) Soient n et m des entiers naturels non nuls et soient $\omega_1, \ldots, \omega_n$ des racines $m^{\text{ièmes}}$ de l'unité. Montrer que

$$\left(\sum_{k=1}^{n} \omega_k = n\right) \Longrightarrow \Big(\forall k \in \{1, \ldots, n\},\ \omega_k = 1\Big).$$

9.2 Un groupe infini d'exposant fini

Soient m un entier naturel supérieur ou égal à 2 et $\mathbb{U}_m$ le groupe des racines $m^{\text{ièmes}}$ complexes de l'unité. On note $\mathcal{F}$ l'ensemble des applications $\mathbb{R} \longrightarrow \mathbb{U}_m$. On munit $\mathcal{F}$ de la loi de composition interne définie par $(f \cdot g)(x) = f(x)g(x)$ pour tous f et g dans $\mathcal{F}$ et pour tout $x \in \mathbb{R}$. Cela munit $\mathcal{F}$ d'une loi de groupe — c'est élémentaire.

(i) On note δ_1 la fonction constante égale à 1. Montrer que δ_1 est l'élément neutre de $\mathcal{F}$; si $f \in \mathcal{F}$, calculer l'inverse de f dans $\mathcal{F}$.

(ii) Montrer que $\forall f \in \mathcal{F},\ f^m = \delta_1$ et que $\mathcal{F}$ est infini.

9.3 Tout groupe *linéaire* d'exposant fini est fini

Soient n et m des entiers naturels non nul et G un sous-groupe de $\mathrm{GL}(n, \mathbb{C})$. On note I_n la matrice identité de dimension n. On suppose que

$$\forall A \in G,\ A^m = I_n.$$

(i) Montrer que pour tout A dans G, les valeurs propres de A sont des racines $m^{\text{ièmes}}$ de l'unité.

(ii) On note $\mathcal{M}_n(\mathbb{C})$ l'espace vectoriel de toutes les matrices carrées de taille n à coefficients complexes. Soit $\mathcal{T}$ l'ensemble des traces des éléments de G ; autrement dit,

$$\mathcal{T} = \{\mathrm{Tr}(A),\ A \in G\}.$$

Démontrer que $\mathcal{T}$ est un ensemble fini.

(iii) Soit E le sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$ engendré par G.
Dire rapidement pourquoi E est de dimension finie.
Soient d la dimension de E et $(E_1, \ldots, E_d)$ une base de E formée d'éléments de G (pourquoi en existe-t-il ?). Soit $t : G \longrightarrow \mathcal{T}^d$ l'application définie par

$$\begin{array}{rcl} t : G & \longrightarrow & \mathcal{T}^d \\ A & \longmapsto & \Big(\mathrm{Tr}(AE_1), \ldots, \mathrm{Tr}(AE_d)\Big). \end{array}$$

Montrer que si deux éléments A et B de G vérifient $t(A) = t(B)$, alors $\mathrm{Tr}(AC) = \mathrm{Tr}(BC)$ pour tout C dans G et en déduire que $\mathrm{Tr}\left(AB^{-1}\right) = n$. Montrer que t est injective (on pourra utiliser le prélude 9.1).

(iv) Montrer que G est fini.

10 Sous-groupes de type fini de $\mathbb{Q}$ ou $\mathbb{R}$

10.1) Montrer que $\frac{1}{2}\mathbb{Z} + \frac{3}{5}\mathbb{Z} = \frac{1}{10}\mathbb{Z}$.

10.2) Est-il vrai que si a, b, c et d sont des entiers relatifs non nuls, alors

$$\frac{a}{b}\mathbb{Z} + \frac{c}{d}\mathbb{Z} = \frac{\mathrm{PGCD}\,(ad, bc)}{bd}\mathbb{Z} \ ?$$

10.3) Montrer que si u, v et w sont des nombres rationnels, le sous-groupe de $\mathbb{Q}$ engendré par u, v et w est monogène.

10.4) Montrer que tout sous-groupe de type fini de $\mathbb{Q}$ est monogène.

10.5) Le groupe additif $(\mathbb{Q}, +)$ est-il de type fini ?

10.6) Le groupe additif $(\mathbb{R}, +)$ contient-il un sous-groupe dense de type fini ?

10.7) Le groupe additif $(\mathbb{R}, +)$ est-il de type fini ?

11 Dévissages autour de $\mathrm{GL}\,(n)$

11.1) Montrer que l'application

$$\begin{array}{rccc} f: & \mathbb{C}^* \times \mathrm{SL}\,(n, \mathbb{C}) & \longrightarrow & \mathrm{GL}\,(n, \mathbb{C}) \\ & (z, A) & \longmapsto & zA \end{array}$$

est un homomorphisme de groupes.

11.2) Calculer l'image de f.

11.3) Montrer que le noyau de f est isomorphe au groupe $\mathbb{U}_n$ des racines $n^{\text{ièmes}}$ complexes de l'unité.

11.4) Montrer que $\mathbb{C}^* \times \mathrm{SL}(n, \mathbb{C})$ contient un sous-groupe distingué H isomorphe à $\mathbb{U}_n$ tel que $\mathrm{GL}(n, \mathbb{C})$ soit isomorphe au groupe quotient $\mathbb{C}^* \times \mathrm{SL}(n, \mathbb{C})/H$. Autrement dit, montrer qu'on a une suite exacte

$$1 \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{C}^* \times \mathrm{SL}\,(n, \mathbb{C}) \xrightarrow{f} \mathrm{GL}\,(n, \mathbb{C}) \longrightarrow 1.$$

11.5) Montrer que le résultat subsiste si on remplace $\mathbb{C}$ par n'importe quel corps algébriquement clos.

11.6) Montrer que $\mathrm{GL}^+(2, \mathbb{R}) = \{A \in \mathrm{GL}(2, \mathbb{R}),\ \det(A) > 0\}$ est un sous-groupe distingué de $\mathrm{GL}(2, \mathbb{R})$, et que le quotient $\mathrm{GL}(2, \mathbb{R})/\,\mathrm{GL}^+(2, \mathbb{R})$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

11.7) Montrer que l'application $f : \mathrm{GL}^+(2, \mathbb{R}) \to \mathrm{SL}(2, \mathbb{R}) \times \mathbb{R}_+^*$ définie par

$$f(A) = \left(\frac{A}{\sqrt{\det A}}, \det A\right)$$

est un homomorphisme de groupes. Est-ce un isomorphisme ? Pour aller plus loin, établir le même résultat pour tous les $\mathrm{GL}^+(n, \mathbb{R}) = \{A \in \mathrm{GL}(n, \mathbb{R}),\ \det(A) > 0\}$.

12 Intersection de sous-groupes d'indices finis

Soient G un groupe, H et K deux sous-groupes de G.

12.1) On suppose que H est d'indice fini dans G. Montrer que $H \cap K$ est un sous-groupe d'indice fini de K et que

$$[K : H \cap K] \leq [G : H]\,. \tag{2}$$

12.2) Dans les conditions de la question précédente, montrer que les assertions suivantes sont équivalentes :
(i) l'inégalité (2) est une égalité
(ii) $G = KH$
(iii) $G = HK$.

12.3) Montrer qu'une intersection finie de sous-groupes d'indices finis de G est encore un sous-groupe d'indice fini.

12.4) On suppose que les indices de H et de K dans G sont finis et premiers entre eux. Montrer que $G = HK = KH$.

UVSQ 2024/2025
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)

Feuille d'exercices numéro 2

13 Petites questions en vrac, pour soi

13.1) Calculer le support de la permutation de $\mathfrak{S}_{15}$ définie par le produit

$$(5,12,7,8,9)(10,11,12,1)(7,2)(3,5,8,2,13,4)(15,5)(3,11).$$

13.2) Soit $s = (7,11,8,9)(2,1,7,12)(9,2,10,3,7,5,6)(10,8) \in \mathfrak{S}_{12}$. Calculer l'orbite de 11 sous l'action de s.

13.3) Décomposer les permutations suivantes en produit de cycles à supports disjoints.

(i) $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 1 & 7 & 4 & 12 & 2 & 5 & 14 & 11 & 9 & 10 & 8 & 3 & 6 & 13 \end{bmatrix}$

(ii) $(7,11,8,9)(2,1,7,12)(9,2,10,3,7,5,6)(10,8)$

13.4) Les permutations $(135)(189)(53842)(67)$ et $(173)(394)(61542)(83)$ sont-elles conjuguées ?

13.5) Soient n et p des entiers naturels tels que $1 \leq p \leq n$. Quel est le cardinal de la classe de conjugaison d'un p-cycle de $\mathfrak{S}_n$?

13.6) Trouver tous les sous-groupes d'ordre 15, 20 ou 30 de $\mathfrak{A}_5$.

13.7) Expliciter les 4 éléments du groupe cyclique $\mathrm{Aut}\,(\mathbb{Z}/5\mathbb{Z})$. Calculer les facteurs invariants du groupe abélien fini $\mathrm{Aut}\,(\mathbb{Z}/200\mathbb{Z})$.

13.8) Les groupes $\mathbb{Z}/686\mathbb{Z} \times \mathbb{Z}/1372\mathbb{Z}$ et $\mathbb{Z}/98\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z} \times \mathbb{Z}/343\mathbb{Z}$ sont-ils isomorphes ?

13.9) Les groupes $\mathrm{O}(2)$ et $\mathrm{SO}(2) \times \mathbb{Z}/2\mathbb{Z}$ sont-ils isomorphes ? Les groupes $\mathrm{O}(3)$ et $\mathrm{SO}(3) \times \mathbb{Z}/2\mathbb{Z}$ sont-ils isomorphes ? Généraliser.

La suite exacte $1 \to \mathrm{SO} \to \mathrm{O} \to \mathbb{Z}/2\mathbb{Z} \to 1$ induite par le déterminant est scindée en toute dimension, puisque O contient des réflexions qui sont d'ordre 2. En dimension impaire, $-I_n$ est impaire et fournit une section centrale : le produit est direct. En dimension paire supérieure ou égale à 4, non, le centre de $\mathrm{O}(2n)$ est d'ordre 2, celui de $\mathrm{SO}(2n) \times \mathbb{Z}/2\mathbb{Z}$ d'ordre 4. En dimension 2, $\mathrm{SO}(2) \times \mathbb{Z}/2\mathbb{Z}$ est abélien, mais pas $\mathrm{O}(2)$.

14 Quelques gammes dans le désordre

14.1) Toujours produit ?

Est-il vrai que si H est un sous-groupe distingué d'un groupe G, les groupes G et $H \times G/H$ sont toujours isomorphes ?

14.2) Deux générateurs de $\mathfrak{A}_5$

Soit G le sous-groupe de $\mathfrak{S}_5$ engendré par les 3-cycles (123) et (345).

(i) Montrer que $G \subseteq \mathfrak{A}_5$.

(ii) Ecrire (123)(345) en produit de cycles à supports disjoints et montrer que $(234) \in G$.

(iii) Calculer le nombre de 3-cycles de $\mathfrak{S}_5$. Démontrer que G contient tous les 3-cycles de $\mathfrak{S}_5$ (on pourra si l'on veut utiliser plusieurs fois la formule de conjugaison des cycles, méthodiquement mais avec économie).

(iv) Montrer que $G = \mathfrak{A}_5$.

14.3) $\mathfrak{A}_n$ est engendré par les 5-cycles

Soit n un entier naturel supérieur ou égal à 5. Montrer que le sous-groupe H de $\mathfrak{S}_n$ engendré par les 5-cycles est distingué dans $\mathfrak{S}_n$. En déduire que H égale le groupe alterné $\mathfrak{A}_n$.

15 Ce qu'engendrent une transposition et un 4-cycle

15.1) Soit A le sous-groupe de $\mathfrak{S}_4$ engendré par la transposition (12) et le 4-cycle (1234). Montrer que A contient les transpositions (23) et (34). En déduire que $A = \mathfrak{S}_4$.

15.2) Soit B le sous-groupe de $\mathfrak{S}_4$ engendré par la transposition (12) et le 4-cycle (1324).

(i) Calculer la décomposition du produit (12)(1324) en produit de cycles à supports disjoints.

(ii) On note $K = \{1, (12)(34), (13)(24), (14)(23)\}$ le groupe de Klein. Montrer que K est un sous-groupe distingué de B.

(iii) Montrer que les classes de (12) et de (1324) dans le groupe-quotient B/K sont inverses l'une de l'autre.

(iv) En déduire que B est d'ordre 8.

15.3) Soit C le sous-groupe de $\mathfrak{S}_5$ engendré par la transposition (12) et le 4-cycle (2345). Montrer que $C = \mathfrak{S}_5$.

15.4) Soit D le sous-groupe de $\mathfrak{S}_6$ engendré par la transposition (12) et le 4-cycle (3456). Montrer que D est un groupe abélien, isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Est-il cyclique ?

15.5) Déduire des questions précédentes que lorsque $n \geq 6$, le sous-groupe de $\mathfrak{S}_n$ engendré par une transposition et un 4-cycle est soit d'ordre 8, soit isomorphe à $\mathfrak{S}_4$, soit isomorphe à $\mathfrak{S}_5$.

15.6) Les groupes B et D, tous les deux d'ordre 8, sont-ils isomorphes ?

16 Il n'y a que deux groupes d'ordre 6

Montrer que tout groupe d'ordre 6 est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ ou à $\mathfrak{S}_3$.

17 Qu'engendrent un Klein et une transposition ?

Soit G le sous-groupe du groupe symétrique $\mathfrak{S}_4$ engendré par la transposition $t = (23)$ et par le produit $k = (12)(34)$.

17.1) Montrer que G contient le groupe de Klein.

17.2) Trouver un 4-cycle contenu dans G et lui donner pour nom c.

17.3) Calculer le conjugué de c par t.

17.4) Montrer que tout élément de G s'écrit, de manière unique, sous la forme $t^a c^b$ où $a \in \{0, 1\}$ et $b \in \{0, 1, 2, 3\}$.

17.5) Calculer l'ordre de G. Le groupe G est-il abélien ? Est-il distingué dans $\mathfrak{S}_4$?

18 Un groupe d'ordre $2(2m+1)$ n'est jamais simple

Soient G un groupe fini et $f : G \to \mathfrak{S}_G$ le plongement canonique de G, defini comme d'habitude par $f(x)(y) = xy$ pour tous x et y de G.

18.1) Pour tout $x \in G$, quelle est la forme de la décomposition de $f(x)$ en produit de cycles à supports disjoint ? Calculer sa signature.

18.2) Suffit-il que G soit d'ordre impair pour que $f(G)$ soit un sous-groupe de $\mathfrak{A}_G$?

18.3) On suppose que G est d'ordre $2n$ où n est un entier naturel impair.

(i) Pourquoi G contient-il au moins un élément d'ordre 2 ?

(ii) Soit z un élément d'ordre 2 de G. Calculer la signature de $f(z)$.

(iii) En déduire que G contient un sous-groupe distingué d'ordre n.

19 Groupes d'ordre $2(2m+1)$

Soit G un groupe fini d'ordre $2n$ où n est un entier naturel impair.

19.1) Pourquoi G contient-il au moins un élément d'ordre 2 ?

19.2) Soit z un élément d'ordre 2 de G. On note

$$\begin{array}{rccc} \sigma : & G & \longrightarrow & G \\ & x & \longmapsto & zx. \end{array}$$

Montrer que σ est une permutation d'ordre 2 sans point fixe de G et calculer sa signature.

19.3) On note $\mathfrak{S}_G$ le groupe des permutations de G. Soit $\Phi : G \longrightarrow \mathfrak{S}_G$ l'application définie par :

$$\forall y \in G,\ \forall x \in G,\ \Phi(y)(x) = yx.$$

Montrer que Φ est un homomorphisme de groupes.

19.4) On note $f = \varepsilon \circ \Phi : G \longrightarrow \{-1, 1\}$, où ε désigne la signature. Montrer que f est surjectif. En déduire que G contient un sous-groupe distingué d'ordre n.

19.5) Existe-t-il un groupe G d'ordre pair qui ne contienne pas de sous-groupe (normal) d'ordre $\frac{|G|}{2}$?

20 Sous-groupes d'indice p min

Soient G un groupe fini et p le plus petit nombre premier qui divise l'ordre de G. Il s'agit de montrer que *tout sous-groupe d'indice p de G est distingué.*

(i) Soit H un sous-groupe de G d'indice p. Montrer que l'action de G sur l'ensemble $(G/H)_g$ des classes à gauche modulo H par translation à gauche induit un homomorphisme de groupes $\Phi : G \to \mathfrak{S}_p$.

(ii) Montrer que l'image de Φ est un groupe abélien (et même cyclique).

(iii) En déduire que $H \triangleleft G$.

21 Groupes ayant exactement trois classes de conjugaison

Où l'on montre que les seuls groupes finis ayant exactement 3 classes de conjugaison sont $\mathbb{Z}/3\mathbb{Z}$ et $\mathfrak{S}_3$.

Soit G un groupe fini d'ordre n ayant exactement trois classes de conjugaison. On note a et b les ordres des groupes d'isotropie des deux classes qui ne sont pas la classe triviale $\{1\}$ et on suppose que $a \leq b$.

21.1) Montrer que $1 = \frac{1}{n} + \frac{1}{a} + \frac{1}{b}$, que $a|n$ et que $b|n$.

21.2) Montrer successivement que $a \in \{1, 2, 3\}$, que le cas $a = 1$ est à rejeter, que $a = 3$ implique $a = b = n = 3$ et, enfin, que $a = 2$ impose $(n, a, b) = (6, 2, 3)$.

21.3) Montrer que seul le groupe $\mathbb{Z}/3\mathbb{Z}$ correspond au cas $(n, a, b) = (3, 3, 3)$ et que seul le groupe $\mathfrak{S}_3$ correspond au cas $(n, a, b) = (6, 2, 3)$.

22 Le groupe diédral

Pour tout entier naturel non nul n, on note $r_n : \mathbb{C} \to \mathbb{C}$ l'application $z \mapsto e^{2i\pi/n}z$. On note aussi $s : \mathbb{C} \to \mathbb{C}$ l'application $z \mapsto \overline{z}$ — c'est la conjugaison complexe. On note enfin $D_n = \langle r_n, s\rangle$ le sous-groupe de $\mathfrak{S}_{\mathbb{C}}$ engendré par r_n et s.

22.1) Montrer que lorsqu'on fait l'identification standard du plan complexe au plan euclidien, tout élément de D_n est une isométrie qui stabilise l'ensemble $\mathbb{U}_n$ des racines n^{e} de l'unité.

22.2) Calculer l'ordre de r_n et de s.

22.3) Calculer sr_ns en fonction de r_n. En déduire que le groupe $C_n = \langle r_n \rangle$ est un sous-groupe distingué de D_n.

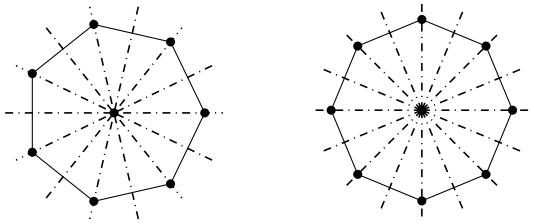
22.4) Montrer que $D_n = \left\{ s^\varepsilon r_n^k,\ \varepsilon \in \{0,1\},\ k \in \{0,\dots,n-1\} \right\}$.

22.5) Montrer que D_n est un groupe d'ordre $2n$, non abélien lorsque $n \geq 3$.

22.6) Montrer que D_n est le groupe des isométries qui stabilisent $\mathbb{U}_n$ et que C_n est son sous-groupe des isométries positives. Décrire toutes les rotations et toutes les symétries orthogonales de D_{2n}.

22.7) Calculer le centre et le groupe dérivé de D_n.

Dessin des axes de symétries des polygones réguliers dans le cas d'un nombre impair ou pair de sommets.



23 Groupe des caractères d'un groupe

Si G est un groupe, on appelle *caractère* de G tout homomorphisme de groupes $G \to \mathbb{C}^\times$.

23.1) Si χ_1 et χ_2 sont des caractères d'un groupe G, montrer que l'application

$$\begin{array}{rccc} \chi_1\chi_2 \ : & G & \longrightarrow & \mathbb{C}^\times \\ & g & \longmapsto & \chi_1(g)\chi_2(g) \end{array}$$

est encore un caractère de G et que l'opération $(\chi_1, \chi_2) \mapsto \chi_1\chi_2$ confère à l'ensemble des caractères de G une structure de groupe. On note $\widehat{G}$ le groupe des caractères du groupe G.

23.2) Soient G un groupe, N un sous-groupe distingué de G et $p : G \to G/N$ la projection canonique. Montrer que l'application

$$\begin{array}{rccc} \Phi : \widehat{G/N} & \longrightarrow & \widehat{G} \\ \chi & \longmapsto & \chi \circ p \end{array}$$

est un homomorphisme injectif de groupes.

23.3) Montrer que $\widehat{\mathbb{Z}}$ est isomorphe à $\mathbb{C}^\times$.

23.4) Montrer que si un groupe est cyclique, il est isomorphe à son groupe des caractères.

23.5) Soient M et N deux groupes. Montrer que l'application

$$\begin{array}{rccc} F : & \widehat{M} \times \widehat{N} & \longrightarrow & \widehat{M \times N} \\ & (\mu, \nu) & \longmapsto & F(\mu,\nu), \end{array}$$

où $F(\mu,\nu)$ est définie par $F(\mu,\nu)(m,n) = \mu(m)\nu(n)$ pour tous $(m,n) \in M \times N$, est un isomorphisme de groupes (on pourra chercher à exprimer l'application réciproque).

23.6) Montrer que tout groupe abélien fini est isomorphe à son groupe des caractères.

23.7) Montrer que tout caractère d'un groupe G est constant sur son sous-groupe dérivé $[G,G]$. En déduire que si G est un groupe, alors les groupes de caractères $\widehat{G}$ et $\widehat{G/[G,G]}$ sont isomorphes.

23.8) Montrer que si G est un groupe fini, alors $\widehat{G}$ et $G/[G,G]$ sont isomorphes.

23.9) Calculer les groupes des caractères de $\mathfrak{A}_4$ et de $\mathfrak{S}_4$. [On trouve respectivement $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$.]

23.10) Lorsque $n \geq 5$, montrer que le groupe des caractères de $\mathfrak{A}_n$ est trivial et que celui de $\mathfrak{S}_n$ est cyclique d'ordre 2.

24 Automorphismes du groupe $\mathbb{Z}/n\mathbb{Z}$, inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$

Soit n un entier naturel non nul.

24.1) Montrer que le groupe $\mathrm{Aut}\,(\mathbb{Z}/n\mathbb{Z})$ des automorphismes du groupe $\mathbb{Z}/n\mathbb{Z}$ est isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Noter, en particulier, que cela montre que $\mathrm{Aut}\,(\mathbb{Z}/n\mathbb{Z})$ est un groupe abélien fini.

24.2) Montrer que si m et n sont premiers entre eux, alors les groupes $(\mathbb{Z}/mn\mathbb{Z})^\times$ et $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ sont isomorphes.

24.3) En déduire que si $n = p_1^{a_1} \dots p_r^{a_r}$ où les p_k sont des nombres premiers distincts et les a_k des entiers naturels non nuls, alors

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{k=1}^{r} (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^\times$$

24.4) *Si p est un nombre premier, alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$.*
Quel théorème (pas si simple) du cours assure cela ?

24.5) Montrer les assertions suivantes, qui serviront dans la suite.

(i) Pour tout nombre premier impair p, pour tout $k \in \mathbb{N}$, il existe $u \in \mathbb{N}$, premier avec p, tel que $(1+p)^{p^k} = 1+up^{k+1}$.

(ii) Si p est un nombre premier impair et si $\alpha \in \mathbb{N}^*$, alors l'ordre de $1+p$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est exactement $p^{\alpha-1}$.

(iii) Pour tout $k \in \mathbb{N}$, il existe un entier naturel impair u tel que $5^{2^k} = 1 + u2^{k+2}$.

(iv) Si $\alpha \geq 3$, l'ordre de 5 dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est exactement $2^{\alpha-2}$.

24.6) Montrer que si p est un nombre premier supérieur ou égal à 3 et si $\alpha \in \mathbb{N}^*$, alors le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique, isomorphe à $\mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.

Indication : on pourra chercher un élément du groupe des inversibles qui soit d'ordre $p^{\alpha-1}(p-1)$. Pour cela, considérer l'homomorphisme de groupes $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ qui vient de la factorisation de la projection canonique $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ *via* la PUQ, prendre un x dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ dont l'image engendre $(\mathbb{Z}/p\mathbb{Z})^\times$. Dans le groupe cyclique, $\langle x\rangle$, dont l'ordre est un multiple de $p-1$, prendre un élément y d'ordre $p-1$. Alors, $(1+p)y$ est d'ordre $p^{\alpha-1}(p-1)$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

24.7) Calculer $(\mathbb{Z}/2\mathbb{Z})^\times$ et $(\mathbb{Z}/4\mathbb{Z})^\times$. Montrer que si $\alpha \geq 3$, alors le groupe $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est non cyclique et que ses facteurs invariants sont 2 et $2^{\alpha-2}$; autrement dit, $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

Indication : considérer l'homomorphisme de groupes surjectif $f : (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times \simeq \{-1, 1\}$ qui vient de la factorisation de la projection canonique $\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ *via* la PUQ. Son noyau est d'ordre $2^{\alpha-2}$ et contient 5, dont l'ordre est précisément $2^{\alpha-2}$. Donc ce noyau est cyclique, engendré par 5. Par ailleurs, $-1 \neq 1$ dans $\mathbb{Z}/2^\alpha\mathbb{Z}$ et donc l'homomorphisme de groupes $\langle -1\rangle \times \langle 5\rangle \to (\mathbb{Z}/2^\alpha\mathbb{Z})^\times$, $(\varepsilon, x) \mapsto \varepsilon x$, qui est injectif, est un isomorphisme de groupes — remarquer qu'on a noté -1 et 5 les classes modulo 2^α des nombres entiers -1 et 5.

24.8) Calculer les composantes de torsion du GAF $(\mathbb{Z}/n\mathbb{Z})^\times$, pour tout entier naturel non nul n.

25 Bases dans les réseaux

Soit n un entier naturel non nul. Si $e_1, \dots, e_n \in \mathbb{Z}^n$, on dit que $(e_1, \dots, e_n)$ est une $\mathbb{Z}$-base de $\mathbb{Z}^n$ lorsque tout vecteur de $\mathbb{Z}^n$ s'écrit de manière unique comme combinaison linéaire de $e_1, \dots, e_n$, à coefficients entiers. Par exemple, la base canonique de $\mathbb{R}^n$ est une $\mathbb{Z}$-base de $\mathbb{Z}^n$.

25.1) Montrer que toute $\mathbb{Z}$-base de $\mathbb{Z}^n$ est une base du $\mathbb{R}$-espace vectoriel $\mathbb{R}^n$ mais que tout n-uplet de vecteurs de $\mathbb{Z}^n$ qui est une base de $\mathbb{R}^n$ n'est pas une $\mathbb{Z}$-base de $\mathbb{Z}^n$.

25.2) On note $(c_1, \dots, c_n)$ la base canonique de $\mathbb{R}^n$. Soient $e_1, \dots, e_n \in \mathbb{Z}^n$. Montrer que $(e_1, \dots, e_n)$ est une $\mathbb{Z}$-base de $\mathbb{Z}^n$ si, et seulement s'il existe $P \in \mathcal{M}_n(\mathbb{Z})$ telle que $\det P = \pm 1$ et ${}^t e_k = P\,{}^t c_k$, pour tout $k \in \{1, \dots, n\}$.

25.3) Soient $e_1, \dots, e_n \in \mathbb{R}^n$. Soit $\mathrm{Vol}\,(e_1, \dots, e_n)$ le volume du parallélépipède des e_k : c'est la mesure de Lebesgue dans $\mathbb{R}^n$ de

$$\sum_{k=1}^{n} [0,1]e_k.$$

Montrer, en s'appuyant sur la formule de changement de variables sous une intégrale, que

$$\mathrm{Vol}\,(e_1, \dots, e_n) = \left|\det{}_{(c_1,\dots,c_n)}\,(e_1, \dots, e_n)\right|.$$

25.4) Soient $e_1, \dots, e_n \in \mathbb{Z}^n$. Montrer que $(e_1, \dots, e_n)$ est une $\mathbb{Z}$-base de $\mathbb{Z}^n$ si, et seulement si $\mathrm{Vol}\,(e_1, \dots, e_n) = 1$.

25.5) Soit $X = (a, b) \in \mathbb{Z}^2$. Montrer que X se complète en une $\mathbb{Z}$-base de $\mathbb{Z}^2$ si, et seulement si a et b sont premiers entre eux.

25.6) Soit $X = (a_1, \dots, a_n) \in \mathbb{Z}^n$. Montrer que X se complète en une $\mathbb{Z}$-base de $\mathbb{Z}^n$ si, et seulement si les a_k sont premiers entre eux (dans leur ensemble).

26 Classes de conjugaison des transvections dans SL

Soit V un espace vectoriel de dimension finie n sur un corps $\mathbb{F}$.

26.1) Montrer que deux dilatations de $\mathrm{GL}(V)$ sont conjuguées si, et seulement si elles ont le même rapport.

26.2) Montrer que toutes les transvections sont conjuguées dans $\mathrm{GL}(V)$.

26.3) Montrer que si $n \geq 3$, toutes les transvections de $\mathrm{SL}(V)$ sont conjuguées dans $\mathrm{SL}(V)$.

26.4) Montrer que les deux matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ ne sont pas conjuguées dans $\mathrm{SL}\,(2, \mathbb{R})$. En déduire que pour $n = 2$, il n'est pas vrai que toutes les transvections de $\mathrm{SL}(V)$ sont conjuguées dans $\mathrm{SL}(V)$.

26.5) On suppose que $n = 2$. Montrer que toute matrice de transvection est conjuguée dans $\mathrm{SL}\,(2, \mathbb{F})$ à une matrice de la forme $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ où $a \in \mathbb{F} \setminus \{0\}$ et que si $a, b \in \mathbb{F} \setminus \{0\}$, les deux matrices $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ sont conjuguées dans $\mathrm{SL}\,(2, \mathbb{F})$ si, et seulement si $\frac{a}{b}$ est un carré dans $\mathbb{F}$.

26.6) Calculer le nombre de classes de conjugaisons des transvections dans $\mathrm{SL}\,(2, \mathbb{F})$ pour $\mathbb{F} = \mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ ou $\mathbb{F}_q$ où q est la puissance d'un nombre premier.

27 Eléments sur les groupes arithmétiques de congruence

On note $\mathrm{PSL}\,(2, \mathbb{Z})$ le quotient de $\mathrm{SL}\,(2, \mathbb{Z})$ par son centre $\{-I_2, I_2\}$. Si G est un sous-groupe de $\mathrm{SL}\,(2, \mathbb{Z})$, on note PG son image par la projection canonique $\mathrm{SL}\,(2, \mathbb{Z}) \to \mathrm{PSL}\,(2, \mathbb{Z})$. Autrement dit, PG est le groupe des classes modulo $\{-I_2, I_2\}$ des éléments de G.
Pour tout entier naturel non nul N, on note $\mathrm{SL}\,(2, \mathbb{Z}/N\mathbb{Z})$ le groupe des matrices 2×2 à coefficients dans $\mathbb{Z}/N\mathbb{Z}$ dont le déterminant égale 1.

27.1) S'assurer que $\mathrm{SL}\,(2, \mathbb{Z}/N\mathbb{Z})$ est bien un groupe pour la multiplication matricielle.

27.2) On note π l'application de réduction modulo N

$$\begin{array}{rccc} \pi : & \mathrm{SL}\,(2, \mathbb{Z}) & \longrightarrow & \mathrm{SL}\,(2, \mathbb{Z}/N\mathbb{Z}) \\ & \begin{pmatrix} a & c \\ b & d \end{pmatrix} & \longmapsto & \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix} \end{array}$$

où $\overline{x}$ désigne la classe modulo N de l'entier x. Montrer rapidement que p est un homomorphisme de groupes.

27.3) Où l'on montre que π est surjectif.

(i) Soient n et d deux entiers naturels non nuls. On suppose que $d|n$. Montrer que la projection canonique $\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ induit un homomorphisme de groupes $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/d\mathbb{Z})^\times$. Montrer que ce dernier est sujectif.

(ii) Déduire de (i) l'assertion suivante : *si x, y et z sont des entiers premiers entre eux et si $x \neq 0$, il existe $k \in \mathbb{Z}$ tel que* $\mathrm{PGCD}(x, y + kz) = 1$.

(iii) Déduire de (ii) la surjectivité de π.

27.4) Montrer que $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ est engendré par les classes modulo N des matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

27.5) Pour tout entier naturel non nul N, on note

$$\Gamma(N) = \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}),\ a = d = 1\ [N] \ \text{ et } \ b = c = 0\ [N] \right\},$$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}),\ b = 0\ [N] \right\},$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}),\ a = d = 1\ [N] \ \text{ et } \ b = 0\ [N] \right\}$$

Autrement dit, $\Gamma(N)$ est l'ensemble des matrices de $\mathrm{SL}(2, \mathbb{Z})$ qui sont congrues à I_2 modulo N, $\Gamma_0(N)$ est l'ensemble des matrices de $\mathrm{SL}(2, \mathbb{Z})$ qui sont trigonales supérieures modulo N et $\Gamma_1(N)$ est le sous-ensemble des matrices de $\Gamma_0(N)$ dont les éléments diagonaux sont congrus à 1 modulo N.
Montrer que $\Gamma(N)$, $\Gamma_0(N)$ et $\Gamma_1(N)$ sont des sous-groupes de $\Gamma(1) = \mathrm{SL}(2, \mathbb{Z})$.

27.6) Dans la chaîne

$$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq \mathrm{SL}(2, \mathbb{Z})$$

montrer que $\Gamma(N) \triangleleft \mathrm{SL}(2, \mathbb{Z})$, que $\Gamma_1(N) \triangleleft \Gamma_0(N)$, mais que $\Gamma_0(N)$ et $\Gamma_1(N)$ ne sont pas distingués dans $\mathrm{SL}(2, \mathbb{Z})$.

27.7) Montrer que $\Gamma(N)$, $\Gamma_0(N)$ et $\Gamma_1(N)$ sont d'indices finis dans $\Gamma(1) = \mathrm{SL}(2, \mathbb{Z})$.

28 Dans $\mathrm{SL}_2(\mathbb{C})$, les centralisateurs non idiots sont abéliens

Pour tout $M \in \mathrm{SL}(2, \mathbb{C})$, on note $Z(M)$ le *centralisateur* de M dans $\mathrm{SL}(2, \mathbb{C})$, à savoir

$$Z(M) = \{ N \in \mathrm{SL}(2, \mathbb{C}),\ MN = NM \}.$$

28.1) Montrer que $Z(M)$ est un sous-groupe de $\mathrm{SL}(2, \mathbb{C})$, pour tout $M \in \mathrm{SL}(2, \mathbb{C})$.

28.2) Montrer que pour tout $M \in \mathrm{SL}(2, \mathbb{C})$ et pour tout $P \in \mathrm{GL}(2, \mathbb{C})$, on a l'égalité

$$Z\left(PMP^{-1}\right) = PZ(M)P^{-1}.$$

28.3) Montrer que tout élément de $\mathrm{SL}(2, \mathbb{C})$ est semblable à une matrice de l'une des cinq formes suivantes :

$$\pm I_2,\ \ \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ \ \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} \text{ où } a \in \mathbb{C} \setminus \{-1, 0, 1\}$$

— on pourra raisonner sur le polynôme caractéristique.

28.4) Montrer que le centralisateur de $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est $Z(T) = \left\{ \pm \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix},\ \alpha \in \mathbb{C} \right\}$.

28.5) Soit $a \in \mathbb{C} \setminus \{0\}$. Calculer le centralisateur de $\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}$.

28.6) On note $\mathbb{C}$ le groupe additif $(\mathbb{C}, +)$ et $\mathbb{C}^\times$ le groupe multiplicatif $(\mathbb{C} \setminus \{0\}, \times)$. On note aussi $S = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$.
Montrer que $Z(T)$ est isomorphe au groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{C}$ et que $Z(S)$ est isomorphe à $\mathbb{C}^\times$.

28.7) Déduire des questions précédentes que $Z(M)$ est un groupe abélien, pour tout $M \in \mathrm{SL}(2, \mathbb{C}) \setminus \{-I_2, I_2\}$.

29 Simplicité de PSL sauf deux cas sporadiques

L'objet de cet exercice est de montrer le résultat suivant :

Théorème
Soient n un entier naturel supérieur ou égal à 2 et $\mathbb{F}$ un corps.

(i) $\mathrm{PSL}(2, \mathbb{Z}/2\mathbb{Z}) \simeq \mathfrak{S}_3$.

(ii) $\mathrm{PSL}(2, \mathbb{Z}/3\mathbb{Z}) \simeq \mathfrak{A}_4$.

(iii) Dans tous les autres cas, $\mathrm{PSL}(n, \mathbb{F})$ *est un groupe simple.*

29.1) On suppose que $n \geq 3$.

(i) Soit G un sous-groupe distingué de $\mathrm{SL}(\mathbb{F}^n)$ contenant strictement le centre Z de $\mathrm{SL}(n, \mathbb{F})$. Montrer qu'il existe $g \in G$ et $h \in \mathbb{F}^n \setminus \{0\}$ tels que $g(h) \notin \mathbb{F}h$.

(ii) Soient g et h comme dans la question précédente ; on note $k = g(h)$. Montrer qu'il existe une transvection $t \in \mathrm{SL}(n, \mathbb{F})$ de droite $\mathbb{F}h$ et un hyperplan H de $\mathbb{F}^n$ qui contient le plan engendré par h et k.

(iii) Dans les conditions des deux questions précédentes, on note $c = [g, t] = gtg^{-1}t^{-1}$. Montrer que $c \in G \setminus \{\mathrm{id}\}$, que l'image de $c - \mathrm{id}$ est incluse dans H, et que H est stable par c.

(iv) On suppose que $t' \in \mathrm{SL}(n, \mathbb{F})$ est une transvection d'hyperplan H qui ne commute pas avec c. Montrer que $[c, t']$ est une transvection non triviale contenue dans G.

(v) On suppose au contraire que c commute avec toutes les transvections d'hyperplan H. Montrer que c est une transvection.

(vi) Déduire des questions précédentes que $\mathrm{PSL}(n, \mathbb{F})$ est simple.

29.2) On suppose que $n = 2$ et que $\mathrm{Card}(\mathbb{F}) \geq 7$.

(i) Montrer que le centre Z de $\mathrm{SL}(2, \mathbb{F})$ est contenu dans $\{\pm I_2\}$. Soit G un sous-groupe distingué de $\mathrm{SL}(2, \mathbb{F})$ contenant strictement Z.

(ii) Soient $a \in \mathbb{F} \setminus \{-1, 0, 1\}$ et $b \in \mathbb{F} \setminus \{0\}$. Montrer qu'il existe $s \in \mathrm{SL}(2, \mathbb{F})$ tel que

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \left[s, \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} \right].$$

(iii) On suppose que $g \in G \setminus \{\pm I_2\}$ a une valeur propre a différente de -1 et de 1. Montrer que g est conjugué dans $\mathrm{SL}(2, \mathbb{F})$ à la matrice $\mathrm{diag}(a, 1/a)$. En déduire que $G = \mathrm{SL}(2, \mathbb{F})$.

(iv) On suppose que $g = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in G \setminus \{\pm I_2\}$, où $b \neq 0$. Montrer qu'il existe $t \in \mathrm{SL}(2, \mathbb{F})$ telle que $t^{-1}g^{-1}tg$ admette $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ pour vecteur propre, associé à une valeur propre différente de 1 et de -1. En déduire que $G = \mathrm{SL}(2, \mathbb{F})$.

(v) On suppose que $g = \pm \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \in G$ avec $c \neq 0$. En notant $i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, calculer igi^{-1}. En déduire que $G = \mathrm{SL}(2, \mathbb{F})$.

(vi) Démontrer que $\mathrm{PSL}(2, \mathbb{F})$ est simple.

29.3) En admettant les isomorphismes classiques suivants (voir la feuille d'exercice numéro 3) :

$$\mathrm{PSL}(2, \mathbb{Z}/2\mathbb{Z}) \simeq \mathfrak{S}_3, \ \ \mathrm{PSL}(2, \mathbb{Z}/3\mathbb{Z}) \simeq \mathfrak{A}_4, \ \ \mathrm{PSL}(2, \mathbb{F}_4) \simeq \mathfrak{A}_5, \ \ \mathrm{PSL}(2, \mathbb{F}_5) \simeq \mathfrak{A}_5,$$

démontrer le théorème annoncé.

UVSQ 2024/2025
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)

Feuille d'exercices numéro 3

30 Petites questions en vrac, pour soi

30.1) $\mathrm{GL}(n,\mathbb{R})$ est-il isomorphe à $\mathrm{SL}(n,\mathbb{R}) \times \mathbb{R}^\times$? Est-il produit direct interne de $\mathrm{SL}(n,\mathbb{R})$ et du sous-groupe $\{xI_n,\ x \in \mathbb{R}^\times\}$ de $\mathrm{GL}(n,\mathbb{R})$? Est-il produit direct interne de $\mathrm{SL}(n,\mathbb{R})$ et du sous-groupe $\{\mathrm{diag}(x,1,\ldots,1),\ x \in \mathbb{R}^\times\}$ de $\mathrm{GL}(n,\mathbb{R}) \times \mathbb{R}^\times$?

30.2) Calculer tous les Sylow de $\mathfrak{A}_n$ et de $\mathfrak{S}_n$, pour $n = (2, 3,)\ 4$ et 5.

30.3) Le groupe $\mathfrak{A}_4$ est-il isomorphe à un produit semi-direct $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z}$?

30.4) Il n'y a pas de groupe simple d'ordre 196.

30.5) Les groupes $\mathrm{GL}(3,\mathbb{Z}/2\mathbb{Z})$ et $\mathrm{GL}(4,\mathbb{Z}/2\mathbb{Z})$ contiennent-il des sous-groupe d'ordre 9 ?

31 Quelques gammes

31.1) Un peu de $\mathbb{H}_8$

(i) Faire la liste des éléments d'ordre 4 de $\mathbb{H}_8$. Calculer les classes de conjugaison dans $\mathbb{H}_8$. Montrer que tous les sous-groupes de $\mathbb{H}_8$ sont normaux.

(ii) Calculer le groupe des commutateurs de $\mathbb{H}_8$ et les facteurs invariants du quotient $\mathbb{H}_8/\{-1,1\}$.

(iii) Soit G un groupe engendré par deux éléments x et y qui vérifient $x^4 = 1$, $x^2 = y^2 \neq 1$ et $xyx^{-1} = y^{-1}$. Montrer que G est isomorphe à $\mathbb{H}_8$.

(iv) Montrer que $\mathbb{H}_8$ n'est pas produit semi-direct de deux groupes non triviaux.

31.2) Groupes d'ordre $2p$

Soit G un groupe fini d'ordre $2p$ où p est un nombre premier impair.

(i) Montrer que G contient un sous-groupe H d'ordre p, un sous-groupe K d'ordre 2, tels que $H \triangleleft G$, $G = HK$ et $H \cap K = \{1\}$.

(ii) Montrer que G est isomorphe au groupe cyclique $\mathbb{Z}/2p\mathbb{Z}$ ou au groupe diédral D_{2p}.

32 Sur les p-Sylow du groupe $\mathfrak{S}_p$

Si p est un entier naturel non nul, on note $\mathfrak{S}_p$ le groupe des permutations de $\{1, \cdots, p\}$.

32.1) D'abord dans $\mathfrak{S}_7$

(i) Calculer l'ordre commun à tous les 7-Sylow de $\mathfrak{S}_7$.

(ii) Montrer que tout 7-cycle de $\mathfrak{S}_7$ est dans un unique 7-Sylow.

(iii) Combien $\mathfrak{S}_7$ contient-il de 7-cycles ?

(iv) En utilisant ce qui précède, calculer le nombre de 7-Sylow de $\mathfrak{S}_7$.

(v) On fait agir $\mathfrak{S}_7$ par conjugaison sur l'ensemble de ses 7-Sylow. Dire quel théorème du cours permet d'affirmer que cette action n'a qu'une seule orbite et calculer l'ordre du groupe d'isotropie du 7-Sylow qui contient le 7-cycle (1234567).

32.2) Où l'on généralise

Soit p un nombre premier. Montrer que $(p-2)! = 1 \mod (p)$, puis que le groupe symétrique $\mathfrak{S}_p$ admet toujours un sous-groupe d'ordre $p(p-1)$.

32.3) Pour aller plus loin
Montrer, lorsque p est premier, que tout sous-groupe d'ordre $p(p-1)$ de $\mathfrak{S}_p$ est le normalisateur du sous-groupe engendré par un p-cycle.

33 D'autres gammes, sur les polynômes symétriques

Si n est un entier naturel non nul, on note σ_0, σ_1, $\sigma_2\ldots$ les polynômes symétriques élémentaires et S_0, S_1, $S_2\ldots$ les polynômes de Newton de l'anneau de polynômes $\mathbb{Z}[X_1,\ldots,X_n]$.

33.1) On suppose, dans cette question, que $n=2$. Calculer σ_1^3 en fonction de S_3, σ_1 et σ_2. En déduire à la main l'écriture de S_3 en fonction des σ_k.

33.2) On suppose que $n\geq 2$. Soit $P(X_1,\ldots,X_n)=\sum_{(i,j),\ i\neq j} X_i^2X_j$.

(i) Combien P a-t-il de monômes ?

(ii) Montrer que P est symétrique.

(iii) Calculer $\sigma_1\sigma_2$ en fonction de P et de σ_3. En déduire l'expression de P en fonction des σ_k — on pourra si l'on veut commencer par le cas $n=3$.

(iv) Calculer S_1S_2 en fonction de S_3 et de P. Trouver le polynôme Q à trois indéterminées tel que $S_3=Q(\sigma_1,\sigma_2,\sigma_3)$.

33.3) En généralisant les démarches des questions précédentes, calculer

$$\sum_{i,j,k \text{ distincts}} X_i^2X_jX_k$$

à partir du développement du produit $\sigma_1\sigma_3$, puis $\sum_{(i,j),\ i\neq j} X_i^2X_j^2$ à partir du calcul de σ_2^2. Arriver ainsi au calcul de S_4 en fonction des σ_k (et comparer aux formules de Newton du cours).

33.4) Calculer

$$\sum_{i,j,k \text{ distincts}} X_i^2X_j^2X_k^2$$

en fonction des σ_k (on pourra considérer à part les cas où $n\leq 5$).

33.5) On suppose ici que $n=3$. Montrer que $(2X_1-X_2-X_3)(2X_2-X_3-X_1)(2X_3-X_1-X_2)$ est symétrique et l'exprimer comme un polynôme en les σ_k.

33.6) Même question pour $n=4$ et $(X_1X_2+X_3X_4)(X_1X_3+X_2X_4)(X_1X_4+X_2X_3)$.

34 Pourquoi "le" groupe diédral

Soit n un entier naturel supérieur ou égal à 3. On note D_n le groupe des isométries du plan (vectoriel) complexe qui stabilisent les points dont les affixes sont les racines n^{e} de l'unité, et C_n son sous-groupe positif.

34.1) Montrer que la suite exacte induite par le déterminant

$$1\longrightarrow C_n\longrightarrow D_n\xrightarrow{\det}\{1,-1\}\longrightarrow 1 \tag{3}$$

est scindée, ou, autrement dit, que D_n est un produit semi-direct $\mathbb{Z}/n\mathbb{Z}\rtimes\mathbb{Z}/2\mathbb{Z}$. Trouver toutes les sections possibles de cette suite exacte et expliciter les actions de $\{1,-1\}\simeq\mathbb{Z}/2\mathbb{Z}$ sur C_n induites par ces sections.

34.2) Montrer que pour toutes $r,r'\in D_n\setminus C_n$, il existe (une unique) $\kappa\in C_n$ telle que $r'=r\kappa$. En déduire que toutes les sections de (3) fournissent la même action $\mathbb{Z}/2\mathbb{Z}\to\mathrm{Aut}\,(C_n)$ et, ainsi, le même produit semi-direct $D_n\simeq\mathbb{Z}/n\mathbb{Z}\rtimes\mathbb{Z}/2\mathbb{Z}$.

34.3) Expliciter l'action de $\{1,-1\}$ sur C_n qui fournit le produit semi-direct de D_n.

34.4) Soient n un entier naturel supérieur ou égal à 3 et G un groupe d'ordre $2n$ engendré par deux éléments r et s qui vérifient : $r^n=s^2=1$ et $srs=r^{-1}$. Montrer que G est isomorphe à D_n.

34.5) Montrer que $\mathfrak{S}_3 \simeq D_3$ (mais que $\mathfrak{S}_n \not\simeq D_n$ si $n \geq 4$).

34.6) Dans l'anneau des fractions rationnelles $\mathbb{Q}(X)$, montrer que le groupe engendré par les homographies $\frac{1}{X}$ et $1 - X$, pour la substitution, est isomorphe à $\mathfrak{S}_3$.

[Autre point de vue : considérer les mêmes homographies vues comme transformations de $\mathbb{C} \setminus \{0, 1\}$, la loi de groupe étant alors la composition des applications.]

35 Birapport

Si $F(X_1, X_2, X_3, X_4)$ est une fraction rationnelle à coefficients rationnels à quatre indéterminées X_1, X_2, X_3 et X_4 et si $\sigma \in \mathfrak{S}_4$, on note

$$\sigma \cdot F\left(X_1, X_2, X_3, X_4\right) = F\left(X_{\sigma(1)}, X_{\sigma(2)}, X_{\sigma(3)}, X_{\sigma(4)}\right).$$

35.1) Montrer que cela définit une action à gauche du groupe $\mathfrak{S}_4$ sur le corps des fractions rationnelles $\mathbb{Q}\left(X_1, X_2, X_3, X_4\right)$.

35.2) On note B la fraction rationnelle *birapport*, définie par

$$B\left(X_1, X_2, X_3, X_4\right) = \frac{X_3 - X_1}{X_3 - X_2} \times \frac{X_4 - X_2}{X_4 - X_1} = \frac{\dfrac{X_3 - X_1}{X_3 - X_2}}{\dfrac{X_4 - X_1}{X_4 - X_2}}.$$

Montrer que le groupe de Klein est un sous-groupe du groupe d'isotropie de B.

35.3) En considérant l'action des transpositions (12), (13) et (14) ainsi que celle des 3-cycles (124) et (142), montrer que l'orbite de B sous l'action de $\mathfrak{S}_4$ contient les cinq autres fractions distinctes

$$\frac{1}{B}\ ,\ \frac{B}{B-1}\ ,\ 1-B\ ,\ \frac{1}{1-B}\ ,\ 1-\frac{1}{B}.$$

35.4) Calculer le groupe d'isotropie et l'orbite de B sous l'action de $\mathfrak{S}_4$.

36 CS pour que deux produit semi-directs soient isomorphes

Soient N et Q deux groupes, et $\varphi : Q \to \mathrm{Aut}(N)$ et $\psi : Q \to \mathrm{Aut}(N)$ deux actions de Q sur N par automorphismes.

36.1) On suppose que :
(i) $\alpha \in \mathrm{Aut}(N)$ est un automorphisme de N
(ii) les actions φ et ψ sont conjuguées par α au sens où $\psi(q) = \alpha \circ \varphi(q) \circ \alpha^{-1}$, pour tout $q \in Q$.
Montrer que dans ces conditions, l'application

$$\begin{array}{ccc} N \rtimes_\varphi Q & \longrightarrow & N \rtimes_\psi Q \\ (n, q) & \longmapsto & (\alpha(n), q) \end{array}$$

est un isomorphisme de groupes.

Slogan *Conjuguer l'action de Q sur N par un automorphisme de N ne change pas un produit semi-direct $N \rtimes Q$.*

36.2) On suppose que :
(i) $\beta \in \mathrm{Aut}(Q)$ est un automorphisme de Q
(ii) $\psi = \varphi \circ \beta$.
Montrer que dans ces conditions, l'application

$$\begin{array}{ccc} N \rtimes_\psi Q & \longrightarrow & N \rtimes_\varphi Q \\ (n, q) & \longmapsto & (n, \beta(q)) \end{array}$$

est un isomorphisme de groupes.

Slogan *Composer l'action de Q sur N par un automorphisme de Q ne change pas un produit semi-direct $N \rtimes Q$.*

37 Il n'y a que cinq groupes d'ordre 8

Montrer que tout groupe d'ordre 8 est isomorphe à un et un seul des groupes de la liste suivante :

$$\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z},\ \left(\mathbb{Z}/2\mathbb{Z}\right)^3,\ D_8,\ \mathbb{H}_8$$

où D_8 est le groupe diédral et $\mathbb{H}_8$ est le groupe quaternionique.

38 Il n'y a pas de groupe simple d'ordre 15309

Soit G un groupe d'ordre $15309 = 3^7 \times 7$.

38.1) Montrer que le nombre de 3-sous-groupes de Sylow de G est inclus dans l'ensemble $\{1, 7\}$.

38.2) On suppose que G est simple et a sept 3-sous-groupes de Sylow. Montrer comment l'action de G par conjugaison sur l'ensemble de ses 3-sous-groupes de Sylow induit un homomorphisme injectif de groupes $G \longrightarrow \mathfrak{S}_7$. Comparer les ordres de G et de $\mathfrak{S}_7$ et conclure à une contradiction.

38.3) Montrer qu'il n'y a pas de groupe simple d'ordre 15309.

39 Un sous-groupe de $\mathrm{GL}\,(2, \mathbb{F}_3)$

On note $\mathbb{F}_3$ le corps $\mathbb{Z}/3\mathbb{Z}$. Dans le groupe linéaire $\mathrm{GL}\,(2, \mathbb{F}_3)$, on note

$$r = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \text{ et } s = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}.$$

On note R (*resp.* S) le sous-groupe de $\mathrm{GL}\,(2, \mathbb{F}_3)$ engendré par r (*resp.* s) et G le sous-groupe engendré par $\{r, s\}$.

39.1) Calculer l'ordre de R et celui de S.

39.2) Montrer que $R \triangleleft G$ et que $R \cap S$ est le groupe trivial.

39.3) En déduire l'ordre de G.

[On pourra montrer que l'ensemble des $\rho\sigma$ où $\rho \in R$ et $\sigma \in S$ est un sous-groupe de G et raisonner dessus.]

39.4) Quel est l'indice de G dans $\mathrm{GL}\,(2, \mathbb{F}_3)$?

40 Un peu de Pauli

On note $\mathcal{P}$ le sous-groupe de $\mathrm{GL}\,(2, \mathbb{C})$ engendré par les trois matrices

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \text{ et } \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

40.1) Calculer les ordres de σ_1, σ_2 et σ_3.

40.2) Calculer $\sigma_1\sigma_2\sigma_3$ et en déduire que iI_2 est dans le centre de $\mathcal{P}$. On note H le sous-groupe de $\mathcal{P}$ engendré par iI_2.

40.3) Montrer que le groupe-quotient $\mathcal{P}/H$ est engendré par les classes modulo H de σ_1 et σ_3.

40.4) En déduire que $\mathcal{P}/H$ est un groupe abélien d'ordre 4 et calculer ses facteurs invariants.

40.5) Montrer que $\mathcal{P}$ est un groupe fini et calculer son ordre.

40.6) On note $\mathcal{Q} = \mathcal{P} \cap \mathrm{SL}\,(2, \mathbb{C})$. Calculer l'indice $[\mathcal{P} : \mathcal{Q}]$ et montrer que tout élément de $\mathcal{P}$ s'écrit de manière unique sous la forme $i^\varepsilon q$ où $\varepsilon \in \{0, 1\}$ et où $q \in \mathcal{Q}$.

40.7) Montrer que $\mathcal{Q}$ n'est pas abélien et qu'il contient au moins trois éléments d'ordre 4.

40.8) Montrer que $\mathcal{Q}$ est isomorphe au groupe quaternionique $\mathbb{H}_8$.

41 Pas de gros symétrique dans l'alterné

Soit n un entier naturel supérieur ou égal à 2. On note $\mathfrak{S}_n$ le groupe symétrique de n objets et $\mathfrak{A}_n$ son sous-groupe des permutations paires.

On cherche à montrer que le groupe alterné $\mathfrak{A}_{n+1}$ ne contient aucun sous-groupe isomorphe à $\mathfrak{S}_n$.

41.1) Montrer que $\mathfrak{A}_4$ n'a pas de sous-groupe isomorphe à $\mathfrak{S}_3$.

41.2) Montrer, par des considérations d'ordres, que si $\mathfrak{A}_{n+1}$ contient un sous-groupe isomorphe à $\mathfrak{S}_n$, alors n est nécessairement impair.

41.3) Soit m un entier supérieur ou égal à 3. On suppose que G est un sous-groupe de $\mathfrak{A}_{2m}$ isomorphe à $\mathfrak{S}_{2m-1}$.

(i) On note $(\mathfrak{A}_{2m}/G)_g$ l'ensemble des classes à gauches modulo G des éléments de $\mathfrak{A}_{2m}$. Calculer le cardinal de $(\mathfrak{A}_{2m}/G)_g$ en fonction de m.

(ii) On fait agir $\mathfrak{A}_{2m}$ sur $(\mathfrak{A}_{2m}/G)_g$ par translation à gauche et on note $\varphi : \mathfrak{A}_{2m} \to \mathfrak{S}_m$ l'homomorphisme de groupes que cette action induit. Montrer que φ est nécessairement injectif.

41.4) Déduire de ce qui précède que $\mathfrak{A}_{n+1}$ n'a pas de sous-groupe isomorphe à $\mathfrak{S}_n$.

42 Exposant d'un groupe

Si G est un groupe, son *exposant* est, lorsqu'il existe, le plus petit entier naturel non nul e qui vérifie : $\forall x \in G$, $x^e = 1$. Si un tel nombre n'existe pas, on dit que G *est d'exposant infini*.

42.1) Soit G un groupe. Montrer que $\{n \in \mathbb{Z},\ \forall x \in G,\ x^n = 1\}$ est un sous-groupe de $\mathbb{Z}$. On note e_G le générateur positif ou nul de ce groupe. Montrer que si $e_G \neq 0$, alors G est d'exposant fini égal à e_G. Montrer que si $e_G = 0$, alors G est d'exposant infini.

42.2) Soient G un groupe et $M \in \mathbb{N}^*$. On suppose que tout élément de G est d'ordre fini et que M est un majorant des ordres des éléments de G. Montrer que l'exposant de G est le PPCM des ordres de ses éléments.

42.3) Montrer que $(\mathbb{Q}/\mathbb{Z}, +)$ est d'exposant infini alors que tous ses éléments sont d'ordres finis.

42.4) Montrer que l'exposant de $\mathfrak{S}_n$ est PPCM $\{2, 3, \ldots, n\}$.

42.5) Soit G un groupe abélien fini d'exposant e.

(i) Montrer, en utilisant le théorème de structure des GAF, que G contient un élément d'ordre e.

(ii) Faire une preuve directe du résultat précédent en suivant les indications ci-dessous.

[Soit $x \in G$, dont l'ordre m est maximum. On montre que l'ordre de tout élément de G divise m, ce qui suffit à prouver que $m = e$ et, ainsi, que x convient. Soit $y \in G$; on note n son ordre. Pour montrer que $n|m$, il suffit de montrer que pour tout nombre premier p, $v_p(n) \leq v_p(m)$. Soit p un nombre premier. En notation additive, calculer l'ordre de $p^{v_p(m)}x$ et celui de $\frac{n}{p^{v_p(n)}}y$; en déduire l'ordre de $p^{v_p(m)}x + \frac{n}{p^{v_p(n)}}y$ et conclure en utilisant la maximalité de m.]

42.6) Utiliser ce qui précède pour établir une nouvelle preuve du théorème suivant : *si G est un sous-groupe fini du groupe multiplicatif d'un corps commutatif, alors G est cyclique.*

42.7) Montrer qu'un groupe (non abélien) ne contient pas nécessairement un élément dont l'ordre soit l'exposant du groupe.

42.8) On note

$$\mathcal{S} = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}\,(3, \mathbb{Z}/3\mathbb{Z}),\ a, b, c \in \mathbb{Z}/3\mathbb{Z} \right\}.$$

Montrer que $\mathcal{S}$ est un sous-groupe non abélien de $\mathrm{SL}\,(3, \mathbb{Z}/3\mathbb{Z})$ dont l'exposant est 3, et qui contient un élément d'ordre 3. Calculer l'ordre de $\mathcal{S}$[♫].

[♫] On pourra se rappeler, c'est écrit dans le cours, que $\mathcal{S}$ est un 3-Sylow de $\mathrm{GL}\,(3, \mathbb{F}_3)$.

(i) Calculer le centre de $\mathcal{S}$, montrer que le quotient $\mathcal{S}/Z$ est isomorphe à $(\mathbb{Z}/3\mathbb{Z})^2$ et montrer que la suite exacte

$$1 \longrightarrow Z \longrightarrow \mathcal{S} \longrightarrow \mathcal{S}/Z \longrightarrow 1$$

n'est pas scindée (d'ailleurs, il n'y a pas de produit semi-direct $\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/3\mathbb{Z})^2$ qui ne soit pas direct, vérifier cela).

(ii) Soit $f : \mathcal{S} \to \mathbb{Z}/3\mathbb{Z}$, $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mapsto c$. Montrer que f est un homomorphisme de groupes, que son noyau est isomorphe à $(\mathbb{Z}/3\mathbb{Z})^2$, et que la suite exacte

$$1 \longrightarrow (\mathbb{Z}/3\mathbb{Z})^2 \longrightarrow \mathcal{S} \xrightarrow{f} \mathbb{Z}/3\mathbb{Z} \longrightarrow 1$$

qu'il induit est scindée. Examiner le produit semi-direct $\mathcal{S} \simeq (\mathbb{Z}/3\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z}$ sous toutes les coutures.

43 Ordre maximal dans $\mathrm{GL}(n, \mathbb{F}_q)$

On note $\mathbb{F}_7$ le corps $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$. On note également $\mathcal{M}_2(\mathbb{F}_7)$ l'espace des matrices carrées 2×2 à coefficients dans $\mathbb{F}_7$ et $\mathrm{GL}(2, \mathbb{F}_7)$ le groupe de ces matrices qui sont inversibles.

L'objet de cette partie consiste à montrer que $\mathrm{GL}(2, \mathbb{F}_7)$ *contient un élément d'ordre* $7^2 - 1 = 48$ *et que tout élément de* $\mathrm{GL}(2, \mathbb{F}_7)$ *a un ordre inférieur ou égal à* 48[♫].

43.1) Décomposer le cardinal de $\mathcal{M}_2(\mathbb{F}_7)$ et l'ordre du groupe $\mathrm{GL}(2, \mathbb{F}_7)$ en produits de facteurs premiers.

43.2) Soit $g \in \mathcal{M}_2(\mathbb{F}_7)$. En faisant la division euclidienne de tout $P \in \mathbb{F}_7[X]$ par le polynôme caractéristique de g et en utilisant le théorème de Cayley-Hamilton, montrer que le cardinal du sous-ensemble

$$\{P(g),\ P \in \mathbb{F}_7[X]\}$$

de $\mathcal{M}_2(\mathbb{F}_7)$ est inférieur ou égal à 49.

43.3) Soit $g \in \mathrm{GL}(2, \mathbb{F}_7)$. En considérant l'ensemble $\left\{g^k,\ k \in \mathbb{N}\right\}$, montrer que l'ordre de g est au plus 48.

43.4) Soit $\gamma = \begin{pmatrix} 0 & -3 \\ 1 & -1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_7)$. Calculer γ^8. En déduire l'ordre de γ dans $\mathrm{GL}(2, \mathbb{F}_7)$.

43.5) Montrer que l'ordre maximal d'un élément de $\mathrm{GL}(2, \mathbb{F}_7)$ est $7^2 - 1$.

43.6) Est-il vrai que l'ordre de tout élément de $\mathrm{GL}(2, \mathbb{F}_7)$ divise 48 ?

44 Groupes d'ordre p^2, pq ou p^2q

44.1) Soient G un groupe et H un sous-groupe du centre de G, tel que le groupe-quotient G/H soit cyclique. Montrer que G est abélien.

44.2) Soit p un nombre premier. Montrer que les seuls groupes d'ordre p^2 sont $\mathbb{Z}/p^2\mathbb{Z}$ et $(\mathbb{Z}/p\mathbb{Z})^2$.

44.3) Soient p et q deux nombres premiers. Montrer qu'il n'y a pas de groupe simple d'ordre p^2q.

44.4) Soient p et q deux nombres premiers distincts et G un groupe d'ordre pq. On suppose que $p < q$. Montrer que :

(i) Si $p \not| q - 1$, alors G est cyclique, isomorphe à $\mathbb{Z}/pq\mathbb{Z}$

(ii) si $p|q - 1$, alors G est ou bien cyclique ou bien isomorphe à l'unique produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

44.5) Soit G un groupe d'ordre 24. En faisant agir G sur ses 2-Sylow par conjugaison, montrer que G n'est pas simple.

[♫] Ce résultat se généralise en remplaçant $\mathbb{F}_7$ par n'importe quel corps fini $\mathbb{F}_q$ et $\mathrm{GL}(2, \mathbb{F}_7)$ par $\mathrm{GL}(n, \mathbb{F}_q)$, $n \geq 1$.

45 Matrices inversibles trigonales par blocs

Soit $\mathbb{F}$ un corps. Soient n, d et e des entiers naturels non nuls tels que $n = d + e$.

45.1) Montrer que l'ensemble de matrices décrites par blocs sous la forme

$$\mathcal{T}_{d,e} = \left\{ \begin{pmatrix} A & B \\ 0 & C \end{pmatrix},\ A \in \mathrm{GL}\,(d, \mathbb{F}),\ C \in \mathrm{GL}\,(e, \mathbb{F}),\ B \in \mathcal{M}_{d,e}\,(\mathbb{F}) \right\},$$

où 0 désigne ici la matrice nulle de l'espace $\mathcal{M}_{e,d}\,(\mathbb{F})$ des matrices à e lignes et d colonnes et à coefficients dans $\mathbb{F}$, est un sous-groupe de $\mathrm{GL}\,(n, \mathbb{F})$.

45.2) Montrer que l'application

$$\begin{array}{rccc} p : & \mathcal{T}_{d,e} & \longrightarrow & \mathrm{GL}\,(d, \mathbb{F}) \times \mathrm{GL}\,(e, \mathbb{F}) \\ & \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} & \longmapsto & (A, C) \end{array}$$

est un homomorphisme de groupes dont on calculera l'image et le noyau.

45.3) Montrer que $\mathcal{T}_{d,e}$ est isomorphe à un produit semi-direct $\mathbb{F}^{de} \rtimes_{\varphi} \big(\mathrm{GL}\,(d, \mathbb{F}) \times \mathrm{GL}\,(e, \mathbb{F}) \big)$. On précisera quelle est l'action de ce produit semi-direct et on l'examinera sous toutes les coutures.

46 Sous-groupe d'indice fini d'un groupe infini

Soit G un groupe *infini*. On suppose que G contient un sous-groupe H différent de G dont l'indice dans G est *fini*.

46.1) On note $n = [G : H]$. Montrer que l'action de G par translation à gauche sur les classes à gauche modulo H induit un homomorphisme de groupes non injectif

$$\varphi : G \to \mathfrak{S}_n.$$

46.2) Montrer que

$$\ker(\varphi) = \bigcap_{x \in G} xHx^{-1}$$

et en déduire que $\ker(\varphi) \neq G$.

46.3) Montrer que G n'est pas simple.

47 Sous-groupes normaux d'un p-groupe, p-sous-groupes d'un groupe

Soit p un nombre premier.

47.1) Soient a un entier naturel et G un p-groupe d'ordre p^a. Montrer que G contient un sous-groupe distingué d'ordre p^b, pour tout $b \in \{0, \ldots, a\}$.

[On pourra raisonner par récurrence sur a.]

47.2) Soient m un entier naturel non nul et G un groupe d'ordre $p^a m$ où p ne divise pas m. Montrer que G contient un sous-groupe d'ordre p^b, pour tout $b \in \{0, \ldots, a\}$.

48 Plus loin que Burnside ; un groupe fini n'est pas union de conjugués d'un sous-groupe strict

Soit G un groupe fini opérant sur un ensemble fini non vide X. Pour tout $g \in G$, on note X^g l'ensemble des points de X fixés par g. On note enfin Ω l'ensemble des orbites de l'action. On rappelle la formule de Burnside :

$$\mathrm{Card}\,\Omega = \frac{1}{|G|} \sum_{g \in G} \mathrm{Card}\,X^g,$$

obtenue en calculant de deux façons le cardinal de la variété d'incidence $\{(g,x) \in G \times X,\ g \cdot x = x\}$.

48.1) On suppose que X a au moins deux éléments distincts. Montrer que $g \cdot (x,y) = (g \cdot x, g \cdot y)$ définit une action de G sur $X \times X$. Déduire alors de la formule de Burnside que

$$\sum_{g \in G} (\operatorname{Card} X^g)^2 \geq 2|G|.$$

Montrer que l'égalité a lieu si, et seulement si l'action de G sur X est 2-transitive, ce qui signifie que

$$\forall (x,y),(x',y') \in X^2,\ (x,y) \neq (x',y') \Longrightarrow \exists g \in G,\ x' = g \cdot x \text{ et } y' = g \cdot y.$$

48.2) On suppose que l'action est transitive et on note $\mathcal{I}$ l'ordre des groupes d'isotropie (ils sont tous conjugués). On note aussi $\mathcal{D}$ l'ensemble des éléments de G qui ne fixent aucun élément de X. Montrer que $\mathcal{I} \leq \operatorname{Card} \mathcal{D}$.

[On pourra majorer la somme $\sum_{g \in G} (\operatorname{Card} X^g - 1)\,(\operatorname{Card} X^g - \operatorname{Card} X)$, puis la minorer à l'aide de la question précédente.]

48.3) Soient G un groupe fini et H un sous-groupe strict de G. On note

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

la réunion des conjugués de G. Montrer que $\operatorname{Card} \mathcal{U} \leq |G| - |H|$. En déduire que G n'est pas la réunion des conjugués de H.

[On pourra faire agir G par conjugaison sur $X = \{gHg^{-1},\ g \in G\}$ et appliquer la question précédente à cette action en montrant, avec les notations de ladite question, que $\mathcal{D} \subseteq G \setminus \mathcal{U}$ et que $|H| \leq \mathcal{I}$.]

48.4) Dans les conditions de la question précédente, en remarquant que le cardinal de $\{gHg^{-1},\ g \in G\}$ est plus petit que l'indice de H dans G, montrer aussi que $\operatorname{Card} \mathcal{U} \leq |G| - [G:H] + 1$ — ce qui permet encore d'aboutir à la conclusion que $\mathcal{U} \subsetneq G$.

48.5) Trouver un groupe (infini) qui soit l'union des conjugués d'un sous-groupe propre.

[On pourra chercher du côté du groupe linéaire.]

49 Du côté de chez Jordan et Frobenius

49.1 Une inégalité de Jordan

Soient G un groupe fini et H un sous-groupe de G.

(i) Soient $g, g' \in G$. Montrer que $gH = g'H$ si, et seulement s'il existe $h \in H$ tel que $g' = gh$.

(ii) Soient $g, g' \in G$. Montrer que si $gH = g'H$, alors $gHg^{-1} = g'Hg'^{-1}$.

(iii) On note $\mathcal{R} \subseteq G$ un système de représentants des classes à gauche modulo H. Autrement dit, pour tout $g \in G$, il existe un unique $r \in \mathcal{R}$ tel que $gH = rH$. Montrer que

$$\bigcup_{g \in G} \left(gHg^{-1} \setminus \{1\}\right) = \bigcup_{r \in \mathcal{R}} \left(rHr^{-1} \setminus \{1\}\right).$$

(iv) Déduire de ce qui précède l'*inégalité de Jordan*

$$\operatorname{Card} \left(\bigcup_{g \in G} gHg^{-1} \right) \leq |G| - [G:H] + 1 \tag{4}$$

(v) Montrer que si $H \neq G$, alors G n'est pas la réunion des conjugués de H.

49.2 L'inégalité de Jordan est optimale

Soient $\mathbb{F}$ un corps fini de cardinal q et $\mathbb{F}^\times$ son groupe multiplicatif. Pour tous $(a,b) \in \mathbb{F}^\times \times \mathbb{F}$, on note $g_{a,b}$ l'application

$$\begin{array}{rccc} g_{a,b} : & \mathbb{F} & \longrightarrow & \mathbb{F} \\ & x & \longmapsto & ax+b. \end{array}$$

On note aussi $G = \{g_{a,b},\ a \in \mathbb{F}^\times,\ b \in \mathbb{F}\}$.

(i) Montrer que tout élément de G est une permutation de $\mathbb{F}$.

(ii) Montrer que G est un sous-groupe du groupe symétrique $\mathfrak{S}_\mathbb{F}$ et calculer son ordre.

(iii) Pour tous $(a,b) \in \mathbb{F}^\times \times \mathbb{F}$, on note h_a l'*homothétie* $h_a = g_{a,0}$ et t_b la *translation* $t_b = g_{1,b}$. Montrer que les sous-ensembles

$$H = \left\{h_a,\ a \in \mathbb{F}^\times\right\} \quad \text{et} \quad T = \{t_b,\ b \in \mathbb{F}\}$$

sont des sous-groupes de G.

(iv) Les groupes H et T sont-ils distingués dans G ?

(v) Soient $t, t' \in T$. Montrer que

$$\left(tHt^{-1}\right) \cap \left(t'Ht'^{-1}\right) \neq \{1\} \Longrightarrow t = t'.$$

(vi) En déduire que le couple (G,H) réalise l'égalité dans l'inégalité (4).

50 Automorphismes du groupe symétrique

Pour tout $n \geq 2$, on note $\operatorname{Aut}\mathfrak{S}_n$ le groupe des automorphismes du groupe $\mathfrak{S}_n$, et $\operatorname{Int}\mathfrak{S}_n$ son sous-groupe des automorphismes intérieurs.

50.1) Soient G un groupe, $\operatorname{Int} G$ le groupe de ses automorphismes intérieurs et $Z(G)$ le centre de G. Montrer que $G/Z(G)$ est un groupe isomorphe à $\operatorname{Int} G$.

50.2) Montrer que $\operatorname{Int}\mathfrak{S}_n \simeq \mathfrak{S}_n$, pour tout $n \geq 3$.

50.3) Soit $f \in \operatorname{Aut}\mathfrak{S}_n$. Montrer que f est intérieur si, et seulement si f transforme toute transposition en une transposition.

50.4) Si $m \in \mathbb{N}$, calculer l'ordre du centralisateur d'un produit de m transpositions à supports disjoints.

50.5) Montrer que $\operatorname{Aut}\mathfrak{S}_n = \operatorname{Int}\mathfrak{S}_n$ pour tout $n \neq 6$.

50.6) Le cas singulier de $\mathfrak{S}_6$

(i) Montrer que le nombre de 5-Sylow de $\mathfrak{S}_5$ est 6.

(ii) Montrer que l'action de $\mathfrak{S}_5$ par conjugaison sur ses 5-Sylow induit un homomorphisme injectif de groupes $\Phi : \mathfrak{S}_5 \to \mathfrak{S}_6$ dont l'image, que l'on notera G, n'est pas le stabilisateur d'un point de $\{1,\ldots,6\}$.

(iii) Montrer que l'action de $\mathfrak{S}_6$ par translation à gauche sur l'ensemble X des classes à gauche de $\mathfrak{S}_6$ modulo G induit un isomorphisme de groupes $\Psi : \mathfrak{S}_6 \to \mathfrak{S}_X$. Montrer que l'image de G par Ψ est le fixateur de G dans $\mathfrak{S}_X$.

(iv) Déduire de Ψ un automorphisme de $\mathfrak{S}_6$ qui n'est pas intérieur.

(v) En conclure que $\operatorname{Aut}\mathfrak{S}_6 \neq \operatorname{Int}\mathfrak{S}_6$.

51 Automorphismes du groupe $\mathrm{SL}(2,\mathbb{F}_3)$

On note $\mathbb{F}_3$ le corps à trois éléments $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$. On note aussi selon l'usage $\mathrm{GL}(2,\mathbb{F}_3)$ le groupe des matrices carrées 2×2 à coefficents dans $\mathbb{F}_3$ inversibles et $\mathrm{SL}(2,\mathbb{F}_3)$ son sous-groupe des matrices dont le déterminant égale 1.

Si G est un groupe, on notera $\operatorname{Aut}(G)$ le groupe des automorphismes de G.

L'objet de cette exercice consiste à montrer que $\operatorname{Aut}(\mathrm{SL}(2,\mathbb{F}_3))$ *est isomorphe au groupe symétrique* $\mathfrak{S}_4$.

51.1) On note $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Calculer l'ordre de $\mathrm{SL}(2, \mathbb{F}_3)$, l'ordre de T et l'ordre de U dans $\mathrm{SL}(2, \mathbb{F}_3)$.

On pourra utiliser — c'est une conséquence du cours sur le groupe modulaire — que T et U engendrent $\mathrm{SL}(2, \mathbb{F}_3)$.

51.2) Déduire de la question précédente que le nombre de 3-Sylow de $\mathrm{SL}(2, \mathbb{F}_3)$ est 4. On note $\mathcal{S}_3$ l'ensemble des 3-Sylow de $\mathrm{SL}(2, \mathbb{F}_3)$.

51.3) Montrer que l'image d'un 3-Sylow de $\mathrm{SL}(2, \mathbb{F}_3)$ par un automorphisme de $\mathrm{SL}(2, \mathbb{F}_3)$ est encore un 3-Sylow de $\mathrm{SL}(2, \mathbb{F}_3)$. En déduire une action du groupe $\mathrm{Aut}(\mathrm{SL}(2, \mathbb{F}_3))$ sur $\mathcal{S}_3$. On notera

$$\Phi : \mathrm{Aut}(\mathrm{SL}(2, \mathbb{F}_3)) \longrightarrow \mathfrak{S}_{\mathcal{S}_3}$$

l'homomorphisme de groupes induit par cette action.

51.4) Montrer que les 3-Sylow de $\mathrm{SL}(2, \mathbb{F}_3)$ sont

$$S_1 = \langle T \rangle \ , \ S_2 = \langle U \rangle \ , \ S_3 = \left\langle UTU^{-1} \right\rangle \text{ et } S_4 = \left\langle U^2TU^{-2} \right\rangle .$$

51.5) Montrer que si $g \in \ker \Phi$, alors $g(T) \in \left\{T, T^2\right\}$ et $g(U) \in \left\{U, U^2\right\}$.

51.6) Calculer l'ordre de TU et celui de TU^2.

51.7) Déduire des questions précédentes que Φ est injectif.

51.8) On note $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_3)$. Calculer les conjugués de S_1, S_2, S_3 et S_4 par A et en déduire que l'image de Φ contient une permutation impaire.

51.9) Soit G un groupe. Expliciter un isomorphisme entre le groupe des isomorphismes intérieurs de G et le groupe-quotient $G/Z(G)$ de G par son centre $Z(G)$.

51.10) Montrer que l'image de Φ contient le groupe alterné $\mathfrak{A}_{\mathcal{S}_3}$.

51.11) Déduire de tout ce qui précède que Φ est surjectif, puis que $\mathrm{Aut}(\mathrm{SL}(2, \mathbb{F}_3))$ est isomorphe au groupe symétrique $\mathfrak{S}_4$.

52 Groupe dérivé de $\mathrm{SL}(2, \mathbb{Z})$

On note $\Gamma = \mathrm{SL}(2, \mathbb{Z})$ le groupe des matrices 2×2 à coefficients entiers dont le déterminant égale 1. Si x et y sont deux matrices de Γ, on note

$$[x, y] = xyx^{-1}y^{-1}$$

le *commutateur* de x et y. On note aussi $D(\Gamma)$ le groupe dérivé de Γ, qui est le sous-groupe de Γ engendré par ses commutateurs.

— *Les deux matrices* $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *et* $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *engendrent* Γ *; c'est un résultat du cours, on le redit ici.* —

52.1) On note $R = ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$. Calculer l'ordre de S et l'ordre de R.

52.2) Montrer que le groupe Γ est engendré par S et R.

52.3) En déduire que l'image de tout homomorphisme de groupes $\Gamma \longrightarrow \mathbb{C}^\times$ est incluse dans le groupe $\mathbb{U}_{12}$ des racines douzièmes de l'unité.

52.4) On note A et B les deux matrices de Γ

$$A = [S, R] = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{et} \quad B = [S^{-1}, R^{-1}] = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Montrer que le sous-groupe $\langle A, B\rangle$ de Γ engendré par A et B est inclus dans $D(\Gamma)$.

52.5) Montrer que $\langle A, B\rangle$ est un sous-groupe distingué de Γ.
[Pas si simple ! On pourra par exemple montrer, en passant, que $RAR^{-1} = A^{-1}B$.]

52.6) Montrer que $AST^3 = B$. En déduire que $\Gamma = \langle A, B, T\rangle$.

52.7) Montrer que le groupe quotient $\Gamma/\langle A, B\rangle$ est monogène.

52.8) Montrer que si G est un groupe dont on note $D(G)$ le groupe dérivé et si H est un sous-groupe distingué de G dont le quotient G/H est abélien, alors $D(G) \subseteq H$.
[On pourra considérer l'image de $D(G)$ par la projection canonique $G \to G/H$.]

52.9) En déduire que $D(\Gamma) = \langle A, B\rangle$.

52.10) Montrer que $\left[A, B^{-1}\right] = -T^6$. En admettant que le centre de $D(\Gamma)$ est trivial[♫], en déduire que le quotient $\Gamma/D(\Gamma)$ est isomorphe à $\mathbb{U}_{12}$.

53 Quelques groupes classiques

Si V est un espace vectoriel, on note $\mathbb{P}(V)$ *l'espace projectif* de V qui est l'ensemble de ses droites.

53.1) Si q est la puissance d'un nombre premier, calculer $\operatorname{Card}\mathbb{P}\left(\mathbb{F}_q^n\right)$.

53.2) Montrer que l'action naturelle de $\mathrm{GL}(2, \mathbb{F}_q)$ sur $\mathbb{P}\left(\mathbb{F}_q^2\right)$ induit un homomorphisme injectif de groupes

$$\mathrm{PGL}(2, \mathbb{F}_q) \longrightarrow \mathfrak{S}_{q+1}. \tag{5}$$

53.3) Montrer que les groupes $\mathrm{GL}(2, \mathbb{F}_2)$, $\mathrm{SL}(2, \mathbb{F}_2)$, $\mathrm{PGL}(2, \mathbb{F}_2)$ et $\mathrm{PSL}(2, \mathbb{F}_2)$ sont tous isomorphes à $\mathfrak{S}_3$.

53.4) En appliquant (5), montrer que $\mathrm{PGL}(2, \mathbb{F}_3) \simeq \mathfrak{S}_4$ et que $\mathrm{PSL}(2, \mathbb{F}_3) \simeq \mathfrak{A}_4$.

53.5) Montrer que $\mathrm{SL}(2, \mathbb{F}_3)$ n'est pas isomorphe à $\mathfrak{S}_4$.

53.6) Montrer que $-I_2$ est l'unique élément d'ordre 2 de $\mathrm{SL}(2, \mathbb{F}_3)$, que $\mathrm{SL}(2, \mathbb{F}_3)$ contient un unique 2-Sylow qui est isomorphe à $\mathbb{H}_8$. En déduire un isomorphisme

$$\mathrm{SL}(2, \mathbb{F}_3) \simeq \mathbb{H}_8 \rtimes \mathbb{Z}/3\mathbb{Z}$$

où l'on étudiera l'action sous toutes les coutures.

53.7) Montrer que $\mathrm{GL}(2, \mathbb{F}_3)$ est un produit semi-direct $\mathrm{SL}(2, \mathbb{F}_3) \rtimes \mathbb{Z}/2\mathbb{Z}$.

53.8) Montrer que le centre de $\mathrm{SL}(2, \mathbb{F}_4)$ est trivial et que les groupes $\mathrm{SL}(2, \mathbb{F}_4)$, $\mathrm{PSL}(2, \mathbb{F}_4)$ et $\mathrm{PGL}(2, \mathbb{F}_4)$ sont isomorphes. Montrer que $\mathrm{PSL}(2, \mathbb{F}_4) \simeq \mathfrak{A}_5$.

53.9) On veut montrer que $\mathrm{PSL}(2, \mathbb{F}_5)$ est isomorphe à $\mathfrak{A}_5$.

(i) Soit H un sous-groupe d'indice 6 de $\mathfrak{S}_6$. En faisant agir $\mathfrak{S}_6$ sur l'ensemble des classes à gauche de $\mathfrak{S}_6$ modulo H par translation à gauche, montrer que H est isomorphe à $\mathfrak{S}_5$.
[Montrer, plus généralement, que tout sous-groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$, pour tout $n \geq 3$.]

(ii) En déduire que $\mathrm{PGL}(2, \mathbb{F}_5) \simeq \mathfrak{S}_5$, puis que $\mathrm{PSL}(2, \mathbb{F}_5) \simeq \mathfrak{A}_5$.

[♫] C'est, par exemple, une conséquence du fait que $D(\Gamma)$ est un groupe *libre* à 2 générateurs A et B. Voir par exemple page 31 pour un exemple de technique de preuve de ce type de résultat.

54 Semi-stabilité par conjugaison

On note t et u les deux matrices $t = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ et $u = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, et G le sous-groupe de $\mathrm{SL}(2,\mathbb{Z})$ qu'elles engendrent.

54.1) Calculer l'ordre de t et l'ordre de u dans G.

54.2) On note H le sous-groupe de G engendré par $\{t^n u t^{-n},\ n \in \mathbb{N} \setminus \{0\}\}$. Montrer que H est la réunion de $\{I_2\}$ et de l'ensemble

$$\Big\{ t^{m_0} u^{n_0} t^{m_1} u^{n_1} \dots t^{m_p} u^{n_p} t^{m_{p+1}},\ p \in \mathbb{N},\ (m_0, \dots, m_{p+1}, n_0, \dots, n_p) \in (\mathbb{Z} \setminus \{0\})^{2p+3},\ m_0 \geq 1,\ m_{p+1} \leq -1,\ \sum_{k=0}^{p+1} m_k = 0 \Big\}.$$

54.3) Montrer que $tHt^{-1} \subseteq H$.

L'objet de la suite de cette partie consiste à montrer que $t^{-1}Ht \not\subseteq H$.

54.4) On fait agir G sur l'ensemble $\mathcal{M}_{2,1}$ des vecteurs-colonne de dimension 2 à coefficients réels par l'action naturelle donnée par le produit matriciel :

$$\forall g = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in G,\ \forall v = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathcal{M}_{2,1},\ g \cdot v = \begin{pmatrix} ax + cy \\ bx + dy \end{pmatrix}.$$

On note A et B les parties de $\mathcal{M}_{2,1}$ définies par

$$A = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathcal{M}_{2,1},\ |x| > |y| > 0 \right\} \quad \text{et} \quad B = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathcal{M}_{2,1},\ |y| > |x| > 0 \right\}.$$

Dessiner A et B.

54.5) Montrer que $t^n \cdot B \subseteq A$ et $u^n \cdot A \subseteq B$, pour tout $n \in \mathbb{Z} \setminus \{0\}$.

54.6) Montrer que $h \cdot B \subseteq A$, pour tout $h \in H \setminus \{I_2\}$.

54.7) En déduire que $u \notin H$.

54.8) Montrer que $t^{-1}Ht \not\subseteq H$.

55 Commutateurs de $\mathrm{SO}(3, \mathbb{F}_5)$

55.1 Carrés et commutateurs

Si G est un groupe, on note $D(G)$ son groupe dérivé et $C(G)$ le sous-groupe de G engendré par ses carrés :

$$C(G) = \left\langle \left\{ x^2,\ x \in G \right\} \right\rangle.$$

55.1) Montrer que $C(G)$ et $D(G)$ sont des sous-groupes distingués de G.

55.2) Montrer que le groupe quotient $G/C(G)$ n'a que des éléments d'ordre 1 ou 2. En déduire que $G/C(G)$ est abélien et que, lorsqu'il est fini, il est isomorphe à un groupe produit de la forme $(\mathbb{Z}/2\mathbb{Z})^r$ où $r \in \mathbb{N}$.

55.3) En considérant la projection canonique $G \longrightarrow G/C(G)$, montrer que $D(G) \subseteq C(G)$.

55.4) Montrer que si un groupe G est engendré par ses éléments d'ordre 2, alors $D(G) = C(G)$.

55.2 Sur le groupe $\mathrm{SO}(3,\mathbb{F}_5)$

On note $\mathbb{F}_5$ le corps $\mathbb{Z}/5\mathbb{Z}$. Selon l'usage, on note aussi $\mathrm{O}(3,\mathbb{F}_5)$ le sous-groupe de $\mathrm{GL}(3,\mathbb{F}_5)$ formé des matrices orthogonales et $\mathrm{SO}(3,\mathbb{F}_5)$ son sous-groupe des matrices orthogonales de déterminant 1 :

$$\mathrm{O}(3,\mathbb{F}_5)=\left\{A\in\mathrm{GL}(3,\mathbb{F}_5)\,,\ {}^tA=A^{-1}\right\}\ \text{ et }\ \mathrm{SO}(3,\mathbb{F}_5)=\left\{A\in\mathrm{O}(3,\mathbb{F}_5)\,,\ \det(A)=1\right\}.$$

On note également V le $\mathbb{F}_5$-espace vectoriel des vecteurs-colonne à 3 lignes et à coefficients dans $\mathbb{F}_5$. On note enfin q la forme quadratique standard sur V et $\langle\cdot|\cdot\rangle$ sa forme polaire, définies par : $\forall(x,y,z)\in(\mathbb{F}_5)^3$, $\forall(x',y',z')\in(\mathbb{F}_5)^3$,

$$q\begin{pmatrix}x\\y\\z\end{pmatrix}=x^2+y^2+z^2\ \text{ et }\ \left\langle\begin{pmatrix}x\\y\\z\end{pmatrix}\,|\,\begin{pmatrix}x'\\y'\\z'\end{pmatrix}\right\rangle=xx'+yy'+zz'.$$

Si v et w sont dans V, on dit que v est *unitaire* lorsque $q(v)=1$ et que v et w sont *orthogonaux* lorsque $\langle v|w\rangle=0$.

On admettra — ou non, c'est élémentaire — que pour toute $A\in\mathrm{GL}(3,\mathbb{F}_5)$, les assertions suivantes sont équivalentes :

(i) A est orthogonale

(ii) $q(Av)=q(v)$, pour tout $v\in V$

(iii) les vecteurs-colonne de A sont unitaires et deux à deux orthogonaux.

Par exemple, si on note

$$D_2=\begin{pmatrix}-1&0&0\\0&1&0\\0&0&-1\end{pmatrix},\ R=\begin{pmatrix}1&0&0\\0&0&-1\\0&1&0\end{pmatrix},\ P=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix},\ T=\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}\ \text{ et }\ M=\begin{pmatrix}2&1&1\\1&2&1\\1&1&2\end{pmatrix},$$

alors D_2, R, P, $-T$ et $-M$ sont dans $\mathrm{SO}(3,\mathbb{F}_5)$.

Pour finir, on admet — ou non, c'est un calcul élémentaire — que les vecteurs unitaires de V sont ceux de la liste suivante :

$$\pm{}^t(1,0,0),\ \ \pm{}^t(0,1,0),\ \ \pm{}^t(0,0,1),{}^t(\pm2,\pm1,\pm1),\ {}^t(\pm1,\pm2,\pm1),\ \text{et}\ \ {}^t(\pm1,\pm1,\pm2).$$

55.5) On note $e_1={}^t(1,0,0)$. On note aussi

$$S=\left\{A\in\mathrm{SO}(3,\mathbb{F}_5)\,,\ \exists x\in\mathbb{F}_5,\ Ae_1=xe_1\right\}\ \text{ et }\ F=\left\{A\in\mathrm{SO}(3,\mathbb{F}_5)\,,\ Ae_1=e_1\right\}.$$

On admettra — ou non, c'est un calcul élémentaire — que S est le sous-groupe de $\mathrm{SO}(3,\mathbb{F}_5)$ engendré par D_2 et R.

(i) Montrer que le groupe engendré par R est distingué dans S.

(ii) En déduire l'ordre de S.

(iii) Faire la liste des éléments de S et en déduire que F est le sous-groupe de S engendré par R.

55.6) Montrer que l'action naturelle de $\mathrm{GL}(3,\mathbb{F}_5)$ sur V induit une action transitive de $\mathrm{SO}(3,\mathbb{F}_5)$ sur l'ensemble des vecteurs unitaires de V.

55.7) En déduire que $|\mathrm{SO}(3,\mathbb{F}_5)|=120$.

55.8) On admet encore — ou non, c'est un calcul élémentaire — que $S=\left\{A\in\mathrm{SO}(3,\mathbb{F}_5)\,,\ AR^2=R^2A\right\}$. Montrer que $\mathrm{SO}(3,\mathbb{F}_5)$ contient exactement 15 matrices d'ordre 2 conjuguées à R^2.

55.9) On admet enfin — ou non, c'est un calcul élémentaire — que le groupe des matrices de $\mathrm{SO}(3,\mathbb{F}_5)$ qui commutent avec P est le sous-groupe de $\mathrm{SO}(3,\mathbb{F}_5)$ engendré par P et $-M$. Démontrer que ce groupe est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ et en déduire le nombre de matrices de $\mathrm{SO}(3,\mathbb{F}_5)$ qui sont conjuguées à P.

55.10) On admet — ça, ce n'est pas si simple — que $-M\in\mathrm{SO}(3,\mathbb{F}_5)\setminus D(\mathrm{SO}(3,\mathbb{F}_5))$. On admet enfin — c'est à la fois classique et élémentaire, comparer au cours sur le groupe orthogonal euclidien — que $\mathrm{SO}(3,\mathbb{F}_5)$ est engendré par ses éléments d'ordre 2.

(i) Montrer que l'ordre du groupe $\mathrm{SO}(3,\mathbb{F}_5)/D(\mathrm{SO}(3,\mathbb{F}_5))$ est dans l'ensemble $\{2,4,8\}$.

(ii) Montrer que P est dans $D(\mathrm{SO}(3,\mathbb{F}_5))$.

(iii) En déduire[♫] que $\mathrm{SO}(3,\mathbb{F}_5)/D(\mathrm{SO}(3,\mathbb{F}_5))\simeq\mathbb{Z}/2\mathbb{Z}$.

[♫] La situation est bien différente du cas réel puisque $\mathrm{SO}(3,\mathbb{R})$ est simple, égal à son groupe des commutateurs.

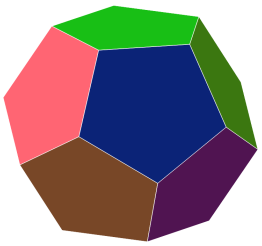
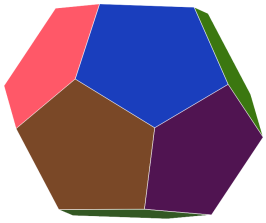
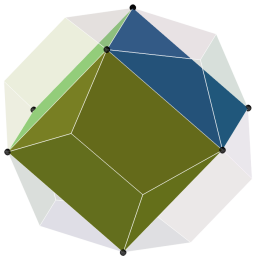
56 Tétraèdre, cube (et octaèdre), icosaèdre (et dodécaèdre)

Pour mieux se représenter les polyèdres réguliers et leurs isométries, on pourra se référer aux dessins des toutes dernières pages de cette liste d'exercices.

56.1) On note $\mathcal{T}$ le groupe des isométries (vectorielles) qui stabilisent un tétraèdre régulier de $\mathbb{R}^3$ et $\mathcal{T}^+$ son sous-groupe positif. En faisant agir $\mathcal{T}^+$ sur les sommets du tétraèdre, montrer que $\mathcal{T}^+ \simeq \mathfrak{A}_4$, puis que $\mathcal{T} \simeq \mathfrak{S}_4$. En passant, faire la liste des 24 isométries de $\mathcal{T}$.

56.2) On note $\mathcal{C}$ le groupe des isométries (vectorielles) qui stabilisent un cube de $\mathbb{R}^3$ et $\mathcal{C}^+$ son sous-groupe positif. En faisant agir $\mathcal{C}^+$ sur les diagonales du cube, montrer que $\mathcal{C}^+ \simeq \mathfrak{S}_4$, puis que $\mathcal{C} \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$. En passant, faire la liste des 48 isométries de $\mathcal{C}$.

56.3) On note $\mathcal{I}$ le groupe des isométries (vectorielles) qui stabilisent un dodécaèdre régulier de $\mathbb{R}^3$ et $\mathcal{I}^+$ son sous-groupe positif. En faisant agir $\mathcal{I}^+$ sur les cinq cubes inscrits dans le dodécaèdre, montrer que $\mathcal{I}^+ \simeq \mathfrak{A}_5$, puis que $\mathcal{C} \simeq \mathfrak{A}_5 \times \mathbb{Z}/2\mathbb{Z}$. En passant, faire la liste des 120 isométries de $\mathcal{I}$.

57 Sous-groupes finis de $\mathrm{GL}(2,\mathbb{R})$ et de $\mathrm{GL}(3,\mathbb{R})$

Soit n un entier naturel non nul.

57.1) Soit V un espace euclidien de dimension n. Se rappeler pourquoi V admet toujours une base orthonormée et en quoi cela implique que le groupe $\mathrm{O}(V)$ est isomorphe à $\mathrm{O}(n)$.

57.2) Soit G un sous-groupe fini de $\mathrm{GL}(n,\mathbb{R})$. On note $\langle\cdot|\cdot\rangle$ le produit scalaire standard sur $\mathbb{R}^n$, ou plutôt sur $\mathcal{M}_{n,1}(\mathbb{R})$. En considérant l'application bilinéaire $\langle\cdot|\cdot\rangle_G$ sur $\mathcal{M}_{n,1}(\mathbb{R})$ définie par

$$\forall X, Y \in \mathcal{M}_{n,1}(\mathbb{R}),\ \langle X|Y\rangle_G = \frac{1}{|G|}\sum_{g\in G}\langle gX|gY\rangle,$$

montrer que G est isomorphe — et même conjugué — à un sous-groupe fini de $\mathrm{O}(n)$.

57.3) Montrer que tout sous-groupe fini de $\mathrm{GL}(2,\mathbb{R})$ est cyclique ou isomorphe à un groupe diédral.

[On sait par ailleurs, c'est dans le cours, que le groupe direct d'un n-gone régulier est cyclique d'ordre n et que son groupe total est diédral d'ordre $2n$.]

57.4) Soient G un sous-groupe fini non trivial de $\mathrm{SO}(3)$ et S^2 la sphère unité de $\mathbb{R}^3$ — ou plutôt de $\mathcal{M}_{3,1}(\mathbb{R})$.

(i) On note X l'ensemble des points de S^2 qui sont fixés par au moins un élément de $G \setminus \{I_3\}$. Montrer que X est fini et que l'action naturelle de G sur $\mathbb{R}^3$ induit une action de G sur X.

(ii) Pour chaque orbite ω pour l'action de G sur X de la question précédente, on note n_ω l'ordre commun des groupes d'isotropie des éléments de ω. On note aussi Ω l'ensemble des orbites de cette action. En calculant de deux façons le cardinal de l'ensemble fini

$$\mathcal{I} = \left\{(g,x) \in (G\setminus\{I_3\}) \times S^2,\ gx = x\right\},$$

montrer que

$$2\left(1 - \frac{1}{|G|}\right) = \sum_{\omega\in\Omega}\left(1 - \frac{1}{n_\omega}\right). \tag{6}$$

(iii) En remarquant d'abord que tous les n_ω sont supérieurs ou égaux à 2 et donc que Ω n'a pas plus de trois éléments, résoudre l'équation arithmétique (6) en montrant que ses solutions sont celles du tableau suivant.

$\lvert G\rvert$	$\#\Omega$	n_1	n_2	n_3
$n \geq 2$	2	n	n	
$2n, n \geq 2$	3	2	2	n
12	3	2	3	3
24	3	2	3	4
60	3	2	3	5

[On peut montrer, par ailleurs, que ces différents cas sont tous atteints par une unique classe de conjugaison de sous-groupes de SO(3). Notamment, les trois dernières lignes du tableau correspondent aux groupes positifs du tétraèdre, du cube (ou de l'octaèdre) et de l'icosaèdre (ou du dodécaèdre). Pour les deux premières lignes, le groupe se représente comme le groupe des rotations d'un polygone régulier à n sommets qui est cyclique d'ordre n (les deux orbites de points fixes, qui sont des singletons, sont diamétralement opposées sur l'axe orthogonal au plan du polygone) ; pour la deuxième ligne qui correspond au groupe diédral, il s'agit d'ajoindre à ce groupe cyclique une rotation d'angle π qui échange les deux points antipodaux — son axe est n'importe laquelle des droites engendrées par l'un des points fixes de l'orbite à n éléments.]

58 Un peu de topologie de groupes linéaires

Soit n un entier naturel non nul. Les groupes de matrices évoqués ci-dessous sont des sous-ensembles d'espaces vectoriels normés de dimension finie $\mathcal{M}_n(\mathbb{R})$ ou $\mathcal{M}_n(\mathbb{C})$. La topologie à laquelle il est fait référence est leur topologie usuelle, à savoir la topologie des normes.

58.1) Montrer que $\mathrm{SO}(n)$ est compact et connexe par arcs (donc connexe).

58.2) Montrer que $\mathrm{GL}(n, \mathbb{C})$ est connexe par arcs, mais que $\mathrm{GL}(n, \mathbb{R})$ a deux composantes connexes.

58.3) Montrer que $\mathrm{SU}(2)$ est compact, connexe et simplement connexe.

59 Du groupe modulaire, vers les pavages hyperboliques

On note S, T et U les matrices de $\mathrm{SL}(2, \mathbb{Z})$

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad U = TS = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix},$$

et s, t et u leurs classes respectives dans $\mathrm{PSL}(2, \mathbb{Z})$.

59.1) On note $\mathcal{H} = \{z \in \mathbb{C},\ \mathrm{im}(z) > 0\}$ le demi-plan de Poincaré. Montrer que $\mathrm{PSL}(2, \mathbb{Z})$ agit fidèlement *par homographies* sur $\mathcal{H}$, *via* la formule

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

59.2) Soit $g \in \mathrm{PSL}(2, \mathbb{Z})$. Montrer que le nombre entier $|\mathrm{Tr}(g)|$ est bien défini et que les assertions suivantes sont équivalentes :

(i) g a au moins un point fixe dans $\mathcal{H}$

(ii) g a un unique point fixe dans $\mathcal{H}$

(iii) $|\mathrm{Tr}(g)| \in \{0, 1\}$.

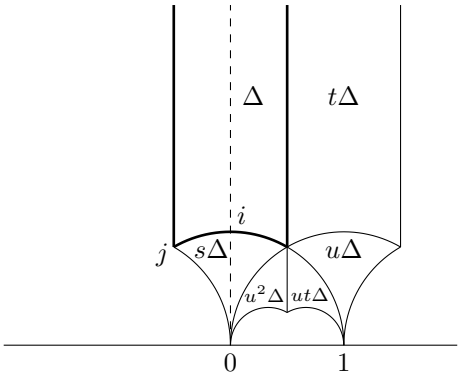
59.3) Soit $\Delta = \left\{z \in \mathbb{C},\ |z| > 1 \text{ et } |\Re z| < \frac{1}{2}\right\}$. Montrer que Δ est un *domaine fondamental* de l'action de $\mathrm{PSL}(2, \mathbb{Z})$ sur $\mathcal{H}$, au sens où :

(i) Δ est un ouvert connexe de $\mathcal{H}$;

(ii) $\forall g, g' \in \mathrm{PSL}(2,\mathbb{Z})$, $g\Delta \cap g'\Delta \neq \emptyset \Rightarrow g = g'$;

(iii) $\mathcal{H} = \bigcup_{g\in \mathrm{PSL}(2,\mathbb{Z})} g\overline{\Delta}$.

En outre, trouver une partie $\widetilde{\Delta}$ de $\overline{\Delta}$ qui soit un système de représentants de l'action de $\mathrm{PSL}(2,\mathbb{Z})$ sur $\mathcal{H}$.



[Pour (iii), si $z \in \mathcal{H}$, on pourra d'abord montrer que l'ensemble des $g \in \mathrm{PSL}(2,\mathbb{Z})$ tels que $\Im(gz) \geq \Im(z)$ est fini, puis translater par une puissance de t un point de l'orbite de z dont la partie imaginaire est maximale.]

59.4) Calculer les ordres de s et u dans $\mathrm{PSL}(2,\mathbb{Z})$ et montrer que

$$\mathrm{PSL}(2,\mathbb{Z}) = \langle s, u \rangle .$$

59.5) *Où l'on montre que tout élément de* $\mathrm{PSL}(2,\mathbb{Z})$ *s'écrit* de manière unique *sous la forme d'un produit*

$$\begin{array}{lll} & (su^{a_1})(su^{a_2})\dots(su^{a_n}) & (i) \\ \text{ou} & u^{a_0}(su^{a_1})(su^{a_2})\dots(su^{a_n}) & (ii) \\ \text{ou} & (su^{a_1})(su^{a_2})\dots(su^{a_n})\,s & (iii) \\ \text{ou} & u^{a_0}(su^{a_1})(su^{a_2})\dots(su^{a_n})\,s & (iv) \end{array} \tag{7}$$

où $n \geq 0$ *et* $a_k \in \{1,2\}$*, pour tout* $k \in \{0,\dots n\}$ *— si* $n = 0$*, le produit* $(su^{a_1})(su^{a_2})\dots(su^{a_n})$ *désigne le neutre de* $\mathrm{PSL}(2,\mathbb{Z})$*. Autrement dit, il n'y a aucune relation entre* s *et* u*.*

(i) Montrer que l'application $\left(\begin{pmatrix} a & c \\ b & d \end{pmatrix}, x\right) \mapsto \begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot x = \frac{ax+c}{bx+d}$ définit une action de $\mathrm{PSL}(2,\mathbb{Z})$ sur $\mathbb{R} \setminus \mathbb{Q}$.

(ii) On note $\mathcal{P}$ l'ensemble des irrationnels strictement positifs et et $\mathcal{N}$ l'ensemble des irrationnels strictement négatifs. Montrer que $s \cdot \mathcal{P} \subseteq \mathcal{N}$, que $u \cdot \mathcal{N} \subseteq \mathcal{P}$ et que $u^2 \cdot \mathcal{N} \subseteq \mathcal{P}$. En déduire qu'un produit de la forme (7) ne peut être trivial que s'il vient de de (7)(i) avec $n = 0$.

(iii) Montrer l'unicité de l'écriture sous la forme (7) attendue[♫].

59.6) Montrer que dans $\mathrm{PSL}(2,\mathbb{Z})$, le produit de deux commutateurs n'est en général pas un commutateur.

59.7) On note $\Gamma(2)$ le sous-groupe (distingué) de $\mathrm{PSL}(2,\mathbb{Z})$ formé des classes de matrices de $\mathrm{SL}(2,\mathbb{Z})$ qui valent I_2 modulo 2 (voir feuille d'exercices numéro 2). Montrer que

$$\mathrm{PSL}(2,\mathbb{Z})/\Gamma(2) \simeq \mathfrak{S}_3.$$

59.8) Montrer que $\mathcal{R}_2 = \{1, s, t, ut, u, u^2\}$ est un système de représentants des classes d'éléments de $\mathrm{PSL}(2,\mathbb{Z})$ modulo $\Gamma(2)$, stable par passage à l'inverse.

59.9) On note Δ_2 l'intérieur (topologique) de $\bigcup_{g\in\mathcal{R}_2} g\cdot\Delta$ — voir le dessin ci-dessus. Montrer que Δ_2 est un domaine fondamental de l'action de $\Gamma(2)$ sur $\mathcal{H}$, au sens où :

(i) Δ_2 est un ouvert connexe de $\mathcal{H}$;

(ii) $\forall g, g' \in \Gamma(2)$, $g\Delta_2 \cap g'\Delta_2 \neq \emptyset \Rightarrow g = g'$;

(iii) $\mathcal{H} = \bigcup_{g\in\Gamma(2)} g\overline{\Delta_2}$.

[♫] L'unicité de cette écriture montre que le groupe modulaire $\mathrm{PSL}(2,\mathbb{Z})$ est le *produit libre* des groupes $\langle s \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ et $\langle u \rangle \simeq \mathbb{Z}/3\mathbb{Z}$. Cette notion est fondamentale dans l'étude de la topologie des variétés ou encore dans ce qui gravite autour des pavages hyperboliques du demi-plan de Poincaré.

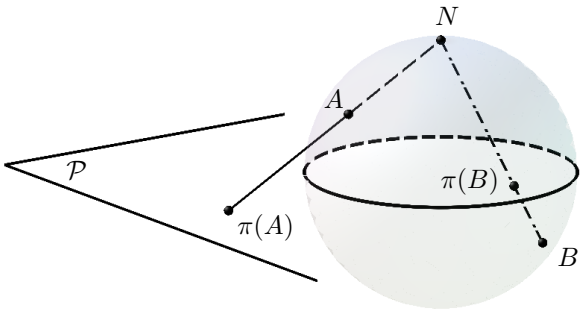
60 Projection stéréographique et revêtement double $\mathrm{SU}(2) \to \mathrm{SO}(3)$

On note S^2 la sphère unité de l'espace euclidien standard $\mathbb{R}^3$:

$$S^2 = \left\{(x,y,z) \in \mathbb{R}^3,\ x^2+y^2+z^2 = 1\right\}$$

et $N = (0,0,1)$ son pôle nord.

60.1) On appelle *projection stéréographique* la projection de S^2 sur son plan équatorial : si $M \in S^2 \setminus \{N\}$, le projeté $\pi(M)$ de M est l'intersection de la droite (NM) avec le plan équatorial $\mathcal{P} = \left\{(x,y,z) \in \mathbb{R}^3,\ z = 0\right\}$. Par ailleurs, on identifie le plan équatorial au plan complexe au moyen de l'isométrie $i : \mathcal{P} \to \mathbb{C}$, $(x,y,0) \mapsto x+iy$. On la note $p : S^2 \to \mathbb{C}$ la composée de la projection stéréographique et de l'isométrie i. Calculer $p(x,y,z)$, pour tout $(x,y,z) \in S^2 \setminus \{N\}$.



60.2) Montrer que p est un homéomorphisme

$$p : S^2 \setminus \{N\} \longrightarrow \mathbb{C}$$

dont on calculera la réciproque. Montrer que $\lim_{|z|\to+\infty} p^{-1}(z)$ existe et vaut N. En déduire que p se prolonge en une bijection

$$p : S^2 \longrightarrow \mathbb{C} \cup \{\infty\}$$

où le symbole ∞ désigne l'image de N par p.

[Il n'est pas difficile de prolonger la topologie usuelle de $\mathbb{C}$ en une topologie de $\mathbb{C} \cup \{\infty\}$ qui fasse de p une homéomorphisme entre les deux compacts S^2 et $\mathbb{C} \cup \{\infty\}$. Le bon cadre pour décrire cet homéomorphisme consiste à remplacer l'artificiel $\mathbb{C} \cup \{\infty\}$ par la droite projective complexe qui est l'ensemble des droites du $\mathbb{C}$-espace vectoriel $\mathbb{C}^2$. On choisit de ne pas en parler davantage ici.]

60.3) On munit le $\mathbb{C}$-espace vectoriel $\mathbb{C}^2$ de son produit hermitien standard

$$\langle (x,y)|(z,t)\rangle = \overline{x}y + \overline{z}t,$$

dont la *norme* est l'application $\mathbb{C}^2 \to \mathbb{R}_+$, $(x,y) \mapsto \|(x,y)\| = \sqrt{\langle (x,y)|(x,y)\rangle} = \sqrt{|x|^2+|y|^2}$. Un endomorphisme u de $\mathbb{C}^2$ est dit *unitaire* lorsque c'est une isométrie pour cette norme, c'est-à-dire lorsque $\|u(v)\| = \|v\|$, pour tout $v \in \mathbb{C}^2$. On note $\mathrm{SU}\left(\mathbb{C}^2\right)$ l'ensemble des endomorphismes unitaires de $\mathbb{C}^2$ dont le déterminant égale 1. Montrer que $\mathrm{SU}\left(\mathbb{C}^2\right)$ est un sous-groupe de $\mathrm{SL}\left(\mathbb{C}^2\right)$.

60.4) Soit u un endomorphisme de $\mathbb{C}^2$. Montrer que les assertions suivantes sont équivalentes.

(i) u est unitaire

(ii) Dans toute base orthonormée de $\mathbb{C}^2$, la matrice M de u vérifie $M\,{}^t\overline{M} = I_2$

(iii) Il existe une base orthonormée de $\mathbb{C}^2$ dans laquelle la matrice M de u vérifie $M\,{}^t\overline{M} = I_2$.

60.5) Si $M \in \mathcal{M}_2(\mathbb{C})$, la matrice ${}^t\overline{M}$ est appelée *transconjuguée* de M. Vérifier rapidement que ${}^t\left(\overline{M}\right) = \overline{{}^tM}$. Une matrice inversible dont l'inverse égale sa transconjuguée est dite *unitaire*. Montrer que l'ensemble $\mathrm{SU}(2)$ des

matrices 2×2 unitaires est un sous-groupe de $\mathrm{SL}(2,\mathbb{C})$, (non canoniquement) isomorphe au groupe $\mathrm{SU}(\mathbb{C}^2)$, et que toute matrice de SU(2) s'écrit sous la forme $\begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix}$ où $u, v \in \mathbb{C}$ vérifient $|u|^2 + |v|^2 = 1$.

60.6) On note $\mathrm{SO}(\mathbb{R}^3)$ le groupe des rotations de l'espace euclidien $\mathbb{R}^3$. Montrer que l'action naturelle de $\mathrm{SO}(\mathbb{R}^3)$ sur $\mathbb{R}^3$ induit une action fidèle et transitive de $\mathrm{SO}(\mathbb{R}^3)$ sur S^2.

60.7) Avec les conventions usuelles sur le maniement du symbole ∞, montrer que l'application

$$\begin{array}{ccc} \mathrm{SU}(2) \times \mathbb{C} \cup \{\infty\} & \longrightarrow & \mathbb{C} \cup \{\infty\} \\ \left(\begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix}, z \right) & \longmapsto & \dfrac{uz - \overline{v}}{vz + \overline{u}} \end{array}$$

définit une action transitive de SU(2) sur $\mathbb{C} \cup \{\infty\}$ — c'est l'action *par homographies*. Calculer le noyau de l'homomorphisme de groupes $\mathrm{SU}(2) \to \mathfrak{S}_{\mathbb{C}\cup\{\infty\}}$, $g \mapsto \sigma_g$ que cette action définit.

60.8) Soit $\Phi : \mathrm{SU}(2) \to \mathfrak{S}_{S^2}$ l'application définie par $\Phi(g) = p^{-1} \circ \sigma_g \circ p$, pour toute $g \in \mathrm{SU}(2)$. Vérifier que Φ est un homomorphisme de groupes.

60.9) Montrer, par un calcul patient, que pour toute $g \in \mathrm{SU}(2)$, la bijection $\Phi(g)$ est la restriction à S^2 d'une isométrie positive de $\mathbb{R}^3$ et qu'en identifiant toute isométrie de $\mathbb{R}^3$ à sa matrice dans la base canonique, Φ s'écrit : $\forall a, b, c, d \in \mathbb{R}$ vérifiant $a^2 + b^2 + c^2 + d^2 = 1$,

$$\begin{array}{ccc} \mathrm{SU}(2) & \xrightarrow{\Phi} & \mathrm{SO}(3) \\ \begin{pmatrix} a+ib & -c+id \\ c+id & a-ib \end{pmatrix} & \longmapsto & \begin{pmatrix} a^2-b^2-c^2+d^2 & 2(-ab+cd) & 2(ac+bd) \\ 2(ab+cd) & a^2-b^2+c^2-d^2 & 2(-ad+bc) \\ 2(-ac+bd) & 2(ad+bc) & a^2+b^2-c^2-d^2 \end{pmatrix} \end{array} \tag{8}$$

[Ce calcul n'est pas miraculeux et trouve deux interprétations géométriques classiques et néanmoins magnifiques : l'une du côté du corps gauche des quaternions, lié à la géométrie de $\mathbb{R}^3$; l'autre du côté des algèbres de Lie des deux groupes SU(2) et SO(3). On ne s'y attarde pas ici ☺]

60.10) Soient $b, c, d \in \mathbb{R}$ tels que $b^2+c^2+d^2 = 1$. Montrer que les vecteurs-colonne ${}^t(d, c, b)$, ${}^t(-b, 0, d)$ et ${}^t(-c, d, 0)$ sont des vecteurs propres de $\Phi \begin{pmatrix} ib & -c+id \\ c+id & -ib \end{pmatrix}$. En déduire que le $\Phi : \mathrm{SU}(2) \to \mathrm{SO}(3)$ est surjectif.

60.11) Montrer que Φ induit un isomorphisme de groupes $\mathrm{PSL}(2) \xrightarrow{\sim} \mathrm{SO}(3)$.

60.12) Déduire de cet isomorphisme une classification des sous-groupes finis de SU(2) — et aussi de $\mathrm{GL}(2,\mathbb{C})$, à conjugaison près.

61 Commutateurs de GL et SL

Soient n un entier naturel supérieur ou égal à 2 et $\mathbb{F}$ un corps.

61.1) Montrer que $D(\mathrm{SL}(n,\mathbb{F})) = \mathrm{SL}(n,\mathbb{F})$, si $(n,\mathbb{F}) \notin \{(2,\mathbb{F}_2), (2,\mathbb{F}_3)\}$.

61.2) Montrer les assertions suivantes.

(i) $D(\mathrm{SL}(2,\mathbb{F}_2)) = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\rangle \simeq \mathbb{Z}/3\mathbb{Z}$;

(ii) $D(\mathrm{SL}(2,\mathbb{F}_3)) = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \right\rangle \simeq \mathbb{H}_8$.

61.3) Montrer les assertions suivantes.

(i) $D(\mathrm{GL}(n,\mathbb{F})) = \mathrm{SL}(n,\mathbb{F})$, si $(n,\mathbb{F}) \neq (2,\mathbb{F}_2)$;

(ii) $D(\mathrm{GL}(2,\mathbb{F}_2)) = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\rangle \simeq \mathbb{Z}/3\mathbb{Z}$.

62 Conjugués vs isomorphes

Pour tout entier naturel non nul, on note $\mathfrak{S}_n$ le groupe des permutations de l'ensemble $\{1, \dots n\}$ et $\mathfrak{A}_n$ son sous-groupe des permutations paires.

62.1 D'abord dans $\mathfrak{S}_6$

62.1) On note $F = \{\sigma \in \mathfrak{S}_6,\ \sigma(5) = 5 \text{ et } \sigma(6) = 6\}$. Vérifier à toute allure que F est un sous-groupe de $\mathfrak{S}_6$. Montrer que $\{1, 2, 3, 4\}$ est stable par tout élement de F et expliciter un isomorphisme de groupes entre F et $\mathfrak{S}_4$.

62.2) On note $I : \mathfrak{S}_6 \to \{0, 1\}$ la fonction indicatrice du complémentaire de $\mathfrak{A}_6$ dans $\mathfrak{S}_6$. Autrement dit,

$$\forall \sigma \in \mathfrak{S}_6,\ I(\sigma) = \begin{cases} 0 \text{ si } \sigma \in \mathfrak{A}_6 \\ 1 \text{ si } \sigma \notin \mathfrak{A}_6. \end{cases}$$

On note également $G = \left\{\sigma \circ (56)^{I(\sigma)},\ \sigma \in F\right\}$, où (56) désigne comme d'habitude la transposition de $\mathfrak{S}_6$ qui échange les nombres 5 et 6.

(i) Montrer que $I(\sigma\tau) = I(\sigma) + I(\tau)$ [mod 2] pour tous $\sigma, \tau \in \mathfrak{S}_6$.

(ii) Montrer que G est un sous-groupe de $\mathfrak{S}_6$.

(iii) Les groupes F et G sont-ils isomorphes ? Sont-ils conjugués ?

62.2 Elargir au cas général

Montrer que pour tout $n \geq 2$, le groupe $\mathfrak{S}_{n+2}$ contient au moins deux classes de conjugaison de sous-groupes isomorphes à $\mathfrak{S}_n$.

63 Action doublement transitive

Lorsqu'un groupe G agit (à gauche) sur un ensemble X à au moins 2 éléments, on dit que l'action est *doublement transitive* lorsque

$$\forall (x, y, z, t) \in X^4,\ x \neq y \text{ et } z \neq t \implies \exists g \in G,\ g \cdot x = z \text{ et } g \cdot y = t.$$

On dit aussi que G *agit doublement transitivement* sur X.

63.1) Montrer que l'action naturelle du groupe alterné $\mathfrak{A}_4$ sur $\{1, 2, 3, 4\}$ est doublement transitive.

63.2) Soit G un groupe fini agissant doublement transitivement sur un ensemble fini X de cardinal $n \geq 2$. On considère l'action naturelle de G sur X^2, définie par

$$\forall g \in G,\ \forall (x, y) \in X^2,\ g \cdot (x, y) = (g \cdot x, g \cdot y)$$

— vérifier que c'est une action est élémentaire. Montrer que cette action admet exactement deux orbites, qui sont la diagonale $D = \{(x, x),\ x \in X\}$ et son complémentaire $X^2 \setminus D$. En déduire que l'ordre de G est un multiple de $n(n-1)$.

63.3) Soient q la puissance d'un nombre premier et $\mathbb{F}_q$ "le" corps à q éléments, dont on note $\mathbb{F}_q^\times$ le groupe des inversibles. Pour tout $(a, b) \in \mathbb{F}_q^\times \times \mathbb{F}_q$, on note $f_{a,b}$ l'application affine

$$\begin{array}{rccc} f_{a,b} : & \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ & x & \longmapsto & ax + b. \end{array}$$

On note aussi $\mathcal{A} = \left\{f_{a,b},\ a \in \mathbb{F}_q^\times,\ b \in \mathbb{F}_q\right\}$; c'est un sous-groupe du groupe $\mathfrak{S}_{\mathbb{F}_q}$ des permutations de $\mathbb{F}_q$, cela se vérifie aussitôt.

(i) Calculer l'ordre de $\mathcal{A}$.

(ii) Montrer que l'action naturelle de $\mathcal{A}$ sur $\mathbb{F}_q$ — définie par $f \cdot x = f(x)$ pour tous $f \in \mathcal{A}$ et $x \in \mathbb{F}_q$ —, est doublement transitive.

(iii) Montrer que les éléments de $\mathcal{A} \setminus \left\{\mathrm{id}_{\mathbb{F}_q}\right\}$ sont de deux types : ceux qui fixent exactement un élément de $\mathbb{F}_q$ d'un côté, ceux qui ne fixent aucun élément de $\mathbb{F}_q$ de l'autre.

La suite de cette partie consiste à montrer que si un groupe d'ordre $n^2 - n$ agit doublement transitivement sur un ensemble à n éléments, alors n est nécessairement la puissance d'un nombre premier.

63.4) Pour toute la suite, soient n un entier naturel, G un groupe fini d'ordre $n^2 - n$ et X un ensemble à n éléments sur lequel G agit doublement transitivement — on notera que $n \geq 2$, nécessairement.

Montrer que l'action de G sur X est transitive, et en déduire que pour tout $x \in X$, le groupe d'isotropie

$$G_x = \{g \in G,\ g \cdot x = x\}$$

est d'ordre $n - 1$.

63.5) Comme dans la question **2.2)**, on considère l'action naturelle de G sur X^2, qui admet exactement deux orbites, à savoir la diagonale D et $X^2 \setminus D$. Démontrer que le groupe d'isotropie de tout élément de $X^2 \setminus D$ est trivial et en déduire que G est partitionné en ses trois sous ensembles suivants :

- $\{1\}$
- l'ensemble des éléments de G qui fixent un unique point de X
- l'ensemble des éléments de G qui ne fixent aucun point de X.

On note Γ la réunion de $\{1\}$ et des éléments de G qui ne fixent aucun point de X.

63.6) En calculant de deux façons le cardinal de l'ensemble $\{(g, x) \in G \times X,\ g \cdot x = x\}$, montrer que Γ a n éléments.

63.7) Pour tout $g \in G$, on note $\mathrm{CONJ}_G(g)$ sa classe de conjugaison dans G et $C_G(g)$ son centralisateur, défini comme d'habitude par

$$C_G(g) = \{h \in G,\ hg = gh\}.$$

Soit $\gamma \in \Gamma \setminus \{1\}$. Montrer que γ ne commute avec aucun élément de $G \setminus \Gamma$ et qu'il n'est conjugué à aucun élément de $G \setminus \Gamma$. En déduire que

$$C_G(\gamma) = \Gamma \quad \text{et} \quad \mathrm{CONJ}_G(\gamma) = \Gamma \setminus \{1\}.$$

63.8) Déduire de la question précédente les trois assertions suivantes :

- Γ est un sous-groupe de G
- Γ est abélien, d'ordre n
- $\Gamma \triangleleft G$.

63.9) Montrer que n est la puissance d'un nombre premier.

[On pourra montrer, en utilisant la théorie de Sylow, que si p et q sont deux nombres premiers qui divisent n, ils sont égaux.]

64 Classes de congruence de matrices symétriques

On note $\mathcal{M}_2(\mathbb{F}_3)$ l'ensemble des matrices à 2 lignes et 2 colonnes et à coefficients dans le corps $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$. On note $\mathcal{S}$ l'ensemble des matrices symétriques de $\mathcal{M}_2(\mathbb{F}_3)$ et $G = \mathrm{GL}(2, \mathbb{F}_3)$ le groupe des matrices inversibles de $\mathcal{M}_2(\mathbb{F}_3)$. Si $M \in \mathcal{M}_2(\mathbb{F}_3)$, on note ${}^tM$ la transposée de M. Enfin, pour toute $M \in \mathcal{M}_2(\mathbb{F}_3)$ et pour toute $P \in G$, on note

$$P \cdot M = P M {}^t P.$$

64.1) Montrer que l'application

$$\begin{array}{ccc} G \times \mathcal{S} & \longrightarrow & \mathcal{S} \\ (P, M) & \longmapsto & P \cdot M \end{array} \tag{9}$$

définit une action à gauche de G sur $\mathcal{S}$.

64.2) Calculer le cardinal de $\mathcal{S}$ et l'ordre de G.

64.3) Pour toute $S \in \mathcal{S}$, on appelle *classe de congruence de* S l'orbite de S sous l'action de G définie par (9). Montrer que deux matrices d'une même classe de congruence ont le même rang.

64.4) (i) Dans $\mathbb{F}_3$, résoudre l'équation $x^2 + y^2 = 1$ dont x et y sont les inconnues.

(ii) Calculer le groupe d'isotropie de I_2 sous l'action (9) et en déduire que la classe de congruence de I_2 contient 6 éléments.

64.5) On note $D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathcal{S}$.

(i) Dans $\mathbb{F}_3$, résoudre l'équation $x^2 - y^2 = 1$ dont x et y sont les inconnues.

(ii) Calculer le groupe d'isotropie de D sous l'action (9) et en déduire le cardinal de la classe de congruence de D.

64.6) Calculer le groupe d'isotropie de $R = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in \mathcal{S}$ et le cardinal de la classe de congruence de R.

64.7) Montrer que les orbites de R et de $-R$ sont distinctes.

64.8) On dit que deux matrices A et B sont *congruentes* lorsqu'il existe une matrice inversible P telle que $B = PA^tP$. Démontrer soigneusement que toute matrice symétrique de $\mathcal{M}_2(\mathbb{F}_3)$ est congruente à l'une exactement des cinq matrices de la liste :

$$O_2,\ I_2,\ R,\ -R,\ D$$

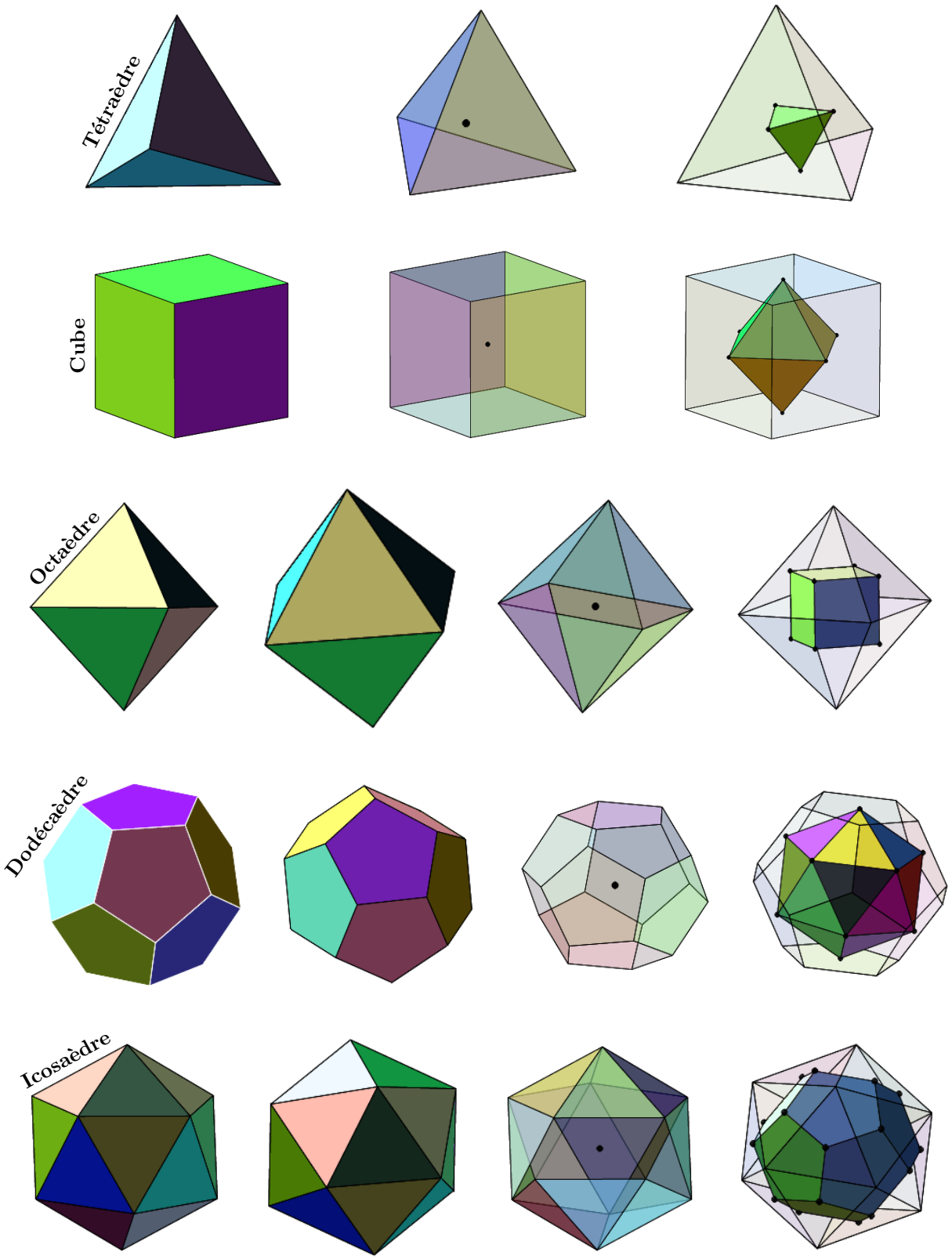
où on a noté O_2 la matrice nulle de $\mathcal{M}_2(\mathbb{F}_3)$.

64.9) (i) Est-il vrai que deux matrices de rang 2 de $\mathcal{S}$ sont toujours congruentes ?

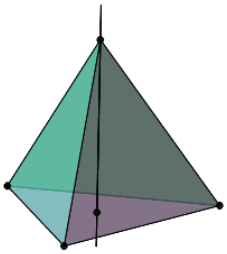
(ii) Est-il vrai que toute matrice de rang 1 de $\mathcal{S}$ est congruente à R ou à $-R$?

(iii) Combien $\mathcal{S}$ contient-il de matrices inversibles ?

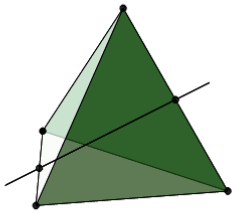
65 Sans paroles : les cinq polyèdres réguliers



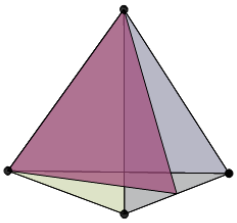
66 Sans paroles : les isométries des polyèdres réguliers



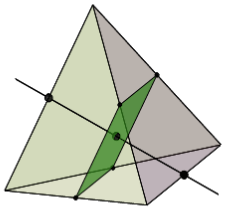
8 rotations



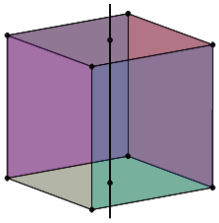
3 rotations



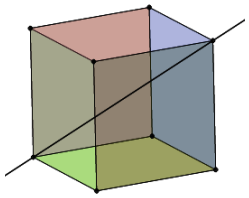
6 symétries



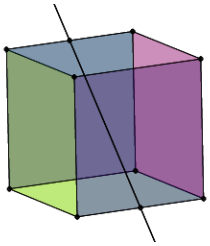
6 anti-rotations



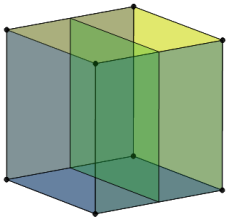
9 rotations



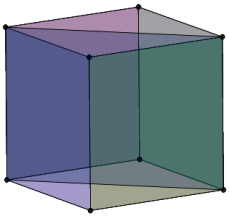
8 rotations



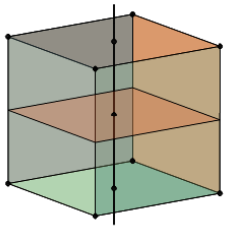
6 rotations



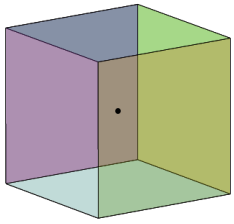
3 symétries



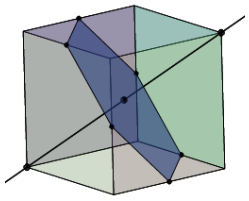
6 symétries



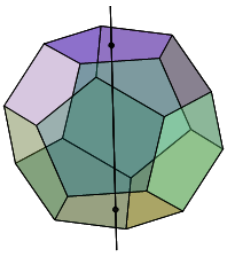
6 anti-rotations



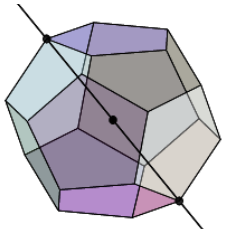
1 anti-rotation
(symétrie centrale)



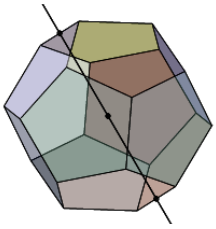
8 anti-rotations



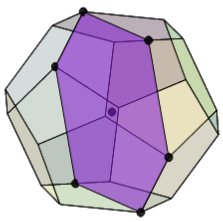
24 rotations



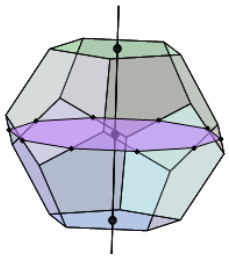
20 rotations



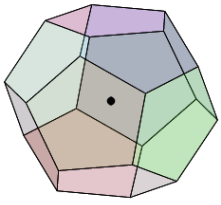
15 rotations



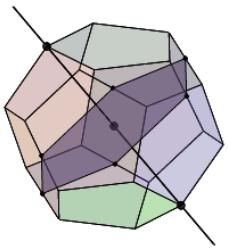
15 symétries



24 anti-rotations



1 anti-rotation
(symétrie centrale)



20 anti-rotations