Agrégation de Mathématiques
Exercices sur les groupes

P. HUBERT

La plupart des exercices ci-dessous se trouvent dans les livres suivants :

- A. Bouvier, D. Richard, Groupes,
- S. Francinou, H. Gianela, Exercices de mathématiques pour l'agrégation (Algèbre 1),
- R. Goblot, thèmes de géométrie (agrégation de mathématiques),
- E. Leichtnam, X. Schaeur, Exercices corrigés de mathématiques posés à l'oral des concours de polytechnique et des écoles normales supérieures (tome 1).
- R. Mneimné, Eléments de géométrie, actions de groupes,
- D. Perrin, Cours d'Algèbre,
- E. Ramis, C. Deschamp, J. Odoux, Cours de mathématiques spéciales (tome 1),
- E. Ramis, C. Deschamp, J. Odoux, Algèbre (exercices avec solutions),

Les énoncés donnés ici sont souvent beaucoup plus détaillés que ceux que l'on que trouve dans les livres, les indications sont mentionnées entre [[ ]]. Les exercices les plus difficiles sont repérés par une $*$ et ceux qui font partie intégrante du cours par un $\diamond$.

Il est nécessaire de faire tous les exercices de la section 1 (qui sont très élémentaires) avant de chercher les autres.

Lorsque ce n'est pas précisé les groupes sont notés multiplicativement et la loi est ., e est l'élément neutre du groupe.

1 Propriétés élémentaires des groupes

Exercice 1: Construire, à isomorphisme près, les groupes à n éléments pour $1 \leq n \leq 4$.

Exercice 2: Soit G un groupe et H une partie finie, non vide, de G stable pour la loi ., montrer que H est un sous-groupe de G.

Exercice 3: Soit G un groupe fini de cardinal n et m un entier premier avec n. Montrer que, pour tout y élément de G, il existe un unique x élément de G tel que $x^m = y$.
[[Utiliser le théorème de Bezout.]]

Exercice 4: Soit $(G, .)$ un groupe fini de cardinal n. On suppose que, tout x élément de G, satisfait l'égalité $x^2 = e$.

1. Montrer que G est un groupe commutatif.
2. Soit $A = \{a_1, \ldots, a_p\}$ une partie génératrice de G, montrer que :
$$\forall x \in G,\ \exists(\varepsilon_1, \ldots, \varepsilon_p) \in (\mathbb{Z}/2\mathbb{Z})^p \text{ tels que, } x = a_1^{\varepsilon_1} \ldots a_p^{\varepsilon_1}.$$
3. On suppose, dans les questions suivantes, que A est une partie génératrice de cardinal minimum p. Montrer que l'écriture :
$$x = a_1^{\varepsilon_1} \ldots a_p^{\varepsilon_1}$$
est unique.
4. Soit Φ l'application définie par :
$$\Phi : \begin{array}{ccc} G & \to & (\mathbb{Z}/2\mathbb{Z})^p \\ x & \mapsto & (\varepsilon_1, \ldots, \varepsilon_p). \end{array}$$
Montrer que Φ est bien définie et que c'est un isomorphisme de groupes. En déduire que le cardinal de G est 2^p.

Exercice 5: Soit p un nombre premier fixé, soit
$$U_p = \{exp(\frac{2i\pi a}{p^\alpha}),\ a \in \mathbb{Z},\ \text{PGCD}(a,p) = 1,\ \alpha \in \mathbb{N}\,\}$$

1. Montrer que U_p est un groupe infini dont tous les éléments sont d'ordre fini. Trouver l'ordre de $exp(\frac{2i\pi a}{p^\alpha})$, pour a entier premier avec p et pour $\alpha \in \mathbb{N}$.
2. Montrer que tout sous-groupe strict de U_p est cyclique.

[[Soit H un sous-groupe de U_p. Montrer tout d'abord que, si $x = exp(\frac{2i\pi a}{p^\alpha})$ appartient à H alors, tout $z = exp(\frac{2i\pi b}{p^\beta})$ avec $\beta \leq \alpha$ appartient à H.]]

Exercice 6: Soit G un groupe.

1. On suppose G muni d'une relation d'ordre noté $\leq$. On suppose de plus que $\leq$ est compatible avec la loi ., c'est-à-dire :
$$\forall a,\ b,\ x \in G,\ a \leq b \Rightarrow \left\{ \begin{array}{ccc} ax & \leq & bx \\ xa & \leq & xb \end{array} \right.$$
On note $\mathcal{P} = \{x \in G,\ x \geq e\}$.

Montrer que :
$$\begin{array}{l} a \leq b \Rightarrow b^{-1} \leq a^{-1} \\ (1)\, \mathcal{P}.\mathcal{P} \subset \mathcal{P} \\ (2)\, \mathcal{P} \cap \mathcal{P}^{-1} = \{e\} \\ (3) \forall x \in G, x\mathcal{P}x^{-1} \subset \mathcal{P} \end{array}$$

2. Réciproquement, étant donné une partie $\mathcal{P}$ de G vérifiant (1), (2), (3), montrer que la relation binaire définie par :

$$\forall a,\, b \in G,\; a \leq b \Leftrightarrow b.a^{-1} \in \mathcal{P}$$

est une relation d'ordre compatible avec . satisfaisant $\mathcal{P} = \{x \in G,\, e \leq x\}$.

Exercice 7: Soit G un groupe et $\Sigma_1, \ldots \Sigma_n$ des morphismes distincts de G dans $(\mathbb{C}^*, \times)$. Montrer que $\Sigma_1, \ldots, \Sigma_n$ sont linéairement indépendants sur $\mathbb{C}$ dans l'espace vectoriel des fonctions de G à valeurs dans $\mathbb{C}$.
[[On pourra faire intervenir une combinaison linéaire des (Σ_i) de cardinal minimum.]]

2 Sous-groupes distingués, groupes quotients

Exercice 8 $\diamond$: [Normalisateur]
Soit H un sous-groupe de G, on appelle normalisateur de H l'ensemble des x éléments de G, tels que $xHx^{-1} = H$; le normalisateur de H est noté N_H.

1. Montrer que N_H est un sous-groupe de G et que H est distingué dans N_H.
2. Soit K un sous groupe de G contenant H et tel que H soit distingué dans K. Montrer que K est un sous-groupe de N_H ; en déduire que N_H est le plus grand sous-groupe de G dans lequel H est distingué.
3. Soit K un sous-groupe de N_H montrer que HK est un groupe et que H est distingué dans HK.
4. Soient H et K deux sous-groupes de G. Montrer que HK est un groupe si et seulement si $HK = KH$.

Exercice 9 $\diamond$:

1. Soit G un groupe, H et K deux sous-groupes de G, on suppose que H est contenu dans le normalisateur de K.

   Montrer que $H \cap K$ est un sous-groupe distingué de H.

   Montrer que $H/(H \cap K)$ est isomorphe à HK/K.

   [[Utiliser le théorème de factorisation des morphismes.]]
2. Soit G un groupe, H et K deux sous-groupes distingués de G tel que K est contenu dans H.

   Montrer que K est distingué dans H.

   Montrer que $(G/K)/(H/K)$ est isomorphe à G/H.

   [[Utiliser le théorème de factorisation des morphismes.]]

Exercice 10:
Soit G un groupe tel que $G/Z(G)$ est cyclique, ($Z(G)$ est le centre de G), montrer que G est abélien.

Exercice 11 $\diamond$: [Sous-groupe dérivé]
Soit G un groupe, on note $D(G)$ (sous-groupe dérivé de G) le sous groupe engendré par :

$$\{xyx^{-1}y^{-1}, \text{ où } x, y \in G\}.$$

1. Montrer que G est abélien si et seulement si $D(G)$ est réduit à l'élément neutre.
2. Montrer que $D(G)$ est invariant par tout automorphisme de G. En déduire que $D(G)$ est un sous-groupe distingué de G.
3. Montrer que $G/D(G)$ est un groupe commutatif.
4. Soit H un sous-groupe de G tel que G/H est commutatif, montrer que $D(G)$ est inclus dans H.

3 Groupes abéliens

Exercice 12 $\diamond$: Soit G un groupe abélien fini, a et b deux éléments de G. On note $O(a)$ l'ordre de a et $O(b)$ l'ordre de b. Le but de l'exercice est de voir quelles sont les valeurs que peut prendre l'ordre de l'élément ab.

1. Soit p entier non nul tel que $(ab)^p = e$, soit m le PPCM de p et $O(a)$, n le PPCM de p et $O(b)$. Montrer que $O(a)$ divise n et que $O(b)$ divise m.
2. En déduire que $O(ab)$ est le PPCM de $O(a)$ et $O(b)$ si aucun facteur premier ne figure à un même exposant non nul dans les décompositions en facteurs premiers de $O(a)$ et $O(b)$.

   En déduire que lorsque $O(a)$ et $O(b)$ sont premiers entre eux, alors $O(ab) = O(a)O(b)$.
3. Montrer que le résultat précédent est faux en général.
4. Notons d le PGCD de $O(a)$ et $O(b)$ et M le PPCM de $O(a)$ et $O(b)$, en utilisant la première question, montrer que :

   $\frac{M}{d}$ divise $O(ab)$ et que $O(ab)$ divise M.
5. En choisissant des éléments convenables dans le groupe $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, vérifier que l'on peut avoir :

$$\frac{M}{d} < O(ab) < M.$$

6. Montrer qu'il existe toujours dans G un élément d'ordre M.

7. Si G est non abélien, donner un exemple où a et b sont d'ordre 2 et où ab est d'ordre infini.

Exercice 13 $\diamond$: [Indicateur d'Euler]
Soit n un nombre entier naturel non nul, on pose :

$$\phi(n) = \text{ card } \{k, 1 \leq k \leq n, \text{ tels que } k \text{ et } n \text{ sont premiers entre eux}\}.$$

Le but de l'exercice est de montrer la formule $(\star)$:

$$\sum_{d/n} \phi(d) = n.$$

[[Soit d un diviseur de n, on montre qu'il y a $\phi(d)$ éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$.]]

1. Soit m un élément d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$, montrer que m appartient au sous-groupe H de $\mathbb{Z}/n\mathbb{Z}$ engendré par $\frac{n}{d}$.
2. Montrer que les éléments d'ordre d dans H sont ceux de la forme : $\frac{kn}{d}$ où k et d sont premiers entre eux.
3. Conclure qu'il y a exactement $\phi(d)$ éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$.
4. Prouver la formule $(\star)$.

Exercice 14 $\diamond$: [Automorphismes de $\mathbb{Z}/n\mathbb{Z}$]
Soit n un entier naturel supérieur ou égal à 2, montrer que le groupe des automorphismes de $\mathbb{Z}/n\mathbb{Z}$ (noté $Aut(\mathbb{Z}/n\mathbb{Z})$) est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$.
[[Considérer l'appplication qui, à un automorphisme ϕ, associe $\phi(1)$ et utiliser le fait que les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les inversibles de $\mathbb{Z}/n\mathbb{Z}$.]]

Exercice 15: Montrer que, pour tout entier naturel non nul n, le groupe additif $\mathbb{Q}/\mathbb{Z}$ possède un seul sous-groupe d'ordre n.
[[Considérer H un sous-groupe de $\mathbb{Q}/\mathbb{Z}$ d'ordre n et Π la projection canonique de $\mathbb{Q}$ dans $\mathbb{Q}/\mathbb{Z}$. En utilisant le fait que les sous-groupes de $\mathbb{R}$ sont soit denses, soit de la forme $a\mathbb{Z}$, montrer que $\Pi^{-1}(H)$ est de la forme $\frac{p}{q}\mathbb{Z}$, avec p et q entiers.]]

Exercice 16* : [Sous-groupes discrets de $\mathbb{R}^n$]
Le but de l'exercice est de montrer qu'un sous-groupe discret de $\mathbb{R}^n$ est isomorphe à $\mathbb{Z}^p$ où p est un entier inférieur ou égal à n.

Plus précisément, étant donné H un sous-groupe discret de $\mathbb{R}^n$, on veut montrer qu'il existe un entier $p \leq n$ et $a_1, \ldots, a_p$ éléments de H linéairement indépendants tels que :

$$H = a_1\mathbb{Z} \bigoplus \ldots \bigoplus a_p\mathbb{Z}.$$

1. On considère E l'espace vectoriel engendré par H et $(e_1, \ldots, e_p)$ une base de E formée d'éléments de H ; on munit E de la norme infini. Montrer que la boule unité de E contient un nombre fini d'éléments de H.
2. Déduire de ce qui précède que $H/(e_1\mathbb{Z} \oplus \ldots \oplus e_p\mathbb{Z})$ est un groupe fini.
3. Montrer qu'il existe un entier m tel que H est inclus dans $\frac{e_1}{m}\mathbb{Z} \oplus \ldots \oplus \frac{e_p}{m}\mathbb{Z}$.
4. Conclure.

4 Groupes de permutations

Exercice 17 $\diamond$ **:** Le but de l'exercice est de montrer que, pour $n \geq 3$, le centre du groupe $\mathcal{S}_n$ ($Z(\mathcal{S}_n)$) est réduit à l'identité.

1. Soit $i \in \{1 \dots n\}$, donner un exemple de permutation s telle que :
$$\begin{cases} s(i) = i \\ \text{et} \\ \forall j \in \{1 \dots n\}, j \neq i \Rightarrow s(j) \neq j. \end{cases}$$
2. Soit $\sigma \in Z(\mathcal{S}_n)$, en utilisant le fait que $s \circ \sigma = \sigma \circ s$, montrer que $\sigma(i) = i$.
3. Déduire du résultat précédent que $\mathcal{S}_n$ n'a pas de sous-groupe distingué d'ordre 2.

Exercice 18 $\diamond$ **:** On dit qu'un groupe G agit sur un ensemble X de façon p transitive si, étant donnés $x_1, \dots, x_p$ éléments de X distincts et $y_1, \dots, y_p$ éléments de X distincts, il existe g élément de G tel que, pour tout i compris entre 1 et p, $g.x_i = y_i$.

1. Montrer que $\mathcal{S}_n$ agit n transitivement sur $\{1, \dots, n\}$.
2. Montrer que $\mathcal{A}_n$ agit $n-2$ transitivement sur $\{1, \dots, n\}$.
3. En déduire que, pour n supérieur ou égal à 5, les 3-cycles sont conjugués dans $\mathcal{A}_n$.

Exercice 19: Soit p et n deux entiers, avec $1 \leq p \leq n$, et s appartenant à S_n définie par :
$$s = \begin{pmatrix} 1 & 2 & \dots & n-p & n-p+1 & \dots & n \\ p+1 & p+2 & \dots & n & 1 & \dots & p \end{pmatrix}$$
On suppose s décomposé en cycles de supports disjoints. Calculer le nombre de cycles, la longueur de chacun d'entre eux. Déterminer un élément dans chaque orbite.
[[Considérer la permutation agissant sur $\mathcal{S}(\mathbb{Z}/n\mathbb{Z})$, montrer que l'orbite de $\overline{0}$ est le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par p. Montrer que ce sous-groupe est aussi engendré par d, le PGCD de n et p.]]

Exercice 20: [Etude du groupe $\mathcal{A}_4$]

1. Faire la liste des éléments de $\mathcal{A}_4$, donner leurs ordres.
2. Soit H l'ensemble formé de l'identité,
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$
Montrer que H est un sous-groupe distingué de $\mathcal{A}_4$ isomorphe au groupe de Klein.

3. Montrer que H est le groupe dérivé de $\mathcal{A}_4$ et que $\mathcal{A}_4$ est un produit semi-direct de H et de $\mathbb{Z}/3\mathbb{Z}$.

4. Montrer que $\mathcal{A}_4$ n'a pas de sous-groupe d'ordre 6.

   [[Raisonner par l'absurde et utiliser le fait qu'un sous-groupe d'indice 2 est distingué.]]

5. Déterminer tous les sous-groupes de $\mathcal{A}_4$, lesquels sont distingués ?

Exercice 21:

1. Soit n un entier supérieur ou égal à 2, montrer que le seul morphisme de groupes non trivial de $\mathcal{S}_n$ dans $(\mathbb{C}^*, \times)$ est la signature.

   [[Montrer que, si l'image d'une transposition par un morphisme est 1 alors le morphisme est constant égal à 1. Utiliser le fait que les transpositions sont conjuguées dans $\mathcal{S}_n$.]]

2. Déduire de la question précédente que le seul sous-groupe de $\mathcal{S}_n$ d'indice 2 est $\mathcal{A}_n$.

3. Supposons $n \geq 5$, montrer que tout sous-groupe H de $\mathcal{S}_n$ d'indice n est isomorphe à $\mathcal{S}_{n-1}$.

   [[Faire agir $\mathcal{S}_n$ sur $\mathcal{S}_n/H$, montrer que l'action est fidèle.

   On peut remarquer que le résultat est vrai pour $n = 3, 4$.]]

5 Action d'un groupe sur un ensemble

Exercice 22 $\diamond$ **:** [Théorème de Cauchy]

Le but de l'exercice est de montrer, qu'étant donné G un groupe fini de cardinal n et p un diviseur premier de n, il existe un élément de G d'ordre p.

1. Soit $\mathcal{A}$ le sous-ensemble de G^p défini par :

$$\mathcal{A} = \{(x_1, \dots, x_p) \in G^p, \text{ tels que } x_1 \dots x_p = e\}.$$

   Montrer que $\mathcal{A}$ est en bijection avec G^{p-1}. En déduire que :

   $\mathrm{card}(\mathcal{A}) = n^{p-1}$.

2. On définit l'application ϕ par :

$$\phi : \begin{array}{ccc} \mathbb{Z}/p\mathbb{Z} \times \mathcal{A} & \to & \mathcal{A} \\ (\overline{k}, (x_1, \dots, x_p)) & \mapsto & (x_{(1+k) mod[p]}, \dots, x_{(p+k) mod[p]}) \end{array}$$

   Montrer que ϕ est bien définie et que c'est une action du groupe $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble $\mathcal{A}$.

3. Soit $(x_1, \ldots, x_p) \in \mathcal{A}$, montrer que le stabilisateur de $(x_1, \ldots, x_p)$ est égal à $\mathbb{Z}/p\mathbb{Z}$ si et seulement si :

   $x_1 = \ldots = x_p$ et x_1 est d'ordre 1 ou p.

4. Appliquer la formule des classes et montrer que le nombre d'éléments d'ordre p de G est congru à -1 modulo p. En déduire qu'il y a, au moins, un élément d'ordre p.

5. Application

   Soit G un groupe fini d'ordre n et p un diviseur premier de n tel que : $\forall x \in G$, $x^p = e$. Montrer qu'il existe un nombre entier k tel que $\text{card}(G) = p^k$.

   [[Supposer que n a un diviseur premier q différent de p et appliquer le théorème de Bezout à p et q.]]

Exercice 23: Soit G un groupe (pas nécessairement fini), et H un sous-groupe de G, d'indice n. Montrer qu'il existe un sous-groupe S de H distingué dans G d'indice divisant $n!$.
[[Faire agir G sur l'ensemble des classes à gauche modulo H et considérer le noyau de l'action.]]

Exercice 24: [Théorème d'Ore]

1. Montrer, de façon élémentaire, que tout sous-groupe d'indice 2 d'un groupe quelconque est distingué.

2. Soit G un groupe fini de cardinal n et p le plus petit diviseur premier de n. Montrer que, si H est un sous-groupe de G d'indice p, alors H est un sous-groupe distingué de G.

   [[Utiliser la même méthode que dans l'exercice précédent, montrer que H est le noyau de l'action, la difficulté est de montrer que H est *contenu* dans le noyau de l'action.]]

Exercice 25: Soit G un groupe fini et H un sous-groupe de G.

1. On note $N(H)$ le normalisateur de H, montrer que l'indice du normalisateur de H est égal au nombre de sous-groupes de G qui sont conjugués à H.

   [[Faire agir G sur ses sous-groupes par conjugaison.]]

2. En déduire qu'il y a un élément de G qui n'est conjugué à aucun élément de H.

   [[Raisonner par l'absurde et utiliser le fait que les sous-groupes conjugués à H ne sont pas disjoints.]]

6 Produits semi-directs

Exercice 26* : Cet exercice donne une condition suffisante pour que 2 produits semi-directs soient isomorphes.

Soient H et N deux groupes et soient ϕ et ψ deux morphismes de H dans $Aut(N)$. On note G le produit semi-direct de N par H au-dessus de ϕ et K celui de N par H au-dessus de ψ.

On suppose qu'il existe $\alpha \in Aut(H)$ tel que $\psi = \phi \circ \alpha$, montrer que G est isomorphe à K.
[[Construire explicitement l'isomorphisme.]]

Exercice 27: [Groupes d'ordre pq]

Soient p et q deux nombres premiers distincts (on supposera $p < q$). Le but de l'exercice est de déterminer tous les groupes d'ordre pq à isomorphisme près.

1. Soit G un groupe de cardinal pq, montrer qu'il y a un seul q Sylow dans G. En déduire qu'il est distingué.

2. Montrer que G est un produit semi-direct de $\mathbb{Z}/q\mathbb{Z}$ et de $\mathbb{Z}/p\mathbb{Z}$.

3. En utilisant l'isomorphisme entre $(Aut(\mathbb{Z}/q\mathbb{Z}), \circ)$, $((\mathbb{Z}/q\mathbb{Z})^*, \times)$ et $(\mathbb{Z}/(q-1)\mathbb{Z}, +)$, montrer que le problème se ramène à étudier les morphismes de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathbb{Z}/(q-1)\mathbb{Z}$.

4. Etant donné a et b deux entiers strictement supérieurs à 1, montrer qu'il existe un morphisme non trivial de $\mathbb{Z}/a\mathbb{Z}$ dans $\mathbb{Z}/b\mathbb{Z}$ si et seulement si a et b ne sont pas premiers entre eux. En déduire qu'il existe un morphisme non trivial de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathbb{Z}/(q-1)\mathbb{Z}$ si et seulement si p divise $q-1$.

5. Montrer que le morphisme trivial correspond au produit direct et que, lorsque p divise $q-1$, tous les produits semi-directs, correspondant à des morphismes non triviaux, sont isomorphes.

   [[On pourra utiliser le résultat de l'exercice précédent.]]

6. Application : Traiter en détail le cas $p = 2$.

Exercice 28* : [Etude des groupes d'ordre 8]

Le but de l'exercice est de déterminer tous les groupes d'ordre 8 à isomorphime près.

Soit G un groupe de cardinal 8.

1. Traiter le cas où G est abélien.

2. Dans les questions suivantes, on suppose que G est non abélien. Montrer qu'il y a forcément un élément d'ordre 4 dans G.

   [[Utiliser le résultat de l'exercice 4 pour montrer que tous les éléments ne peuvent pas être d'ordre 2.]]

3. Soit i un élément d'ordre 4, montrer que le sous-groupe H engendré par i est distingué et qu'on a une suite exacte

$$1 \to \mathbb{Z}/4\mathbb{Z} \to G \to \mathbb{Z}/2\mathbb{Z} \to 1$$

4. Montrer que, si $G \setminus H$ possède un élément d'ordre 2, alors G est un produit semi-direct de $\mathbb{Z}/4\mathbb{Z}$ et de $\mathbb{Z}/2\mathbb{Z}$. Conclure en utilisant la dernière question de l'exercice précédent.

5. Lorsque $G \setminus H$ ne contient que des éléments d'ordre 4, montrer que G est isomorphe au groupe H_8 des quaternions.

   [[Considérer j élément de $G \setminus H$ et $k = ij$ et montrer que ces éléments vérifient les relations classiques des quaternions.]]

Exercice 29: On considère l'ensemble G des matrices de la forme

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

à coefficients dans $\mathbb{Z}/2\mathbb{Z}$.

Montrer que G est un groupe, calculer son cardinal ; à quel groupe connu G est-il isomorphe ?
[[Utiliser l'exercice précédent.]]

7 Groupes et géométrie, groupes de matrices

Exercice 30 $\diamond$: [Groupe diédral D_n]

Le groupe diédral D_n est, à isomorphisme près, le groupe des isométries du plan laissant invariant un polygone régulier convexe à n côtés.

1. Trouver n symétries et n rotations dans D_n.

   [[Etudier séparément le cas n pair et n impair.]]

2. On montre, ci-dessous, que ce sont les seuls éléments de D_n.

   Montrer qu'un élément f de D_n permute les sommets du polygone et qu'il fixe le centre Ω du polygone.

   En déduire, que si f est une rotation, c'est une rotation de centre Ω, et que c'est un des éléments trouvés précédement.

   Faire un raisonnement analogue pour les symétries.

3. Montrer que D_n est un produit semi-direct de $\mathbb{Z}/n\mathbb{Z}$ et de $\mathbb{Z}/2\mathbb{Z}$. Montrer que ce n'est pas un produit direct.

Exercice 31: Soit G le groupe engendré par les deux matrices :

$$T = \begin{pmatrix} \frac{-1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$S = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

Déterminer G (on pourra en donner une interprétation géométrique), calculer son cardinal.

Exercice 32: Soit p un nombre premier et n un nombre entier, on note $F_p = \mathbb{Z}/p\mathbb{Z}$.

1. Calculer le cardinal de $Gl_n(F_p)$.

   [[On pourra remarquer que cela revient à calculer le nombre de bases de l'espace vectoriel $(F_p)^n$.]]

2. En déduire le cardinal de $Sl_n(F_p)$.

3. On note $PGl_n(F_p)$ le quotient de $Gl_n(F_p)$ par son centre. Déduire, de la première question, le cardinal de $PGl_n(F_p)$.

4. On note $P_{n-1}(F_p)$ l'ensemble des droites de l'espace vectoriel $(F_p)^n$. Calculer le cardinal de $P_{n-1}(F_p)$.

Exercice 33* : Cet exercice fait le point sur les isomorphismes remarquables entre certains groupes de permutations et des groupes de matrices.

On utilise les résultats de l'exercice précédent et ceux de l'exercice 21. On note $PSl_2(F_p)$, le quotient de $Sl_2(F_p)$ par son centre.

1. Montrer que $PGl_2(F_3)$ est isomorphe au groupe $\mathcal{S}_4$.

   [[Faire agir $PGl_2(F_3)$ sur $P_1(F_3)$, vérifier que l'action est fidèle et, en déduire, que $PGl_2(F_3)$ s'injecte dans $\mathcal{S}_4$. Conclure en utilisant les cardinaux.]]

2. Montrer que $PSl_2(F_3)$ est isomorphe au groupe $\mathcal{A}_4$.

   [[Faire agir $PSl_2(F_3)$ sur $P_1(F_3)$, vérifier que l'action est fidèle et, en déduire, que $PGl_2(F_3)$ s'injecte dans $\mathcal{S}_4$. En utilisant les cardinaux, montrer que $PSl_2(F_3)$ est isomorphe à un sous-groupe d'indice 2 de $\mathcal{S}_4$. Conclure en utilisant un résultat de l'exercice 21.]]

3. Montrer que $SL_2(F_4)$ est isomorphe à $\mathcal{A}_5$.

   [[Même méthode que précédement, on fait agir $SL_2(F_4)$ sur $P_1(F_4)$ et on remarque que le centre de $SL_2(F_4)$ est réduit à l'identité car F_4 est un corps de caractéristique 2.]]

4. Montrer que $PGL_2(F_5)$ est isomorphe à $\mathcal{S}_5$.

   [[Faire agir $PGL_2(F_5)$ sur $P_1(F_5)$, en déduire que $PGL_2(F_5)$ est un sous-groupe de S_6 et montrer qu'il est d'indice 6. Conclure en utilisant un résultat de l'exercice 21.]]

5. Déduire de la question précédente que $PSL_2(F_5)$ est isomorphe à $\mathcal{A}_5$.

   [[Remarquer que $PSL_2(F_5)$ est un sous groupe d'indice 2 de $PGL_2(F_5)$.]]

Exercice 34:

1. Montrer que le groupe des isométries laissant invariant un tétraèdre régulier est isomorphe à $\mathcal{S}_4$.

   [[Montrer qu'une isométrie qui laisse invariante le tétraèdre permute ses sommets et qu'il y a donc, au plus, 24 éléments dans le groupe. Trouver explicitement suffisamment d'éléments.]]

2. Montrer que le groupe des rotations laissant invariant un cube est isomorphe à $\mathcal{S}_4$.

   [[Faire agir les isométries positives du cube sur les 4 grandes diagonales du cube, en déduire que ce groupe s'injecte dans $\mathcal{S}_4$ et trouver suffisamment d'éléments.]]

Exercice 35: On considère l'ensemble $Aff(\mathbb{R}^n)$ des transformations affines de $\mathbb{R}^n$, c'est-à-dire l'ensemble des applications de la forme $X \mapsto AX + b$, où A appartient à $GL_n(\mathbb{R})$ et b est un élément de $\mathbb{R}^n$.

1. Montrer que $Aff(\mathbb{R}^n)$ est un groupe.

2. Montrer que $Aff(R^n)$ est un produit semi-direct de R^n et $GL_n(\mathbb{R})$.

   [[Introduire le sous-groupe des translations et montrer que c'est un sous-groupe distingué.]]

3. Déterminer le centre de $Aff(\mathbb{R}^n)$.

Exercice 36* : Soit $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$. On considère l'ensemble G des homographies, c'est-à-dire les transformations de $\widehat{\mathbb{C}}$ dans lui-même définie par :

$$\begin{cases} z \mapsto \frac{az+b}{cz+d}, & \text{pour} \quad z \in \mathbb{C},\ z \neq \frac{-d}{c} \\ \frac{-d}{c} \mapsto \infty, & \\ \infty \mapsto \frac{a}{c}, & \end{cases}$$

si $c \neq 0$;

$$\begin{cases} z \mapsto \frac{az+b}{d}, & \text{pour} \quad z \in \mathbb{C} \\ \infty \mapsto \infty, & \end{cases}$$

si $c = 0$,
avec a, b, c, d nombres complexes vérifiant $ad - bc = 1$.

Dans la suite, pour ne pas alourdir les notations, on définira une homographie (appelée aussi transformation de Moebius) uniquement sur $\mathbb{C}$ privé de la pré-image de l'infini. Il est sous-entendu qu'une homographie est une application de $\widehat{\mathbb{C}}$ dans lui-même.

1. Montrer que G est un groupe pour la composition des applications.

2. Montrer que l'ensemble des homographies qui fixent l'infini est le sous-groupe des homothéties-translation à savoir, l'ensemble des homographie de la forme $z \mapsto Az + B$ avec A et B éléments de $\mathbb{C}$.

   Ce sous-groupe est-il distingué ?

3. On note $SL_2(K)$ le groupe des matrices 2×2 à coefficients dans un corps K de déterminant 1. Montrer que le centre de $SL_2(\mathbb{C})$ est égal à $\{\pm id\}$.

4. On note $PSL_2(\mathbb{C})$, le quotient de $SL_2(\mathbb{C})$ par son centre. Montrer que G est isomorphe à $PSL_2(\mathbb{C})$. Dans la suite, on notera f_A, la transformation homographique associée à A.

5. Montrer que l'application Φ :

$$\begin{array}{ccc} PSL_2(\mathbb{C}) \times \widehat{\mathbb{C}} & \rightarrow & \widehat{\mathbb{C}} \\ (A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, z) & \mapsto & \frac{az+b}{cz+d} \end{array}$$

   est une action de $PSL_2(\mathbb{C})$ sur $\widehat{\mathbb{C}}$.

6. Etant donnés (z_1, z_2, z_3), éléments distincts de $\widehat{\mathbb{C}}$, et (w_1, w_2, w_3), éléments distincts de $\widehat{\mathbb{C}}$, montrer qu'il existe une unique transformation homographique qui envoie (z_1, z_2, z_3) sur (w_1, w_2, w_3).

   En d'autres termes, l'action de $PSL_2(\mathbb{C})$ est 3-transitive sur $\widehat{\mathbb{C}}$.

   [[Montrer, tout d'abord, qu'étant donnés (z_1, z_2, z_3), il existe une homographie explicite qui envoie (z_1, z_2, z_3) sur $(O, 1, \infty)$. Pour l'unicité, montrer qu'une homographie qui fixe 0, 1, ∞ est l'identité.]]

7. [Classes de conjugaison dans $PSL_2(\mathbb{C})$]

   Soit A une matrice de $SL_2(\mathbb{C})$ différente de id et $-id$, et f_A, la transformation homographique associée.

   (a) Montrer que, si la trace de A est égale à ± 2, alors f_A est conjuguée dans G à $z \mapsto z + 1$.

   [[Montrer que, lorsque la trace de A vaut 2, la forme de Jordan de A est

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

   et utiliser la question 4.]]

   (b) Lorsque la trace de A est différente de ± 2, montrer que f_A est conjugué dans G à $z \mapsto \lambda z$ avec λ complexe différent de 0 et 1.

   [[On montrera que la matrice A est diagonalisable et que les deux valeurs propres de A sont inverses l'une de l'autre.]]

8. Montrer que les homographies qui laissent invariant le demi-plan $\mathcal{H} = \{z$, tels que $Im(z) > 0\}$, est le groupe K des homographies à coefficients réels (a, b, c, d réels). Montrer que ce groupe est isomorphe à $PSL_2(\mathbb{R})$ (quotient de $SL_2(\mathbb{R})$ par son centre).

   [[Soit f une homographie telle que $f(\mathcal{H}) = \mathcal{H}$, montrer que $f(\mathbb{R}) \subset \mathbb{R} \cup \{\infty\}$ et utiliser la question 6 pour vérifier que les coefficients de f sont réels.]]

   Remarque : L'action de $PSL_2(\mathbb{C})$ est l'action projective des matrices sur la droite projective complexe. Si l'on remarque cela, il évident que G est un groupe et on peut comprendre facilement qu'il est isomorphe au quotient de $GL_2(\mathbb{C})$ par son centre (les matrices diagonales laissant les droites vectorielles globalement invariantes).

   On peut montrer que l'image d'un cercle ou d'une droite par une homographie est un cercle ou une droite et qu'une homographie préserve les bi-rapports. (voir Berger, Géométrie pour toutes ces questions).

   Il est possible d'étudier les classes de conjugaison dans K. (On distinguera 3 cas suivant que l'application a 0,1 ou 2 points fixes dans $\mathbb{R} \cup \{\infty\}$.)