Groupes opérant sur un ensemble et géométrie

Exercice 1

On considère un espace vectoriel E de dimension finie.

1. Le groupe $\mathrm{GL}(E)$ agit naturellement sur E. Cette action est–elle transitive ? Quelles sont ses orbites? Quel est le stabilisateur d'un vecteur u de E ?

2. Mêmes questions pour les actions de $\mathrm{SL}(E)$ et de $\mathrm{O}(E)$, si E est euclidien.

3. Idem pour l'action de $\mathrm{SO}(\mathbb{R}^2)$ sur l'ensemble vecteurs unitaires de $\mathbb{R}^2$ euclidien, puis sur l'ensemble des couples de vecteurs unitaires (action diagonale). Les orbites pour ces couples forment l'ensemble $\mathcal{A}$ des *angles orientés* $(\widehat{u,v})$ *de vecteurs unitaires* du plan.

a. Définir une bijection R de l'ensemble $\mathcal{A}$ de ces angles $(\widehat{u,v})$ sur le groupe abélien $\mathrm{SO}(\mathbb{R}^2)$. Par transport de structure via R, ceci munit $\mathcal{A}$ d'une loi de groupe additif.

b. Montrer la *relation de Chasles* $(\widehat{u,v}) + (\widehat{v,w}) = (\widehat{u,w})$.

c. Si u, u', v, v' sont unitaires dans $\mathbb{R}^2$, montrer que $(\widehat{u,v}) = (\widehat{u',v'})$ ssi $(\widehat{u,u'}) = (\widehat{v,v'})$.

Exercice 2

Soit G un groupe fini opérant transitivement sur un ensemble fini X. On considère un point $x \in X$ et on note H son stabilisateur.

1. Pour $g \in G$, expliciter le stabilisateur du point $g \cdot x$.

2. À quelle condition sur H l'action de G est–elle fidèle ?

3. On dit que G agit *simplement transitivement sur* X si pour tout couple (x, x') dans X^2, il existe un *unique* $g \in G$ tel que $x' = g \cdot x$.

a. Montrer qu'une telle action est fidèle et transitive (noter que réciproquement, l'action de S_3 sur $\{1, 2, 3\}$ n'est *pas* simplement transitive). Montrer que G et X sont en bijection.

b. On suppose G abélien. Montrer que son action sur X est simplement transitive si et seulement si elle est fidèle et transitive.

Deux exemples: **i)** un *espace affine* $\mathcal{E}$ de direction l'espace vectoriel E est un ensemble $\mathcal{E}$ sur lequel le groupe $(E, +)$ agit transitivement et fidèlement, c.a.d. simplement transitivement: pour tous points M, N dans $\mathcal{E}$, il existe un unique $v \in E$ tel que $N = M + v$, ie. $\overrightarrow{MN} = v$, et cela donne un sens à la somme de deux vecteurs $\overrightarrow{MN} + \overrightarrow{M'N'}$; **ii)** de même, on montre exo 1-3 que le groupe abélien $\mathrm{SO}(\mathbb{R}^2)$ agit simplement transitivement sur l'ensemble des vecteurs unitaires de $\mathbb{R}^2$, ce qui fournit le *groupe des angles* de tels vecteurs.

c. Exhiber une action simplement transitive du groupe $\mathrm{GL}_n(\mathbb{F}_q)$ qui permet le calcul du cardinal de ce groupe.

4. Soit K un sous–groupe distingué de G. Montrer que les orbites de X pour l'action de K ont toutes même cardinal.

Donner un contre–exemple dans le cas où K n'est pas distingué.

Exercice 3

Groupe agissant sur $\{1, ..., 10\}$ avec deux orbites et actions prescrites sur ces orbites :

déterminer les sous–groupes G de S_{10} ayant deux orbites ω et ω', tels que $\mathrm{card}\,(\omega) = 4$, $\mathrm{card}\,(\omega') = 6$, et que la restriction de l'action de G sur ω soit d'image isomorphe à $\mathbb{Z}/4\mathbb{Z}$, et celle de l'action de G sur ω' soit d'image isomorphe à $\mathbb{Z}/6\mathbb{Z}$.

Quelques applications à la structure des groupes finis

Exercice 4 *Théorème de Cauchy, preuve de J. McKay*

Soit G un groupe fini d'ordre multiple de p, p un nombre premier. Dans G^p, on considère la partie $S = \{(x_1, \dots, x_p) |\, x_1 \cdots x_p = 1_G\}$.

On fait agir $(\mathbb{Z}/p\mathbb{Z}, +)$ par permutation circulaire sur G^p: pour $\bar{k} \in \mathbb{Z}/p\mathbb{Z}$ et $(x_1, \dots, x_p) \in G^p$, on pose $\bar{k} \cdot (x_1, \dots, x_p) = (x_{1+k}, \dots, x_{p+k})$, où les indices sont vus modulo p: $x_{l+p} = x_l = x_{[l]}$ pour tout l, en notant $[l]$ le représentant de $\bar{l}$ dans $\{1, \dots, p\}$.

1. Montrer que S est stable sous l'action de $\mathbb{Z}/p\mathbb{Z}$. Quelles sont les orbites à 1 élément de S?

2. Calculer le cardinal de S et conclure que G possède au moins un élément d'ordre p.

Exercice 5 *Théorème de Ore (ou Frobenius)*

Soient G un groupe fini, et p le plus petit nombre premier divisant le cardinal de G. On suppose que G possède un sous–groupe H d'indice p.

Montrer que H est distingué dans G (utiliser l'action de G par translation sur le quotient).

Exercice 6

Soit G un groupe fini, p le plus petit nombre premier divisant le cardinal de G. On suppose que G possède un sous–groupe distingué H d'ordre p.

Montrer que H est inclus dans le centre de G.

Exercice 7

Montrer qu'un groupe d'ordre $2n$ avec $n \geq 3$ impair n'est pas simple.

On fera agir G sur lui–même par translation, on regardera l'action d'un élément d'ordre 2 comme élément du groupe de permutation S_G, sa signature, et on conclura que G possède un sous–groupe H d'indice 2 (distingué!) (complément: en considérant l'indice de $H \cap H'$ dans H, montrer l'unicité de H).

Théorèmes de Sylow :

Exercice 8

Soit G un groupe fini, d'ordre $n = p^\alpha m$, où p premier ne divise pas m, et $\alpha \in \mathbb{N}^*$. On se propose de montrer que G possède un sous–groupe d'ordre p^α (dit "p–sous–groupe de Sylow"): c'est le *premier théorème de Sylow*.

On raisonne par récurrence sur l'ordre de G. Le théorème est clair si G est d'ordre p. On suppose dans les questions 1. et 2. que le résultat est vrai pour tout groupe d'ordre $< n$ et multiple de p. On admettra le théorème de Cauchy (voir exo 4) dans le cas où le groupe est *abélien* (la preuve dans ce cas est élémentaire, par exemple par récurrence sur l'ordre).

1. Si G contient un sous–groupe strict dont l'indice est premier à p, justifier que G possède un p–sous–groupe de Sylow.

2. On suppose ici que p divise l'indice de tous les sous–groupes stricts de G.

  a. Écrire l'équation aux classes pour l'action de G par conjugaison sur lui-même, et montrer que le centre de G contient un élément x d'ordre p.

  b. Si $\alpha \geq 2$, justifier que $\langle x \rangle$ est distingué dans G et conclure pour G en utilisant un p–Sylow de $G/\langle x \rangle$.

3. En déduire le premier théorème de Sylow.

Exercice 9

1. Soient H, P des sous–groupes d'un groupe fini G. Soit p un nombre premier divisant card G. On suppose que card $(P) = p^n$ et que $[G : H] = m$ est premier avec p.

Montrer que P est contenu dans un conjugué de H (on fera agir P par translation sur G/H).

2. En déduire que les p–sous–groupes de Sylow de G sont tous conjugués, et que tout p–sous–groupe de G est inclus dans un p–Sylow: c'est le *deuxième théorème de Sylow*.

Exercice 10

1. On note D_4 le groupe des isométries du carré de sommets $\{(\pm 1, \pm 1)\}$ de $\mathbb{R}^2$ euclidien (voir aussi exo12). Montrer que D_4 agit sur l'ensemble $\{A_j | 1 \leq j \leq 4\}$ des 4 sommets. Étudier cette action et énumérer les permutations des 4 sommets obtenues.

2. Montrer que S_4 contient 3 sous–groupes isomorphes à D_4, conjugués. Quelle est leur intersection deux à deux? On reconnaîtra un même sous–groupe distingué de S_4.

Exercice 11

Donner les types d'éléments de A_5 et déterminer leur classe de conjugaison dans A_5. Étudier, pour σ 5–cycle et $k \in \mathbb{N}$, si σ est ou non conjugué à σ^k.

Groupes finis d'isométries (en dimension 2 et 3)

Exercice 12

Déterminer le groupe des isométries du plan qui conservent globalement la partie X suivante:

i) la réunion des axes Ox et Oy

ii) l'ensemble des deux points $(-1, 0)$ et $(1, 0)$

iii) l'ensemble des quatre points $(\pm 1, 0)$ et $\pm(1, 1)$

iv) l'ensemble $\{(\pm 2, \pm 1)\}$ (quatre sommets d'un rectangle)

v) l'ensemble $\mathbb{Z} \times \{0\}$.

Exercice 13 *Groupe diédral, des isométries d'un polygone régulier*

Les polygones à n côtés qui sont *réguliers* sont ceux qui admettent le plus grand groupe "de symétrie" (d'ordre $2n$).

On se fixe un entier $n \geq 3$. On dit qu'un groupe G est *diédral de type D_n*, s'il est engendré par deux éléments r, s tels que: r est d'ordre n, s est d'ordre 2 et $rsrs = 1_G$ (de manière équivalente, $rs = sr^{-1}$).

1. On se place dans le plan euclidien usuel, identifié à $\mathbb{C}$, et on définit les isométries r et s par : $\forall z \in \mathbb{C}, r(z) = e^{2i\pi/n}z, s(z) = \bar{z}$ (r est la rotation d'angle $2\pi/n$ et s est la réflexion d'axe Ox). On note G le sous–groupe $\langle r, s\rangle$ de $\mathrm{O}(\mathbb{R}^2)$.

- **a.** Montrer que G est diédral de type D_n.
- **b.** On considère le polygone convexe régulier à n côtés $\mathcal{P}_n$, de sommets les $\{e^{2ik\pi/n} \mid 0 \leq k \leq n-1\}$. Montrer que le groupe des isométries du plan euclidien qui conservent l'ensemble $\{e^{2ik\pi/n} \mid 0 \leq k \leq n-1\}$ est G (on vérifie que c'est aussi le groupe des isométries du polygone $\mathcal{P}_n$), et que G est d'ordre $2n$. Pour $n = 3$ et $n = 4$, dessiner $\mathcal{P}_n$ les axes des réflexions de son groupe d'isométries.

2. Soit $G = \langle r, s\rangle$ un groupe diédral de type D_n.

a. Montrer que : $G = \{1_G, r, \dots, r^{n-1}\} \cup \{s, sr, \dots, sr^{n-1}\}$ et que G est d'ordre $2n$.

Remarque: le sous–groupe $\langle r \rangle$ est d'indice 2 de G, il est donc distingué, et par suite $s\langle r \rangle = \langle r \rangle s$.

b. Montrer que deux groupes diédraux de type D_n sont isomorphes.

3. Montrer que S_3 est diédral de type D_3 (le groupe du triangle équilatéral).

Exercice 14 *Le groupe des isométries du cube*

Soit $\mathcal{C}$ un cube de $E = \mathbb{R}^3$ centré en l'origine. On numérote les sommets d'une face $A_1, \dots, A_4$, puis on note B_i le sommet opposé de A_i $(1 \leq i \leq 4)$. Les droites $D_i := (A_iB_i)$ sont alors les 4 grandes diagonales du cube. On note G, resp. G^+, le groupe des isométries de $\mathbb{R}^3$ (resp. des rotations) qui laissent globalement invariant l'ensemble des sommets de $\mathcal{C}$; tout élément de G induit une permutation des 8 sommets de $\mathcal{C}$, et il fixe leur isobarycentre (0), c'est donc une isométrie *vectorielle* de $\mathbb{R}^3$.

1. Montrer que G agit naturellement sur l'ensemble $\mathcal{D}$ des grandes diagonales de $\mathcal{C}$. En utilisant la numérotation des D_i, on en déduit un morphisme φ de G dans S_4.

2. Montrer que $\varphi(-\mathrm{id}_E) = \mathrm{id}_{S_4}$ et que $\ker\varphi \cap G^+ = \{\mathrm{id}_E\}$ (on étudiera la restriction d'un élément g du noyau à chaque grande diagonale, on se ramènera au cas où $g_{|D_1} = \mathrm{id}$).

3. Dans cette question on montre que les transpositions sont dans $\varphi(G^+)$. Sans perte de généralité, on cherche $g \in G^+$ telle que $\varphi(g)$ soit la transposition (12). On note I le milieu de l'arête A_1A_2, J le milieu de l'arête B_1B_2 et r le retournement (rotation d'angle π) d'axe (IJ).

Montrer que r est dans G^+, puis que $\varphi(r) = (12)$.

4. Conclure que la restriction de φ à G^+ est un isomorphisme sur S_4.

5. Faire la liste des types de rotations de G^+, en identifiant leur axe et angle, suivant le type de la permutation qu'elles induisent sur $\mathcal{D}$.

6. Notons G^- l'ensemble des isométries négatives de G. Montrer que G^- est l'ensemble des $-g$, où g parcourt G^+.

7. En déduire que G est isomorphe à $G^+ \times \{-\mathrm{id}_E\}$ et donc à $S_4 \times \mathbb{Z}/2\mathbb{Z}$.

8. Reprendre la liste donnée en 5. et donner pour chaque type d'élément g le nombre d'orbites de l'action de $\langle g \rangle$ sur l'ensemble des 6 faces de $\mathcal{C}$ (ceci sert pour dénombrer, à rotation près, les *coloriages* des faces de $\mathcal{C}$ à l'aide d'une palette de q couleurs, voir 17-6).

Exercice 15 *Groupe des isométries du tétraèdre régulier, et applications*

Dans $\mathcal{E}$ espace affine euclidien de dimension 3 on considère un tétraèdre régulier T et on note G le groupe des isométries qui laissent globalement invariant l'ensemble $\mathcal{S}$ des sommets de T .

1. Montrer que G est isomorphe à un sous–groupe de S_4.

2. Montrer que G est isomorphe à S_4 et que le groupe G^+ des *déplacements* qui laissent $\mathcal{S}$ globalement invariant est isomorphe au groupe alterné A_4.

3. Expliciter géométriquement les deux types d'isométries négatives de G.

4. Justifier que les arêtes joignant des paires disjointes de sommets de T sont orthogonales.

5. En considérant les produits d'isométries réalisant les doubles transpositions sur $\mathcal{S}$, montrer que les droites joignant les milieux de deux arêtes opposées de T sont perpendiculaires deux à deux.

On note $\mathcal{A}$ cet ensemble de droites. On dispose alors d'une version *géométrique* de l'existence d'un morphisme surjectif de S_4 sur S_3:

6. Justifier que G agit sur $\mathcal{A}$. Montrer que cette action définit un morphisme *surjectif* de $G \simeq S_4$ sur $S(\mathcal{A}) \simeq S_3$. Quel est son noyau?

Exercice 16

Soit G un sous–groupe fini de $\mathrm{GL}(E)$, où E est un espace vectoriel euclidien, pour le produit scalaire $b = < \, , \, >$. On notera $\mathrm{O}(E)$ le groupe des isométries de (E, b).

Pour tous x, y dans E on définit $b'(x, y) = \frac{1}{\mathrm{card}\, G} \sum_{g \in G} < g(x), g(y) >$.

1. Montrer que b' est un produit scalaire sur E et que les éléments de G sont des isométries *de l'espace euclidien* (E, b').

2. Soient B, B' des bases orthonormées de E pour les produit scalaires b, resp. b', et u l'endomorphisme de E dont la matrice dans B est la matrice M de passage de B' à B.

Montrer que le conjugué $u\, G\, u^{-1}$ de G est un sous–groupe de $\mathrm{O}(E)$. Qu'en déduisez–vous sur les sous–groupes finis de $\mathrm{GL}_n \mathbb{R})$?

3. Montrer que tout sous–groupe fini de $\mathrm{O}(2, \mathbb{R})$ (donc de $\mathrm{GL}(2, \mathbb{R})$) est cyclique ou diédral (cf. exo13; on s'appuiera sur son intersection avec $\mathrm{SO}(2, \mathbb{R})$); de plus *tout* groupe cyclique ou diédral est isomorphe à un sous–groupe de $\mathrm{O}(2, \mathbb{R})$.

Complément (une jolie application) :

Exercice 17 *G–coloriages*

1. Soit G un groupe fini qui agit sur un ensemble X fini. Montrer la *formule de Burnside* qui donne le nombre N d'orbites pour cette action :

$$N = \frac{1}{\mathrm{card}\, G} \sum_{g \in G} \mathrm{card}\, \mathrm{Fix}(g)\,,$$

où $\mathrm{Fix}(g)$ ($g \in G$) désigne l'ensemble des $x \in X$ tels que $g \cdot x = x$ *(on pourra dénombrer de deux manières l'ensemble* $E = \{(g, x) \in G \times X |\, g \cdot x = x\}$*).*

Un ensemble $\mathcal{C}$ de q couleurs étant fixé, on appelle *G–coloriage* de X par $\mathcal{C}$ toute G–orbite de l'ensemble $\mathcal{F}$ des fonctions de X dans $\mathcal{C}$, où on munit $\mathcal{F}$ de l'action induite.

2. Expliciter l'action de G sur $\mathcal{F}$ et montrer qu'une fonction f de $\mathcal{F}$ est fixe par l'élément g de G ($g \in G$) ssi f est constante sur les $\langle g \rangle$–orbites de X.

3. En déduire que le nombre de G–coloriages de X vaut $\frac{1}{\mathrm{card}\, G} \sum_{g \in G} q^{|X/\langle g \rangle|}$, où pour tout g on note $|X/\langle g \rangle|$ le nombre de $\langle g \rangle$–orbites de X.

Des exemples:

4. Montrer que le nombre de roulettes différentes à n secteurs (considérées à rotation près) que l'on peut colorier à partir de q couleurs est

$$\frac{1}{n} \sum_{d | n} \varphi\big(\frac{n}{d}\big)\, q^d\,.$$

5. À partir de perles de couleur rouge ou bleue, combien peut–on faire de colliers de 6 perles différents? (on identifie deux colliers à rotation et symétrie près, *ie* modulo l'action du groupe diédral D_6.)

6. Dénombrer les coloriages possibles d'un cube, à rotation près, où chaque face est coloriée avec l'une des 3 couleurs blanche, rouge, ou bleue (voir 14-8).

$\diamondsuit \diamondsuit \diamondsuit$