Concours Agrégation, Mathématiques générales

Leçon 01- Groupe opérant sur un ensemble. Exemples et applications

Commentaires du jury 2015 :

Il faut bien dominer les deux approches de l'action de groupe : l'approche naturelle et l'approche, plus subtile, via le morphisme qui relie le groupe agissant et le groupe des permutations de l'ensemble sur lequel il agit. Des exemples de nature différente doivent être présentés : actions sur un ensemble fini, sur un espace vectoriel (en particulier les représentations), sur un ensemble de matrices, sur des polynômes. Les exemples issus de la géométrie ne manquent pas (groupes d'isométries d'un solide). Certains candidats décrivent les actions naturelles de $PGL(2, \mathbb{F}_q)$ sur la droite projective qui donnent des injections intéressantes pour $q = 2, 3$ et peuvent plus généralement en petit cardinal donner lieu à des isomorphismes de groupes. Enfin, on pourra noter que l'injection du groupe de permutations dans le groupe linéaire par les matrices de permutations donne lieu à des représentations dont il est facile de déterminer le caractére.

Commentaires du jury 2016 :

Dans cette leçon, il faut bien dominer les deux approches de l'action de groupe : l'approche naturelle et l'approche via le morphisme du groupe agissant vers le groupe des permutations de l'ensemble sur lequel il agit. La formule des classes et ses applications immédiates sont incontournables. Des exemples de natures différentes doivent être présentés : actions sur un ensemble fini, sur un espace vectoriel (en particulier les représentations), sur un ensemble de matrices, sur des groupes ou des anneaux. Les exemples issus de la géométrie ne manquent pas (groupes d'isométries d'un solide). S'ils le désirent, les candidats peuvent aller plus loin en décrivant les actions naturelles de $PGL_2(\mathbb{F}_q)$ sur la droite projective qui donnent des injections intéressantes pour $q = 2,\ 3$ et peuvent plus généralement en petit cardinal donner lieu à des isomorphismes de groupes. En notant que l'injection du groupe de permutations dans le groupe linéaire par les matrices de permutations donne lieu à des représentations, ils pourront facilement en déterminer le caractère.

Remarque : Dans la leçon Exemples d'actions de groupes sur les espaces de matrices nous verrons des développements qui ont leur place dans cette leçon ; par exemples : matrices équivalentes, matrices semblables, matrices congruentes, matrices orthogonalement équivalentes . . . .On pourra utilement consulter le tableau récapitulatif dans Caldero tome 1 p. 62-63 et plus généralement les chapitres 1 et 2.

Bibliographie

[F. M. 1] Fresnel J., Matignon M. *Algèbre et Géométrie* (Hermann 2011)
[F. M. 1'] Errata, https://www.math.u-bordeaux.fr/∼mmatigno/Errata-Alg-Géom.pdf
[F. M. 2] Fresnel J., Matignon M. *Algèbre et Géométrie-81 thèmes pour l'agrégation* (ellipses 2017)
[F. M. 2']Compléments et errata, https://www.math.u-bordeaux.fr/∼mmatigno/Errata-FM2.pdf
[Fr. A.] Fresnel J. *Algèbre des matrices* (Hermann 2011)
[Fr. B.C.D.] Fresnel J. *Espaces quadratiques, euclidiens, hermitiens* (Hermann 1999)
[Fr. E.] Fresnel J. *Groupes* (Hermann 2001)
[Fr. F.] Fresnel J. *Anneaux* (Hermann 2001)
[Fr. MMG96] Fresnel J. *Méthodes modernes en géométrie* (Hermann 1996)
[Fr. MMG10] Fresnel J. *Méthodes modernes en géométrie* (Hermann 2010)
et
[C. G.] Caldero P., Germoni J. *Histoires hédonistes de groupes et de géométries* (Calvage Mounet 2016)
[La.] Lang S. *Algebra*
[Pe.] Perrin D. *Cours d'algèbre* (ellipes 1996)
[Ta.] Tauvel P. *Algèbre* (Dunod 2005)

Développements conseillés :

(1) Un théorème de Burnside et coloriage des roulettes et des colliers (une variante : coloriages des faces ou des sommets du tétraédre) [F. M. 1] $N°59$ et $N°60$.

(2) Le théorème de Wederburn, [Fr. F.] p. 157, [Pe.] p. 82 (ces preuves utilisent le lemme arithmétique $(q^a-1, q^b-1) = q^{(a,b)}-1$. On peut avantageusement se limiter à montrer que si $q^d-1|q^n-1$, alors $d|n$. Pour cela on écrit $n = dm+r$ avec $0 \leq r < d$, ainsi $q^r-1 = q^n-1-q^r(q^{dm}-1)$. Il suit que $q^d-1|q^r-1$ et donc $r=0$) , [Ta] p. 294 évite l'utilisation du lemme par une récurence sur le cardinal du corps.
(3) Théorème de Sylow, [Fr. E.] Théorème 3.3 p. 34 et exercice 1 ci-dessous.

Exercice 1

Action de groupe et d'un sous-groupe. Un critère de transitivité et le deuxième théorème de Sylow. Exercice corrigé.

(1) Soit G un groupe agissant sur l'ensemble X et $H \subset G$ un sous-groupe de G.
   (a) Montrer que l'action de G sur X induit une action de H sur X.
   Preuve. La restriction à $H \times X$ de l'application $(g,x) \in G \times X \to g \star x \in X$ qui définit l'action de G est induite par la restriction à H de l'homomorphisme $\Phi : G \to \mathcal{S}(X)$ avec $\Phi(g)(x) = g \star x$. C'est donc un homomorphisme de groupes. ///
   (b) Soit $G \star x$ une orbite sous G, montrer que c'est une réunion disjointe d'orbites sous H.
   Preuve. L'orbite $G \star x = \bigcup_{i \in I} Hg_i \star x$ où $g_{i,i\in I}$ parcourt un système de représentants des classes à droite de G modulo le sous-groupe H. Ainsi $G \star x$ est réunion d'orbites sous H et puisque deux orbites sous H sont ou bien égales ou bien disjointes on en extrait une réunion disjointe de telles orbites. ///
(2) Soit G un groupe fini agissant sur l'ensemble fini X. On suppose qu'il existe un nombre premier p tel que pour tout $x \in X$ il existe un p-groupe P_x tel que l'ensemble de ses points fixes $\mathrm{Fix}(P_x) := \{y \in X,\ \forall g \in P_x,\ g \star y = y\}$ est réduit à $\{x\}$. Il s'agit de montrer que l'action de G sur X est alors transitive. Notez que l'on peut supposer que $|X| \geq 2$, ce que nous supposons dans ce qui suit.
   (a) Soient $x_0, x_1 \in X$, montrer que l'orbite $G \star x_0$ est réunion disjointe d'orbites $P_{x_1} * y$ sous l'action de P_{x_1} sur X induite par l'action de G sur X.
   Preuve. C'est un cas particulier de la question (1). ///
   (b) En déduire que $|G \star x_0|$ est une somme de puissance de p.
   Preuve. Le stabilisateur de y sous l'action de P_{x_1} est un sous-groupe de P_{x_1} donc aussi un p-groupe, enfin le cardinal de l'orbite $P_{x_1} * y$ est égal à l'indice du stabilisateur; c'est donc une puissance de p. ///
   (c) En prenant $x_1 = x_0$, montrer que $|G \star x_0|$ est congru à 1 modulo p.
   Preuve. Le cardinal de l'orbite $P_{x_1} * y$ est égal à 1 si et seulement si $P_{x_1} * y = y$, i.e. $y \in \mathrm{Fix}\, P_{x_1}$ qui vaut x_1 par hypothèse. Si $x_1 = x_0$ alors une et une seule des orbites sous P_{x_1} dans la décomposition de $G \star x_0$ est réduite à un élément, c'est $P_{x_1} \star x_0$. ///
   (d) Dans le cas où x_1 est quelconque en déduire qu'il existe $y \in G \star x_0$ avec $|P_{x_1} * y| = 1$. Conclure.
   Preuve. On a vu que $G \star x_0$ est réunion disjointe d'orbites $P_{x_1} * y$ sous l'action de P_{x_1} et que chacune de ces orbites a un cardinal qui est une puissance de p. Puisque $|G \star x_0|$ est congru à 1 modulo p et si x_1 est quelconque il y a donc encore une orbite à 1 élément et cet élément est nécessairement x_1, ainsi il existe $g \in G$ avec $x_1 = g \star x_0$. ///
   (e) Montrer que $|X|$ est congru à 1 modulo p.
   Preuve. On vient de montrer que $X = G \star x_0$. ///
(3) En déduire le second théorème de Sylow. On rappelle que le deuxième théorème de Sylow affirme que si G est un groupe fini avec p premier qui divise $|G|$ alors les p-sous-groupes de Sylow de G sont conjugués et leur nombre est congru à 1 modulo p.

Preuve. Si $\mathcal{P}$ désigne l'ensemble des p-sous-groupes de Sylow de G, le groupe G agit par conjugaison sur $\mathcal{P}$ et le stabilisateur du groupe $P \in \mathcal{P}$ contient P. De plus si $P, Q \in \mathcal{P}$ et si $P \star Q = Q$, alors l'ensemble PQ est un sous-groupe de G et puisque par le théorème d'isomorphisme $\frac{PQ}{Q} \simeq \frac{P}{P \cap Q}$ il suit que PQ est un p-groupe contenant le p-Sylow P donc égal à P. Ainsi $Q \subset P$ et donc $P = Q$.

Ainsi les conditions de la question (2) sont satisfaites et l'action est donc transitive. Par la même occasion on a montré que le nombre de p-groupes de Sylow est congru à 1 modulo p. ///

(4) Soient $n \geq 1$ et $i \in \{1, 2, ..., n\}$, σ_i une involution du groupe symétrique S_n avec $\mathrm{Fix}\,\sigma_i = \{i\}$ (nécessairement $n = 2m + 1$ et σ_i est produit de m transpositions à supports disjoints). Soit G le sous groupe de S_n engendré par les $\sigma_i,\ i \in \{1, 2, ..., n\}$. Montrer que G agit transitivement sur $\{1, 2, ..., n\}$.

Preuve. On vérifie pour $p = 2$ les conditions de la question (2). ///

Exercice 2 Action d'un groupe sur les classes à gauche modulo un sous-groupe, [F. M. 1] $N°55$ p. 144

Exercice 3 Sur les sous-groupes d'indice 2, [F. M. 1] $N°56$ p. 145

Exercice 4 Le défaut de commutativité d'un groupe non abélien, [F. M. 1] $N°61$ p. 151

Exercice 5 A propos du commentaire du jury "on pourra noter que l'injection du groupe de permutations dans le groupe linéaire par les matrices de permutations donne lieu à des représentations dont il est facile de déterminer le caractére" on pourra consulter [F. M. 2] p.164

Exercice 6 Un théorème de Jordan [F. M. 1] $N°58$. Notez l'application suivante : soit G un groupe fini et $H \subset G$ un sous-groupe avec $H \neq G$. Montrer que $\cup_{g\in G} gHg^{-1} \neq G$ (considérer pour cela l'action transitive par translation à gauche de G sur $G/H := \cup_{g\in G} gH$ et noter que $g' \in G$ est tel que $g' \star gH = gH$ ssi $g' \in gHg^{-1}$).

Exercice 7 Nombre minimal de transpositions pour engendrer S_n (utilise la représentation linéaire de S_n par permutation de la BON canonique de $\mathbb{R}^n$, [Fr. E.] p. 28). Noter que ce résultat est aussi une conséquence de la théorie des graphes [F. M. 2] p. 143 et [F. M. 2] Compléments-errata.

Exercice 8 Comptage des matrices de rang $n - 1$ (resp. rang $n - 1$ et nilpotentes) dans $M_n(\mathbb{F}_q)$, [F. M. 2] p. 8 et 10

Exercice 9 Comptage des matrices diagonalisables sur $\mathbb{F}_q$, [F. M. 2] p. 6 , Caldero Tome 1 p. 264

Exercice 10 Orbites de l'action de $\mathrm{GL}(E)$ sur $L_K(E, F)$ par multiplication à gauche et sous-espaces vectoriels de E. Exercice corrigé.

(1) Applications linéaires et théorème de factorisation.

Soient E, F, 2 K-espaces vectoriels de dimension respectives p et n et $L_K(E, F)$, le K-espace vectoriel des applications linéaires de E dans F. On considère l'action de groupe $(w, v) \in \mathrm{GL}(F) \times L_K(E, F) \to w \circ v \in L_K(E, F)$. Montrer que $u, v \in L_K(E, F)$ sont dans la même orbite si et seulement si $\mathrm{Ker}\, u = \mathrm{Ker}\, v$.

Preuve. On note $F' := \mathrm{Im}\, v$ et $v' :\ E \to F'$ avec $v'(x) = v(x),\ \forall x \in F'$. Alors $\mathrm{Ker}\, v' = \mathrm{Ker}\, v$. Puisque v' est surjective, par le théorème de factorisation des applications linéaires ([Fr. A.] p.??) il existe une et une seule application K-linéaire $w' :\ F' \to F$ avec $w' \circ v' = u$ si et seulement si $\mathrm{Ker}\, v' \subset \mathrm{Ker}\, u$.

Ainsi si il existe $w \in L_K(E, F)$ avec $u = w \circ v$, alors $u = w' \circ v'$ où $w' := w_{\|F'}$ et donc $\mathrm{Ker}\, v = \mathrm{Ker}\, v' \subset \mathrm{Ker}\, u$.

Réciproquement si $w' \in L_K(F', F)$ avec $u = w' \circ v'$, il suffit de prolonger w' à F. Pour cela on choisit un supplémentaire S de F' dans F et si $f_i,\ 1 \leq i \leq s$ est une base de S on définit w par $w(f' + \sum_{1\leq i\leq s} \lambda_i f_i) := w'(f) + \sum_{1\leq i\leq s} \lambda_i g_i,\ \forall f' \in F'$ où les $g_i \in F$ sont arbitraires.

Si de plus on veut que $w \in \mathrm{GL}(F)$ i.e. w injective. une condition nécessaire est que $\mathrm{Ker}\, v = \mathrm{Ker}\, u$ et c'est aussi une condition suffisante puisqu'alors $u = v$ et donc $F = \mathrm{Im}\, u \bigoplus T$ avec $\dim T = \dim S$ et il suffit d'imposer aux $g_i = w(f_i),\ 1 \leq i \leq s$ d'être une base de T. ///

(2) En déduire que les orbites sont en bijection avec les sous-espaces vectoriels V de E de dimension $\geq \dim E - \dim F$.

Preuve. Par la question précédente l'application qui à $v \in L_K(E, F)$ associe $\mathrm{Ker}\, v \subset E$ définit par passage au quotient ensembliste une application injective de l'ensemble des orbites dans l'ensemble des sous-espaces vectoriels de E de dimension $\geq \dim E - \dim F$ (théorème du rang). Il suffit de montrer qu'elle est surjective. Si $V \subset E$ est un sous-espace vectoriel de E avec $\dim V \geq \dim E - \dim F$, soit S un supplémentaire de V, alors $s := \dim S = \dim E - \dim V \leq \dim F$, ainsi il existe $(g_i)_{1\leq i\leq s}$ une famille libre de F et si $(f_i)_{1\leq i\leq s}$ est une base de S alors l'application linéaire v avec $v(x) = 0,\ \forall x \in V$ et $v(f_i) = g_i$ pour $1 \leq i \leq s$ est telle que $\mathrm{Ker}\, v = V$.

Remarque. Si $\dim E \leq \dim F$, il n'y a pas de condition de dimension pour les sous-espaces vectoriels V de E. ///

Exercice 11 Orbites de l'action de $\mathrm{GL}_n(K)$ sur $M_{n,p}(K)$ par la multiplication à gauche, matrices échelonnées normalisées et sous-espaces vectoriels de K^n (version matricielle de l'exercice précédent). Exercice corrigé.

Rappel, [Fr. A.] p. 47-49.

Les matrices échelonnées normalisées sont les matrices $N(a) = [C_1, C_2, ..., C_p] \in M_{n,p}(K)$ de rang r telles que les colonnes $C_{j_k},\ 1 \leq i \leq r$ avec $j_1 < j_2 < ... < j_{r-1}$ sont les r premiers vecteurs de la base canonique $(e_i)_{1\leq i\leq n}$ de K^n, $C_{j_r} = ae_{j_r}$ avec $a = 1$ si $r < n$ et $a \in K_{\{}0\}$ si $r = n$. Les autres colonnes étant sujettes à la règle suivante : $C_i = 0$ pour $1 \leq i \leq j_1$, $(C_j,\ j_k \leq i \leq j_{k+1}) \in \bigoplus_{1\leq i\leq k} Ke_i$ et enfin $(C_j,\ j_r \leq i) \in \bigoplus_{1\leq i\leq r} Ke_i$.

Dans ce qui suit les matrices "échelonnée normalisées unité "sont les matrices échelonnées normalisées avec $a = 1$. Dans [Fr. A.] p. 47-49, on montre que les matrices échelonnées normalisées forment un système de représentants des orbites de l'action de $\mathrm{SL}_n(K)$ sur $M_{n,p}(K)$ par la multiplication à gauche.

On va montrer que les matrices "échelonnée normalisées unité " forment un système de représentants des orbites de l'action de $\mathrm{SL}_n(K)$ sur $M_{n,p}(K)$ par la multiplication à gauche.

(1) Soit $A \in M_{n,p}(K)$ avec , montrer que les orbites de A sous $\mathrm{GL}_n(K)$ et $\mathrm{SL}_n(K)$ coïncident.
Preuve. En effet $\mathrm{SL}_n(K)A = \mathrm{SL}_n(K)N_r(1)$ où $N_r(1)$ est le représentant échelonné normalisé avec $a = 1$ puisque $(A) < n$. Soit $b \in K^\times$ et $D_n(b)$ la dilatation de diagonale $(1, ..., 1, b)$, alors $N_r(1) = D_n(b)N_r(1)$; ainsi $\mathrm{SL}_n(K)N_r(1) = \mathrm{SL}_n(K)D_n(K^\times)N_r(1)$ et donc $\mathrm{SL}_n(K)N_r(1) = \mathrm{GL}_n(K)N_r(1)$ et $\mathrm{GL}_n(K)A = \mathrm{SL}_n(K)A$. ///

(2) Soit $A \in M_{n,p}(K)$ avec $(A) = n$. Montrer qu'il existe $P \in \mathrm{GL}_n(K)$ avec $PA = N$ échelonnée normalisée unité.
Preuve. Comme rappelé au-dessus il existe $S \in \mathrm{SL}_n(K)$ avec $SA = N_n(a)$ échelonnée normalisée. Ainsi $P := D_n(\frac{1}{a})$ convient.

(3) Mêmes notations que précédemment. Montrer l'unicité d'un représentant échelonné normalisé unité dans l'orbite $\mathrm{GL}_n(K)A$).
Preuve. Soit $P \in \mathrm{GL}_n(K)$ avec $PA = N_n(1)$, alors $D_n(\frac{1}{\det P})PA = D_n(\frac{1}{\det P})N_n(1)$ est échelonnée normalisée et $S := D_n(\frac{1}{\det P})P \in \mathrm{SL}_n(K)$. Ainsi $D_n(\frac{1}{\det P})N_n(1) = N_n(a)$ est **le** *représentant échelonné normalisé dans l'orbite $\mathrm{SL}_n(K)A$. ///*

(4) Montrer par un procédé algorithmique que deux matrices échelonnées normalisées unité sont égales si et seulement si elles ont le même noyau. Ainsi on retrouve la bijection entre les orbites sous $\mathrm{GL}_n(K)$ des matrices de $M_{n,p}(K)$ et les sous-espaces vectoriels V de K^p avec $\dim V \geq p - n$;

précisément si $A \in M_{n,p}(K)$ l'espace V correspondant est l'ensemble des solutions du système linéaire homogène $A(x_1, x_2, ..., x_p)^t = 0$.
Preuve. Soient donc $N = (n_{i,j}$ *et* $N' = (n'_{i,j}$ *deux matrices échelonnées normalisées unité de rang* r *resp.* r' *avec* $\operatorname{Ker} N = \operatorname{Ker} N'$. *Par le théorème du rang on a* $r = r'$. *On note* C_{j_k}, $1 \leq k \leq r$ *resp.* $C'_{j'_k}$, $1 \leq k \leq r$ *la colonne de* N *resp.* N' *qui est égale à* e_k.
Ainsi $e_1, ..., e_{j_1 - 1} \in \ker N$ *d'où* $j'_1 \geq j_1$ *et par symétrie* $j'_1 = j_1$.
Soit $j_1 < j < j_2$, *montrons que* $n_{1,j} = n'_{1,j}$ *et* $n_{i,j} = n'_{i,j}$ *si* $i > 1$. *Pour cela on remarque que* $n_{1,j}e_{j_1} - e_j \in \operatorname{Ker} N = \operatorname{Ker} N'$, *il suit que* $0 = N'(_{1,j}e_{j_1} - e_j) == (n_{1,j} - n'_{1,j})e_1 + \sum_{i>1} n'_{i,j}e_i$ *d'où le résultat. Il suit en sus de cela que* $j'_2 \geq j_2$ *avec égalité par symétrie.*
Si $j_2 < j < j_3$, *alors* $n_{1,j}e_{j_1} + n_{2,j}e_{j_2} - e_j \in \operatorname{Ker} N = \operatorname{Ker} N'$ *et donc* $0 = (n_{1,j} - n'_{1,j})e_1 + (n_{2,j} - n'_{2,j})e_2 + \sum_{i>2} n'_{i,j}e_i$ *...etc... .///*

Exercice 12 La décomposition LDU, [F. M. 2] I.4 p. 27

Exercice 13 La décomposition de Bruhat [F. M. 1] $N°5$ et [F. M. 2] p. 43

Exercice 13 Action à gauche du groupe $SL_n(K)$ sur $M_{n,p}(K)$ et matrices échelonnées, [Fr. A.] p. 47-53. Application. Si $A, B \in M_{n,p}(K)$ alors $KerA = KerB$ ssi il existe $P \in GL_n(K)$ avec $B = PA$. Si $K = \mathbb{F}_q$, en déduire le nombre de matrices échelonnées de rang $n - s$ dans $M_n(\mathbb{F}_q)$.

Exercice 14 Voir [Fr. MMG10] p. 221 et [F. M. 2'] complément à la page 121. On rappelle la présentation du groupe diédral $D_{2n} =< r, s >$ avec ordre de r égal n, ordre de s égal 2 et $srs^{-1} = r^{-1}$. Pour $\theta \in \mathbb{R}$ on note $R(\theta) := \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \in M_2(\mathbb{R})$ et $S(\theta) := \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \in M_2(\mathbb{R})$

(1) Montrer que $S(\theta) \in O_2(\mathbb{R}) - SO_2(\mathbb{R})$ est la symétrie orthogonale par rapport à $\mathbb{R}(\cos\frac{\theta}{2}, \sin\frac{\theta}{2})$.
Preuve. On vérifie que $S(\theta)\ {}^tS(\theta) = Id$ *et que* $S(\theta)^2 = Id$; *ainsi* $S(\theta)$ *est une symétrie orthogonale et puisque* $S(\theta)\ {}^t(1, 0) = {}^t(\cos\theta, \sin\theta)$ *le résultat suit.///*
(2) Montrer que le groupe $G_n(\theta)$ engendré par $R(\frac{2\pi}{n})$ et $S(\theta)$ est isomorphe au groupe diédral D_{2n} de cardinal $2n$.
Preuve. On vérifie que $S(\theta)R(\frac{2\pi}{n})S(\theta)\ {}^t(1, 0) = {}^t(\cos\frac{2\pi}{n}, -\sin\frac{2\pi}{n})$ *et puisque* $\det S(\theta)R(\frac{2\pi}{n})S(\theta) = 1$ *il suit que* $S(\theta)R(\frac{2\pi}{n})S(\theta) = R(-\frac{2\pi}{n})$.*///*
(3) Soit G un sous-groupe de $SO_2(\mathbb{R})$. Montrer que G est soit dense dans $SO_2(\mathbb{R})$ soit fini et si son cardinal est n alors $G =< R(\frac{2\pi}{n}) >$ (on pourra utiliser le fait qu'un sous groupe de $(\mathbb{R}, +)$ est soit dense soit monogène i.e. de la forme $\mathbb{Z}a$, [Fr. B-C-D] p. 84).
Preuve. L'application $R : \mathbb{R} \to SO_2(\mathbb{R})$ *est un homomorphisme de groupes (formules d'addition). Il est surjectif par la paramétrisation polaire du cercle unité. Enfin le noyau est* $2\pi\mathbb{Z}$; *ainsi* R *induit un isomorphisme* $\tilde{R}$ *entre* $\frac{\mathbb{R}}{2\pi\mathbb{Z}}$ *et* $SO_2(\mathbb{R})$. *De plus* $\frac{\mathbb{R}}{2\pi\mathbb{Z}}$ *est compact, il suit que* $\tilde{R}$ *est un homéomorphisme. Il s'agit donc de préciser la nature des sous-groupes* G *de* $\mathbb{R}$ *qui contiennent* $2\pi\mathbb{Z}$. *Si* G *est discret alors* $G = a\mathbb{Z}$ *avec* $2\pi \in a\mathbb{Z}$; *ainsi* $2\pi = na$ *avec* $n \in \mathbb{N}$ *et donc* $a = \frac{2\pi}{n}$. *Il suit que* $R(G) =< R(\frac{2\pi}{n}) >$ *est fini de cardinal* n. *Si* G *n'est pas discret, il est dense dans* $\mathbb{R}$ *et il en est donc de même de* $R(G)$.*///*
(4) Soit G un sous-groupe de $O_2(\mathbb{R})$ et $G^+ := G \cap SO_2(\mathbb{R})$. On suppose qu'il existe $\sigma \in G - G^+$. Montrer que $G = G^+ \cup \sigma G^+$, en déduire que G est soit dense dans $O_2(\mathbb{R})$ soit fini et si son cardinal est m alors $m = 2n$ et G est isomorphe au groupe diédral D_{2n}.
Preuve. Seule l'inclusion $G^+ \cup \sigma G^+ \subset G$ *est à prouver. Si* $g \in G - G^+$ *alors* $\sigma g \in G^+$ *et puisque* $\sigma^2 = Id$ *l'inclusion suit. Notez que la réunion* $G^+ \cup \sigma G^+ \subset G$ *est de plus disjointe (déterminant).///*

(5) Le groupe $G_n(\theta) \subset O_2(R)$ opère sur l'ensemble T des points $m = (x_m, y_m) \in \mathbb{R}^2$ avec $x_m^2 + y_m^2 = 1$ par la formule $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \star (x_m, y_m) = (ax_m + by_m, cx_m + dy_m)$. On note $G_n(\theta)_m$ le groupe d'isotropie de m.
Montrer que $G_n(\theta)_m$ est d'ordre 1 ou 2; en déduire une description de l'orbite de M sous $G_n(\theta)$.
Preuve. Puisque $m \neq (0,0)$ il suit que $SO_2(\mathbb{R})_m = \{Id\}$ et donc $G_n(\theta)^+_m = \{Id\}$. Si $\sigma, \tau \in G_n(\theta)_m - G_n(\theta)^+_m$ alors $\sigma\tau^{-1} \in G_n(\theta)^+_m$; ainsi $\sigma = \tau$ et $G_n(\theta)_m = \{Id, \sigma\}$ est d'ordre 2. Si $G_n(\theta)_m = \{Id\}$, alors l'orbite $G_n(\theta) \star m$ est le polygone régulier à n côtés $< R(\frac{2\pi}{n}) > \star m$ et si $G_n(\theta)_m = \{Id, \sigma\}$ c'est la réunion de deux polygones réguliers à n côtés qui sont $< R(\frac{2\pi}{n}) > \star m$ et $< R(\frac{2\pi}{n}) > \sigma \star m$; de plus ils sont distincts puisque l'orbite a $2n$ éléments et c'est un polygone régulier à $2n$ côtés pour les n valeurs de $\theta = k\frac{\pi}{n}$ avec $k = 1, 3, ..., 2n-1$ avec k impair (cf. 2.c) de l'exercice suivant).///

(6) Montrer que l'application qui à $\theta \in [0, \frac{2\pi}{n}[$ associe $G_n(\theta)$ définit une bijection sur les sous-groupes de $O_2(\mathbb{R})$ d'ordre $2n$ qui ne sont pas inclus dans $SO_2(\mathbb{R})$.
Preuve. Il faut montrer que tout groupe $G_n(\varphi)$ avec $\varphi \in \mathbb{R}$ est égal à un unique groupe $G_n(\theta)$ avec $\theta \in [0, \frac{2\pi}{n}[$. Pour cela on remarque que l'ensemble des symétries dans $G_n(\varphi)$ est $G_n(\varphi) - G_n(\varphi)^+ = \{R(k\frac{2\pi}{n})S(\varphi) = S(\varphi + k\frac{2\pi}{n}),\ k = 0, 1, ..., n-1\}$ et puisqu'il n'y a qu'une seule valeur $k_0 := -\lfloor \frac{n\varphi}{2\pi} \rfloor$ mod n de k telle que $0 \leq \varphi + k\frac{2\pi}{n} < \frac{2\pi}{n}$, le résultat suit avec $G_n(\varphi) = G_n(\theta)$ et $\theta = \varphi - \lfloor \frac{n\varphi}{2\pi} \rfloor \frac{2\pi}{n}$.///

Exercice 15 Orbites sous l'action d'un sous-groupe de $O_2(\mathbb{R})$ sur l'ensemble T des points $m = (x_m, y_m) \in \mathbb{R}^2$ avec $x_m^2 + y_m^2 = 1$.

Soit G un sous-groupe de $O_2(\mathbb{R})$ et $G^+ := G \cap SO_2(\mathbb{R})$, on rappelle que si il existe $\sigma \in G - G^+$ alors $G = G^+ \cup \sigma G^+$.

Soit $\Sigma \subset T$ une partie non vide de T avec $G \star \Sigma = \Sigma$, alors Σ est réunion disjointe d'orbites $G \star s$ de points $s \in \Sigma$.

Dans ce qui suit Σ est réduit à un point s, G désigne un sous-groupe de $O_2(\mathbb{R})$ et $O(s) := G \star s$, l'orbite de s sous l'action de G. Enfin $\hat{G} := \{g \in O_2(\mathbb{R}) \mid g \star O(s) = O(s)\}$ le stabilisateur dans $O_2(\mathbb{R})$ de $O(s)$.

(1) On suppose que $G \subset SO_2(\mathbb{R})$.

(a) Montrer que $\hat{G}^+ = G$.
Preuve. Soit $r \in \hat{G}^+$, ainsi r est une rotation avec $r \star O(s) = O(s)$; ainsi il existe $g \in G$ avec $r \star s = g \star s$ et puisque $G \subset SO_2(\mathbb{R})$ il suit que la rotation $g^{-1}r$ fixe le point s; c'est donc l'identité.///

(b) Soit σ_s la symétrie orthogonale avec $\sigma_s(s) = s$. Montrer que $\hat{G} = G^+ \cup \sigma_s G^+$.///
Preuve. On a $\sigma_s \in \hat{G}^+$ et puisque $\hat{G}$ est un sous-groupe de $O(2)(\mathbb{R})$, il suit que $\hat{G} = \hat{G}^+ \cup \sigma_s \hat{G}^+ = G^+ \cup \sigma_s G^+$.///

(2) On suppose qu'il existe $\sigma \in G - G^+$. Soit ρ, l'unique rotation telle que $\rho(s) = \sigma(s)$. On note $O(s)^+ := G^+ \star s$ et $O(s)^- := G^+\sigma \star s$; ainsi $O(s) = O(s)^+ \cup O(s)^-$.

(a) Montrer que $O(s)^+ = O(s)^-$ ou bien que $O(s)^+ \cap O(s)^- = \emptyset$.
Preuve. L'intersection $O(s)^+ \cap O(s)^-$ est non vide si et seulement si il existe $r, r' \in G^+$ avec $r \star s = r'\sigma \star s$ autrement dit si $r'^{-1}r \star s = \rho \star s$ et donc puisque $\rho \in SO_2(\mathbb{R})$, $O(s)^+ \cap O(s)^-$ est non vide si $\rho = r'^{-1}r \in G^+$ (réciproquement si $\rho \in G^+$, $r = \rho$ et $r' =$ conviennent). Dans ce cas on a $O(s)^+ = G^+ \star s = G^+\rho \star s = G^+\sigma \star s = O(s)^-$.///

(b) On suppose que $O(s)^+ = O(s)^-$. Montrer que $\hat{G} = G$. Construire un exemple.
Preuve. On a $O(s) = O(s)^+ \cup O(s)^- = O(s)^+ = O(s)^-$. Si $g \in \hat{G}^+$ il existe $r \in G^+$ avec $g \star s = r \star s$ et donc $g = r \in G$. Enfin si $g \in \hat{G}^+\sigma$, puisque $g \star O(s)^- = O(s)^-$ il existe $r \in G^+$ avec $g \star s = r\sigma \star s$, ainsi $g\sigma \star (\sigma \star s) = r \star (\sigma \star s)$ i.e. les deux rotations $g\sigma$ et r sont égales et donc $g = r\sigma \in G$.

Exemples. Soit $n > 1$ et $G_n :=< r, \sigma >$, avec r la rotation d'angle $2\frac{\pi}{n}$ et σ la symétrie orthogonale avec $\sigma(1,0) = (1,0)$. Soit $s := (1,0)$ alors $O(s)^+ = O(s)^-$ (on peut aussi noter que $\rho =$). ///

(c) On suppose que $O(s)^+ \cap O(s)^- = \emptyset$. Montrer que si $\rho^2 \notin G^+$ alors $\hat{G} = G$ et que si $\rho^2 \in G^+$ alors $\hat{G}^+ = G^+ \cup \rho G^+$ et donc $\hat{G} = \hat{G}^+ \cup \hat{G}^+\sigma$. Construire un exemple dans chacune des deux situations.

Preuve. Nous sommes donc dans la situation où $\rho \notin G$ et $O(s)$ est réunion disjointe de $G^+ \star s$ et de $G^+\sigma \star s$. Soit donc $h \in \hat{G}$ i.e. $h \in O_2(\mathbb{R})$ avec $h \star O(s) = O(s)$ ce qui équivaut aux deux conditions $h \star s \in O(s)$ et $h \star (\sigma \star s) \in O(s)$ (discuter en fonction de la nature de h, on n'a pas besoin de l'équivalence) . On distingue 2 cas.

- *On suppose que la rotation $\rho^2 \in G$ (et $\rho \notin G$). Il s'agit de montrer que $h \in G^+ \cup \rho G^+$. Il existe $g, g' \in G$ avec (1) $h \star s = g \star s$ et (2) $h \star (\sigma \star s) = g' \star s$. On discute en fonction de la nature de h.*
  - *Supposons que $h \in SO_2(\mathbb{R})$. Si $g \in SO_2(\mathbb{R})$ la relation (1) montre que $h = g \in G^+$. Si $g \in O_2(\mathbb{R}) - SO_2(\mathbb{R})$ la relation (1) devient $h \star s = g\sigma \star (\sigma \star s) = g\sigma\rho \star s$; ainsi (3) $h = (g\sigma)\rho = \rho(g\sigma)$ puisque $SO_2(\mathbb{R})$ est commutatif. Ainsi $h \in \rho G^+$.*
  - *Supposons que $h \in O_2(\mathbb{R}) - SO_2(\mathbb{R})$. Alors $h' := \sigma h \in SO_2(\mathbb{R})$ et puisque les relations (1) et (2) sont équivalentes aux relations analogues pour h' à condition de remplacer g resp. g' par σg resp. $\sigma g'$ le résultat est alors conséquence du cas précédent appliqué à h'.*

    Exemples. Soit $n > 1$ et $G = G_n :=< R(2\frac{\pi}{n}), \sigma >$, avec r la rotation d'angle $2\frac{\pi}{n}$ et $\sigma = S(\theta)$ la symétrie orthogonale avec $S(\theta) \star (1,0) = (\cos\theta, \sin\theta)$. Soit $s := (1,0)$ alors $\rho = R(\theta)$, ainsi il faut et il suffit de choisir $\theta \notin \{2k\frac{\pi}{n} \mod 2\pi\}$ mais que $2\theta \in \{2k\frac{\pi}{n} \mod 2\pi\}$ avec $k \in \{0, 1, .., n-1\}$ pour que $\rho \notin G_n^+$ et $\rho^2 \in G_n^+$. Cela donne n possibilités qui sont $\theta = k\frac{\pi}{n}$ avec $k = 1, 3, ..., 2n-1$ avec k impair. L'orbite $O(s)$ est l'ensemble des $2n$ sommets d'un polygone régulier dont le groupe des isométries est G_{2n} puisque $\hat{G_n} = G_{2n}$.
- *On suppose que la rotation $\rho^2 \notin G$. Il s'agit de montrer que $h \in G$.*
  - *Si $h \in SO_2(\mathbb{R})$ et si $g \in SO_2(\mathbb{R})$ comme précédemment on déduit que $h \in G$ et si $g \in O_2(\mathbb{R}) - SO_2(\mathbb{R})$ que (3) $h = \rho(g\sigma)$. On va conclure à l'aide de la relation (2) $h \star (\sigma \star s) = g' \star s$.*

    Si $g' \in O_2(\mathbb{R}) - SO_2(\mathbb{R})$ on a $\sigma h\sigma \star s = \sigma g' \star s$ avec $\sigma h\sigma,\ \sigma g' \in SO_2(\mathbb{R})$, ainsi $\sigma h\sigma = \sigma g'$ et donc $h = g'\sigma \in G^+$.

    Si $g' \in SO_2(\mathbb{R})$ on a $h \star (\sigma \star s) = h\rho \star s = g' \star s$, ainsi avec (3) $g' = h\rho = \rho(g\sigma)\rho = (g\sigma)\rho^2$ et donc $\rho^2 \in G$; contradiction!
  - *Supposons que $h \in O_2(\mathbb{R}) - SO_2(\mathbb{R})$ on conclut comme précédemment en considérant σh.*

    Exemples. Soit $n > 1$ et $G = G_n :=< R(2\frac{\pi}{n}), \sigma >$, avec r la rotation d'angle $2\frac{\pi}{n}$ et $\sigma = S(\theta)$ la symétrie orthogonale avec $S(\theta) \star (1,0) = (\cos\theta, \sin\theta)$. Soit $s := (1,0)$ alors $\rho = R(\theta)$, ainsi il faut et il suffit de choisir $\theta \notin \{k\frac{\pi}{n} \mod 2\pi\}$ avec $k \in \{0, 1, .., n-1\}$ pour que $\rho^2 \notin G_n^+$ et donc aussi $\rho \notin G_n^+$; autrement dit il faut éviter les exemples construits dans la question précédente. Dans ce cas $O(s)$ est l'ensemble des $2n$ sommets d'un polygone convexe qui n'est pas régulier et dont le groupe des isométries est G_n puisque $\hat{G_n} = G_n$.///

Exercice 16 Sous-groupes finis de $\mathrm{GL}_2(\mathbb{R})$ (voir [Fr. B-C-D] p. 165), $\mathrm{GL}_2(\mathbb{Z})$ et $\mathrm{GL}_2(\mathbb{Q})$ (voir [F. M. 1] $n°26$ question 4) p. 49 et question 1) p. 46).

(1) Soit G un sous-groupe fini de $\mathrm{GL}_2(\mathbb{R})$. On va montrer qu'il existe $P \in \mathrm{GL}_2(\mathbb{R})$ avec $PGP^{-1} \subset O_2(\mathbb{R})$; ainsi si $G \subset \mathrm{SL}_2(\mathbb{R})$, le groupe G est cyclique et sinon G est diédral.

(a) On note q la forme quadratique euclidienne sur $\mathbb{R}^2$ i.e. $q((x,y)) = x^2 + y^2$. Montrer que $q_G((x,y)) = \sum_{g\in G} q((x,y)\ {}^t g))$ est une forme quadratique définie positive sur $\mathbb{R}^2$.
Preuve. La forme $\Phi_G((x,y),(x',y')) := \sum_{g\in G}((x,y)\ {}^t g)|(x,y)\ {}^t g))$ *où* $(.|.)$ *désigne le produit scalaire, est une forme bilinéaire symétrique et* $q_G((x,y)) = \Phi_G((x,y),(x,y))$ *est la forme quadratique associée. Enfin puisque* $q((x,y)\ {}^t g))) \geq 0$ *et c'est nul si et seulement si* $(x,y) = (0,0)$ *il suit que* Φ_G *est un produit scalaire.///*

(b) Montrer que $G \subset O(q_G)$, le groupe orthogonal de q_G.
Preuve. Soit $g \in G$, *alors* $q_G((x,y)\ {}^t g') = \sum_{g\in G} q((x,y)\ {}^t g'\ {}^t g)) = q_G((x,y))$ *puisque* $Gg' = G.///$

(c) Montrer que $O(q_G)$ et $O(q)$ sont des sous-groupes conjugués de $\mathrm{GL}_2(\mathbb{R})$.
Preuve. Soit $S \in Sym_2(\mathbb{R})$ *avec* $q_G((x,y)) = (x,y)S\ {}^t(x,y)$. *Soit* (e_1,e_2) *une BON de* $\mathbb{R}^2$ *pour* q_G; *si* P *est la matrice de passage telle que* $(x,y) = (x',y')\ {}^t P$ *avec* $x'e_1 + y'e_2 = (x,y)$ *alors* $q_G((x,y)) = x'^2 + y'^2$; *ainsi si* $g \in O(q_G)$ *alors* $q_G((x,y)) = q_G((x,y)\ {}^t g) = q_G((x',y')\ {}^t P\ {}^t g)$ *ainsi* ${}^t P\ {}^t g S g P = Id$ *et puisque* ${}^t P S P = Id$ *(cas* $g = Id$*) on a* $P^{-1}gP \in O_2(\mathbb{R}).///$

(d) Montrer qu'il existe $P \in \mathrm{GL}_2(\mathbb{R})$ avec $P^{-1}GP \subset O_2(\mathbb{R})$ en déduire que si $G \subset \mathrm{SL}_2(\mathbb{R})$, le groupe G est cyclique et sinon G est diédral.
Preuve. L'inclusion $P^{-1}GP \subset O_2(\mathbb{R})$ *est conséquence de la question qui précède. Ainsi le groupe fini* $P^{-1}GP$ *est cyclique et sinon* G *est diédral par l'exercice 1 .///*

(e) On suppose que G est un sous-groupe fini de $\mathrm{SL}_2(\mathbb{R})$ de cardinal n. Montrer qu'il existe $P \in \mathrm{SL}_2(\mathbb{R})$ avec $PGP^{-1} =< R(\frac{2\pi}{n}) >$ où $R(\theta) := \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \in M_2(\mathbb{R})$.
Preuve. Puisque $\det PgP^{-1} = 1$ *si* $g \in G$, *ainsi* PGP^{-1} *est égal à l'unique sous-groupe de* $SO_2(\mathbb{R})$ *de cardinal* n *(voir exercice 1).///*

(f) Pour $a \in \mathbb{R}$, on note $B_{1,2}(a) := \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \in SL_2(\mathbb{R})$.
On suppose que $n \neq 2$, montrer que les deux groupes $< B_{1,2}(a)R(\frac{2\pi}{n})B_{1,2}(-a) >$ et $< B_{1,2}(b)R(\frac{2\pi}{n})B_{1,2}(-b) >$ sont égaux si et seulement si $a = b$.
Preuve. Pour simplifier le calcul on écrit $c(k)$ *resp.* $s(k)$ *pour* $\cos k$ *resp.* $\sin k$. *Une CNS est qu'il existe* $k \mid (k,n) = 1$ *avec* $B_{1,2}(a-b)R(\frac{2\pi}{n})B_{1,2}(b-a) = R(\frac{2k\pi}{n})$. *Ce qui donne les 4 conditions* $c(1) + (a-b)s(1) = c(k)$, $s(1) = s(k)$, $(a-b)c(k) - s(k) = -s(1) + (a-b)c(1)$, $c(k) + (a-b)s(k) = c(1)$. *Il suit que* $s(k) = s(1)$ *et* $c(k) = c(1)$; *ainsi* $k = 1 \mod n$ *et donc* $(a-b)s(1) = 0$. *Si* $n \neq 2$ *alors* $s(1) \neq 0$ *et donc* $a = b.///$

(2) Montrer que $\mathrm{SL}_2(\mathbb{R})$ contient un unique sous-groupe d'ordre 2.
Preuve. Soit $A := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{R})$, *avec* $A^2 = Id$. *Ainsi le polynôme minimal de* A *divise* $X^2 - 1$; *il est donc scindé à racines simples. Il suit que* A *est diagonalisable et puisque* $\det A = 1$, *il suit que* A *est l'homothétie* $\pm Id.///$

(3) Soit G un sous-groupe fini de $\mathrm{GL}_2(\mathbb{Z})$ non inclus dans $\mathrm{SL}_2(\mathbb{Z})$. Ainsi par ce qui précède on sait que $G \simeq D_{2n}$.

(a) En considérant la trace des éléments de G, montrer que $n \in \{1,2,3,4,6\}$.
Preuve. On a montré précédement qu'il existe $P \in \mathrm{GL}_2(\mathbb{R})$ *avec* $G^+ = P < R(\frac{2\pi}{n}) > P^{-1} \subset \mathrm{SL}_2(\mathbb{Z})$; *ainsi* $\mathrm{Tr}\, R(\frac{2\pi}{n}) = 2\cos\frac{2\pi}{n} \in \mathbb{Z}$ *et donc* $2\cos\frac{2\pi}{n} \in \{-2,-1,0,1,2\}.///$

(b) Réciproquement montrer que pour $n \in \{1,2,3,4,6\}$, $\mathrm{GL}_2(\mathbb{Z})$ contient un sous-groupe isomorphe à D_{2n} (on pourra considérer la matrice compagnon du polynôme caractéristique de la rotation $R(2\frac{\pi}{n})$).
Preuve. Si $n \in \{1,2,3,4,6\}$, *comme vu précédement* $\mathrm{Tr}\, R(\frac{2\pi}{n}) \in \mathbb{Z}$ *et puisque* $\det R(\frac{2\pi}{n}) = 1$, *il suit que le polynôme caractéristique de* $R(\frac{2\pi}{n})$ *est dans* $\mathbb{Z}[X]$ *et par conséquent la matrice*

compagnon $CompR(2\frac{\pi}{n})$ *du polynôme caractéristique de la rotation* $R(2\frac{\pi}{n})$ *est dans* $\mathrm{SL}_2(\mathbb{Z})$*; c'est la matrice de la rotation dans la base* $(1,0),(1,0)$ ${}^tR(2\frac{\pi}{n})$ *(l'espace est monogène!) si* $n \notin \{1,2\}$ *auquel cas* $s(1) \neq 0$.

Supposons que $n \notin \{1,2\}$*. La matrice de passage est* $P = \begin{bmatrix} 1 & c(1) \\ 0 & s(1) \end{bmatrix}$ *et* $P^{-1} = \begin{bmatrix} 1 & -\frac{c(1)}{s(1)} \\ 0 & -\frac{1}{s(1)} \end{bmatrix}$.

On vérifie que $P^{-1}R(\frac{2\pi}{n})P = \begin{bmatrix} 0 & -1 \\ 1 & 2c(1) \end{bmatrix} = CompR(2\frac{\pi}{n})$.

On calcule $P^{-1}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}P = \begin{bmatrix} 1 & 2c(1) \\ 0 & -1 \end{bmatrix} =: S \in \mathrm{GL}_2(\mathbb{Z})$*. Ainsi* $G =< CompR(2\frac{\pi}{n}), S >$ *convient.*

Supposons que $n \in \{1,2\}$*. Dans ces cas* $R(\frac{2\pi}{n}) \in \mathrm{SL}_2(\mathbb{Z})$ *et alors* $G =< R(\frac{2\pi}{n}), \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} >$ *convient.///*

(4) Soit G un sous-groupe fini de $\mathrm{GL}_2(\mathbb{Q})$. On note $M := \sum_{g\in G}\mathbb{Z}(1,0)g + \sum_{g\in G}\mathbb{Z}(0,1)g \in \mathbb{Q}^2$ et $p_1 : \mathbb{Q}^2 \to \mathbb{Q}$ la première projection i.e. $p_1((x,y)) = x$.

(a) Montrer qu'il existe $d \in \mathbb{N} - \{0\}$ avec $d\mathbb{Z}^2 \subset dM \subset \mathbb{Z}^2$.
Preuve. Puisque $G \subset \mathrm{GL}_2(\mathbb{Q})$ *est fini; il existe* $d \in \mathbb{N} - \{0\}$ *un dénominateur commun aux coefficients des matrices dans* G*; ainsi* $dG \subset M_2(\mathbb{Z})$ *et donc le sous groupe* dM *de* $\mathbb{Q}^2$ *engendré par* dG *est dans* $\mathbb{Z}^2$*. Enfin par construction* M *contient* $\mathbb{Z}^2$ *donc* $d\mathbb{Z}^2 \subset dM$*.///*

(b) Montrer que $p_1(dM) = a\mathbb{Z}$ avec $a \in \{\mathbb{Z} - \{0\}$.
Preuve. Il suit de la question précédente que la projection $p_1(dM)$ *est un sous-groupe de* $p_1(\mathbb{Z}^2) = \mathbb{Z}$ *et donc* $p_1(dM) = a\mathbb{Z}$ *avec* $a \in \mathbb{Z}$*. Puisque* $d\mathbb{Z}^2 \subset dM$*, il suit que* $d\mathbb{Z} \subset a\mathbb{Z}$*; ainsi* $a \neq 0$*.///*

(c) Montrer que $dM \cap \mathbb{Z}(0,1) = \mathbb{Z}(0,b)$ avec $b \neq 0$.
Preuve. Puisque $d\mathbb{Z}^2 \subset dM$*, il suit que* $d\mathbb{Z}(0,1) \subset dM \cap \mathbb{Z}(0,1)$*; ainsi* $dM \cap \mathbb{Z}(0,1)$ *est un sous-groupe non réduit à* 0 *du groupe monogène* $\mathbb{Z}(0,1)$*.///*

(d) Montrer que $M = \mathbb{Z}m_1 \bigoplus \mathbb{Z}m_2$.
Preuve. Soit $m \in M$*.Par ce qui précède* $dm = (x,y)$ *avec* $x = p_1(dm) \in a\mathbb{Z}$ *ainsi* $x = \lambda a$ *avec* $\lambda \in \mathbb{Z}$*. Puisque* $p_1(dM) = a\mathbb{Z}$*, il existe* $m_1 \in M$ *avec* $p_1(dm_1) = a$*; ainsi* $p_1(dm - \lambda m_1) = 0$ *et donc* $dm - \lambda m_1 \in dM \cap \mathbb{Z}(0,1) = \mathbb{Z}(0,b)$*. Soit* $m_2 \in M$ *avec* $dm_2 = (0,b)$*, alors* $m \in \mathbb{Z}m_1 + \mathbb{Z}m_2$*. Puisque* $p_1(m_2) = 0$*, il suit que la somme est directe.///*

(e) Soit $H := \{h \in \mathrm{GL}_2(\mathbb{Q}) \mid M\ {}^th = M$, montrer que $H = P\,\mathrm{GL}_2(\mathbb{Z})P^{-1}$, avec $P \in \mathrm{GL}_2(\mathbb{Q})$.
Preuve. Soit $B := ((1,0),(0,1))$ *et* $B' := (m_1, m_2)$*; ce sont des bases de* $\mathbb{Q}^2$*. Si* $h \in H$ *alors* $m_1\ {}^th \in \mathbb{Z}m_1 \bigoplus \mathbb{Z}m_2$*; ainsi la matrice* $[h]_{B'}$ *de* h *dans la base* B' *est dans* $M_2(\mathbb{Z})$*; en considérant* h^{-1} *il suit que son inverse est aussi dans* $M_2(\mathbb{Z})$ *et donc* $[h]_{B'} \in \mathrm{GL}_2(\mathbb{Z})$*. Réciproquement si* $h \in \mathrm{GL}_2(\mathbb{Q})$ *avec* $[h]_{B'} \in \mathrm{GL}_2(\mathbb{Z})$ *on a* $M\ {}^th = M$ *et donc* $h \in H$*. Soit* P *la matrice de l'identité de la base* B' *dans la base* B *alors* P *convient.///*

(f) En déduire la liste des sous-groupes finis à isomorphisme près de $\mathrm{GL}_2(\mathbb{Q})$.
Preuve. Soit G *un sous-groupes fini de* $\mathrm{GL}_2(\mathbb{Q})$*. On a construit précédemment un sous groupe* M *de* $\mathbb{Q}^2$*. Par construction* $G \subset H$*; ainsi* $P^{-1}HP$ *est un sous-groupe fini de* $\mathrm{GL}_2(\mathbb{Z})$ *et donc les sous-groupes finis à isomorphisme près de* $\mathrm{GL}_2(\mathbb{Q})$ *sont les sous-groupes finis de* $\mathrm{GL}_2(\mathbb{Z})$ *donc les sous-groupes de* D_{2n} *avec* $n \in \{1,2,3,4,6\}$*.///*

Exercice 17 Groupes et propriétés géométriques de l'orbite, [Fr. MMG96] C.1.6.11, partie 00 , [Fr. MMG10] C.1.6.11.

Soient E un espace affine euclidien, $f \in (E)$, G le sous-groupe de (E) engendré par f, $o \in E$. Alors on a les équivalences suivantes :

(1) L'orbite de o sous G est bornée,

(2) Toute orbite sous G d'un point de E est bornée,

(3) f a un point fixe.

Preuve.

- *Montrons que (1) implique (2).*
  Soit $m \in E$ avec $f(m) = m$ alors $\forall k \in \mathbb{N}$ on a $d(m, f^k(o)) = d(f^k(m), f^k(o)) = d(m, o)$ ainsi l'orbite de m sous G est bornée.
- *Montrons que (2) implique (3).*
  Il existe $r > 0$ avec $d(o, f^k(o)) \leq r$ pour tout $k \in \mathbb{N}$. Soit $m \in E$ alors $d(f^k(o), f^k(m)) = d(o, m)$ et donc $d(o, f^k(m)) \leq d(o, f^k(o)) + d(f^k(o), f^k(m)) \leq r + d(o, m)$.///
- *Montrons que (3) implique (1).*
  Par le théorème de la forme réduite des isométries de E il existe $g \in Is(E)$ avec un point fixe A et $\vec{v} \in \mathrm{Ker}(\vec{f} - Id_E)$ avec $f = t_{\vec{v}} \circ g = g \circ t_{\vec{v}}$. Ainsi $f^k(A) = A + k\vec{v}$ et donc $d(A, f^k(A)) = k\|\vec{v}\| \to \infty$ si $\vec{v} \neq \vec{0}$. Puisque la suite $f^k(A)$ est bornée il suit que $\vec{v} = \vec{0}$ ainsi $f = g$ a un point fixe.///