EPFL Automne 2017
Geometrie, MATH-120

Solution 6

Dans ces exercices, on va classifier a isomorphisme pres les petits groupes finis.

Exercice 1. Montrer qu'a isomorphisme pres il n'existe qu'un seul groupe d'ordre 1,2, 3, 5, 7.

Solution 1. Remarquons que 1,2, 3, 5 et 7 sont des nombres premiers. En généralisant un peu l'énoncé, considérons un groupe G d'ordre p où p est premier. Pour $p = 1$, $G = \{e_G\}$. Pour $p \neq 1$, par le théorème de Lagrange, l'ordre de tout élément de G divise p. Comme p est premier, l'ordre d'un élément de G est égal à 1 ou p. Soit $g \in G$ un element différent de l'élément neutre alors g est d'ordre p et génère G qui est donc cyclique. Par l'exercice 4 de la série 5, G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Donc tout groupe d'ordre p premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Exercice 2. On discute le cas des groupes d'ordre 4.

1. Montrer que le groupe $\mathbb{Z}/4\mathbb{Z}$ et le groupe produit $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes (regarder les ordres des elements.) On va montrer que ce sont les seuls.
2. Soit $(G, .)$ un groupe d'ordre 4. Que dire de G si il possede un element d'ordre 4.
3. Si ce n'est pas le cas, quels sont les ordres des elements de G ? Montrer que $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 3. Soit G un groupe d'ordre 6. On va montrer qu'il n'existe a isomorphisme pres que deux groupes possibles.

1. Quels sont les ordres possibles des elements de G ?
2. Que dire si G possede un element d'ordre 6 ? Dans la suite on suppose que G n'a pas d'element d'ordre 6.
3. On suppose que tous les elements non triviaux de G sont d'ordre 2 ; Montrer qu'alors
$$\forall g \in G,\ g^{-1} = g \text{ et que } \forall g, g' \in G,\ g.g' = g'.g.$$
Montrer que G contiendrait alors un groupe d'ordre 4 et que c'est impossible.
4. Ainsi G possede au moins un element d'ordre 3. On notera cet element r et $r^{\mathbb{Z}} = \{e_G, r, r^2\}$ le groupe qu'il engendre. Quel est l'ordre de r^2 ?

5. Soit $s \in G - r^{\mathbb{Z}}$. Montrer que

$$G - r^{\mathbb{Z}} = \{s, s.r, s.r^2\}.$$

6. Montrer que $s^2 \in r^{\mathbb{Z}}$ et que necessairement s est d'ordre 2 (montrer que sinon s serait d'ordre 6).
7. Montrer que $s.r$ et $s.r^2$ sont egalement d'ordre 2 et que

$$s.r.s = s.r.s^{-1} = r^{-1} = r^2.$$

8. Ecrire la table de multiplication de ce groupe. Ce groupe est le groupe dihedral d'ordre 6.
9. Ce groupe existe bien et est isomorphe au groupe des isometries d'un triangle equilateral centre a l'origine : trouver les isometries qui correspondent aux elements r et s.

Solution 3. 1. L'ordre d'un élément de G doit diviser $|G| = 6$. Les ordres possibles pour les éléments de G sont donc 1 (l'élément neutre), 2, 3 et 6.

2. Supposons qu'il existe $g \in G$ d'ordre 6. Alors le sous-groupe $g^{\mathbb{Z}}$ de G engendré par g a pour cardinal 6, i.e. $\left|g^{\mathbb{Z}}\right| = 6 = |G|$. Donc $g^{\mathbb{Z}} = G$ et G est cyclique. D'après l'exercice 4 de la série 5, G est isomorphe à $\mathbb{Z}/6\mathbb{Z}$.

3. Supposons que tout élément de G est d'ordre 2, c'est-à-dire

$$\forall g \in G, g^2 = e_G.$$

En multipliant cette égalité (à gauche ou à droite) par g^{-1}, on obtient

$$\forall g \in G, g = g^{-1}.$$

De même, G étant un groupe, pour tout couple $(g, g') \in G^2$, $gg' \in G$. Ainsi

$$\forall (g, g') \in G^2, gg' = (gg')^{-1} = g'^{-1}g^{-1} = gg'$$

où la première égalité vient du calcul précédent disant que tout élément de G est égal à son inverse, la seconde de la définition de l'inverse d'un produit et la dernière de l'application du calcul précédent une nouvelle fois.

On peut ainsi vérifier que pour tout $(g, g') \in (G \setminus \{e_G\})^2$, le groupe engendré par g et g' est égal à $< g, g' >= \{e_G, g, g', gg'\}$ (on peut vérifier le critère de sous-groupe à la main). Ce sous-groupe est alors d'ordre 4. Ceci est impossible car 4 ne divise pas 6 contredisant le théorème de Lagrange.

Donc il existe au moins un élément de G d'ordre 3.

4. Soit $r \in G$ un élément d'ordre 3. On a $r^{\mathbb{Z}} = \{e_G, r, r^2\}$. $r^2 \neq e_G$ implique que r^2 est d'ordre 2, 3 ou 6 en tant qu'élément de G. Comme $r^2 \in r^{\mathbb{Z}}$ appartient à un sous-groupe d'ordre 3, son ordre doit aussi diviser 3 et donc y être égal, i.e. r^2 est d'ordre 3.

5. Soit $s \in G \setminus r^{\mathbb{Z}}$. Montrons d'abord que pour tout $k \in \mathbb{Z}$, $sr^k \in G \setminus r^{\mathbb{Z}}$. Pour cela, on raisonne par l'absurde. Supposons

$$\exists k \in \mathbb{Z}\,,\ sr^k \in r^{\mathbb{Z}}$$

c'est-à-dire

$$\exists (k,l) \in \mathbb{Z}^2\,,\ sr^k = r^l.$$

Alors, en multipliant cette égalité à droite par $r^{-k} = (r^{-1})^k$, on a

$$\exists (k,l) \in \mathbb{Z}^2\,,\ s = r^{l-k}$$

ce qui contredit $s \notin r^{\mathbb{Z}}$.

Donc pour tout $k \in \mathbb{Z}$, $sr^k \in G \setminus r^{\mathbb{Z}}$. En particulier sr et sr^2 appartiennent à $G \setminus r^{\mathbb{Z}}$. Montrons maintenant que s, sr et sr^2 sont tous distincts. Pour cela, on écrit

$$\forall (i,j) \in \{0,1,2\}^2\,,\ sr^i = sr^j \Leftrightarrow r^{j-i} = e_G \Leftrightarrow i = j$$

où la première équivalence est obtenue en multipliant à gauche par $(sr^i)^{-1} = r^{-i}s^{-1}$ et la seconde en tenant compte du fait que r est d'ordre 3. Ainsi, $G = \{e_G, r, r^2, s, sr, sr^2\}$.

6. Par l'absurde, supposons $s^2 \in G \setminus r^{\mathbb{Z}}$. Alors $s^2 \in \{s, sr, sr^2\}$, i.e.

$$\exists i \in \{0,1,2\}\,,\ s^2 = sr^i.$$

En multipliant à gauche cette égalité par s^{-1}, on obtient

$$\exists i \in \{0,1,2\}\,,\ s = r^i$$

ce qui est impossible puisque $s \notin r^{\mathbb{Z}}$. Donc $s^2 \in r^{\mathbb{Z}} = \{e_G, r, r^2\}$.

Si s^2 était égal à r ou r^2, alors il serait d'ordre 3. Donc s serait d'ordre 6, ce qui est impossible par hypothèse. Donc $s^2 = e_G$ et s est d'ordre 2.

7. Nous avons défini s comme un élément *quelconque* de $G \setminus r^{\mathbb{Z}}$ et avons prouvé qu'il était d'ordre 2. Nous aurions pu prendre n'importe quel autre élément de $G \setminus r^{\mathbb{Z}}$ et raisonner de la même manière. Donc tout élément de $G \setminus r^{\mathbb{Z}} = \{s, sr, sr^2\}$ est d'ordre 2.

s étant d'ordre 2, on a $s^{-1} = s$. Donc $srs^{-1} = srs$. De plus, $r^3 = e_G$ implique que $r^2 = r^{-1}$ par multiplication (à droite ou à gauche) par r^{-1}. Finalement, sr est d'ordre 2 implique

$$sr = (sr)^{-1} = r^{-1}s^{-1}.$$

En multipliant à droite par s, on obtient la dernière égalité $srs = r^{-1}$.

8. La table de multiplication de G est donnée par

$\cdot$	e_G	r	r^2	s	sr	sr^2
e_G	e_G	r	r^2	s	sr	sr^2
r	r	r^2	e_G	sr^2	s	sr
r^2	r^2	e_G	r	sr	sr^2	s
s	s	sr	sr^2	e_G	r	r^2
sr	sr	sr^2	s	r^2	e_G	r
sr^2	sr^2	s	sr	r	r^2	e_G

Les seuls éléments demandant du calcul sont $rs = s^{-1}r^2 = sr^2$ où la première égalité vient de $srs = r^2$ prouvé dans la question précédente et la seconde vient de $s = s^{-1}$ puisque s est d'ordre 2. On obtient de même $r^2s = r(rs) = r(sr^2) = (rs)r^2 = sr^4 = sr$. Les autres produit non-triviaux sont obtenus par multiplication à droite par r et r^2.

9. Soit (ABC), un triangle équilatéral centré en l'origine O. On peut alors générer les isométrie de ce triangle par deux transformations.

- D'une part, une rotation r centrée en O échangeant les sommets A, B et C. C'est-à-dire une rotation d'angle $2\pi/3$ ou $-2\pi/3$. Le choix du signe correspond à choisir r ou r^2 comme élément d'ordre 3
- D'autre part, une symétrie orthogonale s par rapport à l'une des droites OA, OB ou OC. Le choix de l'une des droites correspond à choisir un élément d'ordre 2 dans $G \setminus r^{\mathbb{Z}}$. Si s correspond à OA, alors sr et sr^2 correspondent aux symétries par rapport à OB et OC.

Définition 1. *Soit X un ensemble. Une distance est une application*

$$d(\cdot,\cdot) : \begin{array}{ccc} X \times X & \mapsto & \mathbb{R}_{\geqslant 0} \\ (P,Q) & \mapsto & d(P,Q) \end{array}$$

qui verifie les proprietes suivantes

- *Separation des points : pour tout $P, Q \in X$,*

$$d(P,Q) = 0 \iff P = Q.$$

- *Symetrie : pour tout $P, Q \in X$,*

$$d(P,Q) = d(Q,P).$$

— *Inegalite du triangle : pour tout $P, Q, R \in X$,*

$$d(P,R) \leqslant d(P,Q) + d(Q,R).$$

Exercice 4. Montrer que les applications suivantes definissent des distances sur $\mathbb{R}^2$. Pour chacune de ces distances, dessiner la boule unite centree a l'origine (on note $\mathbf{0} = (0,0)$)

$$B_d(\mathbf{0},1) := \{(x,y) \in \mathbb{R}^2,\ d(\mathbf{0},(x,y)) \leqslant 1\}.$$

$$d_0((x,y),(x',y')) = \delta_{x\neq x'} + \delta_{y\neq y'},\ \text{avec } \delta_{x\neq x'} = \begin{cases} 0 & si\ x = x' \\ 1 & si\ x \neq x' \end{cases}.$$

$$d_1((x,y),(x',y')) = |x-x'| + |y-y'|.$$

$$d_4((x,y),(x',y')) = (|x-x'|^4 + |y-y'|^4)^{1/4}.$$

$$d_\infty((x,y),(x',y')) = \max(|x-x'|, |y-y'|).$$

Pour la distance d_4 on pourra introduire la "norme"

$$\|\vec{u}\|_4 := (x^4 + y^4)^{1/4}$$

et montrer

$$\forall \vec{u}, \vec{v} \in \mathbb{R}^2,\ \|\vec{u} + \vec{v}\|_4 \leqslant \|\vec{u}\|_4 + \|\vec{v}\|_4.$$

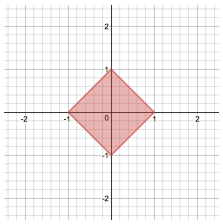
Pour cela on pourra utiliser la propriete d'homogeneite (ie.

$$\forall \vec{u} \in \mathbb{R}^2,\ \lambda \in \mathbb{R},\ \|\lambda\vec{u}\|_4 = |\lambda|\|\vec{u}\|_4\ )$$

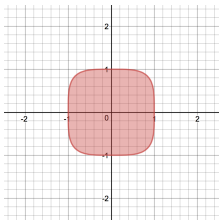
Solution 4. Montrer que ces applications définissent bien des distances est obtenu en vérifiant les axiomes de la définition pour chaque cas.

La boule unité $B_{d_0}(\mathbf{0},1)$ est la croix obtenue comme l'union de l'axe des abscisse et des ordonnées : $B_{d_0}(\mathbf{0},1) = \{x=0\} \bigcup \{y=0\}$.

$B_{d_1}(\mathbf{0},1) = \{(x,y) \in \mathbb{R}^2, |x| + |y| \leqslant 1\}$ donnée :



$B_{d_4}(\mathbf{0}, 1)$ est donnée par



$B_{d_\infty}(\mathbf{0}, 1)$ est donnée par