INTRODUCTION À LA THÉORIE DES GROUPES

DOSSIER D'EXERCICES (1)

1

Groupes diédraux

On rappelle que $\mathbf{Is}(P)$ désigne le groupe des isométries affines du plan affine euclidien orienté P. Ce groupe contient exactement quatre types d'éléments :

(1) les rotations (déterminées par leur centre et leur angle);
(2) les translations (déterminées par leur vecteur);
(3) les symétries orthogonales (ou réflexions) (déterminées par leur axe);
(4) les réflexions glissées (produit du'une symétrie orthogonale s_Δ avec une translation $t_{\vec{u}}$ de vecteur parallèle à l'axe Δ).

Les deux premières familles regroupent les isométries directes qui forment un sous-groupe de $\mathbf{Is}(P)$ noté $\mathbf{Is}^+(P)$. Les isométries directes sont celles qui préservent l'orientation. Le déterminant de leur partie linéaire dans une base orthonormée directe est positif ($= 1$).

1.1. Dans le plan affine euclidien P on place les points M_j, $j = 0,1,2$ d'affixe respectif $z_i = \exp(2ij\pi/3)$. Ce sont les sommets d'un triangle équilatéral. On note $T = \{M_0,M_1,M_2\}$ et on appelle $\mathbf{D}_3$ l'ensemble des isométries du plan qui conservent T :

$$\mathbf{D}_3 : \{f \in \mathbf{Is}(P) : f(T) = T\}.$$

1.1.1. Montrer que $\mathbf{D}_3$ est un sous-groupe de $(\mathbf{Is}(P),\circ)$.

1.1.2. Montrer que $\mathbf{D}_3$ est formé de 6 éléments. On pourra d'abord établir que tout élément de $\mathbf{D}_3$ laisse invariant le centre de gravité du triangle. Montrer que tous les éléments s'expriment en fonctions de deux d'entre eux que l'on précisera (on dit que ces deux éléments forment un ensemble générateur de $\mathbf{D}_3$. Cette notion sera étudiée dans le cours).

1.1.3. Faire une table de $\mathbf{D}_3$. (C'est un tableau à double entrée, avec la liste des éléments de $\mathbf{D}_3$ et leur produit — comme dans une table de multiplication élémentaire.)

1.2. On considère maintenant les points N_j, $j = 0,1,2,3$ d'affixe respectif $z_i = \exp(2ij\pi/4)$. Ce sont les sommets d'un carré. On note $C = \{N_0,N_1,N_2,N_3\}$ et on appelle $\mathbf{D}_4$ l'ensemble des isométries du plan qui conservent C :

$$\mathbf{D}_4 = \{f \in \mathbf{Is}(P) : f(C) = C\}.$$

1.2.1. Montrer que $\mathbf{D}_4$ est un sous-groupe de $(\mathbf{Is}(P),\circ)$.

1.2.2. Montrer que $\mathbf{D}_4$ est formé de 8 éléments.

1.2.3. Faire une table de $\mathbf{D}_4$.

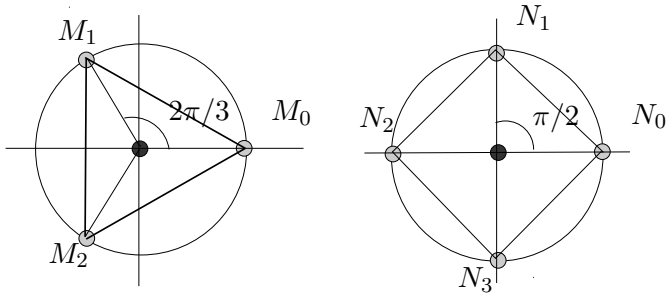

FIG. 1. *Les figures T et C*

1.3. Plus généralement, si P_n désigne le polygone régulier à n sommets M_j d'affixes respectifs $z_j = \exp(2ij\pi/n)$, $j = 0, \ldots, n-1$, on appelle $\mathbf{D}_n$ le sous-groupe de $\mathbf{Is}(P)$ formé des isométries qui laissent P_n *globalement* invariant. Montrer que $\mathbf{D}_n$ contient $2n$ éléments et dresser la liste de ses éléments en montrant qu'ils peuvent tous s'exprimer à partir de deux d'entre eux.

2

LE CENTRE D'UN GROUPE

Soit $(G,*)$ un groupe. On définit le sous-ensemble $Z(G)$ par

$$Z(G) = \{u \in G : gu = ug \text{ pour tout } g \in G\}$$

Autrement dit, u est un élément de $Z(G)$ s'il commute avec *tous* les éléments de G.

2.1. Montrer que $Z(G)$ est un sous-groupe de G. (On l'appelle *le centre* de G.) A quelle(s) condition(s) a-t-on G=Z(G)?

2.2. Dans cette partie, on cherche $Z(\mathbf{GL}_2(\mathbb{R}))$.

2.2.1. Soit

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(\mathbf{GL}_2(\mathbb{R})).$$

En utilisant le fait que A commute avec les matrices J et K données par

$$I = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

montrer qu'on a nécessairement $a = d$ et $b = 0 = c$.

2.2.2. En déduire $Z(\mathbf{GL}_2(\mathbb{R}))$.

2.3. Montrer que si ϕ est un isomorphisme de $(G,*)$ sur $(G',.)$ alors $\phi(Z(G)) = Z(G')$.

3

RECHERCHE DES GÉNÉRATEURS DE $\mathbf{GL}_2(\mathbb{K})$, $\mathbb{K} = \mathbb{R},\mathbb{Q}$ OU $\mathbb{C}$

Pour $\alpha \in \mathbb{K}$ et $\beta \in \mathbb{K}^\star$ on définit les matrices

$$t_{12}(\alpha) = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, t_{21}(\alpha) = \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}, d_{11} = \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix} \text{ et } \quad d_{22}(\beta) = \begin{pmatrix} 1 & 0 \\ 0 & \beta \end{pmatrix}$$

3.1. si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ calculer $t_{ij}(\alpha)\,A$ et $A\,t_{ij}(\alpha)$.

3.2. Montrer que si $d \neq 0$ alors

$$t_{12}\left(\frac{-b}{d}\right) \cdot A \cdot t_{21}\left(\frac{-c}{d}\right) = \begin{pmatrix} a - \frac{bc}{d} & 0 \\ 0 & d \end{pmatrix}.$$

En déduire que

$$A \in \langle t_{ij}(\alpha), d_{ii}(\beta) : (\alpha,\beta) \in \mathbb{K} \times \mathbb{K}^\star \rangle$$

3.3. Montrer, en se ramenant au cas $d \neq 0$ que les $t_{ij}(\alpha), d_{ii}(\beta) : (\alpha,\beta) \in \mathbb{K} \times \mathbb{K}^\star$ forment un ensemble générateur de $\mathbf{GL}_2(\mathbb{K})$.

3.4. Trouver un ensemble générateur pour $\mathbf{GL}_3(\mathbb{K})$ et indiquer, sans donner de détail, comment trouver plus généralement un ensemble générateur de $\mathbf{GL}_n(\mathbb{K})$.

4

LIEN ENTRE $\mathbb{C}$ ET UN SOUS-GROUPE DE $\mathbf{GL}_2(\mathbb{R})$

Ce problème fait intervenir les groupes:

a) $(\mathbf{GL}_2(\mathbb{R}),\cdot)$ formé de l'ensemble des matrices 2×2 inversibles à coefficients réels que l'on munit de la multiplication habituelle des matrices,

b) $(\mathbb{C}^*,\cdot)$ formé des nombres complexes *non nuls* que l'on munit de la multiplication habituelle des nombres complexes,

c) $(\mathbb{R}^{\star+},\cdot)$ formé de l'ensemble des nombres réels *strictement positifs* que l'on munit de la multiplication habituelle des nombres réels. On a d'ailleurs $\mathbb{R}^{\star+} < (\mathbb{C}^*,\cdot)$.

On rappelle que

$$\text{si } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{GL}_2(\mathbb{R}) \text{ alors } A^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

4.1. Soit G l'ensemble des matrices **inversibles** M de la forme

$$M = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$$

où α et β sont des nombres **réels**. (On a donc $G \subset \mathbf{GL}_2(\mathbb{R})$.)

(1) Montrer que G est un sous-groupe de $(\mathbf{GL}_2(\mathbb{R}),\cdot)$.

(2) Montrer que l'application ψ définie par

$$\psi(M) = \alpha + i\beta \quad \text{si} \quad M = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$$

est un **isomorphisme** de $(G,\cdot)$ sur $(\mathbb{C}^*,\cdot)$. (On vérifiera d'abord qu'elle prend bien ses valeurs dans $\mathbb{C}^*$.)

(3) Soit $n \in \mathbb{N}^*$. On définit $M_n \in G$ par

$$M_n = \begin{pmatrix} \cos(\frac{2\pi}{n}) & \sin(\frac{2\pi}{n}) \\ -\sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{pmatrix}.$$

Quel est l'ordre de M_n ? Donner la liste (en justifiant votre réponse) des éléments du groupe $\langle M_n \rangle$. (On pourra utiliser la question précédente et calculer notamment $\psi(M_n^k)$. On rappelle que

$$M_n^k = \underbrace{M_n \cdot M_n \cdot \cdots \cdot M_n}_{k\,fois}.)$$

4.2. On considère $S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{R})$ et H, le sous-groupe de $\mathbf{GL}_2(\mathbb{R})$ engendré par S et $M_4 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Autrement dit, $H = \langle S, M_4 \rangle$.

(1) Quel est l'ordre de S? Montrer que $M_4^3 = M_4^{-1}$.
(2) Montrer que $M_4 \cdot S = S \cdot M_4^{-1}$. Que dire de $M_4^{-1}.S$?
(3) Donner la liste (en justifiant votre réponse) de tous les éléments de H. (Indication. On devra montrer que H contient **huit et seulement huit** éléments.)

4.3. On rappelle que pour un groupe $(W, \cdot .)$ quelconque, $Aut(W)$ désigne l'ensemble des automorphismes du groupe $(W,\cdot)$, c'est-à-dire les morphismes bijectifs de $(W,\cdot)$ dans lui-même. Cet ensemble $Aut(W)$ devient un groupe lorsqu'on le munit de la loi de composition des applications. L'élément neutre de ce groupe $(Aut(W),\circ)$ est l'application identité. *Ces propriétés sont admises, on ne demande pas de les démontrer.*

(1) Les trois applications suivantes sont-elles des **automorphismes** de $(\mathbb{C}^*,\cdot)$?

$$\phi_1 : \begin{array}{ccc}(\mathbb{C}^*,\cdot) & \longrightarrow & (\mathbb{C}^*,\cdot) \\ z & \longmapsto & \overline{z}\end{array}, \quad \phi_2 : \begin{array}{ccc}(\mathbb{C}^*,\cdot) & \longrightarrow & (\mathbb{C}^*,\cdot) \\ z & \longmapsto & z^2\end{array}, \quad \phi_3 : \begin{array}{ccc}(\mathbb{C}^*,\cdot) & \longrightarrow & (\mathbb{C}^*,\cdot) \\ z & \longmapsto & \frac{z}{|z|^2}\end{array}$$

(2) On considère à présent le groupe $(\mathbb{R}^{*+},\cdot)$. Montrer que si $f \in Aut(\mathbb{R}^{*+})$ alors $\phi_f \in Aut(\mathbb{C}^\star)$ où ϕ_f est définie par

$$\phi_f : \begin{array}{ccc}(\mathbb{C}^*,\cdot) & \longrightarrow & (\mathbb{C}^*,\cdot) \\ z & \longmapsto & f(|z|) \cdot \frac{z}{|z|}\end{array}$$

(3) Montrer que $Aut(\mathbb{C}^*)$ contient une infinité d'éléments.
(4) Montrer que les groupes $Aut(\mathbb{C}^*)$ et $Aut(G)$ sont isomorphes. (On pourra construire un isomorphisme Ψ entre $Aut(\mathbb{C}^*)$ et $Aut(G)$ en utilisant l'isomorphisme ψ de I) b).)

(Partiel avril 2004)

5

SOUS-GROUPES FINIS DE $\mathbf{Is}(P)$

On détermine tous les sous-groupes finis de $\mathbf{Is}(P)$ en montrant qu'ils sont tous de la forme $\mathbf{D_n}$ ou $\mathbf{D}_n \cap \mathbf{Is}^+(P)$.

Soit donc G un sous-groupe fini de $\mathbf{Is}(P)$.

5.1. Supposons que $G \subset \mathbf{Is}^+(P)$ et appelons m l'ordre de G.

Soit $A \in P$. Nous appelons Ω_G l'isobarycentre des points $\{f(A) : f \in G\}$, Pour tout point M du plan, on a

$$\sum_{f \in G} \overrightarrow{\Omega f(A)} = \vec{0}.$$

5.1.1. Démontrer que quelle que soit $h \in G$, on a $h(\Omega) = \Omega$. On pourra utiliser le fait que $h(\Omega)$ est l'isobarycentre des points $\{hf(A) : f \in G\}$.

5.1.2. En déduire que G est formé de rotations de même centre.

5.1.3. Montrer que les angles de ces rotations sont tous de la forme $2k\pi/m$, $k \in \{0, \ldots, m-1\}$.

5.1.4. Montrer finalement que G est de la forme $G = \{\mathcal{R}(A, 2k\pi/m) : k = 0, \ldots, m-1\}$.

5.2. Nous étudions maintenant le cas général où G n'est plus supposé être inclus dans $\mathbf{Is}^+(P)$.

5.2.1. Montrer que $G^+ := G \cap \mathbf{Is}^+(P)$ est un sous-groupe fini de $\mathbf{Is}(P)$ auquel on peut appliquer les résultats précédents pour obtenir

$$G^+ = \{R^k \,:\, k = 0, \ldots, m-1\}$$

avec $R = \mathcal{R}(A, 2k\pi/m)$.

5.2.2. Supposons que $G \neq G^+$ et prenons s une isométrie négative dans $G^- := G \cap \mathbf{Is}^-(P)$.

(1) Montrer que l'application $f \in G^+ \to s \circ f \in G^-$ est une bijection.
(2) Montrer que $sRs = R^{n-1}$ (que dire de $sRsR$?) et en déduire que G est un groupe diédral.

6

GROUPE DES AUTOMORPHISMES INTÉRIEURS

Soit $(G,\cdot)$ un groupe.

6.1. Montrer que l'ensemble $\mathbf{Aut}(G)$ formé de tous les automorphismes de G est un groupe lorsqu'on le munit de la loi de composition des applications.

6.2. On appelle automorphisme intérieur de G, toute application de la forme $\phi_g = x \in G \to g^{-1} \cdot x \cdot g$.

6.2.1. Vérifier que les automorphismes inrérieurs sont effectivement des automorphismes de G.

6.2.2. Montrer que $\mathbf{Int}(G) \leq \mathbf{Aut}(G)$ et que $\mathbf{Int}(G) \simeq G/Z(G)$. (On recherchera un morphisme de G dans $\mathbf{Int}(G)$.)

6.3. $\mathbf{Int}(G)$ est-il un sous-groupe distingué de $\mathbf{Aut}(G)$?

7

UN SOUS-GROUPE DE $\mathbf{S}_4$

On considère les éléments suivants du groupe de permutation $\mathbf{S}_4$: $\sigma_1 = (12)(34)$, $\sigma_2 = (13)(24)$, $\sigma_3 = (14)(23)$. On rappelle que e désigne l'élément neutre de $(\mathbf{S}_4,\cdot)$, autrement dit e est la bijection *identité*.

(1) Déterminer l'ordre de chaque élément de $H := \{e, \sigma_1, \sigma_2, \sigma_3\}$.
(2) Montrer que H est un sous-groupe de $\mathbf{S}_4$. (On pourra construire une table.) H est-il commutatif?
(3) Déterminer tous les sous-groupes de H. (Justifier votre réponse.)
(4) (a) Soit $f \in \mathbf{S}_4$. Montrer que
$$f \cdot (12)(34) \cdot f^{-1} = \big(f(1)f(2)\big)\big(f(3)f(4)\big).$$
(b) Montrer que H est un sous-groupe *distingué* de $\mathbf{S}_4$.
(5) Montrer que H est isomorphe à $\big(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\,,\,+\big)$. (On pourra construire un isomorphisme explicite entre H et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.)

(Contrôle terminal juin 2005)

8

GÉNÉRATEURS DES GROUPES SYMÉTRIQUES ET ALTERNÉS

Soit $n \geq 2$.

8.1. Montrer que tout cycle $(a_1,a_2,\cdots,a_p)$ $(p \geq 2)$ s'écrit comme un produit de transpositions.

8.2. Montrer que toute permutation (i,j) avec $i < j$ vérifie

$$(i,j) = (i,i+1)(i+1,i+2)\cdots(j-1,j)(j-2,j-1)(j-3,j-2)\cdots(i,i+1).$$

8.3. Montrer que

$$(k,k+1) = (1,k)(1,k+1)(1,k).$$

8.4. Montrer les égalités suivantes

(1) $\mathbf{S}_n = \langle(1,2),(1,3),\ldots,(1,n)\rangle$.
(2) $\mathbf{S}_n = \langle(1,2),(1,2,\ldots,n)\rangle$
Indication : Posant $\sigma = (1,2,\ldots,n)$, on pourra montrer que

$$\sigma^k(12)\sigma^{-k} = (k+1,k+2).$$

8.5. Soit $n \geq 3$. Montrer que $(a,b)(a,c) = (a,c,b)$ et $(a,b)(c,d) = (a,c,b)(a,c,d)$. En déduire

(3) $\mathbf{A}_n$ est engendré par l'ensemble des 3-cycles.

9

GROUPES OPÉRANT SUR UN ENSEMBLE

9.1. Définitions. Soient G un groupe de neutre e et Ω un ensemble non vide. Une application Ψ de $G \times \Omega \to \Omega$ pour laquelle on note $g \cdot x := \Psi(g,x)$ est appelée une *opération* de G sur Ω si elle vérifie les deux conditions suivantes

(1) $\forall g,g' \in G\ \forall x \in \Omega\ g \cdot (g' \cdot x) = (gg') \cdot x$,
(2) $\forall x \in \Omega,\ e \cdot x = x$.

On dit alors que G *opère* sur Ω (par Ψ). Pour être précis, il faudrait parler d'opération à gauche et l'on pourrait définir de manière similaire (comment ?) une opération à droite dont l'étude ne différerait en rien.

9.2. On désigne par $\hat{g}$ l'application $x \in \Omega \to g \cdot x \in \Omega$.

9.2.1. Montrer que $\hat{g} \in \mathbf{S}(\Omega)$ où $\mathbf{S}(\Omega)$ est le groupe des bijections de Ω dans lui-même.

9.2.2. Montrer que l'application $g \in G \to \hat{g} \in \mathbf{S}(\Omega)$ est un morphisme de groupe. Lorsque ce morphisme est injectif, on dit que l'opération Ψ est *fidèle* ou *effective*.

9.3. Exemples. Les groupes les plus usuels sont déjà des groupes de fonctions sur un ensemble Ω et il y a alors une opération triviale : on applique la fonction g à l'élément x. Par exemple si G est le groupe des permutations $\mathbf{S}_n$ alors on prend $\Omega = \Omega(n) = \{1,\ldots,n\}$ et $\sigma \cdot n := \sigma(n)$. Si G est un sous-groupe de $\mathbf{GL}_n(\mathbb{K})$ (le groupe des matrices inversibles d'ordre n à coefficients dans K) alors chaque élément de G comme toute matrice s'identifie à une application linéaire sur $\mathbb{K}^n$ et l'opération de G sur $\mathbb{K}^n$ est $g \cdot x = g(x)$. Le cas suivant couvre pratiquement toutes les applications non théoriques du concept d'opération.

(1) Soit G un groupe et ϕ un morphisme de G dans $\mathbf{GL}_n(\mathbb{K}^n)$. Montrer que l'application définie sur $G \times \mathbb{K}^n$ par $g \cdot x = \phi(g)(x)$ est une opération de G sur $\mathbb{K}^n$. En déduire une opération de $\mathbf{S}_n$ sur $\mathbb{K}^n$.

(2) Construire à partir d'une opération de G sur Ω, une opération de G sur Ω^n.

Il est cependant souvent très commode pour étudier les groupes pour eux-mêmes d'utiliser des opérations dans le cas où Ω est égal au groupe opérant ou, au moins, est directement construit à partir de ce groupe. Voici quelques exemples.

(3) *L'opération par translation à gauche.* On prend $\Omega = G$ et $g \cdot x = gx$ (le produit de g par x. Vérifier que c'est bien une opération

(4) *L'opération par conjugaison.* On prend $\Omega = G$ et $g \cdot x = gxg^{-1}$. Vérifier que c'est bien une opération.

(5) *L'opération par conjugaison sur les sous-groupes.* On prend pour Ω l'ensemble des sous-groupes de G et si X est un de ces sous-groupes on pose $g \cdot X = gXg^{-1} = \{gxg^{-1} : x \in X\}$. vérifier que c'est bien une opération.

9.4. Orbites et Stabilisateurs. Si G opère sur Ω, on définit un relation sur Ω par xRy s'il existe $g \in G$ tel que $g \cdot x = y$.

9.4.1. Montrer que R est une relation d'équivalence. Les classes d'équivalence de cette opération sont appelées *orbites*. L'orbite de $x \in \Omega$, notée $O(x)$ est ainsi donnée par

$$O(x) = \{g \cdot x : g \in G\}. \tag{9.1}$$

9.4.2. Exemples d'orbites.

(1) Le groupe des rotations de centre A opère sur le plan. Décrire les orbites.

(2) Soit $\sigma \in \mathbf{S}_n$. le groupe cyclique engendré par σ opère sur Ω_n. Décrire les orbites.

(3) Le groupe $\mathbf{Is}(\mathcal{P})$ des isométries (affines) du plan opère sur $\mathcal{P}$ par $f \cdot (M,N) = (f(M),f(N))$. A quelle(s) conditions(s) deux couples (M,N) et (M',N') sont-ils sur la même orbite ?

(4) Lorsque G opère sur lui-même par conjugaison, à quelle condition l'orbite de x est-elle réduite à x ?

Lorsque l'opération contient une et une seul orbite, on dit que l'opération est *transitive*. Pour $x \in \Omega$, on note $Stab(x)$ l'ensemble des $g \in G$ tel que $g \cdot x = x$.

(5) Montrer que $Stab(x)$ est un sous-groupe de g.

Puisque $Stab(x)$ est un groupe, on peut définir le quotient $G/Stab(x)$ comme l'ensemble des classes d'équivalences de la relation gRg' si $g^{-1}g' \in Stab(x)$ (ce n'est pas nécessairement un groupe).

(6) On veut définir une application ϕ sur $O(x)$ par $\phi(g \cdot x) = g\,stab(x)$, autrement dit $\phi(g \cdot x)$ est la classe de g dans $G/Stab(x)$. Montrer que cette définition est consistante. (Où est le problème ?) Montrer ensuite qu'elle est bijective puis les théorèmes suivants.

Théorème. *Si $x' = g \cdot x$ alors $stab(x') = g\,stab(x)\,g^{-1}$.*

Théorème. *Si Ω est fini et que l'opération de G sur Ω possède r orbites $O(x_i)$, $i = 1, \ldots, r$, alors*

$$|\Omega| = \sum_{i=1}^{r} |G/stab(x_i)| \tag{9.2}$$

où $|\cdot|$ désigne le cardinal.

9.5. Soit G un groupe fini que l'on fait opérer sur lui-même par conjugaison (voir au dessus). Montrer que le nombre d'orbites ayant un cardinal égal à 1 est égal à $|Z(G)|$ où $|Z(G)|$ désigne le centre du groupe. En déduire une démonstration basée sur (9.2) du théorème suivant.

Théorème. *Si G un groupe fini de cardinal p^n où p est un nombre premier > 1 alors le centre de G n'est pas réduit à l'élément neutre.*