X2010 2ème Composition de Mathématiques

1- $\forall g \in G,\ g^k = Id$ avec $k = |G|$ (l'ordre de tout élément divise l'ordre du groupe, théorème de Lagrange) ; tout élément de G possède donc un annulateur à racines simples, à savoir $X^k - 1$; il en résulte que tout élément de G est diagonalisable. Si de plus G est commutatif, on sait que deux endomorphismes diagonalisables qui commutent le sont dans une même base, ceci vaut donc pour l'ensemble des éléments de G .

(ce résultat s'appuie sur les deux Lemmes suivants : si deux endomorphismes commutent, alors tout sous-espace propre de l'un est stable par l'autre, et le polynôme minimal de la restriction à un sous-espace stable est un diviseur du minimal sur tout l'espace)

2a- O est invariant par tout élément de $\widetilde{D_3}$ (toute isométrie, en tant qu'application affine, préserve le barycentre), et à chaque élément g de D_3 est associée une permutation $(g(A), g(B), g(C))$ de (A, B, C) (en effet, les sommets sont les points du triangle à distance maximale de , donc chaque sommet est transformé en un sommet, et g est bijective). Comme la donnée des images de 4 points formant un repère affine suffit à déterminer une application affine, cette correspondance entre $\widetilde{D_3}$ et $\mathcal{S}_3$ est un isomorphisme de groupes, d'où $\left|\widetilde{D_3}\right| = |\mathcal{S}_3| = 3! = 6$

Dressons l'inventaire :

si $\big(g(A), g(B), g(C)\big) = (A, B, C)$ alors $g = Id$

si $\big(g(A), g(B), g(C)\big) = (A, C, B)$ alors $g = s_{/OA}$ (symétrie par rapport à (OA), hauteur issue de A)

si $\big(g(A), g(B), g(C)\big) = (C, B, A)$ alors $g = s_{/OB}$

si $\big(g(A), g(B), g(C)\big) = (B, A, C)$ alors $g = s_{/OC}$

si $\big(g(A), g(B), g(C)\big) = (B, C, A)$ alors $g = \rho_{\frac{2\pi}{3}}$ (rotation autour de O d'angle $\frac{2\pi}{3}$)

si $\big(g(A), g(B), g(C)\big) = (C, A, B)$ alors $g = \rho_{\frac{4\pi}{3}}$

Aux trois transpositions de $\mathcal{S}_3$ correspondent les trois symétries de $\widetilde{D_3}$, au sous-groupe des cycles les trois rotations.

2b- Dans la base $(\overrightarrow{OA}, \overrightarrow{OB})$ on écrit sans difficulté les matrices des transformations de $\widetilde{D_3}$ (sachant que $\overrightarrow{OC} = -\overrightarrow{OA} - \overrightarrow{OB}$) :

$Id : \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $s_{/OA} : \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$, $s_{/OB} : \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix}$, $s_{/OC} : \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\rho_{\frac{2\pi}{3}} : \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, $\rho_{\frac{4\pi}{3}} : \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$

2c- Le polynôme caractéristique de $\rho_{\frac{2\pi}{3}}$ s'écrit : $det\begin{pmatrix} 1-\lambda & -1 \\ 0 & -1-\lambda \end{pmatrix} = \lambda^2 + \lambda + 1$

et sa diagonalisation dans $\mathbb{C}$ donne, sans surprise : $\begin{pmatrix} e^{i\frac{2\pi}{3}} & 0 \\ 0 & e^{-i\frac{2\pi}{3}} \end{pmatrix}$; $\rho_{\frac{4\pi}{3}} = \left(\rho_{\frac{2\pi}{3}}\right)^2 = \left(\rho_{\frac{2\pi}{3}}\right)^{-1}$ est diagonalisable dans la même base, de matrice $\begin{pmatrix} e^{-i\frac{2\pi}{3}} & 0 \\ 0 & e^{i\frac{2\pi}{3}} \end{pmatrix}$; cette base de diagonalisation est représentée par la matrice de passage $\begin{pmatrix} -1 & -1 \\ e^{i\frac{2\pi}{3}} & e^{-i\frac{2\pi}{3}} \end{pmatrix}$; effectuons ce changement de base pour $s_{/OC}$

$$s_{/OC}\begin{pmatrix} -1 \\ e^{i\frac{2\pi}{3}} \end{pmatrix} = \begin{pmatrix} e^{i\frac{2\pi}{3}} \\ -1 \end{pmatrix} = -e^{i\frac{2\pi}{3}}\begin{pmatrix} -1 \\ e^{-i\frac{2\pi}{3}} \end{pmatrix} \text{ et } s_{/OC}\begin{pmatrix} -1 \\ e^{-i\frac{2\pi}{3}} \end{pmatrix} = \begin{pmatrix} e^{-i\frac{2\pi}{3}} \\ -1 \end{pmatrix} = -e^{-i\frac{2\pi}{3}}\begin{pmatrix} -1 \\ e^{i\frac{2\pi}{3}} \end{pmatrix}$$

ce qui donne pour matrice représentative de $s_{/OC}$ dans la nouvelle base : $\begin{pmatrix} 0 & -e^{-i\frac{2\pi}{3}} \\ -e^{i\frac{2\pi}{3}} & 0 \end{pmatrix}$

Pour les deux autres symétries, compte tenu des relations $s_{/OB} = \rho_{\frac{2\pi}{3}} \circ s_{/OC}$, $s_{/OA} = \rho_{\frac{4\pi}{3}} \circ s_{/OC}$ on obtient dans la nouvelle base les matrices :

$$s_{/OB} : \begin{pmatrix} e^{i\frac{2\pi}{3}} & 0 \\ 0 & e^{-i\frac{2\pi}{3}} \end{pmatrix} \times \begin{pmatrix} 0 & -e^{-i\frac{2\pi}{3}} \\ -e^{i\frac{2\pi}{3}} & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

$$s_{/OA} : \begin{pmatrix} e^{-i\frac{2\pi}{3}} & 0 \\ 0 & e^{i\frac{2\pi}{3}} \end{pmatrix} \times \begin{pmatrix} 0 & -e^{-i\frac{2\pi}{3}} \\ -e^{i\frac{2\pi}{3}} & 0 \end{pmatrix} = \begin{pmatrix} 0 & -e^{i\frac{2\pi}{3}} \\ -e^{-i\frac{2\pi}{3}} & 0 \end{pmatrix}$$

Les matrices représentatives des transformations du groupe du triangle $\widetilde{D_3}$ dans la nouvelle base sont donc exactement celles du groupe D_3 , d'où l'isomorphisme annoncé.

3- $i(B)$ est une application linéaire de $\mathcal{A}$ dans lui-même :

$$\forall M, N \in \mathcal{A}, \quad \forall \alpha, \beta \in \mathbb{C}, \quad B(\alpha M + \beta N)B^{-1} = \alpha BMB^{-1} + \beta BNB^{-1}$$

(par linéarité du produit matriciel), qui est injective : $BMB^{-1} = 0 \Longrightarrow M = 0$

c'est donc bien un élément de $GL(\mathcal{A})$; i est un morphisme de groupes, en effet :

$$\forall M \in \mathcal{A}, \forall B, C \in G, i(BC)(M) = (BC)M(BC)^{-1} = (BC)M(C^{-1}B^{-1}) = B(CMC^{-1})B^{-1} = i(B)(i(C)(M))$$

autrement dit : $i(BC) = i(B) \circ i(C)$, cqfd.

Le noyau de i est l'intersection du centre de $\mathcal{A}$ avec G , or le centre de $\mathcal{A}$ est constitué des homothéties, d'où le résultat demandé sur l'injectivité de .

4- $M \in \mathcal{A}^{\tilde{G}}$ commute avec tout $B \in G$, il en résulte que $Ker(M), Im(M)$ sont stables par B :

$$x \in Ker(M) \Leftrightarrow Mx = 0 \Longrightarrow BMx = MBx = 0 \Longrightarrow Bx \in Ker(M)$$

$$y \in Im(M) \Leftrightarrow \exists x \in E \ tq \ y = Mx \Longrightarrow By = BMx = MBx \Longrightarrow By \in Im(M)$$

5- D'après 4-, si $M \in \mathcal{A}^{\tilde{G}}$ alors $Ker(M)$ est stable par G , comme on suppose E irréductible pour , cela implique, ou bien $Ker(M) = E$, auquel cas $M = 0$, ou bien $Ker(M) = \{0\}$, auquel cas M est inversible.

Raisonnons par l'absurde, et supposons que $\mathcal{A}^{\tilde{G}}$ contienne deux matrices linéairement indépendantes M et N (non-nulles, donc inversibles d'après ce qui précède) :

on sait alors que M est équivalente à I_n , $PMQ = I_n$ avec P, Q inversibles.

Posons $PNQ = S$ et considérons $S - \lambda I_n$, comme on se place sur le corps des complexes, il existe un scalaire λ qui soit valeur propre de , tel que $S - \lambda I_n$ soit non inversible, mais alors :

$P^{-1}(S - \lambda I_n)Q^{-1} = N - \lambda M$ est non inversible, et élément de la sous-algèbre $\mathcal{A}^{\tilde{G}}$ de , par conséquent $N - \lambda M = 0$, ce qui contredit l'hypothèse d'indépendance linéaire.

Par conséquent $\mathcal{A}^{\tilde{G}}$, qui n'est pas réduit à {0} puisque $I_n \in \mathcal{A}^{\tilde{G}}$, ne peut être que la droite vectorielle engendrée par I_n, c'est-à-dire l'algèbre des homothéties.

6- Utilisons le vocabulaire de la dualité pour démontrer cette relation ; $(e_i)_{i=1,\dots,n}$ étant la base canonique de $\mathbb{C}^n$, et $(e_i{}^*)_{i=1,\dots,n}$ étant sa base duale, on peut écrire (1) $tr(M) = \sum_{i=1}^{n} < e_i{}^*, M(e_i) >$ (le crochet de dualité $< \varphi, x >$ entre E^* et E désigne le scalaire image du vecteur x par la forme linéaire φ) ;

on se donne alors la base $E_{ij} =< e_j{}^*, . > e_i$ de l'espace $\mathcal{A}$, dont on peut expliciter la base duale :

(2) $< E_{ij}{}^*, M > = < e_i{}^*, M(e_j) >$ d'où on tire $tr(\phi)$ (formule analogue à (1) par dualité $\mathcal{A}^*$- $\mathcal{A}$) :

$tr(\phi) = \sum_{i,j} < E_{ij}{}^*, \phi(E_{ij}) > = \sum_{i,j} < e_i{}^*, (M\, E_{ij} N)(e_j) >$

avec $ME_{ij} =< e_j{}^*, . > M(e_i)$ et $ME_{ij}(N(e_j)) =< e_j{}^*, N(e_j) > M(e_i)$

ce qui donne :

$$tr(\phi) = \sum_{i,j} < e_i{}^*, M(e_i) >< e_j{}^*, N(e_j) > = \sum_{i=1}^{n} < e_i{}^*, M(e_i) > \times \sum_{j=1}^{n} < e_j{}^*, N(e_j) > = tr(M)tr(N)$$

cqfd.

7a- Soit $B_0 \in G$, $B_0 P = \frac{1}{|G|} \sum_{B \in G} B_0 B$, lorsque B décrit G, son translaté à gauche $B_0 B$ décrit G (la translation à gauche est une bijection de G sur lui-même), par conséquent : $\forall B_0 \in G$, $B_0 P = P$, d'où :

$$P^2 = \left(\frac{1}{|G|} \sum_{B_0 \in G} B_0 \right) \times P = \frac{1}{|G|} \sum_{B_0 \in G} B_0\, P = \frac{1}{|G|} \times |G| P = P$$

P est donc un projecteur, d'après le Lemme des noyaux, avec pour sous-espaces propres :

$KerP$, $Ker(P - I) = ImP$ en somme directe, ce qui diagonalise .

7b- $\forall B \in G$, $B\, P = P$ montre $ImP \subseteq E^G$, en effet, $\forall y \in ImP$, $y = Px, \forall B \in G$, $By = BPx = Px = y$

réciproquement, soit $\in E^G$, $Py = \frac{1}{|G|} \sum_{B \in G} B\, y = \frac{1}{|G|} \times |G| y = y$ d'où $y \in Ker(P - I) = ImP$

On en conclut : $\dim(E^G) = \dim(ImP) = tr(P) = \frac{1}{|G|} \sum_{B \in G} tr(B)$

8- Dans le cas où le morphisme i est injectif, on applique 7b en faisant agir $\tilde{G}$ sur $\mathcal{A}$ (au lieu de faire agir G sur), ce qui donne : $\dim(\mathcal{A}^{\tilde{G}}) = \frac{1}{|G|}\sum_{B\in G} tr(i(B))$ et on calcule $tr(i(B))$ par la formule établie en 6- , d'où $tr(i(B)) = tr(B^{-1})tr(B)$, et $\dim(\mathcal{A}^{\tilde{G}}) = \frac{1}{|G|}\sum_{B\in G} tr(B^{-1})tr(B)$, cqfd.

Si le morphisme i n'est pas injectif, on fait agir le groupe quotient $G/Ker(i)$ sur $\mathcal{A}$:

$$\dim(\mathcal{A}^{\tilde{G}}) = \frac{1}{|G/Ker(i)|}\sum_{\bar{B}\in G/Ker(i)} tr(i(B) = \frac{1}{|G|}\times|Ker(i)|\sum_{\bar{B}\in G/Ker(i)} tr(i(B)$$

$$= \frac{1}{|G|}\sum_{B\in G} tr\big(i(B)\big) = \frac{1}{|G|}\sum_{B\in G} tr(B^{-1})tr(B)$$

9a- D'après 5-, on sait que $\mathcal{A}^{\tilde{G}}$ (commutant de G dans $\mathcal{A}$) est la droite vectorielle $\mathbb{C}I_n$; toute matrice $X \in \mathcal{A}^{\tilde{G}}$ est donc de la forme : $X = \lambda I_n$, avec $tr(X) = \lambda tr(I_n) = \lambda n$, $\lambda = \frac{1}{n}tr(X)$ d'où $X = \frac{1}{n}tr(X)I_n$

9b- Y commute avec toute matrice $B_0 \in G$, en effet :

$$B_0 Y = \sum_{B\in G} tr(B^{-1})B_0 B = \sum_{B\in G} tr(B^{-1})B_0\big({B_0}^{-1}BB_0\big) = \sum_{B\in G} tr(B^{-1})BB_0 = YB_0$$

(on a effectué le changement de variable bijectif $B \to {B_0}^{-1}BB_0$ dans la somme, sachant que $tr(B^{-1})$ est égale à $tr(({B_0}^{-1}BB_0)^{-1})$ puisque la trace est un invariant de similitude)

D'après 8- et 5- $\dim(\mathcal{A}^{\tilde{G}}) = \frac{1}{|G|}\sum_{B\in G} tr(B^{-1})tr(B) = 1$ d'où $tr(Y) = \sum_{B\in G} tr(B^{-1})tr(B) = |G|$

puis d'après 9a- on conclut : $Y = \frac{1}{n}tr(Y)I_n = \frac{|G|}{n}I_n$

10a- Toute matrice $B \in G$ est diagonalisable, avec $Sp(B) \subseteq \{1, \varsigma, \varsigma^2, \dots, \varsigma^{|G|-1}\}$, groupe des racines $|G|$-ièmes de l'unité d'où il résulte $tr(B) \in \mathbb{Z}_G$; par conséquent $Y = \sum_{B\in G} tr(B^{-1})B \in \mathbb{Z}_G[G]$, puisque chaque coefficient $tr(B^{-1})$ est dans $\mathbb{Z}_G$.

10b- D'après 10a-, Y est combinaison à coefficients dans $\mathbb{Z}$ des matrices C_l ; il en va de même de chaque matrice $C_k Y$ du fait que l'ensemble des matrices C_l est stable par produit.

10c- Compte tenu de l'expression de Y démontrée en 9b-, on en déduit :

$$\frac{|G|}{n}C_k = \sum_{1\le l\le|G|^2} a_{lk}\,C_l$$

Soit $x = (x_l)_{1\le l\le|G|^2}$ le vecteur constitué des coordonnées $< {E_{ij}}^*, C_l > = < {e_i}^*, C_l(e_j) >$ des matrices C_l ; il existe au moins un couple (i,j) tel que le vecteur x soit non-nul (sinon toutes les matrices C_l seraient nulles, ce qui est absurde), mais alors la relation $\frac{|G|}{n}x_k = \sum_{1\le l\le|G|^2} a_{lk}\,x_l$ montre que x est vecteur propre de la matrice A pour la valeur propre $\frac{|G|}{n}$, ce qui s'exprime par le critère $\det(R) = 0$

10d- Ce polynôme n'est autre que le polynôme caractéristique de A, à savoir $P(\lambda) = \det(\lambda I_{|G|^2} - A)$; écrivons $P(\lambda) = \lambda^k + \alpha_{k-1}\lambda^{k-1} + \cdots + \alpha_1\lambda + \alpha_0$, avec $k = |G|^2$ et $\alpha_0, \alpha_1, .., \alpha_{k-1} \in \mathbb{Z}$; si on écrit la fraction $\frac{|G|}{n}$ sous forme irréductible : $\frac{|G|}{n} = \frac{p}{q}$, $p \in \mathbb{N}$, $q \in \mathbb{N}^*$, $p \wedge q = 1$, alors on a

$p^k + \alpha_{k-1}p^{k-1}q + \cdots + \alpha_1 pq^{k-1} + \alpha_0 q^k = 0$ d'où q/p^k, ce qui implique q/p , et par suite $q = 1$

On vient de démontrer le résultat classique suivant : tout rationnel qui est entier algébrique est un entier relatif.

On en conclut : $\frac{|G|}{n} \in \mathbb{N}$, c'est-à-dire $n/|G|$, cqfd.

11a- $< . , . >_0$ est une forme bilinéaire définie positive, comme combinaison des formes bilinéaires définies positives $< B(.) , B(.) >$; chacune de ces formes est non dégénérée parce que chaque matrice B est inversible : $< B(v) , B(v) > = 0 \Longrightarrow B(v) = 0 \Longrightarrow v = 0$

On vérifie facilement que chaque $B \in G$ est une isométrie pour le produit scalaire $< . , . >_0$:

$$< B(v) , B(w) >_0 = \frac{1}{|G|} \sum_{S \in G} < SB(v), SB(w) > = < v , w >_0$$

en effet, pour $B \in G$ fixée, les SB décrivent G lorsque S décrit G (la translation à droite $S \to SB$ étant une bijection de G sur lui-même)

11b- Pour les éléments de G qui sont des homothéties, n'importe quelle base orthogonale pour $< . , . >_0$ convient ; occupons-nous des $B \in G$ qui ne sont pas des homothéties.

Il existe par hypothèse un sous-espace strict F de l'espace $E = \mathbb{C}^2$ qui soit stable par G, comme F est nécessairement une droite vectorielle, la restriction de chaque B à F est une homothétie de F , enfin comme on suppose que B n'est pas une homothétie sur E cela signifie que $F = Ker(B - \lambda_B I_2)$, droite propre de B pour une certaine valeur propre λ_B .

Comme B est une isométrie pour $< . , . >_0$, on sait classiquement que $F^\perp = Ker(B - \lambda_B I_2)^\perp$ est stable par B , en effet :

$$\begin{aligned} w \in Ker(B - \lambda_B I_2)^\perp \iff & \forall v \in Ker(B - \lambda_B I_2), < v , w >_0 = 0 \\ \Rightarrow & \forall v \in Ker(B - \lambda_B I_2), < B(v) , B(w) >_0 = \lambda_B < v , B(w) >_0 = 0 \\ \Rightarrow & \forall v \in Ker(B - \lambda_B I_2), \quad < v , B(w) >_0 = 0 \quad (car\ \lambda_B \neq 0) \\ \Rightarrow & B(w) \in Ker(B - \lambda_B I_2)^\perp \end{aligned}$$

et cette autre droite stable $F^\perp$ est commune à tous les $B \in G$, et apparaît pour chacun de ceux qui ne sont pas des homothéties sur E comme une nouvelle droite propre $F^\perp = Ker(B - \mu_B I_2)$; en définitive, la somme directe orthogonale $F \oplus F^\perp = E$ définit une base orthogonale qui diagonalise simultanément tous les éléments de G ; il en résulte bien que G est commutatif, puisque ces matrices diagonales, qui représentent les éléments de G dans la nouvelle base, commutent entre elles.

12a- D'après le Lemme des noyaux, on sait que $Ker(B-I_2) \oplus Ker(B+I_2) = E = \mathbb{C}^2$, dans un premier cas, cette décomposition est non triviale, en somme directe de deux droites vectorielles, auquel cas B est une symétrie, de déterminant égal à -1 ; dans un deuxième cas, la décomposition est triviale, l'un des deux sous-espaces de la somme étant réduit à $\{0\}$, auquel cas $B = \pm I_2$, $\det(B) = +1$.

En conclusion, $SL_2(\mathbb{C}) = \{-I_2, I_2\}$

12b- Si G est non commutatif, alors d'après 11b- on peut affirmer que $E = \mathbb{C}^2$ est irréductible pour G, et d'après 10d- que $|G|$ est pair. Le théorème de Lagrange, rappelé en préambule, assure qu'il existe dans G un élément d'ordre 2, cet élément ne peut être que $B = -I_2$ d'après 12a-

13a&b- Si G_0 était non commutatif, alors par le même raisonnement qu'en 12b-, en appliquant les résultats de 11b- et 10d-, on sait que $|G_0|$ serait pair, et que G_0 contiendrait un élément d'ordre 2, qui ne pourrait être autre que $-I_2$, et G contiendrait donc une homothétie autre que l'identité, contradiction.

Par conséquent, G_0 est commutatif, et d'après la question 1-, tous les éléments de G_0 sont diagonalisables dans une même base, de matrice de passage P , avec pour valeurs propres des racines $|G|$-ièmes de l'unité ; la condition $G_0 \subseteq SL_2(\mathbb{C})$ implique que $\forall B \in G_0$, $PBP^{-1} = \begin{pmatrix} \lambda_B & 0 \\ 0 & {\lambda_B}^{-1} \end{pmatrix}$ avec $\lambda_B \in \mathcal{U}_{|G|}$

Il est clair que les applications $B \to PBP^{-1} \to \lambda_B$ sont des isomorphismes de groupes, avec pour images respectives le sous-groupe annoncé Γ_0 , et un sous-groupe de $\mathcal{U}_{|G|}$, qui ne peut être que $\mathcal{U}_m$, avec $m = |G_0|$; ceci prouve que G_0 est cyclique, isomorphe à $\Gamma_0 = \mathcal{Z}_m$

13c- Le morphisme de groupes $\det: G \to \mathbb{C}^*$ a pour noyau G_0 , si on suppose $G_0 = \{I_2\}$, alors G est isomorphe à un sous-groupe de $\mathbb{C}^*$, donc il est commutatif.

14a&b- $G_0 = \mathcal{Z}_m$ est distingué dans G en tant que noyau du morphisme $\det: G \to \mathbb{C}^*$, autrement dit :

$$\forall C \in \mathcal{Z}_m, \forall B \in G, \quad BCB^{-1} \in \mathcal{Z}_m$$

Ceci s'applique en particulier au cas d'une matrice B_0 de G qui n'est pas diagonale, remarquons d'ailleurs qu'il existe au moins une telle matrice dans G car si ce n'était pas le cas, G serait constitué de matrices toutes diagonales et serait donc commutatif.

Posons $B_0 = \begin{pmatrix} a & b \\ b' & a' \end{pmatrix}$ et calculons $B_0 C {B_0}^{-1}$ avec $C = \begin{pmatrix} c^k & 0 \\ 0 & c^{-k} \end{pmatrix} \in \mathcal{Z}_m$:

$${B_0}^{-1} = \frac{1}{aa' - bb'} {}^t({}^cB_0) = \frac{1}{aa' - bb'} \begin{pmatrix} a' & -b \\ -b' & a \end{pmatrix}$$

$$B_0 C {B_0}^{-1} = \frac{1}{aa' - bb'} B_0 \begin{pmatrix} c^k & 0 \\ 0 & c^{-k} \end{pmatrix} \begin{pmatrix} a' & -b \\ -b' & a \end{pmatrix}$$

$$= \frac{1}{aa' - bb'} \begin{pmatrix} a & b \\ b' & a' \end{pmatrix} \begin{pmatrix} a'c^k & -bc^k \\ -b'c^{-k} & ac^{-k} \end{pmatrix}$$

$$= \frac{1}{aa' - bb'} \begin{pmatrix} aa'c^k - bb'c^{-k} & ab(c^{-k} - c^k) \\ a'b'(c^k - c^{-k}) & aa'^{c^{-k}} - bb'c^k \end{pmatrix}$$

Exprimons que la matrice obtenue est diagonale : $ab = a'b' = 0$, comme on suppose $bb' \neq 0$ (B_0 n'est pas diagonale), cela implique $aa' = 0$, mais alors on aura $\det(B_0) = -bb' \neq 0$ (car $B_0 \in G \subseteq GL_2(\mathbb{C})$), d'où finalement $a = a' = 0$.

Dans ces conditions $B_0 C {B_0}^{-1} = \begin{pmatrix} c^{-k} & 0 \\ 0 & c^k \end{pmatrix} = \begin{pmatrix} c^{m-k} & 0 \\ 0 & -c^{-(m-k)} \end{pmatrix}$ sera bien dans $\mathcal{Z}_m$, et B_0 est nécessairement de la forme annoncée $B_0 = \begin{pmatrix} 0 & b \\ b' & 0 \end{pmatrix}$, avec ${B_0}^2 = bb' I_2 \in G$, or par hypothèse G ne contient pas de matrice d'homothétie autre que l'identité, ce qui impose $bb' = 1$, soit $b' = b^{-1}$.

14c- En définitive, B_0 est de la forme $B_0 = \begin{pmatrix} 0 & b \\ b^{-1} & 0 \end{pmatrix}$, et avec $Q = \begin{pmatrix} 1 & 0 \\ 0 & -b \end{pmatrix}$ on vérifie bien :

$$QB_0Q^{-1} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

15a- Si $B \in G$ est une matrice diagonale : $B = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$, alors B commute avec Q (puisque Q est elle-même diagonale), d'où :

$$BB_0 = (Q^{-1}BQ)\left(Q^{-1}\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}Q\right) = Q^{-1}\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}Q = Q^{-1}\begin{pmatrix} 0 & -\alpha \\ -\beta & 0 \end{pmatrix}Q$$

et, comme précédemment : $(BB_0)^2 = \alpha\beta I_2 \in G$ impose $\alpha\beta = 1$, soit $\det(B) = 1$, ce qui prouve $B \in G_0 = \mathcal{Z}_m$

15b- On considère la congruence modulo $\mathcal{Z}_m$, qui est distingué dans G

D'après 15a-, la classe $\mathcal{Z}_m$ est constituée des matrices diagonales ; montrons que toute matrice non diagonale B' est congrue à B_0 modulo $\mathcal{Z}_m$, ce qui prouvera qu'il n'y a que deux classes dans cette congruence.

D'après 14-, B' est de la forme $B' = \begin{pmatrix} 0 & b' \\ b'^{-1} & 0 \end{pmatrix}$ d'où :

$B_0 {B'}^{-1} = \begin{pmatrix} bb'^{-1} & 0 \\ 0 & b^{-1}b' \end{pmatrix} \in \mathcal{Z}_m$ (d'après 15a-), cqfd.

En conclusion, $G = \mathcal{Z}_m \cup (B_0\mathcal{Z}_m)$, et en appliquant à G la conjugaison $B \longrightarrow Q^{-1}BQ$ on trouve bien comme groupe image le groupe D_m

16a- On sait d'après 1- que les matrices de G sont diagonalisables dans une même base, de matrice de passage P , avec pour valeurs propres des racines $|G|$-ièmes de l'unité ; on peut donc écrire :

$B = P\begin{pmatrix} \chi_1(B) & 0 \\ 0 & \chi_2(B) \end{pmatrix}P^{-1}$ et on vérifie facilement que χ_1, χ_2 sont des morphismes de G dans $\mathcal{U}_{|G|}$, groupe des racines $|G|$-ièmes de l'unité , en effet :

$\forall B, B' \in G,\ BB' = P\begin{pmatrix} \chi_1(B)\chi_1(B') & 0 \\ 0 & \chi_2(B)\chi_2(B') \end{pmatrix}P^{-1}$ d'où $\chi_j(BB') = \chi_j(B)\chi_j(B'),\ j = 1,2$

16b- C'est un morphisme de G dans $\mathcal{U}_{|G|}$ d'après 16a- :

$$\chi_1(BB')\chi_2(BB')^{-1} = \chi_1(B)\chi_1(B')\big(\chi_2(B)\chi_2(B')\big)^{-1} = \chi_1(B)\chi_2(B)^{-1} \times \chi_1(B')\chi_2(B')^{-1}$$

et son noyau est défini par la condition $\chi_1(B)\chi_2(B)^{-1} = 1$ ce qui implique $B = I_2$ puisque G ne contient pas d'autre matrice d'homothétie que l'identité ; on a donc un isomorphisme de G sur $\mathcal{U}_{|G|}$

16c- Mettons de côté le cas où le groupe G est réduit à l'identité.

D'après 16b-, G est cyclique puisqu'il est isomorphe à un groupe cyclique, soit B_1 un générateur de G, posons $\chi_1(B_1) = c = e^{\frac{2i\pi p}{|G|}}$, $\chi_2(B_1) = d = e^{\frac{2i\pi q}{|G|}}$

Supposons que $p - q$ ne soit pas premier avec $|G|$, et notons $\delta = (p-q)\wedge|G|$, et $r = \frac{|G|}{\delta}$, $r\wedge|G| = 1$

Il vient : $\chi_1({B_1}^r)\chi_2({B_1}^r)^{-1} = e^{\frac{2i\pi(p-q)r}{|G|}} = e^{\frac{2i\pi(p-q)}{\delta}} = 1$, avec ${B_1}^r \neq I_2$

(en effet, ${B_1}^r = I_2 \Rightarrow \chi_1({B_1}^r) = \chi_2({B_1}^r) = 1 \Rightarrow |G|/pr \; et \; |G|/qr \Longrightarrow |G|/p \; et \; |G|/q$ ce qui redonnerait le cas où G est réduit à l'identité)

Or, ceci contredit le résultat du 16b-, puisqu'il existerait alors une matrice ${B_1}^r \neq I_2$ dans le noyau du morphisme $B \to \chi_1(B)\chi_2(B)^{-1}$

En conclusion, G est bien de la forme annoncée.