ÉCOLE POLYTECHNIQUE **FILIÈRE MP**

CONCOURS D'ADMISSION 2010

DEUXIÈME COMPOSITION DE MATHÉMATIQUES

(Durée : 4 heures)

L'utilisation des calculatrices n'est pas autorisée pour cette épreuve.

⋆ ⋆ ⋆

Sur les sous-groupes finis de $\mathrm{GL}_2(\mathbf{C})$

Le but de ce problème est de caractériser les sous-groupes finis de $\mathrm{GL}_2(\mathbf{C})$ ne contenant pas d'homothétie autre que l'identité.

Notations et conventions

Soit G un groupe fini (noté multiplicativement) de cardinal $|G|$. On note $\mathbf{1}_G$ l'unité de G. On rappelle que tout élément g de G vérifie $g^{|G|} = \mathbf{1}_G$ et on admet que si p est un nombre premier qui divise $|G|$, alors il existe $g \in G \setminus \{\mathbf{1}_G\}$ tel que $g^p = \mathbf{1}_G$.

Si E est un $\mathbf{C}$-espace vectoriel de dimension finie, on note $\mathrm{GL}(E)$ le groupe des endomorphismes inversibles de E et Id_E l'identité de E. Si φ un endomorphisme de E, on note $\mathrm{Tr}(\varphi)$ la trace de φ et $\det(\varphi)$ son déterminant.

Si G est un sous-groupe fini de $\mathrm{GL}(E)$, et V un sous-espace vectoriel de E, on note V^G l'ensemble des vecteurs fixés par G : $V^G = \{v \in V | \, \forall g \in G,\, g(v) = v\}$. On dit que V est **stable** par G si quels que soient $g \in G$, $v \in V$, on a $g(v) \in V$ et on dit que E est **irréductible** pour G si ses seuls sous-espaces stables par G sont E et $\{0\}$.

On note $\mathcal{M}_n(\mathbf{C})$ l'espace des matrices carrées de taille n à coefficients complexes et $\mathrm{GL}_n(\mathbf{C})$ le groupe des matrices inversibles dans $\mathcal{M}_n(\mathbf{C})$.

On note D_n le sous-groupe de $\mathrm{GL}_2(\mathbf{C})$ à $2n$ éléments formé des matrices $\begin{pmatrix} c^k & 0 \\ 0 & c^{-k} \end{pmatrix}$ et $\begin{pmatrix} 0 & -c^k \\ -c^{-k} & 0 \end{pmatrix}$, où k est un entier compris entre 0 et $n-1$ et $c = e^{2i\pi/n}$ (on ne demande pas de vérifier que D_n est un groupe).

I – Sous-groupes finis de $\mathrm{GL}(E)$

1. Soit E un $\mathbf{C}$-espace vectoriel de dimension finie et soit G un sous-groupe fini de $\mathrm{GL}(E)$. Démontrer que, pour tout $g \in G$, g est diagonalisable et que, si G est commutatif, tous les éléments de G sont diagonalisables dans une même base.

II – Isométries du triangle

2. On se place dans le plan euclidien, muni d'un repère orthonormé centré en O. On s'intéresse au sous-groupe $\widetilde{D}_3$ des isométries du plan qui préservent un triangle équilatéral ABC de centre O.

2a. Faire l'inventaire des éléments de $\widetilde{D}_3$ et démontrer que $\widetilde{D}_3$ est de cardinal 6.

2b. En se plaçant dans la base (non orthonormée) $(\overrightarrow{OA}, \overrightarrow{OB})$, démontrer que le groupe $\widetilde{D}_3$ est isomorphe à un sous-groupe de $\mathrm{GL}_2(\mathbf{C})$ formé de matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ où a, b, c, d sont dans $\{-1, 0, 1\}$.

2c. Diagonaliser dans $\mathbf{C}$ la matrice $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. En déduire que le groupe $\widetilde{D}_3$ est isomorphe au groupe D_3.

III – Lemme de Schur

Notons $\mathcal{A} = \mathcal{M}_n(\mathbf{C})$ et $E = \mathbf{C}^n$. Notons I_n la matrice identité de $\mathcal{M}_n(\mathbf{C})$. On appelle homothétie une matrice de la forme λI_n, $\lambda \in \mathbf{C}$. Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbf{C})$. Pour tout $B \in G$, on note $i(B)$ l'application :

$$i(B) : \begin{cases} \mathcal{A} \longrightarrow \mathcal{A} \\ M \mapsto BMB^{-1} \end{cases} .$$

3. Montrer que $i : B \mapsto i(B)$ est un morphisme de groupes de G dans $\mathrm{GL}(\mathcal{A})$, et que i est injectif si et seulement si G ne contient pas d'homothéties autres que l'identité.

On note $\widetilde{G}$ l'image par i de G et $\mathcal{A}^{\widetilde{G}}$ l'ensemble des matrices $M \in \mathcal{A}$ telles que $i(B)(M) = M$ pour tout B dans $\widetilde{G}$.

4. Soit $M \in \mathcal{A}^{\widetilde{G}}$. Démontrer que $\mathrm{Ker}(M)$ et $\mathrm{Im}\,(M)$ sont des sous-espaces stables par G.

5. On suppose que E est irréductible pour G. Soit $M \in \mathcal{A}^{\widetilde{G}}$, démontrer que M est soit nulle, soit inversible. En déduire que $\mathcal{A}^{\widetilde{G}}$ est de dimension 1.

6. Soient M, $N \in \mathcal{A}$. On considère l'endomorphisme de $\mathcal{A}$ suivant, $\Phi : X \mapsto MXN$.

Démontrer que $\mathrm{Tr}(\Phi) = \mathrm{Tr}(M)\,\mathrm{Tr}(N)$.

7. Soit $P = \dfrac{1}{|G|} \displaystyle\sum_{B \in G} B$.

7a. Démontrer que $P^2 = P$. En déduire que P est diagonalisable.

7b. Démontrer que $\mathrm{Im}\,(P) = E^G$ et en déduire que $\dim(E^G) = \dfrac{1}{|G|} \displaystyle\sum_{B \in G} \mathrm{Tr}\,(B)$.

8. Démontrer que $\dim(\mathcal{A}^{\widetilde{G}}) = \dfrac{1}{|G|} \displaystyle\sum_{B \in G} \mathrm{Tr}(B^{-1})\,\mathrm{Tr}(B)$.

(On pourra considérer d'abord le cas où i est injectif.)

On suppose, jusqu'à la fin de cette partie, que E est irréductible pour G.

9a. Soit X dans $\mathcal{A}$ une matrice qui commute avec toutes les matrices de G. Démontrer que $X = \dfrac{1}{n}\operatorname{Tr}(X) I_n$.

9b. Soit $Y = \displaystyle\sum_{B\in G} \operatorname{Tr}(B^{-1})B$. Démontrer que $Y = \dfrac{|G|}{n} I_n$.

10. On garde la notation Y jusqu'à la fin de cette partie. Soit $\zeta = e^{2i\pi/|G|}$. On note

$$\mathbf{Z}_G = \{a_0\zeta^0 + a_1\zeta^1 + \cdots + a_{|G|-1}\zeta^{|G|-1}, a_i \in \mathbf{Z}\}$$

et $\mathbf{Z}_G[G]$ les combinaisons linéaires, à coefficients dans $\mathbf{Z}_G$, de matrices de G.

10a. Démontrer que pour tout $B \in G$, $\operatorname{Tr}(B)$ est dans $\mathbf{Z}_G$, puis que Y est dans $\mathbf{Z}_G[G]$.

10b. On note $(C_k)_{1\le k\le |G|^2}$ les $|G|^2$ matrices $\zeta^i B$ (où $1 \le i \le |G|$ et $B \in G$) de $\mathbf{Z}_G[G]$. Démontrer que pour tous $1 \le k \le |G|^2$, on peut trouver des coefficients $(a_{ij})_{1\le i,j\le |G|^2}$ dans $\mathbf{Z}$ tels que $YC_k = \displaystyle\sum_{1\le \ell\le |G|^2} a_{\ell k} C_\ell$.

10c. On pose $A = (a_{ij})_{1\le i,j\le |G|^2}$ et $R = \dfrac{|G|}{n} I_{|G|^2} - A$. Démontrer que $\det(R) = 0$.

10d. Démontrer que $\dfrac{|G|}{n}$ est racine d'un polynôme à coefficients dans $\mathbf{Z}$ de degré $|G|^2$ et de terme dominant égal à 1. En déduire que n divise $|G|$.

IV - Une caractérisation de D_n, n impair

Soit G un sous-groupe fini de $\mathrm{GL}_2(\mathbf{C})$. Notons $\langle .,. \rangle$ le produit scalaire hermitien usuel sur $\mathbf{C}^2$, et posons pour tout $v, w \in \mathbf{C}^2$

$$\langle v, w\rangle_0 = \frac{1}{|G|}\sum_{B\in G} \langle B(v), B(w)\rangle.$$

11a. Montrer que $\langle .,. \rangle_0$ est un produit scalaire hermitien sur $\mathbf{C}^2$, vérifiant quels que soient $v, w \in \mathbf{C}^2$ et $B \in G$, $\langle B(v), B(w)\rangle_0 = \langle v, w\rangle_0$.

11b. Démontrer que si $\mathbf{C}^2$ n'est pas irréductible pour G, il existe une base orthogonale de $\mathbf{C}^2$ pour le produit scalaire hermitien $\langle .,. \rangle_0$ qui diagonalise les matrices de G. En déduire que G est commutatif.

12a. On note $\mathrm{SL}_2(\mathbf{C})$ le sous-groupe de $\mathrm{GL}_2(\mathbf{C})$ des matrices de déterminant 1. Quels sont les matrices $B \in \mathrm{SL}_2(\mathbf{C})$ telles que $B^2 = I_2$?

12b. Démontrer que si $G \subset \mathrm{SL}_2(\mathbf{C})$ est non commutatif, alors $|G|$ est pair. En déduire que $-I_2 \in G$. (Utiliser les rappels du préambule.)

On suppose par la suite que G est un sous groupe fini de $\mathrm{GL}_2(\mathbf{C})$ ne contenant aucune homothétie autre que l'identité. On note $G_0 = G \cap \mathrm{SL}_2(\mathbf{C})$

13a. Démontrer que G_0 est commutatif. En déduire qu'il existe P dans $\mathrm{GL}_2(\mathbf{C})$ et un sous-

groupe Γ_0 de $\mathrm{GL}_2(\mathbf{C})$ formé de matrices diagonales de la forme $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ tels que $B \mapsto PBP^{-1}$ soit un isomorphisme de G_0 sur Γ_0.

13b. Démontrer qu'il existe un entier m tel que Γ_0 soit le groupe $\mathcal{Z}_m$ des matrices $\begin{pmatrix} c^k & 0 \\ 0 & c^{-k} \end{pmatrix}$ où $c = e^{2i\pi/m}$ et k prend les valeurs de 0 à $m-1$.

13c. Si $G_0 = \{I_2\}$ démontrer qu'alors G est commutatif (considérer le morphisme de groupe $\det : G \to \mathbf{C}^*$).

On suppose dans les questions 14 et 15 que G n'est pas commutatif et que G_0 est exactement le groupe $\mathcal{Z}_m$.

14. Soit B_0 une matrice dans G qui n'est pas diagonale.

14a. Démontrer que pour tout $C \in \mathcal{Z}_m$ on a $B_0 C B_0^{-1} \in \mathcal{Z}_m$. En déduire que B_0 est de la forme $B_0 = \begin{pmatrix} 0 & b \\ b' & 0 \end{pmatrix}$ avec b, $b' \in \mathbf{C}$.

14b. Calculer B_0^2 et en déduire que $b' = b^{-1}$.

14c. Montrer qu'il existe $Q \in \mathrm{GL}_2(\mathbf{C})$ diagonale telle que $QB_0Q^{-1} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$.

15a. Soit B une matrice diagonale dans G. Montrer que $B \in \mathcal{Z}_m$.

15b. Montrer que $B \mapsto QBQ^{-1}$ est un isomorphisme de G sur le groupe D_m.

16. Soit G un sous-groupe fini commutatif de $\mathrm{GL}_2(\mathbf{C})$ qui ne contient pas d'homothétie autre que l'identité.

16a. Montrer qu'il existe une matrice $P \in \mathrm{GL}_2(\mathbf{C})$ et deux morphismes de groupes $\chi_1, \chi_2 : G \to \mathbf{C}^*$ tels que toute matrice de G s'écrive $B = P \begin{pmatrix} \chi_1(B) & 0 \\ 0 & \chi_2(B) \end{pmatrix} P^{-1}$.

16b. Montrer que $B \mapsto \chi_1(B)\chi_2(B)^{-1}$ est un isomorphisme de G dans le groupe des racines $|G|$-ièmes de l'unité.

16c. Montrer que G est le groupe des matrices de la forme $P \begin{pmatrix} c^k & 0 \\ 0 & d^k \end{pmatrix} P^{-1}$, k variant de 0 à $|G|-1$, où l'on a posé $c = e^{2i\pi p/|G|}$ et $d = e^{2i\pi q/|G|}$, p et q étant deux entiers tels que $p-q$ est premier avec $|G|$.

17. Décrire à partir des questions précédentes tous les sous-groupes finis de $\mathrm{GL}_2(\mathbf{C})$ ne contenant pas d'homothétie autre que l'identité.

18. Montrer que le groupe fini commutatif $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ ne peut pas être isomorphe à un sous-groupe de $\mathrm{GL}_2(\mathbf{C})$.

* *
*

Composition B – École Polytechnique 2010 - MP

PARTIE I - Sous-groupes finis de $\mathrm{GL}(E)$

1. Soit g dans G. D'après le théorème de Lagrange rappelé en préambule le polynôme, simplement scindé sur $\mathbf{C}$, $X^{|G|}-1$ annule g et donc $\boxed{g \text{ est diagonalisable.}}$

   Pour n entier, on note $(\mathbf{H}_n)$ le prédicat suivant : pour tout $\mathbf{C}$-espace vectoriel F de dimension finie inférieure à n et toute famille commutative d'endorphismes diagonalisables, il existe une base commune de diagonalisation de ces endomorphismes.

   Pour $n=1$, tout endomorphisme est diagonal dans toute base, donc $(\mathbf{H}_1)$ est vrai.

   Soit maintenant n dans $\mathbf{N}^*$, F un $\mathbf{C}$-espace vectoriel de dimension $n+1$, et $(u_i)_{i\in I}$ une famille commutative d'endomorphismes diagonalisables de F.

   Si cette famille est composée uniquement d'homothéties, alors toute base de F est une base de diagonalisation simultanée de ces endomorphismes. Sinon soit i un indice dans I tel que u_i ne soit pas une homothétie et F' un espace propre de u_i. Alors, par commutativité de $(u_j)_{j\in I}$, F' est stable par tous les endomorphismes $(u_j)_{j\in I}$ et leurs bi-restrictions à F' forment une famille commutative d'endomorphismes de F'. De plus en tant que restrictions à un espace stable d'endomorphismes diagonalisables, ils le sont aussi. Comme $\dim(F')\leq n$, si $(\mathbf{H}_n)$ est vrai, alors on dispose d'une base commune de diagonalisation pour la famille $(u_{j|F'})_{j\in I}$ et donc, en concaténant les bases obtenues pour chacun des sous-espaces propres de u_i, on obtient une base commune de diagonalisation pour la famille $(u_j)_{j\in I}$.

   D'après le principe de récurrence on en conclut que $(\mathbf{H}_n)$ est vrai pour tout entier naturel non nul n. Par conséquent $\boxed{\text{les éléments de } G \text{ sont diagonalisables dans une même base.}}$

PARTIE II - Isométries du triangle

2.

2a. Puisque (A,B,C) forme un repère affine du plan, tout élément de $\widetilde{D}_3$ est entièrement déterminé par les images de A, B et C. Comme tout point du triangle, hormis ces trois points, est barycentre de deux points distincts du triangle, son image par un élément de $\widetilde{D}_3$ l'est aussi et n'est donc pas un des sommets. Il en résulte que les trois sommets du triangles ont pour image un sommet (nécessairement distinct) du triangle. Par conséquent le cardinal de $\widetilde{D}_3$ est inférieur à celui de $\mathcal{S}_3$, i.e. à 6.

Or les trois symétries par rapport à chacune des médiatrices du triangle ainsi que les trois rotations de centre O et d'angle $2k\pi/3$ avec $k\in\{0,1,2\}$ sont des éléments de $\widetilde{D}_3$. Comme ils sont tous distincts, $\widetilde{D}_3$ est de cardinal au moins 6 et, finalement,

$\boxed{\begin{array}{l}\widetilde{D}_3 \text{ est de cardinal 6 et est formé des trois symétries par rapport à chacune des médiatrices}\\ \text{du triangle ainsi que des trois rotations de centre } O \text{ et d'angle } 2k\pi/3 \text{ avec } k\in\{0,1,2\}.\end{array}}$

2b. Puisque ABC est un triangle équilatéral, $(\overrightarrow{OA},\overrightarrow{OB})$ est un repère du plan.

Or l'isomorphisme canonique entre l'anneau des endomorphismes du plan muni d'une base et $\mathcal{M}_2(\mathbf{C})$, obtenu en associant à un endomorphisme sa matrice dans la base donnée, induit un morphisme de groupes sur les éléments inversibles et donc $\widetilde{D}_3$ est isomorphe au sous-groupe de $\mathrm{GL}_2(\mathbf{C})$ donné par les matrices de ces endomorphismes dans la base $(\overrightarrow{OA},\overrightarrow{OB})$.

L'image de la symétrie par rapport à la médiatrice de (AB) est $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ puisque $\overrightarrow{OA}$ et $\overrightarrow{OB}$ sont échangés par cette symétrie.

Puisque O est l'isobarycentre de ABC, on a $\overrightarrow{OC} + \overrightarrow{OA} + \overrightarrow{OB} = \overrightarrow{0}$, l'image de la rotation de centre O envoyant A sur B est $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ puisqu'alors B est envoyé sur C.

L'ensemble des matrices de rotations dans $\widetilde{D}_3$ est l'ensemble des puissances de ce dernier élément, i.e.

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Les matrices de symétrie s'obtiennent par multiplication (à gauche) des trois matrices précédentes par celle de la matrice de symétrie déjà obtenue, i.e.

$$\begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

et donc

$\widetilde{D}_3$ est isomorphe à un sous-groupe de $\mathrm{GL}_2(\mathbf{C})$ formé de ces six matrices, toutes à coefficients dans $\{-1, 0, 1\}$.

2c. Puisque la matrice $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ est celle d'une rotation d'angle $2\pi/3$, elle est d'ordre 3 et elle est donc diagonalisable et ses valeurs propres sont des racines cubiques de l'unité, non réelles.

Soit $c = e^{2i\pi/3}$ et $P = \begin{pmatrix} 1 & 1 \\ -c & -c^2 \end{pmatrix}$. Il vient :

$$\begin{aligned} P^{-1} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} P &= \frac{1}{c - c^2} \begin{pmatrix} -c^2 & -1 \\ c & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -c & -c^2 \end{pmatrix} \\ &= \frac{1}{c(1-c)} \begin{pmatrix} -1 & -c \\ 1 & c^2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -c & -c^2 \end{pmatrix} \\ &= \frac{1}{c(1-c)} \begin{pmatrix} c^2 - 1 & 0 \\ 0 & 1 - c \end{pmatrix} \\ &= \begin{pmatrix} c & 0 \\ 0 & c^2 \end{pmatrix} \end{aligned}$$

car $c^3 = 1$ et $1 + c + c^2 = 0$, donc $c^2 - 1 = (c+1)(c-1) = -c^2(c-1) = c^2(1-c)$. De plus les images des éléments du groupe obtenu à la question précédente par l'automorphisme

intérieur de $\mathrm{GL}_2(\mathbf{C})$ donné par $M \mapsto P^{-1}MP$ sont respectivement

$$P^{-1}\begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix}P = \begin{pmatrix}c & 0\\ 0 & c^{-1}\end{pmatrix} \qquad P^{-1}\begin{pmatrix}-1 & 0\\ -1 & 1\end{pmatrix}P = \begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}$$
$$P^{-1}\begin{pmatrix}-1 & 1\\ -1 & 0\end{pmatrix}P = \begin{pmatrix}c^2 & 0\\ 0 & c^{-2}\end{pmatrix} \qquad P^{-1}\begin{pmatrix}1 & -1\\ 0 & -1\end{pmatrix}P = \begin{pmatrix}0 & -c\\ -c^{-1} & 0\end{pmatrix}$$
$$P^{-1}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}P = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \qquad P^{-1}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}P = \begin{pmatrix}0 & -c^2\\ -c^{-2} & 0\end{pmatrix}$$

et donc $\boxed{\widetilde{D}_3 \text{ est isomorphe à } D_3.}$

PARTIE III - Lemme de Schur

3. Pour B dans G, $i(B)$ est un automorphisme intérieur et donc i est à valeurs dans $\mathrm{GL}(\mathcal{A})$. De plus pour M dans $\mathcal{A}$ et B et B' dans G, on a

$$i(BB')(M) = BB'M(BB')^{-1} = BB'MB'^{-1}B^{-1} = i(B)\circ i(B')(M)$$

et donc $i(BB') = i(B)\circ i(B')$. Par conséquent
$\boxed{i \text{ est un morphisme de groupes de } G \text{ dans } \mathrm{GL}(\mathcal{A}).}$
De plus $\mathrm{Ker}(i)$ est formé des éléments de G commutant à tous les éléments de $\mathcal{A}$. Or les élements de $\mathcal{A}$ commutant à tous les autres sont les homothéties et donc i est injectif si et seulement si $\boxed{G \text{ ne contient pas d'autre homothétie que l'identité.}}$

4. Il y a une erreur de notation de l'énoncé, juste avant cette question : B varie dans G et non dans $\widetilde{G}$.
On identifie canoniquement les matrices dans $\mathcal{A}$ avec des endomorphismes de $\mathbf{C}^n$. Par définition tous les éléments de G commutent avec M et donc $\boxed{\text{laissent stables } \mathrm{Ker}(M) \text{ et } \mathrm{Im}(M).}$

5. D'après ce qui précède, $\mathrm{Ker}(M)$ est stable et est donc soit réduit à $\{0\}$, soit égal à E, et donc $\boxed{M \text{ est soit inversible, soit nulle.}}$
Puisque $\mathbf{C}$ est algébriquement clos, on dispose d'une valeur propre λ de M. Comme M commute à tous les éléments de G, il en va de même pour $M - \lambda I_n$ et donc $M - \lambda I_n$ est une matrice non inversible dans $A^{\widetilde{G}}$. D'après ce qui précède on en déduit $M = \lambda I_n$. Comme, réciproquement, les homothéties appartiennent à $A^{\widetilde{G}}$, il vient $A^{\widetilde{G}} = \mathbf{C}I_n$ et, en particulier, $\boxed{A^{\widetilde{G}} \text{ est de dimension 1.}}$

6. On munit $\mathcal{A}$ de sa base canonique $(E_{kl})_{1\le k,l\le n}$ et on note $(E^*_{kl})_{1\le k,l\le n}$ la base duale de $(E_{kl})_{1\le k,l\le n}$. En posant $M = (\mu_{kl})_{1\le k,l\le n}$ et $N = (\nu_{kl})_{1\le k,l\le n}$, on a, pour $1 \le k,l \le n$, $\langle E^*_{kl} \mid \Phi(E_{kl})\rangle = \mu_{kk}\nu_{ll}$. Il en résulte $\mathrm{Tr}(\Phi) = \displaystyle\sum_{k=1}^{n}\sum_{l=1}^{n}\mu_{kk}\nu_{ll}$, i.e. $\boxed{\mathrm{Tr}(\Phi) = \mathrm{Tr}(M)\,\mathrm{Tr}(N).}$

7.

7a. Puisque la multiplication à gauche par un élément de G est une bijection de G sur lui-même, on a, pour B dans G, $PB = \dfrac{1}{|G|}\sum_{B'\in G} B'B = \dfrac{1}{|G|}\sum_{g\in G} g = P = BP$ et il en résulte directement $\boxed{P^2 = P.}$

Il en résulte que P est un projecteur, annulé par le polynôme simplement scindé $X(X-1)$ et donc $\boxed{P \text{ est diagonalisable.}}$

7b. Soit x dans E^G, on a alors $Bx = x$ pour tout élément B de G et donc $Px = x$, donc $x \in \mathrm{Im}(P)$ puisque P est un projecteur. Réciproquement si $Px = x$, alors pour B dans G on a $BP = P$ et donc $Bx = BPx = Px = x$, d'où $\boxed{\mathrm{Im}(P) = E^G.}$

Comme P est un projecteur, son rang est égal à sa trace, et donc par linéarité de la trace

$$\boxed{\dim(E^G) = \frac{1}{|G|}\sum_{B\in G} \mathrm{Tr}(B).}$$

8. D'après 3. on peut appliquer la question précédente à $\widetilde{G}$ vu comme sous-groupe de $\mathrm{GL}(\mathcal{A})$ et il vient donc $\dim(\mathcal{A}^{\widetilde{G}}) = \dfrac{1}{|\widetilde{G}|}\sum_{g\in\widetilde{G}} \mathrm{Tr}(g)$.

Si i est injectif, alors à tout g dans $\widetilde{G}$ correspond un unique B dans G tel que $g = i(B)$ et alors, d'après 6., on a $\mathrm{Tr}(g) = \mathrm{Tr}(B)\,\mathrm{Tr}(B^{-1})$. De plus on a alors $|\widetilde{G}| = |G|$, d'où la formule recherchée.

Sinon, pour g dans $\widetilde{G}$, on dispose de B dans G tel que $g = i(B)$ et on a, pour B' dans G, $i(B') = g \Leftrightarrow i(B') = i(B) \Leftrightarrow B'B^{-1} \in \mathrm{Ker}(i)$. De plus, pour B' dans G tel que $i(B') = i(B)$, on a $\mathrm{Tr}(B'^{-1})\,\mathrm{Tr}(B') = \mathrm{Tr}(g) = \mathrm{Tr}(B^{-1})\,\mathrm{Tr}(B)$. On a donc

$$\begin{aligned}
\frac{1}{|G|}\sum_{B\in G} \mathrm{Tr}(B^{-1})\,\mathrm{Tr}(B) &= \frac{1}{|G|}\sum_{g\in\widetilde{G}}\sum_{B\in i^{-1}(g)} \mathrm{Tr}(B^{-1})\,\mathrm{Tr}(B)\\
&= \frac{1}{|G|}\sum_{g\in\widetilde{G}}\sum_{B\in i^{-1}(g)} \mathrm{Tr}(g)\\
&= \frac{1}{|G|}\sum_{g\in\widetilde{G}} |i^{-1}(g)|\,\mathrm{Tr}(g)\\
&= \frac{|\,\mathrm{Ker}(i)|}{|G|}\sum_{g\in\widetilde{G}} \mathrm{Tr}(g)\ .
\end{aligned}$$

Or $|G| = \sum_{B\in G} 1 = \sum_{g\in\widetilde{G}} |i^{-1}(g)| = |Ker(i)| \times |\widetilde{G}|$ et donc

$$\boxed{\dim(\mathcal{A}^{\widetilde{G}}) = \frac{1}{|G|}\sum_{B\in G} \mathrm{Tr}(B^{-1})\,\mathrm{Tr}(B).}$$

9.

9a. D'après 5. $\mathcal{A}^{\widetilde{G}}$ est formé des matrices scalaires. Comme c'est exactement l'ensemble des matrices de $\mathcal{A}$ commutant aux matrices de G, et puisque $\mathrm{Tr}(I_n) = n$, une telle matrice X vérifie $\boxed{X = \frac{1}{n}\mathrm{Tr}(X)I_n.}$

9b. Soit B dans G, alors $i(B)_{|G}$ est un automorphisme intérieur de G et donc une bijection de G dans lui-même. De plus la trace est invariante par conjugaison et donc $\mathrm{Tr} \circ i(B) = \mathrm{Tr}$, il en résulte $i(B)(Y) = Y$ et donc, d'après ce qui précède, $Y = \frac{1}{n}\mathrm{Tr}(Y)I_n$. Comme $\mathrm{Tr}(Y) = |G|$ d'après 8., on en déduit $\boxed{Y = \frac{|G|}{n}I_n.}$

10.

10a. Soit B dans G. D'après les arguments développés en 1., B a des valeurs propres racines de $X^{|G|} - 1$. Comme la trace est la somme de ces valeurs propres, $\boxed{\mathrm{Tr}(B) \in \mathbf{Z}_G.}$

Par définition de Y et puisque G est stable par passage à l'inverse, le résultat précédent entraîne $\boxed{Y \in \mathbf{Z}_G[G].}$

10b. L'énoncé est incorrect. Les coefficients cherchés ne dépendent pas de k.

Puisque l'ensemble des racines de l'unité d'ordre $|G|$ et G sont stables par multiplication, l'ensemble des $(C_k)_{1\leq k\leq |G|^2}$ est stable par produit et donc $\mathbf{Z}_G$ aussi. Enfin, par définition, tout élément de $\mathbf{Z}_G$ est combinaison linéaire à coefficients entiers d'éléments de $(C_k)_{1\leq k\leq |G|^2}$. C'est donc en particulier le cas pour YC_k, pour $1 \leq k \leq |G|^2$, i.e.

$\boxed{\text{on peut trouver } (a_{ij})_{1\leq i,j\leq |G|^2} \text{ dans } \mathbf{Z}^{|G|^2} \text{ tels que } YC_k = \sum_{1\leq l\leq |G|^2} a_{l,k}C_l.}$

10c. D'après ce qui précède , pour $1 \leq k \leq |G|^2$, $\frac{|G|}{n}C_k = \sum_{1\leq l\leq |G|^2} a_{l,k}C_l$ ou encore

$$\sum_{1\leq l\leq |G|^2} \left(\frac{|G|}{n}\delta_{lk} - a_{l,k}\right) C_l\,,$$

où δ_{lk} est le symbole de Kronecker.

Autrement dit en posant C la matrice par blocs de taille $n|G|^2 \times n$ dont les $|G|^2$ blocs sont les C_k, on a ${}^tRC = 0$. Puisque C n'est pas la matrice nulle, car sinon G serait constitué de matrices nulles, ${}^tR$ n'est pas injective et donc elle n'est pas inversible. Il en est donc de même pour R, i.e. $\boxed{\det(R) = 0.}$

10d. Puisque A est à coefficients entiers, il en va de même pour son polynôme caractéristique. Ce dernier est unitaire et admet $|G|/n$ comme racine d'après ce qui précède. Or un polynôme unitaire T de degré m et à coefficients entiers n'admet pas de racine rationnelle non entière car si p/q est une telle racine, avec p et q entiers premiers entre eux, on a $q^m T(p/q) = 0$ exhibe p^m comme combinaison linéaire à coefficients entiers de nombres de la forme $q^k p^{m-k}$ avec $1 \leq k \leq m$ et donc $q|p$, ce qui entraîne $q = 1$ et donc p/q est entier.

Il en résulte $|G|/n$ entier, i.e. $\boxed{n \text{ divise } |G|.}$

PARTIE IV - Une caractérisation de D_n, n impair

11.

11a. Soit B dans G, on pose, pour v et w dans $\mathbf{C}^2$, $\langle v \mid w\rangle_B = \langle B(v) \mid B(w)\rangle$. Puisque B est linéaire et $\langle \cdot \mid \cdot\rangle$ est sequi-linéaire $\langle \cdot \mid \cdot\rangle_B$ l'est aussi. Puisque $\langle \cdot \mid \cdot\rangle$ est à symétrie hermitienne, $\langle \cdot \mid \cdot\rangle_B$ aussi. Puisque $\langle \cdot \mid \cdot\rangle$ est positif, $\langle \cdot \mid \cdot\rangle_B$ l'est aussi. Enfin puisque $\langle \cdot \mid \cdot\rangle$ est défini et B est bijectif, $\langle \cdot \mid \cdot\rangle_B$ est défini positif. Donc $\langle \cdot \mid \cdot\rangle_B$ est un produit scalaire hermitien.

Il en va donc de même pour $\langle \cdot \mid \cdot\rangle_0$ puisque c'est une combinaison linéaire à coefficients strictement positifs de produits scalaires hermitiens.

De plus, pour tous B et B' dans G et tous v et w dans $\mathbf{C}^2$, on a $\langle B(v) \mid B(w)\rangle_{B'} = \langle v \mid w\rangle_{B'B}$ et donc, puisque $B' \mapsto B'B$ est une bijection de G dans lui-même

$\boxed{\langle \cdot \mid \cdot\rangle_0 \text{ est un produit scalaire hermitien vérifiant } \langle B(v) \mid B(w)\rangle_0 = \langle v \mid w\rangle_0.}$

11b. On suppose $\mathbf{C}^2$ réductible. On dispose donc d'une droite D stable par G. Soit u un vecteur directeur de D de norme 1 pour $\langle \cdot \mid \cdot\rangle_0$. Comme on a affaire à un produit scalaire, on peut compléter (u) en une base orthonormée pour $\langle \cdot \mid \cdot\rangle_0$, i.e. on dispose de v dans $\mathbf{C}^2$ tel que $\langle u \mid v\rangle_0 = 0$. Or, pour B dans G, on a $\langle B(u) \mid B(v)\rangle_0 = \langle u \mid v\rangle_0 = 0$ et $B(u)$ est un vecteur proportionnel à u, par stabilité de D et non nul par injectivité de B. Donc $B(v)$ est un vecteur orthogonal à u pour $\langle u \mid v\rangle_0 = 0$ et est donc colinéaire à v, puisque l'orthogonal d'une droite dans un plan est une droite.

Autrement dit la base (u, v) est une base propre pour tous les éléments de G, i.e.

$\boxed{\text{cette base diagonalise tous les éléments de } G.}$

Les endomorphismes canoniquement associés aux éléments de G commutent donc quand on les exprime dans la base (u, v), donc dans n'importe quelle base, en particulier la base canonique, i.e. $\boxed{G \text{ est commutatif.}}$

12.

12a. Soit B dans $\mathrm{SL}_2(\mathbf{C})$. D'après le théorème de Cayley-Hamilton, on a $B^2 - \mathrm{Tr}(B)B + I_2 = 0$ et donc $B^2 = I_2 \Leftrightarrow \mathrm{Tr}(B)B = 2I_2$. Dans ce cas $\mathrm{Tr}(B)^2 = 4$ et B est scalaire, puisque $\mathrm{Tr}(B)$ est non nul. Il en résulte $B = \pm I_2$. La réciproque étant immédiate, $\boxed{B^2 = I_2 \text{ si et seulement si } B = \pm I_2\,?}$

12b. Si G n'est pas commutatif alors, d'après 11.b, $\mathbf{C}^2$ est irréductible pour G et donc, d'après 10.d $\boxed{|G| \text{ est pair.}}$

En outre, d'après le résultat admis en préambule, il existe G admet un élément d'ordre 2. Comme G est inclus dans $\mathrm{SL}_2(\mathbf{C})$, il vient d'après la question précédente $\boxed{-I_2 \in G.}$

13.

13a. Par contraposée de la question précédente, puisque G_0 est un sous-groupe de $\mathrm{SL}_2(\mathbf{C})$ ne contenant pas $-I_2$, $\boxed{G_0 \text{ est commutatif.}}$

Les éléments de G_0 sont donc simultanément diagonalisables, d'après 1., i.e. on dispose de P dans $\mathrm{GL}_2(\mathbf{C})$ tel que $i(P)(G_0)$ est inclus dans l'ensemble des matrices diagonales. De plus $i(P)$ préservant le déterminant, $i(P)(G_0)$ est formé de matrices diagonales de déterminant 1. En notant Γ_0 cette image, $\boxed{i(P) \text{ induit un isomorphisme de } G_0 \text{ sur } \Gamma_0.}$

13b. Soit $m = |\Gamma_0|$. D'après le théorème de Lagrange, rappelé en préambule, pour tout γ dans Γ_0, on a $\gamma^m = I_2$, de sorte que la diagonale de γ est formée de racines de l'unités, i.e. $\gamma = \mathrm{diag}(\lambda, \lambda^{-1})$ avec $\lambda^m = 1$. Comme l'ensemble des racines de l'unité est de cardinal m et que l'application $\gamma \mapsto \lambda$ est injective, elle est en fait bijective, i.e. $\boxed{\Gamma_0 = \mathcal{Z}_m.}$

13c. Si $G_0 = \{I_2\}$, alors le déterminant induit un morphisme injectif de groupes de G sur son image. Par conséquent G est isomorphe à un sous-groupe de $\mathbf{C}^*$. Comme ce dernier est abélien, il en va de même pour G, i.e. $\boxed{G \text{ est commutatif.}}$

14.

14a. L'existence de B_0 provient de la non-commutativité de G car l'ensemble des matrices diagonales est commutatif.

Puisque $\mathcal{Z}_m = G \cap \mathrm{SL}_2(\mathbf{C})$ et que $i(B_0)$ stabilise G, car G est un groupe, et $\mathrm{SL}_2(\mathbf{C})$, $i(B_0)$ stabilise $\mathcal{Z}_m$, i.e. pour tout C dans $\mathcal{Z}_m$, $\boxed{B_0 C B_0^{-1} \in \mathcal{Z}_m.}$

Puisque G n'est pas commutatif, $m > 1$ d'après 13.c, et m est impair puisque G ne contient pas $-I_2$. On dispose donc de B dans G_0 distinct de l'identité et donc de valeurs propres distinctes, par imparité de m. D'après ce qui précède les sous-espaces propres de $i(B_0)(B)$ sont les mêmes que ceux de B et donc ils sont soit conservés, soit échangés par B_0. Comme B_0 n'est pas diagonale, elle ne saurait conserver les droites engendrées par la base canonique et donc elle les échange, i.e. on dispose de b et b' dans $\mathbf{C}$ tels que $\boxed{B_0 = \begin{pmatrix} 0 & b \\ b' & 0 \end{pmatrix}.}$

14b. On a $\boxed{B_0^2 = bb' I_2.}$

Comme B_0^2 appartient à G et est scalaire, il vient $B_0^2 = I_2$, i.e. $\boxed{b' = b^{-1}.}$

14c. On pose $Q = \begin{pmatrix} -1 & 0 \\ 0 & b \end{pmatrix}$. Il vient $Q^{-1} = \begin{pmatrix} -1 & 0 \\ 0 & b' \end{pmatrix}$ et donc

$$\boxed{Q \text{ est diagonale et } QB_0Q^{-1} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.}$$

15.

15a. Puisque B est diagonale et B_0 ne l'est pas, $B_0 B$ ne l'est pas non plus. Il résulte de 14.a et 14.b qu'on a donc $\det(B_0 B) = -1 = \det(B_0)$ et donc $\det(B) = 1$ et ainsi $\boxed{B \in \mathcal{Z}_m.}$

15b. Soit B dans G qui n'est pas diagonale. D'après 14.a, B est anti-diagonale et donc $B_0 B$ est diagonale. Donc $B_0 B \in G_0$ et $B \in B_0 G_0$, puisque $B_0^{-1} = B_0$. On a donc $G = G_0 \cup B_0 G_0$ et cette réunion est disjointe. De plus $i(Q)$ laisse $\mathcal{Z}_m$ fixe et envoie B_0 sur $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$, donc l'image de $B_0 G_0$ par $i(Q)$ est $D_m \setminus \mathcal{Z}_m$. Par conséquent $i(Q)$ induit un

$\boxed{\text{isomorphisme entre } G \text{ et } D_m.}$

16.

16a. D'après 1., les matrices de G sont co-diagonalisables et on dispose de Q tel que $i(Q)$ soit un morphisme de groupe, injectif d'après 3., de G dans l'ensemble des matrices diagonales inversibles. Comme ce dernier est un groupe isomorphe à $(\mathbf{C}^*)^2$ et les applications coordonnées de $(\mathbf{C}^*)^2$ dans $\mathbf{C}$ sont des morphismes, par composition, on dispose de deux morphismes de groupes de G dans $\mathbf{C}^*$, χ_1 et χ_2 tels que l'image de B dans G par $i(Q)$ soit $\begin{pmatrix} \chi_1(B) & 0 \\ 0 & \chi_2(B) \end{pmatrix}$. En posant $P = Q^{-1}$, il vient $\boxed{B = P \begin{pmatrix} \chi_1(B) & 0 \\ 0 & \chi_2(B) \end{pmatrix} P^{-1}.}$

16b. Puisque χ_1 et χ_2 le sont, $\chi_1\chi_2^{-1}$ est un morphisme de groupes. Il est injectif car son noyau est formé des matrices de G qui sont scalaires. Or d'après le théorème de Lagrange, χ_1 et χ_2, donc aussi $\chi_1\chi_2^{-1}$, sont à valeurs dans le groupe des racines $|G|$-ièmes de l'unité. Par cardinalité $\boxed{\chi_1\chi_2^{-1} \text{ est un isomorphisme de } G \text{ sur ce groupe.}}$

16c. La question précédente montre que G est isomorphe à groupe cyclique et l'est donc lui-même. Si g en est un générateur, on pose $c = \chi_1(g)$ et $d = \chi_2(g)$. Ce sont des racines $|G|$-ièmes de l'unité, d'après les arguments de la question précédente et, de plus, c/d est une racine primive. Autrement dit on dispose de p et q entiers tels que $c = e^{2ip\pi/|G|}$, $d = e^{2iq\pi/|G|}$, $p - q$ premier avec $|G|$, $g = P \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} P^{-1}$, et donc G est formé des matrices

$\boxed{P \begin{pmatrix} c^k & 0 \\ 0 & d^k \end{pmatrix} P^{-1}, \text{ pour } 0 \leq k \leq |G| - 1.}$

17. L'ensemble des matrices précédentes, pour $P = I_2$, est un groupe fini commutatif ne contenant pas d'autre homothétie que l'identité et donc son conjugué par $i(P)$ aussi. Le groupe D_m est un groupe fini non commutatif ne contenant pas d'autre homothétie que l'identité si m est impair.

Il résulte donc des question 13. à 16. que les sous-groupes finis de $\mathrm{GL}_2(\mathbf{C})$ ne contenant pas d'autre homothétie que l'identité sont les groupes de la forme

$\boxed{i(P)(D_m) \text{ pour } m \text{ impair et } P \text{ dans } \mathrm{GL}_2(\mathbf{C})}$ ou bien

$\boxed{\left\{ d^k P \begin{pmatrix} \zeta^k & 0 \\ 0 & 1 \end{pmatrix} P^{-1} \;\middle|\; 1 \leq k \leq m \right\} \text{ pour } m \text{ dans } \mathbf{N}^*, d \text{ une racine } m\text{-ième de l'unité, } \zeta \text{ une racine primitive } m\text{-ième de l'unité et } P \text{ dans } \mathrm{GL}_2(\mathbf{C}).}$

18. Soit G un sous-groupe de $\mathrm{GL}_2(\mathbf{C})$ isomorphe à $(\mathbf{Z}/2\mathbf{Z})^3$, alors G est commutatif et donc, d'après 1., il est conjugué à un sous-groupe des matrices diagonales inversibles. Comme tous ses éléments sont d'ordre diviseur 2, un tel isomorphisme envoie les matrices de G sur des matrices diagonales de carré I_2. Comme ces dernières sont au nombre de 4, un tel isomorphisme ne saurait exister donc $\boxed{\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \text{ n'est isomorphe à aucun sous-groupe } \mathrm{GL}_2(\mathbf{C}).}$