Corrigé du devoir d'algèbre de septembre 2020

Remarque : le sujet identifie, comme c'est souvent fait, les endomorphismes de $\mathbb{C}^n$ à leurs matrices dans la base canonique.

I - Centre de GL(E)

Remarque : L'objectif de cette partie est de donner une preuve "dynamique" (par action de groupe) du fait que le centre de $\mathrm{GL}(E)$ est réduit aux homothéties. Ce résultat de groupe s'étend à l'anneau des matrices : les matrices qui commutent avec toutes les matrices de $M_n(\mathbb{K})$ sont les matrices d'homothéties. Ce n'est plus un résultat sur les groupes mais un résultat sur l'anneau $M_n(\mathbb{K})$ (sur sa structure multiplicative). On peut déduire ce deuxième résultat du premier par translation (réponse à la question 8). La preuve classique (rappelée aussi à la question 8) consiste à regarder la condition donnée par la commutation avec les matrices élémentaires, qui engendrent l'espace vectoriel des matrices.

1. On a $gfg^{-1}(g(x) = gf(x) = g(\lambda x) = \lambda g(x)$, donc $g(x)$ est un vecteur propre de gfg^{-1} pour la valeur propre λ.
2. Supposons qu'un automorphisme g de E commute avec f. On a alors $gfg^{-1} = f$. Soit $i \in \{1, ..., n\}$. D'après la question précédente, $g(e_i)$ est un vecteur propre de f pour la valeur propre i. Comme l'espace propre de f pour la valeur propre i est de dimension 1, engendré par e_i, cela montre que $g(e_i)$ est colinéaire à e_i. Cela signifie que e_i est un vecteur propre de g. Donc la matrice de g est dans la base $\mathcal{B}$ est diagonale. La réciproque est immédiate du fait que deux matrices diagonales commutent.
3. Notons λ_i la valeur propre associée au vecteur propre e_i de f. Supposons que f commute avec les endomorphismes $g_{\sigma,\mathcal{B}}$, c'est-à-dire que $g_{\sigma,\mathcal{B}} f g_{\sigma,\mathcal{B}}^{-1} = f$. D'après la première question, comme e_i est vecteur propre de f pour la valeur propre λ_i, $g_{\sigma,\mathcal{B}}(e_i)$ est vecteur propre de f pour cette même valeur propre. Mais par définition $g_{\sigma,\mathcal{B}}(e_i) = e_{\sigma(i)}$, qui est vecteur propre de f pour la valeur propre $\lambda_{\sigma(i)}$. Cela montre que $\lambda_i = \lambda_{\sigma(i)}$ pour tout i et tout $\sigma \in S_n$. Ceci montre que f est une homothétie.
4. Soit f un automorphisme de E qui commute avec tous les automorphismes de E. D'après la question 2, f est diagonalisable dans la base $\mathcal{B}$, donc d'après la question 3, f est une homothétie. Réciproquement une homothétie commute avec tout endomorphisme de E.

II - Sous-groupes finis de GL(E)

5. Pour $g \in G$, on a, d'après le résultat rappelé (lemme de Cauchy) $g^{|G|} = id_E$. Le polynôme $X^{|G|} - 1$, scindé à racines simples sur $\mathbb{C}$, annule g qui est donc diagonalisable.

   Remarque : les valeurs propres de g sont donc des racines $|G|$-ièmes de l'unité. On notera par la suite U_m le groupe des racines m-ièmes de l'unité.

6. Supposons que G est commutatif. Montrons par récurrence sur la dimension de E le résultat plus général suivant : "Soit $(u_i)_{i\in I}$ une famille d'endomorphismes diagonalisables qui commutent ; alors il existe une base de E qui diagonalise tous les u_i."
   - Si E est de dimension 1, le résultat est évident.
   - Soit $n \in \mathbb{N}^*$; supposons le résultat établi dans tout espace de dimension $\leq n$, et soit E un $\mathbb{C}$-espace vectoriel de dimension $n+1$, et $(u_i)_{i\in I}$ une famille d'endomorphismes de E diagonalisables qui commutent.
   - Si tous les u_i sont des homothéties, n'importe quelle base de E convient.
   - Sinon, soit $i_0 \in I$ tel que u_{i_0} n'est pas une homothétie. Soit F un sous-espace propre de u_{i_0} : F est de dimension $\leq n$, et stable par tous les u_i (car ils commutent avec u_{i_0}). En outre, les restrictions $u_i|_F$ sont également diagonalisables et commutent : on peut leur appliquer l'hypothèse de récurrence, et il existe une base de F formée de vecteurs propres communs à tous les $u_i|_F$. Cela vaut pour tous les sous-espaces propres de u_{i_0}, dont la somme directe vaut E : en recollant, on obtient une base de E qui diagonalise tous les u_i.

Le résultat que nous venons de prouver par récurrence s'applique alors aux éléments de G, diagonalisables et qui commutent deux à deux.

III - Isométries du triangle

Cette partie étudie le groupe diédral D_n lorsque $n = 3$.

7. Il suffit de montrer que D_n est un sous-groupe de $\mathrm{GL}_2(\mathbb{C})$. Notons $r_k = \begin{pmatrix} c^k & 0 \\ 0 & c^{-k} \end{pmatrix}$ et $s_k = \begin{pmatrix} 0 & -c^k \\ -c^{-k} & 0 \end{pmatrix}$ et on généralise cette notation à $k \in \mathbb{Z}$ quelconque, en notant que par périodicité, tous les r_k, s_k sont dans D_n. On constate facilement que $D_n \subset \mathrm{GL}_2(\mathbb{C})$ et que $\mathrm{id} = r_0$ est dans D_n. Pour tous k, l on a $r_k \circ r_l = r_{k+l}$, $r_k \circ s_l = s_{k+l}$, $s_k \circ r_l = s_{k-l}$ et $s_k \circ s_l = r_{k-l}$, donc G est stable par produit. L'inverse de r_k est r_{n-k} (ou r_0 si $k = n$) et s_k est son propre inverse. Cela montre que D_n est un groupe.

   Remarque : on reconnait la matrice de rotation d'angle $\frac{2k\pi}{n}$ pour r_k, une matrice de symétrie pour s_k et le groupe diédral pour D_n.

8. (a) Les applications affines préservant le barycentre et les isométries étant des bijections, chaque élément de $\tilde{\mathrm{D}}_3$ envoie bijectivement $\{A, B, C\}$ sur lui-même, et donc l'isobarycentre de $\{A, B, C\}$ sur lui-même.

   (b) Un élément de $\tilde{\mathrm{D}}_3$ est une isométrie affine laissant O invariant, c'est donc ou bien une rotation de centre O, ou bien une symétrie orthogonale par rapport à une droite passant par O. Selon que l'image de A est A, B ou C, dans le premier cas il s'agit de la rotation de centre O d'angle $\in \{0, \frac{2\pi}{3}, \frac{4\pi}{3}\}$ (on suppose implicitement le plan orienté) ; dans le second de la symétrie par rapport à OA, OC ou OB. Réciproquement ces 6 isométries laissent invariant le triangle.

   (c) On en déduit que $\tilde{\mathrm{D}}_3$ est de cardinal 6. Or les éléments de $\tilde{\mathrm{D}}_3$ laissent $\{A, B, C\}$ stable, donc la restriction de l'action de $\tilde{\mathrm{D}}_3$ sur le plan affine à cet ensemble définit un morphisme de $\tilde{\mathrm{D}}_3$ sur le groupe des permutations de $\{A, B, C\}$, lui-même isomorphe au groupe symétrique S_3. Le morphisme de $\tilde{\mathrm{D}}_3$ sur $S(\{A, B, C\})$ est injectif car une application affine envoyant le repère affine (A, B, C) du plan sur lui-même est l'identité. Comme les deux groupes sont de même cardinal, le morphisme injectif est un isomorphisme. Cela conclut.

   Remarque : on peut voir à la main que le morphisme est surjectif : on retrouve les 6 éléments de $S(\{A, B, C\})$ comme la restriction à $\{A, B, C\}$ des 6 isométries.

   (d) Compte-tenu de la relation $\vec{OC} = -\vec{OA} - \vec{OB}$, les matrices respectives dans $(\vec{OA}, \vec{OB})$ de l'identité, des rotations de centre O d'angle $\frac{2\pi}{3}, \frac{4\pi}{3}$, enfin des symétries orthogonales par rapport aux droites OA, OB, OC s'écrivent : $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. L'ensemble de ces 6 matrices constitue alors un sous-groupe de $\mathrm{GL}_2(\mathbb{C})$, que je noterai $\mathcal{G}$, isomorphe à $\tilde{\mathrm{D}}_3$.

   (e) Son polynôme caractéristique étant $X^2 + X + 1 = (X - j)(X - j^{-1})$ (où $j = e^{\frac{2i\pi}{3}}$), scindé à racines simples sur $\mathbb{C}$, la matrice $A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ est diagonalisable sur $\mathbb{C}$.

   En résolvant $AX = \lambda X$, avec $\lambda \in \{j, j^{-1}\}$, on diagonalise effectivement : soit $P = \begin{pmatrix} 1 & 1 \\ -j & -j^{-1} \end{pmatrix}$, il vient : $P^{-1}AP = \begin{pmatrix} j & 0 \\ 0 & j^{-1} \end{pmatrix}$.

   En conjuguant les éléments de $\mathcal{G}$ par P, on obtient enfin le sous-groupe suivant de $\mathrm{GL}_2(\mathbb{C})$:
   $\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} j & 0 \\ 0 & j^{-1} \end{pmatrix}, \begin{pmatrix} j^{-1} & 0 \\ 0 & j \end{pmatrix}, \begin{pmatrix} 0 & -j \\ -j^{-1} & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -j^{-1} \\ -j & 0 \end{pmatrix}\}$.
   On reconnaît D_3, qui est bien isomorphe à $\tilde{\mathrm{D}}_3$.

   Remarque : On a ici "représenté" le groupe diédral dans $\mathrm{GL}_2(\mathbb{C})$.

IV - Lemme de Schur

Le lemme de Schur est un lemme de la théorie des représentations des groupes finis (au programme de l'agrégation externe), c'est à dire des morphismes d'un groupe fini dans un groupe linéaire.

L'ensemble $\mathcal{A}^{\tilde{G}}$ est l'ensemble des matrices qui commutent avec tous les éléments de G, on l'appelle le "commutant" de G. C'est plutôt une notion d'anneau que de groupe, car $\mathcal{A}$ est un anneau. Dans un groupe on parle de "centralisateur" d'une partie pour désigner l'ensemble des éléments du groupe qui commutent avec tous les éléments de la partie.

9. — Pour $B \in G$ fixée, $i(B)$ est un endomorphisme de $\mathcal{A}$ (car $\forall(\lambda,\mu,M,N) \in \mathbb{C}^2 \times \mathcal{A}^2$, $B(\lambda M+\mu N)B^{-1} = \lambda BMB^{-1} + \mu BMB^{-1}$) ; de plus, pour $(B,B',M) \in G^2 \times \mathcal{A}$, on a :

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

Comme $i(I_n) = id_{\mathcal{A}}$, on déduit de **(1)** que $i(B)$ est bijectif, de bijection réciproque $i(B^{-1})$. Ceci établit que $i(B) \in GL(\mathcal{A})$. Enfin, **(1)** implique que i est un morphisme de groupes de G dans $GL(\mathcal{A})$.
On a $B \in \mathrm{Ker}(i)$ si et seulement si $\forall M \in \mathcal{A}, BM = MB$. On a vu dans la partie I que si $B \in \mathrm{GL}_n(\mathbb{C})$, B commute avec tous les éléments de $\mathcal{A}$ si et seulement si B est une homothétie. Si B n'est pas inversible, il existe λ tel que $B - \lambda I_n$ n'est pas inversible (si λ n'est pas valeur propre), et $B - \lambda I_n$ commute avec tous les éléments de $\mathcal{A}$ si et seulement si B commute avec tous les éléments de $\mathcal{A}$. Cela montre que les éléments de $\mathcal{A}$ qui commute avec tous les éléments de $\mathcal{A}$ sont les homothéties. Cela montre que i est injective si et seulement si G ne contient pas pour homothétie que l'élément neutre, la matrice identité.

Remarque : Voici la preuve élémentaire et classique de ce résultat. Soit $B \in \mathcal{A}$ un matrice qui commute avec tous les éléments de $\mathcal{A}$. Soit $(i,j) \in \{1,..,n\}^2$ et $E_{i,j}$ la matrice comportant un 1 sur la i-ème ligne, j-ème colonne et des 0 ailleurs ; $E_{i,j}B = BE_{i,j}$ impose $b_{i,i} = b_{j,j}$ et $b_{i,j} = 0$ si $i \neq j$: ceci valant pour toutes les valeurs de i et j, B est donc une matrice d'homothétie (de la forme λI_n).

10. Par définition, $M \in \mathcal{A}^{\tilde{G}}$ si et seulement si M commute avec tous les éléments de G. Il est connu (et facile à montrer, c'est fait à la question 1 pour le noyau) que lorsque deux endomorphismes commutent, le noyau et l'image de l'un sont stables par l'autre, ce qui garantit le résultat.

11. — De l'irréductibilité de E pour G et de la stabilité de $\mathrm{Ker}(M)$ par G, découle l'alternative : ou bien $\mathrm{Ker}(M) = \{0\}$, ou bien $\mathrm{Ker}(M) = E$. Dans le premier cas, M est inversible ; elle est nulle dans le second.
— Observons ici que $\mathcal{A}^{\tilde{G}}$ est un sous-espace vectoriel de $\mathcal{A}$ contenant I_n, donc aussi $\mathbb{C}.\mathbb{I}_n$. Pour $M \in \mathcal{A}^{\tilde{G}}$, soit alors $\lambda \in \mathbb{C}$ une valeur propre de M (rappelons qu'il en existe car le polynôme caractéristique de M possède au moins une racine complexe) ; $M - \lambda I_n \in \mathcal{A}^{\tilde{G}}$ n'est pas inversible (puisque λ est valeur propre de M), donc $M - \lambda I_n = 0$. Ceci prouve que $\mathcal{A}^{\tilde{G}} = \mathbb{C}.\mathbb{I}_n$, et qu'il s'agit d'un sous-espace de $\mathcal{A}$ de dimension 1.

12. Avec les notations introduites dans la question 3., les $\{E_{i,j}, (i,j) \in \{1,...,n\}^2\}$ forment une base (canonique) de $\mathcal{A}$. Pour $(i,j) \in \{1,...n\}^2$, un calcul aisé établit que la coordonnée de $ME_{i,j}N$ selon $E_{i,j}$ vaut $m_{i,i}n_{j,j}$ (en notant $M = (m_{i,j}), N = (n_{i,j})$). Par définition de la trace, il s'ensuit que $\mathrm{Tr}(\Phi) = \sum_{(i,j)\in\{1,...,n\}^2} m_{i,i}n_{j,j} = \sum_{1\leq i\leq n} m_{i,i} \times \sum_{1\leq j\leq n} n_{j,j} = \mathrm{Tr}(M)\ \mathrm{Tr}(N)$.

13. (a) Soit $B_0 \in G$; l'application τ_{B_0} de G dans G qui à B associe BB_0 est bijective (de bijection réciproque $\tau_{B_0^{-1}}$). En réindexant, on en déduit que $B_0P = \frac{1}{|G|}\sum_{B\in G} B_0B = \frac{1}{|G|}\sum_{B\in G} B = P$. Ceci valant pour tout $B_0 \in G$, il en découle que $P^2 = \frac{1}{|G|}\sum_{B\in G} BP = \frac{1}{|G|}\sum_{B\in G} B = P$. P est donc un projecteur, diagonalisable car annulé par le polynôme scindé à racines simples $X(X-1)$.

(b) — P étant un projecteur, son image est aussi l'ensemble des inavariants, i.e. $\mathrm{Ker}(P - I_n)$. Or $\forall x \in E^G, \forall B \in G, Bx = x$ donc $Px = x$. Réciproquement, si $Px = x$ alors $\forall B \in G, Bx = BPx = Px = x$, donc $x \in E^G$. Ainsi on a bien $\mathrm{Im}(P) = \mathrm{Ker}(P - I_n) = E^G$.
— Comme P est un projecteur, son rang est égal à sa trace, d'où $\mathrm{rg}(P) = \dim(E^G) = \mathrm{Tr}(P) = \frac{1}{|G|}\sum_{B\in G} \mathrm{Tr}(B)$.

14. — On peut généralement appliquer le 12b. à $\mathcal{A}$ à la place de E et $\tilde{G}$ à celle de G, et on obtient :

$$\dim(\mathcal{A}^{\tilde{G}}) = \frac{1}{|\tilde{G}|}\sum_{B'\in\tilde{G}} \mathrm{Tr}(B') \quad \textbf{(2)}$$

— Le cas où i est injectif ne présente pas de difficulté, puisqu'alors i induit un isomorphisme de G sur $\tilde{G}$ (en particulier, $|G| = |\tilde{G}|$) ; **(2)** s'écrit :
$\dim(\mathcal{A}^{\tilde{G}}) = \frac{1}{|G|}\sum_{B\in G} \mathrm{Tr}(i(B)) = \frac{1}{|G|}\sum_{B\in G} \mathrm{Tr}(B)\mathrm{Tr}(B^{-1})$ d'après 12.
— On peut, dans le cas général, se ramener à celui où i est injectif en effectuant la "décomposition canonique" du morphisme i. Comme cette notion est assez hors programme, nous allons en détailler la mise en œuvre.
L'idée est de regrouper les éléments de G ayant même image par i, en définissant la relation d'équivalence $\mathcal{R}$ sur G par : $B_1\mathcal{R}B_2$ si et seulement si $i(B_1) = i(B_2)$ si et seulement si $i(B_1B_2^{-1}) = id_{\mathcal{A}}$ si et seulement si $B_1B_2^{-1} \in \mathrm{Ker}(i)$ (cela équivaut aussi, d'après 7., à : $\exists\lambda \in \mathbb{C}, \mathbb{B}_{\mathbb{1}} = \lambda\mathbb{B}_2$, et $\lambda I_n = B_1B_2^{-1} \in G$).
— Ce qui précède montre que toutes les classes d'équivalence pour $\mathcal{R}$ ont même cardinal : celui de $\mathrm{Ker}(i)$. Cela revient à dire que tous les élements de $\tilde{G}$ ont —$\mathrm{Ker}(i)$— antécédents par i. D'où, en regroupant les éléments de G selon leur classe : $|G| = |\mathrm{Ker}(i)| \times |\tilde{G}|$.
— Enfin, si $B_1\mathcal{R}B_2$, alors $\mathrm{Tr}(i(B_1)) = \mathrm{Tr}(i(B_2)) = \mathrm{Tr}(B_1)\ \mathrm{Tr}(B_1^{-1}) = \mathrm{Tr}(B_2)\mathrm{Tr}(B_2^{-1})$. Il s'ensuit, toujours en regroupant les éléments de G selon leur classe, et puisque toutes les classes ont —$\mathrm{Ker}(i)$— élements, que
$\frac{1}{|G|}\sum_{B\in G} \mathrm{Tr}(B)\mathrm{Tr}(B^{-1}) = \frac{1}{|\tilde{G}|}\sum_{B'\in\tilde{G}} \mathrm{Tr}(B') = \dim(\mathcal{A}^{\tilde{G}})$ (d'après **(2)**) : C.Q.F.D.

Remarque : si l'on tient absolument à suivre l'indication de l'énoncé, il faut passer au quotient, et définir le morphisme i' du groupe quotient $G/\mathcal{R}$ dans $\tilde{G}$: $i'(\overline{B}) = i(B)$. i' devient injectif, et on peut lui appliquer le résultat correspondant.

15. (a) Si X commute avec toutes les matrices de G, 11. assure que c'est une homothétie. Si $X = \lambda I_n$, il vient : $\mathrm{Tr}(X) = n\lambda$, d'où $X = \frac{1}{n}\ \mathrm{Tr}(X)I_n$.

(b) Soit $B_0 \in G$; les applications $B \to BB_0$ et $B' \to B_0^{-1}B'$ sont des bijections de G dans G (cf. 13.a). Il vient :
$YB_0 = \sum_{B\in G} \mathrm{Tr}(B^{-1})BB_0 = \sum_{B'\in G}\mathrm{Tr}(B_0B'^{-1})B_0B_0^{-1}B'$
(en réindexant, et posant $B' = BB_0$)
$= B_0\sum_{B''\in G}\mathrm{Tr}(B''^{-1})B'' = B_0Y$
(posant $B'' = B_0^{-1}B'$, et tenant compte de $\mathrm{Tr}(B_0B'^{-1}) = \mathrm{Tr}(B'^{-1}B_0) = \mathrm{Tr}(B''^{-1})$).
Le 9.a assure alors que $Y = \frac{1}{n}\mathrm{Tr}(Y)I_n$.
Or $\mathrm{Tr}(Y) = \sum_{B\in G} \mathrm{Tr}(B^{-1})\ \mathrm{Tr}(B) = |G|\times \dim(\mathcal{A}^{\tilde{G}})$ (d'après 13.) $= |G|$ (d'après 11.).
Finalement : $Y = \frac{|G|}{n}I_n$.

16. (a) On a remarqué au 8. que les valeurs propres de B étaient des racines $|G|$-ièmes de l'unité : elles appartiennent donc à l'ensemble $\{\zeta^k, k \in \{1, ...|G| - 1\}\}$. En diagonalisant (cf 1. ; trigonaliser suffit d'ailleurs) B, on obtient $\mathrm{Tr}(B) = \sum_{0\le k\le|G|-1} a_k\zeta^k$
$\in \mathbb{Z}_{\mathbb{G}}$ (où $a_k \in \mathbb{N}$ est la multiplicité, éventuellement nulle, de ζ^k dans le polynôme caractéristique de B).
La définition de $Y = \sum_{B\in G} \mathrm{Tr}(B^{-1})B$ implique immédiatement que $Y \in \mathbb{Z}_{\mathbb{G}}[\mathbb{G}]$ (G étant un groupe, $\forall B \in G, B^{-1} \in G$ et $\mathrm{Tr}(B^{-1}) \in \mathbb{Z}_{\mathbb{G}}$).

(b) Notons $H = \{C_k, 1 \le k \le |G|^2\}$. Il est immédiat que H est un sous-groupe de $GL_n(\mathbb{C})$ (car G l'est, et l'ensemble des racines $|G|$-ièmes de l'unité est un sous-groupe de $(\mathbb{C}^*, \times)$). Par définition, $\mathbb{Z}_{\mathbb{G}}[\mathbb{G}]$ est l'ensemble des combinaisons linéaires à coefficients dans $\mathbb{Z}$ des éléments de H ; il en résulte que $\mathbb{Z}_{\mathbb{G}}[\mathbb{G}]$ est stable par produit (écrire $\sum_{1\le k\le|G|^2} \alpha_kC_k \times \sum_{1\le l\le|G|^2} \beta_lC_l = \sum_{1\le k,l\le|G|^2} \alpha_k\beta_lC_kC_l \in \mathbb{Z}_{\mathbb{G}}[\mathbb{G}]$ par stabilité de H par produit).
Ainsi, pour $1 \le k \le |G|^2, YC_k \in \mathbb{Z}_{\mathbb{G}}[\mathbb{G}]$ et $\exists(a_{l,k})_{1\le k,l\le|G|^2} \in \mathbb{Z}^{|\mathbb{G}|^2}$ tels que
$YC_k = \sum_{1\le l\le|G|^2} a_{l,k}C_l$.

(c) Soit, pour $(i,l) \in \{1,...,n\} \times \{1,...,|G|^2\}, \mathcal{C}_{i,l}$ la i-ème colonne de C_l ; le 16.b (aidé du 15.b) fournit :

$$\forall (i,k) \in \{1,...,n\} \times \{1,...,|G|^2\}, \frac{|G|}{n}\mathcal{C}_{i,k} = \sum_{1 \leq l \leq |G|^2} a_{l,k}\mathcal{C}_{i,l}.$$

D'où, en formant $D_i = (\mathcal{C}_{i,1}...\mathcal{C}_{i,|G|^2}) \in \mathcal{M}_{n,|G|^2}(\mathbb{C})$: $\forall \mathbb{i} \in \{\mathbb{1},...,\mathbb{n}\}, \mathbb{D}_{\mathbb{i}}\mathbb{R} = \mathbb{0}$ (produit par blocs) et $\exists i \in \{1,...,n\}, D_i \neq 0$ (car les éléments de G sont non nuls) donc R n'est pas inversible.

(d) Ce qui précède signifie exactement que $\frac{|G|}{n}$ est racine du polynôme caractéristique de A, qui est un polynôme de degré $|G|^2$, de coefficient dominant 1, et à coefficients dans $\mathbb{Z}$ car les $a_{i,j}$ sont des entiers relatifs.
Soit alors $Q = b_0 + ... + b_{|G|^2-1}X^{|G|^2-1} + X^{|G|^2} \in \mathbb{Z}[\mathbb{X}]$ ce polynôme et réduisons $\frac{|G|}{n} = \frac{p}{q}$ avec $(p,q) \in \mathbb{N} \times \mathbb{N}^*, \mathbb{p} \wedge \mathbb{q} = \mathbb{1}$.
$Q(\frac{p}{q}) = 0$ implique $b_0 q^{|G|^2} + ... + b_{|G|^2-1}qp^{|G|^2-1} = -p^{|G|^2}$, d'où $q|p^{|G|^2}$. Comme $p \wedge q = 1$, nécessairement $q = 1$ et n divise $|G|$.
(On vient de prouver que la dimension d'une représentation irréductible d'un groupe divise le cardinal du groupe.)

V - Une caractérisation de D_n, n impair

17. (a) $< .,. >_0$ est clairement linéaire par rapport à la première variable, hermitien positif (car $< .,. >$ l'est sur $\mathbb{C}^2$). De plus, soit $v \in \mathbb{C}^2$: si $< v, v >_0 = 0$, alors
$\forall B \in G, < Bv, Bv >= 0$; en particulier, comme $I_2 \in G : < v, v >= 0$ et $v = 0$. $< .,. >_0$ est donc bien un produit scalaire hermitien sur $\mathbb{C}^2$.
Par ailleurs, pour $v, w \in \mathbb{C}^2$ et $B_0 \in G$, on a :
$< B_0 v, B_0 w >_0 = \frac{1}{|G|}\sum_{B \in G} < BB_0 v, BB_0 w >=< v, w >_0$ puisque $B \to BB_0$ est une bijection de G dans G (cf. 7.b).
On a ainsi construit un produit scalaire sur $\mathbb{C}^2$ pour lequel les éléments de G sont des isométries.

(b) Si $\mathbb{C}^2$ n'est pas irréductible pour G, il existe un sous-espace F de $\mathbb{C}^2$ stable par G et différent de $\{0\}$ et E ; F est donc de dimension 1, et il existe $e_1 \in F$ tel que $< e_1, e_1 >_0 = 1$.
Or, comme l'orthogonal d'un sous-espace stable par une isométrie est encore stable par cette isométrie, l'orthogonal H de F pour $< .,. >_0$ est également stable par G (puisque les éléments de G sont des isométries pour $< .,. >_0$).
Soit donc $e_2 \in H$ tel que $< e_2, e_2 >_0 = 1$; $\mathcal{B} = (e_1, e_2)$ est une base orthonormée de $\mathbb{C}^2$ pour $< .,. >_0$, et la stabilité de $F = \mathbb{C}.\mathbb{e}_{\mathbb{1}}$ et $H = \mathbb{C}.\mathbb{e}_{\mathbb{2}}$ par tous les éléments de G implique que e_1 et e_2 sont des vecteurs propres communs à tous les éléments de G.
Finalement, $\mathcal{B}$ diagonalise toutes les matrices de G : cela signifie qu'il existe $P \in GL_2(\mathbb{C})$ telle que $\forall B \in G, P^{-1}BP$ est diagonale. Les $\{P^{-1}BP, B \in G\}$ commutent, donc aussi les matrices de G : C.Q.F.D.

18. (a) Soit $B \in SL_2(\mathbb{C}), \mathbb{B}^2 = \mathbb{I}_2$. B est diagonalisable, de valeurs propres appartenant à $\{-1, +1\}$ (car $X^2 - 1$ annule B). Si -1 et 1 étaient tous deux valeurs propres de B, en diagonalisant on obtiendrait $\det B = -1$. Nécessairement $Sp(B) = \{-1\}$ ou $\{1\}$, et (B étant diagonalisable) $B \in \{I_2, -I_2\}$. Réciproquement, $-I_2$ et I_2 appartiennent bien à $SL_2(\mathbb{C})$ et ont pour carré I_2.

(b) Si G n'est pas commutatif, d'après 11.b $\mathbb{C}^2$ est irréductible pour G, et 10.d impose 2 divise $|G|$.
En outre, d'après le résultat admis en préambule, il existe $B \in G \backslash \{I_2\}, B^2 = I_2$. Comme $G \subset SL_2(\mathbb{C})$, le 12.a s'applique et $B = -I_2 \in G$.

19. (a) Si G_0 n'était pas commutatif, le 18.b impliquerait $-I_2 \in G_0 \subset G$, ce qui n'est pas par hypothèse. G_0 est donc commutatif.
La question 6. garantit alors l'existence de $P \in GL_2(\mathbb{C})$ telle que $\forall B \in G_0, PBP^{-1}$ est diagonale.
Comme $G_0 \subset SL_2(\mathbb{C}), \forall \mathbb{B} \in \mathbb{G}_{\mathbb{0}}, \mathbb{P}\mathbb{B}\mathbb{P}^{-\mathbb{1}} \in \mathbb{SL}_{\mathbb{2}}(\mathbb{C})$ et PBP^{-1} est de la forme $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \lambda \in \mathbb{C}^*$.
En notant $\Gamma_0 = \{PBP^{-1}, B \in G_0\}$, on obtient le résultat requis.

(b) L'application de $(\Gamma_0, \times)$ dans $(\mathbb{C}^*, \times)$ qui à $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ associe λ est assez évidemment un morphisme injectif de groupes. Son image Γ_1 est un sous-groupe fini de $(\mathbb{C}^*, \times)$ isomorphe à Γ_0. Notons $m = |\Gamma_1|$; le théorème de Lagrange (premier résultat admis dans le préambule) implique que $\forall \lambda \in \Gamma_1, \lambda^m = 1$. Donc Γ_1 est inclus dans le groupe U_m des racines m-ièmes de l'unité. Comme $|U_m| = m$, il s'ensuit que $\Gamma_1 = U_m$, et $\Gamma_0 = \{\begin{pmatrix} c^k & 0 \\ 0 & c^{-k} \end{pmatrix}, c = e^{\frac{2i\pi}{m}}, 0 \leq k \leq m-1\}$.

(c) Si $G_0 = \{I_2\}$, alors $\det : G \to \mathbb{C}^*$ est un morphisme injectif de groupes (par définition, $G_0 = G \bigcap SL_2(\mathbb{C})$ est le noyau de ce morphisme) ; G est alors isomorphe à $\det(G)$, sous-groupe fini de $(\mathbb{C}^*, \times)$. G est donc commutatif, et même, d'après la question précédente, cyclique (ce qui est mieux).

20. (a) L'existence de B_0 résulte de la non-commutativité de G (si toutes les matrices de G étaient diagonales, elles commuteraient deux à deux). Il vient : $B_0 C B_0^{-1} \in G$ (par stabilité), et $\det(B_0 C B_0^{-1}) = \det(C) = 1$, donc $B_0 C B_0^{-1} \in G_0 = Z_m$.
Observons ici que $-I_2$ n'appartient pas à Z_m (car G ne contient pas d'autre homothétie que l'identité) et $Z_m \neq \{I_2\}$ (d'après 13.c, G étant supposé non commutatif), donc m est impair et ≥ 3 : ainsi $c \neq 1$ et $c \neq -1$, donc $c \neq c^{-1}$.
Notons $B_0 = \begin{pmatrix} d & e \\ f & g \end{pmatrix}$; $B_0 C B_0^{-1} \in G_0 = Z_m$, donc $\exists 0 \leq k \leq m-1, B_0 C B_0^{-1} = \begin{pmatrix} c^k & 0 \\ 0 & c^{-k} \end{pmatrix}$, c'est-à-dire :
$\begin{pmatrix} d & e \\ f & g \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix} = \begin{pmatrix} c^k & 0 \\ 0 & c^{-k} \end{pmatrix} \begin{pmatrix} d & e \\ f & g \end{pmatrix}$, d'où $dc = dc^k, fc = fc^{-k}, ec^{-1} = ec^k, gc^{-1} = gc^{-k}$.
On en déduit que si $d \neq 0$ ou $g \neq 0$, alors $c^{k-1} = 1$, et, comme $0 \leq k \leq m-1$: $k = 1$. Cela implique $fc = fc^{-1}$ et $ec = ec^{-1}$; or $c \neq c^{-1}$ d'où $f = e = 0$ et B_0 est diagonale, ce qu'on a exclu. Nécessairement, $d = g = 0$ et B_0 possède bien la forme requise.
(Notons d'ailleurs que, B_0 étant inversible et puisque $\det(B_0) = -ef$: e et f sont $\neq 0$, donc $c^{k+1} = 1$ et $k = m-1$.)

(b) $B_0^2 = bb' I_2 \in G$. Par hypothèse sur G, $B_0^2 = I_2$ et $b' = b^{-1}$.

(c) Soit $\mathcal{B}_0 = (\epsilon_1, \epsilon_2)$ la base canonique de $\mathbb{C}^2$, et $u \in \mathcal{L}(\mathbb{C}^2)$ l'endomorphisme de $\mathbb{C}^2$ qui a pour matrice B_0 dans $\mathcal{B}_0$; alors $u(\epsilon_1) = b^{-1}\epsilon_2$ et $u(\epsilon_2) = b\epsilon_1$, donc $u(b\epsilon_1) = \epsilon_2$ et $u(-\epsilon_2) = -b\epsilon_1$: $Q = \begin{pmatrix} \frac{1}{b} & 0 \\ 0 & -1 \end{pmatrix}$ convient.

21. (a) Si $B = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$, alors $BB_0 = \begin{pmatrix} 0 & \alpha b \\ \frac{\beta}{b} & 0 \end{pmatrix}$ est une matrice de G non diagonale ; d'après 14.b, $\frac{\beta}{b} = \frac{1}{\alpha b}$, d'où aussi $\alpha\beta = 1$ et $B \in G_0 = Z_m$.

(b) Notons, une fois pour toutes, $R_k = \begin{pmatrix} c^k & 0 \\ 0 & c^{-k} \end{pmatrix}$ pour $0 \leq k \leq m-1$, et soit $\phi : G \to GL_2(\mathbb{C})$ défini par : $\forall B \in G\ \phi(B) = QBQ^{-1}$.
— ϕ est un morphisme de groupes injectif, donc induit un isomorphisme de G sur son image.
— Comme Q est diagonale, elle commute avec les éléments de Z_m, et $\forall k \in \{0, ..., m-1\}, \phi(R_k) = R_k$.
— Si $B \in G$ n'est pas diagonale, elle est d'après 14.b de la forme $B = \begin{pmatrix} 0 & d \\ d^{-1} & 0 \end{pmatrix}$, et $BB_0^{-1} = BB_0 = \begin{pmatrix} \frac{d}{b} & 0 \\ 0 & \frac{b}{d} \end{pmatrix}$ est une matrice diagonale de G, donc $\exists k \in \{0, ..., m-1\}, BB_0^{-1} = R_k$ (d'où $d = c^k b$).
Réciproquement, par stabilité, $\forall k \in \{0, ..., m-1\}, R_k B_0 \in G$: cela (et ce qui précède) montre que G est la réunion disjointe de Z_m et de $Z_m B_0$.
— Enfin, un calcul élémentaire établit que $\forall k \in \{0, ..., m-1\} \phi(R_k B_0) = \begin{pmatrix} 0 & -c^k \\ -c^{-k} & 0 \end{pmatrix}$. On peut conclure : l'image de ϕ est précisément D_m, et ϕ induit un isomorphisme de G sur D_m.

22. (a) D'après 6., les matrices de G sont co-diagonalisables : $\exists P \in GL_2(\mathbb{C}), \forall \mathbb{B} \in \mathbb{G}, \mathbb{P}^{-1}\mathbb{B}\mathbb{P}$ est diagonale. Si l'on note $P^{-1}BP = \begin{pmatrix} \chi_1(B) & 0 \\ 0 & \chi_2(B) \end{pmatrix}$, les règles de calcul sur les matrices diagonales montrent que χ_1 et χ_2 sont deux morphismes de groupes de $G \to \mathbb{C}^*$.

(b) On a remarqué au 8. que les valeurs propres des éléments de G étaient des racines $|G|$-ièmes de l'unité ; il en découle que χ_1 et χ_2, donc aussi $\chi : B \to \chi_1(B)\chi_2(B)^{-1}$, sont des morphismes de G dans $U_{|G|}$. χ est de plus injectif, car si $\chi_1(B) = \chi_2(B)$ alors $P^{-1}BP$ est une homothétie, donc aussi B et par hypothèse sur $G : B = I_2$. Comme enfin $|G| = |U_{|G|}|$, il s'agit bien d'un isomorphisme (bijectif, car application injective d'un ensemble fini dans un autre de même cardinal).

(c) L'énoncé est encore une fois imprécis : le choix de p et q n'est pas arbitraire, contrairement à ce qu'il laisse entendre.

— $P^{-1}GP$ est un groupe de matrices (diagonales) isomorphe à G, donc à $U_{|G|}$: ce dernier groupe étant cyclique, soit $\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$ un générateur (pour le produit matriciel) de $P^{-1}GP = \{\begin{pmatrix} c^k & 0 \\ 0 & d^k \end{pmatrix}, 0 \leq k \leq |G|-1\}$.

— Le résultat admis en préambule implique que $\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}^{|G|} = I_2$, d'où c et $d \in U_{|G|}$: $\exists (p,q) \in \{0,...,|G|-1\}^2, c = e^{\frac{2ip\pi}{|G|}}, d = e^{\frac{2iq\pi}{|G|}}$.
Alors $\chi(G) = \{e^{\frac{2ik(p-q)\pi}{|G|}}, 0 \leq k \leq |G|-1\} = U_{|G|}$.

— On en déduit que $\frac{c}{d} = e^{\frac{2i(p-q)\pi}{|G|}}$ est une racine primitive $|G|$-ième de l'unité, c'est-à-dire qu'elle engendre (multiplicativement) $U_{|G|}$.
Nécessairement $p - q \wedge |G| = 1$ (raisonner par isomorphisme avec $\mathbb{Z}/|G|\mathbb{Z}$).

— Nous pouvons conclure : G est le groupe des matrices de la forme $P\begin{pmatrix} c^k & 0 \\ 0 & d^k \end{pmatrix}P^{-1}, 0 \leq k \leq |G|-1$.

23. Si G est commutatif, on est dans le cas précédent ; on vérifie d'ailleurs aisément que pour tout couple d'entiers (p,q) tels que $p-q\wedge|G| = 1$ et pour toute matrice $P \in GL_2(\mathbb{C})$, l'ensemble $\{P\begin{pmatrix} c^k & 0 \\ 0 & d^k \end{pmatrix}P^{-1}, 0 \leq k \leq |G|-1\}$ est un sous-groupe fini (et même cyclique) de $GL_2(\mathbb{C})$ ne contenant pas d'autre homothétie que I_2.

Si au contraire G n'est pas commutatif, les questions 19., 20. et 21. montrent que G est conjugué à D_m, où $m = \frac{|G|}{2}$ (c'est-à-dire qu'il existe $P \in GL_2(_C)$ tel que $G = PD_mP^{-1}$) ; réciproquement les conjugués de D_m sont bien des sous-groupes finis non commutatifs de $GL_2(\mathbb{C})$ ne contenant pas d'autre homothétie que I_2.

24. Si $\mathcal{G} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ était isomorphe à un sous-groupe G de $GL_2(\mathbb{C})$, alors d'après 6. tous les élements de G seraient co-diagonalisables, et tous les élements de $\mathcal{G}$ étant d'ordre 1 ou 2, les seules valeurs propres possibles sont -1 et 1 : on obtient dans une base de co-diagonalisation au plus 4 matrices distinctes : $I_2, -I_2, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, ce qui n'est pas assez. (Cette question ne requiert guère que le 6. pour être traitée...)