

CORRIGÉ X-2010, MP, SECONDE ÉPREUVE

I - Sous-groupes finis de $GL(E)$

- (1) Pour $g \in G$, on a, d'après le résultat rappelé (Théorème de Lagrange, qui n'est d'ailleurs pas au programme) : $g^{|G|} = id_E$. Le polynôme $X^{|G|} - 1$, scindé à racines simples sur \mathbb{C} , annule g qui est donc diagonalisable.

Notons d'ailleurs que les valeurs propres de g sont des racines $|G|$ -ièmes de l'unité. (Je noterai par la suite U_m le groupe des racines m -ièmes de l'unité.)

Si à présent 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 un peu 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.

II - Isométries du triangle

- (2) (a) Un élément de \tilde{D}_3 est une isométrie qui fixe le centre de gravité (isobarycentre) O du triangle ABC : 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 .

Comme réciproquement ces 6 isométries laissent invariant le triangle, on en déduit que \tilde{D}_3 est de cardinal 6.

Remarque : on vérifie aisément que \tilde{D}_3 est isomorphe au groupe symétrique σ_3 .

- (b) 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 $GL_2(\mathbb{C})$, que je noterai \mathcal{G} , isomorphe à \tilde{D}_3 .

(c) 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 $\text{GL}_2(\mathbb{C})$:

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} j & 0 \\ 0 & j^{-1} \end{pmatrix}, \begin{pmatrix} j^{-1} & 0 \\ 0 & j \end{pmatrix}, \begin{pmatrix} 0 & -j \\ -j^{-1} & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -j^{-1} \\ -j & 0 \end{pmatrix} \right\}.$$

On reconnaît D_3 , qui est bien isomorphe à \tilde{D}_3 .

Remarque : généralement, D_n est isomorphe au groupe *diédral* des isométries planes laissant invariant un polygone régulier à n côtés : on a ici "représenté" le groupe diédral dans $\text{GL}_2(\mathbb{C})$.

III - Lemme de Schur

(3) • Pour $B \in G$ fixée, $i(B)$ est un endomorphisme de \mathcal{A} (car $\forall (\lambda, \mu, M, N) \in \mathbb{C}^2 \times \mathcal{A}^2, B(\lambda M + \mu N)B^{-1} = \lambda BMB^{-1} + \mu BNB^{-1}$) ; de plus, pour $(B, B', M) \in G^2 \times \mathcal{A}$, on a $i(BB')(M) = BB'M(BB')^{-1} = BB'MB'^{-1}B^{-1} = [i(B) \circ i(B')](M)$ (identité que je note **(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 $GL(\mathcal{A})$.

• Par ailleurs, $B = (b_{i,j}) \in \text{Ker}(i)$ si et seulement si $\forall M \in \mathcal{A}, BM = MB$. Si c'est le cas, soit $(i, j) \in \{1, \dots, n\}^2$ 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). La réciproque étant évidente, on en déduit que $\text{Ker}(i)$ est exactement l'ensemble des matrices d'homothéties de G , et i est injectif si et seulement si I_n est la seule homothétie de G .

(4) **N.B. : Pour des raisons typographiques, je noterai G' au lieu de \tilde{G} .**

Il faut naturellement rectifier l'erreur de notation de l'énoncé, et rétablir : $M \in \mathcal{A}^{G'}$ si et seulement si $i(B)(M) = M$ pour tout B dans G (et non dans \tilde{G}).

Par définition, $M \in \mathcal{A}^{G'}$ si et seulement si M commute avec tous les éléments de G . On sait d'ailleurs que lorsque deux endomorphismes (il s'agit ici en réalité de matrices, que le texte identifie aux endomorphismes de \mathbb{C}^n canoniquement associés à ces matrices) commutent, le noyau et l'image de l'un sont stables par l'autre, ce qui garantit le résultat.

(5) • De l'irréductibilité de E pour G et de la stabilité de $\text{Ker}(M)$ par G , découle l'alternative : ou bien $\text{Ker}(M) = \{0\}$, ou bien $\text{Ker}(M) = E$. Dans le premier cas, M est inversible ; elle est nulle dans le second.

• Observons ici que $\mathcal{A}^{G'}$ est un sous-espace de \mathcal{A} (c'est le "commutant" de G) contenant I_n , donc aussi $\mathbb{C}I_n$. Pour $M \in \mathcal{A}^{G'}$, 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) ; $M - \lambda I_n \in \mathcal{A}^{G'}$ n'est pas inversible (puisque λ est valeur propre de M), donc $M - \lambda I_n = 0$. Ceci prouve que $\mathcal{A}^{G'} = \mathbb{C}I_n$, et qu'il s'agit d'un sous-espace de \mathcal{A} de dimension 1.

(6) Avec les notations introduites dans la question 3., les $\{E_{i,j}, (i, j) \in \{1, \dots, n\}^2\}$ forment une base (canonique) de \mathcal{A} . Pour $(i, j) \in \{1, \dots, n\}^2$, 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 $\text{Tr}(\Phi) = \sum_{(i,j) \in \{1, \dots, n\}^2} m_{i,i} n_{j,j} = \sum_{1 \leq i \leq n} m_{i,i} \times \sum_{1 \leq j \leq n} n_{j,j} = \text{Tr}(M) \text{Tr}(N)$.

(Φ est l'endomorphisme associé au *produit tensoriel* de M par N .)

(7) (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 invariants, i.e. $\text{Ker}(P - I_n)$. 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 $\text{Im}(P) = \text{Ker}(P - I_n) = E^G$.

• Comme P est un projecteur, son rang est égal à sa trace, d'où $\text{rg}(P) = \dim(E^G) = \text{Tr}(P) = \frac{1}{|G|} \sum_{B \in G} \text{Tr}(B)$.

(8) • On peut généralement appliquer le 7b. à \mathcal{A} à la place de E et G' à celle de G , et on obtient : $\dim(\mathcal{A}^{G'}) = \frac{1}{|G'|} \sum_{B' \in G'} \text{Tr}(B')$ (formule notée **(2)**).

• Le cas où i est injectif ne présente pas de difficulté, puisqu'alors i induit un isomorphisme de G sur G' (en particulier, $|G| = |G'|$) ; **(2)** s'écrit :

$$\dim(\mathcal{A}^{G'}) = \frac{1}{|G|} \sum_{B \in G} \text{Tr}(i(B)) = \frac{1}{|G|} \sum_{B \in G} \text{Tr}(B) \text{Tr}(B^{-1}) \text{ d'après 6.}$$

• 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 $i(B_1 B_2^{-1}) = id_{\mathcal{A}}$ si et seulement si $B_1 B_2^{-1} \in \text{Ker}(i)$ (cela équivaut aussi, d'après 3., à : $\exists \lambda \in \mathbb{C}, B_1 = \lambda B_2$, et $\lambda I_n = B_1 B_2^{-1} \in G$).

• Ce qui précède montre que toutes les classes d'équivalence pour \mathcal{R} ont même cardinal : celui de $\text{Ker}(i)$. Cela revient à dire que tous les éléments de G' ont $|\text{Ker}(i)|$ antécédents par i . D'où, en regroupant les éléments de G selon leur classe : $|G| = |\text{Ker}(i)| \times |G'|$.

• Enfin, si $B_1 \mathcal{R} B_2$, alors $\text{Tr}(i(B_1)) = \text{Tr}(i(B_2)) = \text{Tr}(B_1) \text{Tr}(B_1^{-1}) = \text{Tr}(B_2) \text{Tr}(B_2^{-1})$. Il s'ensuit, toujours en regroupant les éléments de G selon leur classe, et puisque toutes les classes ont $|\text{Ker}(i)|$ éléments, que

$$\frac{1}{|G|} \sum_{B \in G} \text{Tr}(B) \text{Tr}(B^{-1}) = \frac{1}{|G'|} \sum_{B' \in G'} \text{Tr}(B') = \dim(\mathcal{A}^{G'}) \text{ (d'après (2)) : C.Q.F.D.}$$

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 $G' : i'(\overline{B}) = i(B)$. i' devient injectif, et on peut lui appliquer le résultat correspondant. Mais cela nous écarte un peu du programme officiel...

(9) (a) Si X commute avec toutes les matrices de G , 5. assure que c'est une homothétie. Si $X = \lambda I_n$, il vient : $\text{Tr}(X) = n\lambda$, d'où $X = \frac{1}{n} \text{Tr}(X) I_n$.

(b) Soit $B_0 \in G$; les applications $B \rightarrow BB_0$ et $B' \rightarrow B_0^{-1} B'$ sont des bijections de G dans G (cf. 7.a). Il vient :

$$Y B_0 = \sum_{B \in G} \text{Tr}(B^{-1}) B B_0 = \sum_{B' \in G} \text{Tr}(B_0 B'^{-1}) B_0 B_0^{-1} B'$$

(en réindexant, et posant $B' = B B_0$)

$$= B_0 \sum_{B'' \in G} \text{Tr}(B''^{-1}) B'' = B_0 Y$$

(posant $B'' = B_0^{-1} B'$, et tenant compte de $\text{Tr}(B_0 B'^{-1}) = \text{Tr}(B'^{-1} B_0) = \text{Tr}(B''^{-1})$).

Le 9.a assure alors que $Y = \frac{1}{n} \text{Tr}(Y) I_n$.

Or $\text{Tr}(Y) = \sum_{B \in G} \text{Tr}(B^{-1}) \text{Tr}(B) = |G| \times \dim(\mathcal{A}^{G'})$ (d'après 8.) = $|G|$ (d'après 5.).

Finalemment : $Y = \frac{|G|}{n} I_n$.

- (10) (a) On a remarqué au 1. que les valeurs propres de B étaient des racines $|G|$ -ièmes de l'unité : elles appartiennent donc à l'ensemble $\{\zeta^k, k \in \{1, \dots, |G| - 1\}\}$. En diagonalisant (cf 1. ; trigonaliser suffit d'ailleurs) B , on obtient $\text{Tr}(B) = \sum_{0 \leq k \leq |G|-1} a_k \zeta^k \in \mathbb{Z}_G$ (où $a_k \in \mathbb{N}$ est la multiplicité, éventuellement nulle, de ζ^k dans le polynôme caractéristique de B).

La définition de $Y = \sum_{B \in G} \text{Tr}(B^{-1})B$ implique immédiatement que $Y \in \mathbb{Z}_G[G]$ (G étant un groupe, $\forall B \in G, B^{-1} \in G$ et $\text{Tr}(B^{-1}) \in \mathbb{Z}_G$).

- (b) Notons $H = \{C_k, 1 \leq k \leq |G|^2\}$. 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, $\mathbb{Z}_G[G]$ est l'ensemble des combinaisons linéaires à coefficients dans \mathbb{Z} des éléments de H ; il en résulte que $\mathbb{Z}_G[G]$ est stable par produit (écrire $\sum_{1 \leq k \leq |G|^2} \alpha_k C_k \times \sum_{1 \leq l \leq |G|^2} \beta_l C_l = \sum_{1 \leq k, l \leq |G|^2} \alpha_k \beta_l C_k C_l \in \mathbb{Z}_G[G]$ par stabilité de H par produit).

Ainsi, pour $1 \leq k \leq |G|^2, Y C_k \in \mathbb{Z}_G[G]$ et $\exists (a_{l,k})_{1 \leq k, l \leq |G|^2} \in \mathbb{Z}^{|G|^2}$ tels que $Y C_k = \sum_{1 \leq l \leq |G|^2} a_{l,k} C_l$.

Remarque : la quantification de l'énoncé est incorrecte : les coefficients $a_{i,j}$ ne dépendent en réalité pas de k . Il faut rétablir : "Démontrer qu'on peut trouver des coefficients $(a_{i,j})_{1 \leq i, j \leq |G|^2}$ dans \mathbb{Z} tels que pour tous $1 \leq k \leq |G|^2$..."

Du reste, les éléments de H n'ayant aucune raison de former une famille libre, les $a_{i,j}$ ne sont *a priori* pas uniques.

- (c) Soit, pour $(i, l) \in \{1, \dots, n\} \times \{1, \dots, |G|^2\}, C_{i,l}$ la i -ème colonne de C_l ; le 10.b (aidé du 9.b) fournit :

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

D'où, en formant $D_i = (C_{i,1} \dots C_{i,|G|^2}) \in \mathcal{M}_{n,|G|^2}(\mathbb{C}) : \forall i \in \{1, \dots, n\}, D_i R = 0$ (produit par blocs) et $\exists i \in \{1, \dots, n\}, D_i \neq 0$ (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 $Q = b_0 + \dots + b_{|G|^2-1} X^{|G|^2-1} + X^{|G|^2} \in \mathbb{Z}[X]$ ce polynôme et réduisons $\frac{|G|}{n} = \frac{p}{q}$ avec $(p, q) \in \mathbb{N} \times \mathbb{N}^*, p \wedge q = 1$.

$Q(\frac{p}{q}) = 0$ implique $b_0 q^{|G|^2} + \dots + b_{|G|^2-1} q p^{|G|^2-1} = -p^{|G|^2}$, 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.)

IV - Une caractérisation de D_n, n impair

- (11) (a) $\langle \dots \rangle_0$ est clairement linéaire par rapport à la première variable, hermitien positif (car $\langle \dots \rangle$ l'est sur \mathbb{C}^2). De plus, soit $v \in \mathbb{C}^2$: si $\langle v, v \rangle_0 = 0$, alors

$\forall B \in G, \langle Bv, Bv \rangle = 0$; en particulier, comme $I_2 \in G : \langle v, v \rangle = 0$ et $v = 0$.

$\langle \dots \rangle_0$ 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 :

$\langle B_0v, B_0w \rangle_0 = \frac{1}{|G|} \sum_{B \in G} \langle BB_0v, BB_0w \rangle = \langle v, w \rangle_0$ puisque $B \rightarrow BB_0$ 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 $\langle e_1, e_1 \rangle_0 = 1$.

Or, comme l'orthogonal d'un sous-espace stable par une isométrie est encore stable par cette isométrie, l'orthogonal H de F pour $\langle \cdot, \cdot \rangle_0$ est également stable par G (puisque les éléments de G sont des isométries pour $\langle \cdot, \cdot \rangle_0$).

Soit donc $e_2 \in H$ tel que $\langle e_2, e_2 \rangle_0 = 1$; $\mathcal{B} = (e_1, e_2)$ est une base orthonormée de \mathbb{C}^2 pour $\langle \cdot, \cdot \rangle_0$, et la stabilité de $F = \mathbb{C}.e_1$ et $H = \mathbb{C}.e_2$ 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.

- (12) (a) Soit $B \in SL_2(\mathbb{C}), B^2 = I_2$. 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 $B \in G \setminus \{I_2\}, B^2 = I_2$. Comme $G \subset SL_2(\mathbb{C})$, le 12.a s'applique et $B = -I_2 \in G$.

Remarque : le résultat admis s'appelle le théorème de Cauchy. Dans le cas particulier $p = 2$, on peut le démontrer élémentairement ainsi : on obtient une partition de G en regroupant chaque élément de G avec son inverse. Les parties de cette partition sont de cardinal 1 si l'élément est son propre inverse, 2 sinon. Comme $|G|$ est pair, il existe nécessairement $g \in G \setminus \{1_G\}, g = g^{-1}$, soit $g^2 = 1_G$.

- (13) (a) Si G_0 n'était pas commutatif, le 12.b impliquerait $-I_2 \in G_0 \subset G$, ce qui n'est pas par hypothèse. G_0 est donc commutatif.

La question 1. garantit alors l'existence de $P \in GL_2(\mathbb{C})$ telle que $\forall B \in G_0, PBP^{-1}$ est diagonale. Comme $G_0 \subset SL_2(\mathbb{C}), \forall B \in G_0, PBP^{-1} \in SL_2(\mathbb{C})$ 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 (Γ_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 $\Gamma_0 = \left\{ \begin{pmatrix} c^k & 0 \\ 0 & c^{-k} \end{pmatrix}, c = e^{\frac{2i\pi}{m}}, 0 \leq k \leq m-1 \right\}$.

- (c) Si $G_0 = \{I_2\}$, alors $\det : G \rightarrow \mathbb{C}^*$ est un morphisme injectif de groupes (par définition, $G_0 = G \cap SL_2(\mathbb{C})$ 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).

- (14) (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 : $B_0CB_0^{-1} \in G$ (par stabilité), et $\det(B_0CB_0^{-1}) = \det(C) = 1$, donc $B_0CB_0^{-1} \in G_0 = Z_m$.

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 $B_0 = \begin{pmatrix} d & e \\ f & g \end{pmatrix}$; $B_0CB_0^{-1} \in G_0 = Z_m$, donc $\exists 0 \leq k \leq m-1$, $B_0CB_0^{-1} =$

$\begin{pmatrix} c^k & 0 \\ 0 & c^{-k} \end{pmatrix}$, 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.

- (15) (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 $\phi : G \rightarrow GL_2(\mathbb{C})$ 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 $\forall k \in \{0, \dots, m-1\}$, $\phi(R_k) = R_k$.

- 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 $\exists k \in$

$\{0, \dots, m-1\}$, $BB_0^{-1} = R_k$ (d'où $d = c^k b$). Réciproquement, par stabilité, $\forall k \in \{0, \dots, m-1\}$, $R_k B_0 \in G$: 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 $\forall k \in \{0, \dots, m-1\} \phi(R_k B_0) = \begin{pmatrix} 0 & -c^k \\ -c^{-k} & 0 \end{pmatrix}$. On peut conclure : l'image de ϕ est précisément D_m , et ϕ induit un isomorphisme de G sur D_m .

- (16) (a) D'après 1., les matrices de G sont co-diagonalisables : $\exists P \in GL_2(\mathbb{C}), \forall B \in G, P^{-1}BP$ 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 $G \rightarrow \mathbb{C}^*$.
- (b) On a remarqué au 1. 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 $\chi : B \rightarrow \chi_1(B)\chi_2(B)^{-1}$, 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 $P^{-1}GP = \left\{ \begin{pmatrix} c^k & 0 \\ 0 & d^k \end{pmatrix}, 0 \leq k \leq |G| - 1 \right\}$.
 - Le résultat admis en préambule implique que $\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}^{|G|} = I_2$, d'où c et $d \in U_{|G|} : \exists (p, q) \in \{0, \dots, |G| - 1\}^2, c = e^{\frac{2ip\pi}{|G|}}, d = e^{\frac{2iq\pi}{|G|}}$.
Alors $\chi(G) = \left\{ e^{\frac{2ik(p-q)\pi}{|G|}}, 0 \leq k \leq |G| - 1 \right\} = U_{|G|}$.
 - 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 $P \begin{pmatrix} c^k & 0 \\ 0 & d^k \end{pmatrix} P^{-1}, 0 \leq k \leq |G| - 1$.

- (17) 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 $\left\{ P \begin{pmatrix} c^k & 0 \\ 0 & d^k \end{pmatrix} P^{-1}, 0 \leq k \leq |G| - 1 \right\}$ 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 13., 14. et 15. montrent que G est conjugué à D_m , où $m = \frac{|G|}{2}$ (c'est-à-dire qu'il existe $P \in GL_2(\mathbb{C})$ 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 .

- (18) 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 1. tous les éléments de G seraient co-diagonalisables, et tous les éléments 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 1. pour être traitée...)

[Pour toute remarque ou suggestion concernant ce corrigé, contacter denis.favennec@prepas.org.]