Aix–Marseille Université 2019-2020

Mathématiques –Master 1

ALGÈBRE-GÉOMÉTRIE

Exercice 1

1. On munit G de la multiplication matricielle.
   - Il s'agit bien d'un produit interne car le produit de deux matrices inversibles est inversible.
   - Il est associatif car le produit matriciel est associatif.
   - Il possède un élément neutre, à savoir la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
   - Par définition des matrices inversibles, tout élément de G admet bien un inverse.

   Cela munit donc bien G d'une structure de groupe.

3. On a $|E| = |K^2| = |K|^2 = 2^2 = 4$.

2. Une matrice dans $\mathcal{M}_2(K)$ est inversible ssi ses lignes sont linéairement indépendantes. Pour la première ligne, il y a donc $4-1=3$ possibilités, et dans chaque cas, il y a ensuite $4-2=2$ possibilités pour la seconde ligne, à savoir tous les vecteurs non colinéaires à la première ligne. Il y a donc six éléments, à savoir

$$G := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}; \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}; \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}; \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}.$$

4. Soit $f \in \mathrm{Aut}(E)$, alors f est bijective et fixe $0 \in E$. Elle envoie donc tout élément non nul sur un élément non nul. Sa restriction à $E \setminus \{0\}$ reste injective et surjective sur $E \setminus f(\{0\}) = E \setminus \{0\}$. L'application $f_{|E\setminus\{0\}}$ est donc une bijection de $E \setminus \{0\}$ dans lui-même, c'est à dire un élément de $\mathfrak{S}_{E\setminus\{0\}}$.

5. Considérons l'application

$$\widetilde{\psi} : \begin{array}{ccc} \mathrm{Aut}(E) & \to & \mathfrak{S}_{E\setminus\{0\}} \\ f & \mapsto & f_{|E\setminus\{0\}} \end{array}.$$

   C'est un morphisme de groupes car, pour tous $f, g \in \mathrm{Aut}(E)$, on a $f(0) = g(0) = 0$ et donc $\widetilde{\psi}(f \circ g) = (f \circ g)_{|E\setminus\{0\}} = f_{|E\setminus\{0\}} \circ g_{|E\setminus\{0\}} = \widetilde{\psi}(f) \circ \widetilde{\psi}(g)$. L'application est injective, car si $f \in \mathrm{Ker}(\widetilde{\psi})$, alors $f_{|E\setminus\{0\}} = \mathrm{Id}_{E\setminus\{0\}}$; et comme $f_{|\{0\}} = \mathrm{Id}_{\{0\}}$, on a $f = \mathrm{Id}_E$.

   Or, en fixant une base arbitraire de E, on a $G \cong \mathrm{Aut}(E)$, et en fixant un numérotation arbitraire des trois éléments de $E\setminus\{0\}$, on a $\mathfrak{S}_{E\setminus\{0\}} \cong \mathfrak{S}_3$. En pré et post-composant $\widetilde{\psi}$, on obtient donc un monomorphisme de groupe $\psi : G \to \mathfrak{S}_3$. Or $|G| = 6 = |\mathfrak{S}_3|$, on en déduit que ψ est un isomorphisme, et donc que $G \cong \mathfrak{S}_3$.

6. Commençons par remarquer que, sur $\mathbb{Z}/2\mathbb{Z}$, les seuls polynômes de degré 1 sont X et $X+1$, et $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est le seul élément de G annulé par l'un d'eux. Tous les autres

ont donc un polynôme annulateur de degré 2, égal au polynôme caractéristique. Par calcul direct, on obtient donc les polynômes minimaux suivants :

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \rightsquigarrow X+1\,; \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \rightsquigarrow (X+1)^2\,;$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rightsquigarrow X^2+1=(X+1)^2\,; \qquad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \rightsquigarrow X^2+X+1\,;$$

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \rightsquigarrow X^2+X+1\,; \qquad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rightsquigarrow (X+1)^2.$$

7. Une matrice est diagonalisable ssi son polynôme minimal est scindé à racines simples. En remarquant que $(X+1)^2$ est scindé à racine multiple, et que X^2+X+1 n'est pas scindé sur $\mathbb{Z}/\mathbb{Z}$ puisque ni 0 ni 1 n'en est racine, on en déduit que $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est le seul élément diagonalisable de G.

   Sans calculer aucun polynôme minimal, on aurait également pu conclure en remarquant que, puisqu'ils sont inversibles, 1 est la seule valeur propre possible pour les éléments de G. Ces dernières ne peuvent donc se diagonaliser qu'en l'identié, et la seule matrice diagonalisable est donc

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

8. On considère l'application

$$\varphi : \begin{array}{ccc} \mathrm{SL}_2(\mathbb{Z}) & \to & G \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \mapsto & \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \end{array}$$

   où la barre dénote la réduction modulo 2. Cette dernière application étant un morphisme d'anneau, on en déduit que cette application est bien définie car, pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, on a $\begin{vmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{vmatrix} = \overline{a}.\overline{d} - \overline{c}.\overline{b} = \overline{a.d-c.b} = \overline{1} \neq \overline{0}$; et qu'il s'agit bien d'un morphisme de groupes. Par définition de l'indice et d'après le premier théorème d'isomorphisme, on a alors $[\mathrm{SL}_2(\mathbb{Z}) : \mathrm{Ker}(\varphi)] = |\mathrm{SL}_2(\mathbb{Z})/\mathrm{Ker}(\varphi)| = |\mathrm{Im}(\varphi)|$. Or φ est surjective car

$$\varphi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}\,; \qquad \varphi\left(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right) = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix}\,;$$

$$\varphi\left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right) = \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix}\,; \qquad \varphi\left(\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\right) = \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix}\,;$$

$$\varphi\left(\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}\right) = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix}\,; \qquad \varphi\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}.$$

   On en déduit donc que $[\mathrm{SL}_2(\mathbb{Z}) : \mathrm{Ker}(\varphi)] = |G| = 6$.

Exercice 2

1. On vérifie directement que ${}^tR.R = {}^tS.S = \mathrm{Id}$ et donc que $R, S \in O(2)$. Par minimalité du sous-groupe engendré, on a donc $G \subset O(2)$.

   En tant que groupe engendré par R et S, tout élément de G s'écrit sous la forme $R^{k_1}.S^{k_2}.R^{k_3}.S^{k_4}.\cdots.R^{k_{2r-1}}.S^{k_{2r}}$ pour un certain $r \in \mathbb{N}^*$, avec $k_1, k_{2r} \in \mathbb{Z}$ et $k_i \in \mathbb{Z}^*$ pour tout $i \in [\![1, 2r-1]\!]$. Mais par calcul direct, on a $S.R = R^2.S$. Tous les S peuvent donc être récursivement poussé à droite, montrant que tout élément de G s'écrit sous la forme $R^{\ell_1}.S^{\ell_2}$, avec $\ell_1, \ell_2 \in \mathbb{Z}$. De plus, encore par calcul direct, on a également $R^3 = S^2 = \mathrm{Id}$. On en déduit que l'on peut supposer $\ell_1 \in \{0,1,2\}$ et $\ell_2 \in \{0,1\}$. Enfin, toujours par calcul direct, on observe que Id, R, R^2, S, $R.S$ et $R^2.S$ sont tous distincts, montrant que G est un sous-groupe fini (d'ordre 6) de $O(2)$.

2. Il est clair que l'application

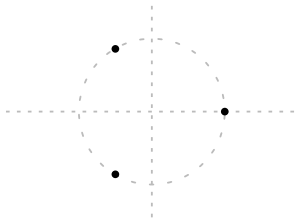
$$a : \begin{array}{ccc} G & \to & \mathrm{Bij}(\mathbb{R}^2) \\ M & \mapsto & (x \mapsto M.x) \end{array}$$

   vérifie bien

   - pour tout $x \in \mathbb{R}^2$, $a(\mathrm{Id})(x) = \mathrm{id}.x = x$;
   - pour tout $M_1, M_2 \in G$ et $x \in \mathbb{R}^2$, $a(M_1)\big(a(M_2)(x)\big) = a(M_1)(M_2.x) = M_1.M_2.x = a(M_1.M_2)(x)$,

   définissant ainsi une action de G sur $\mathbb{R}^2$.

3. Notons $x_0 := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Par calcul direct, on a $\mathcal{O}(x_0) = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -\frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix}, \begin{pmatrix} -\frac{1}{2} \\ -\frac{\sqrt{3}}{2} \end{pmatrix} \right\}$.



4. D'après la formule aux classes, on a $|\mathcal{O}(x_0)| = \frac{|G|}{|\mathrm{Stab}_G(x_0)|}$. On en déduit que $|\mathrm{Stab}_G(x_0)| = \frac{|G|}{|\mathcal{O}|(x_0)} = \frac{6}{3} = 2$.

   Remarquons toutefois que, quitte à avoir fait tous les calculs, on aurait pu directement observer que $|\mathrm{Stab}_G(x_0)| = |\{\mathrm{Id}, S\}| = 2$.

5. Par calcul direct, on a $R.S \neq S.R$, le groupe G n'est donc pas abélien, mais $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ l'est. Ces deux groupes ne sont donc pas isomorphes.

Exercice 3

1. Notons

$$I := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad J := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad K := \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

Par calcul direct, on a la table de multiplication suivante :

	I	J	K
I	$-\mathrm{Id}$	$-K$	J
J	K	$-\mathrm{Id}$	$-I$
K	$-J$	I	$-\mathrm{Id}$

.

On en déduit que $\{\pm\mathrm{Id}, \pm I, \pm J, \pm K\}$ est un sous-groupe car il est stable par produit et par inverse, et donc qu'il contient G. Mais réciproquement, G contient $-\mathrm{Id} = I^2$, $-I = I^3$, $-J = J^3$ et $-K = K^3$. On en déduit que $G = \{\pm\mathrm{Id}, \pm I, \pm J, \pm K\}$. De plus, on a $|G| = 8$, $|\pm I| = |\pm J| = |\pm K| = 4$, $|-\mathrm{Id}| = 2$ et $|\mathrm{Id}| = 1$.

2. On a $I.J = -K \neq K = J.I$. On en déduit que G n'est pas abélien.

3. (a) Le centre de G n'est pas réduit à Id car il contient clairement $-\mathrm{Id}$.

   (b) D'après la table de multiplication ci-haut, on a $\pm I, \pm J, \pm K \notin Z(G)$. On en déduit que $Z(G) = \{\pm\mathrm{Id}\}$.

4. D'après le théorème de Lagrange, un sous-groupe (distingué) de G ne peut être de cardinal que 1, 2, 4 ou 8. Bien entendu, $\{\mathrm{Id}\}$ et G sont les seuls sous-groupes de cardinal 1 ou 8, et ils sont clairement distingués. Un sous-groupe de cardinal 2 doit contenir un élément d'ordre 2, et $-\mathrm{Id}$ est le seul à l'être ; le seul candidat est donc $\{\pm\mathrm{Id}\}$ qui est bien distingué car il s'agit du centre de G. Considérons maintenant un sous-groupe $H \subset G$ d'ordre 4. S'il contient $\pm I$ (resp. $\pm J$, $\pm K$), alors il contient $-\mathrm{Id} = (\pm I)^2$ (resp. $(\pm J)^2$, $(\pm K)^2$) ainsi que $\mp I = (\pm I)^3$ (resp. $\mp J = (\pm J)^3$, $\mp K = (\pm K)^3$), et on en déduit que $H = \{\pm\mathrm{Id}, \pm I\}$ (resp. $\{\pm\mathrm{Id}, \pm J\}$, $\{\pm\mathrm{Id}, \pm K\}$). Or, puisque $|H| = 4 > 2 = |G \setminus \{\pm I, \pm J, \pm K\}|$, H contient nécessairement un de ces six éléments. De plus, tous ces sous-groupes sont distingués car d'indice 2.

   Au final, la liste des sous-groupes distingués de G est

$$\Big\{\{\mathrm{Id}\}\ ,\ \{\pm\mathrm{Id}\}\ ,\ \{\pm\mathrm{Id}, \pm I\}\ ,\ \{\pm\mathrm{Id}, \pm J\}\ ,\ \{\pm\mathrm{Id}, \pm K\}\ ,\ G\Big\}.$$