Groupes et géométrie, feuille 8

N. Perrin

À rendre le mercredi 01.04.2020

Correction le jeudi 02.04.2020

Exercice 1 (20 × 5 = 100 Points) Soit $n \geq 3$ un entier. On considère les matrices suivantes de $\mathrm{GL}_2(\mathbb{R})$:

$$\sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ et } \tau = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}.$$

On note G le sous-groupe de $\mathrm{GL}_2(\mathbb{R})$ engendré par σ et τ, on note H le sous-groupe de G engendré par σ et K le sous-groupe engendré par τ : $G = \langle \sigma, \tau \rangle$, $H = \langle \sigma \rangle$, $K = \langle \tau \rangle$. On pose $K' = \{g \in G \mid \det(g) = 1\}$ et on définit les vecteurs X_0 et Y_0 de $\mathbb{R}^2$ par

$$X_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ et } Y_0 = \begin{pmatrix} -1 \\ 0 \end{pmatrix}.$$

(i) Donner l'ordre de σ.

(ii) Donner une interprétation géométrique pour τ et donner son ordre.

(iii) Si G est d'ordre fini, que peut-on dire sur son ordre ?

(iv) Montrer que $\sigma\tau = \tau^{n-1}\sigma$.

(v) Donner tous les éléments de G, H et K.

(vi) Combien y a-t-il de classe à gauche de G modulo H ?

(vii) Décrire G/H.

(viii) A-t-on $H \triangleleft G$? Si oui décrire le groupe quotient G/H.

(ix) A-t-on $K \triangleleft G$? Si oui décrire le groupe quotient G/K.

(x) Le sous-ensemble K' de G est-il un sous-groupe de G ? Si oui, a-t-on $K' \triangleleft G$?

(xi) Comparer K et K'.

(xii) Existe-t-il un sous-groupe de G isomorphe à G/K ?

(xiii) Calculer $D(G)$. À quel groupe est isomorphe $G/D(G)$?

(xiv) Montrer que la multiplication des matrices définit une action $G\times\mathbb{R}^2 \to \mathbb{R}^2$, $(M,X) \mapsto M\cdot X = MX$.

(xv) L'action est-elle transitive ?

(xvi) L'action est elle fidèle ?

(xvii) Quels sont les points fixes de l'action ?

(xviii) Quel est le stabilisateur G_{X_0} du vecteur X_0 ?

(xix) Décrire l'orbite du vecteur X_0.

(xx) Quel est le stabilisateur G_S du segment $S = [X_0Y_0]$.

Solution.

(i) On a $\sigma \neq \mathrm{Id}$ mais $\sigma^2 = \mathrm{Id}$ donc σ est d'ordre 2.

(ii) On voit que τ est la rotation de centre $O = (0,0)$ et d'angle $\frac{2\pi}{n}$. EN particulier τ est d'ordre n. On peut facilement calculer (avec un peu de trigonométrie) que l'on a

$$\tau^k = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) & -\sin\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) & \cos\left(\frac{2k\pi}{n}\right) \end{pmatrix}.$$

(iii) Si G est fini, son ordre est divisible par 2 et par n et donc par $\mathrm{ppcm}(2,n)$.

(iv) On calcule

$$\sigma\tau\sigma^{-1} = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & \sin\left(\frac{2\pi}{n}\right) \\ -\sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{-2\pi}{n}\right) & \sin\left(\frac{-2\pi}{n}\right) \\ -\sin\left(\frac{-2\pi}{n}\right) & \cos\left(\frac{-2\pi}{n}\right) \end{pmatrix} = \tau^{-1}.$$

On en déduit $\sigma\tau\sigma^{-1} = \tau^{n-1}$ puis $\sigma\tau = \tau^{n-1}\sigma$.

Posons $G' = \{x_1\cdots x_r \mid r\in\mathbb{N},\ x_i \in \{\sigma,\tau\}\}$.

(v) Comme σ est d'ordre 2, on a $H = \{1,\sigma\}$. Comme τ est d'ordre n, on a $K = \{1,\tau,\cdots,\tau^{n-1}\}$. Montrons que l'on a

$$G = \{1,\tau,\cdots,\tau^{n-1},\sigma,\tau\sigma,\cdots,\tau^{n-1}\sigma\}.$$

Posons $G' = \{1,\tau,\cdots,\tau^{n-1},\sigma,\tau\sigma,\cdots,\tau^{n-1}\sigma\}$. Comme $G = \langle\sigma,\tau\rangle$, on a l'inclusion $G' \subset G$. Pour montrer l'inclusion réciproque, il suffit de montrer que G' est un sous-groupe de G. Soit $x \in G'$, montrons que $x^{-1} \in G'$. On a $x = \tau^k$ ou $x = \tau^k\sigma$ avec $k \in [0,n-1]$. Si $k = 0$, alors $x = 1$ ou $x = \sigma$ et $x^{-1} = 1$ ou $x^{-1} = \sigma$ donc $x^{-1} \in G'$. Sinon, on a $x^{-1} = \tau^{-k}$ ou $x^{-1} = \sigma^{-1}\tau^{-k}$. Dans le premier cas, on a $x^{-1} = \tau^{n-k}$ avec $n-k \in [0,n-1]$ donc $x^{-1} \in G'$. Dans le second cas, on a

$$x^{-1} = \sigma\tau^{n-k} = \tau^{n-1}\sigma\tau^{n-k-1} = \tau^{2(n-1)}\sigma\tau^{n-k-2} = \cdots = \tau^{(n-1)(n-k)}\sigma.$$

On obtient $x^{-1} = \tau^{n^2-(k+1)n+k}\sigma$ et comme τ est d'ordre n, on obtient $x^{-1} = \tau^k\sigma \in G'$.

Montrons maintenant que si $x,y \in G'$, alors $xy \in G'$. On a $x = \tau^k$ ou $x = \tau^k\sigma$ avec $k \in [0,n-1]$ et $y = \tau^l$ ou $y = \tau^l\sigma$ avec $l \in [0,n-1]$. On obtient $xy = \tau^{k+l}$ ou $xy = \tau^{k+l}\sigma$ ou $xy = \tau^k\sigma\tau^l$ ou $xy = \tau^k\sigma\tau^l\sigma$. Dans les deux premiers cas, on a $xy \in G'$. Dans le troisième cas, on a $xy = \tau^k\sigma\tau^l = \tau^k\tau^{l(n-1)}\sigma = \tau^{k+l(n-1)}\sigma \in G'$. Dans le dernier cas, on a $xy = \tau^k\sigma\tau^l\sigma = \tau^k\tau^{l(n-1)}\sigma\sigma = \tau^{k+l(n-1)} \in G'$. Ainsi G' est un sous-groupe et $G = G'$.

(vi) L'ensemble des classes à gauche de G modulo H est l'ensemble G/H. Son cardinal est $|G/H| = [G : H] = |G|/|H|$. D'après la question précédente, on a $|G| = 2n$ et $|H| = 2$ donc $|G/H| = n$.

(vii) Par la description de G, on a $G/H = \{[1], [\tau], \cdots, [\tau^{n-1}]\}$.

(viii) On a $\tau^{-1}\sigma\tau = \tau^{-1}\tau^{n-1}\sigma = \tau^{n-2}\sigma \notin H$ donc H n'est pas un sous-groupe distingué.

(ix) On a $[g : K] = |G|/|K| = 2n/n = 2$ donc K est un sous-groupe d'indice 2 donc il est distingué. Le groupe quotient est d'ordre 2 donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$. On a $G/K = \{[1], [\sigma]\}$.

(x) L'application $\det : G \to \mathbb{R}^*$ est un morphisme de groupe et K' est son noyau. Ainsi K' est un sous-groupe de G et doit être distingué.

(xi) On a $\det(\tau) = \cos^2\left(\frac{2\pi}{n}\right)+\sin^2\left(\frac{2\pi}{n}\right) = 1$ donc $\tau \in K'$ et ainsi $K = \langle\tau\rangle \subset K'$. De plus $\det(\sigma) = -1$ donc $\det(\tau^k\sigma) = -1$ et donc $K = K'$.

(xii) Le groupe G/K est d'ordre 2 et le sous-groupe H est aussi d'ordre 2. Ils doivent être isomorphe donc il existe un sous-groupe de G (le sous-groupe H) isomorphe à G/K.

ICI

(xiii) On a vu que G n'est pas commutatif (car $\sigma\tau = \tau^{n-1}\sigma =\neq \tau\sigma$ parceque $n \neq 2$). Donc $D(G) \neq \{1\}$. De plus G/K est commutatif donc $D(G) \subset K$.

Calculons $(\sigma, \tau) = \sigma\tau\sigma^{-1}\tau^{-1} = \tau^{-1}\tau^{-1} = \tau^{-2}$. Ainsi $\tau^{-2} \in D(G)$ donc $\tau^2 \in D(G)$ et donc $\langle\tau^2\rangle \subset D(G)$.

Si n est impair, alors n est premier avec 2 et $\mathrm{ord}(\tau^2) = \frac{n}{\mathrm{pgcd}(2,n)} = n$ donc $\langle\tau^2\rangle = \langle\tau\rangle$ et $K = \langle\tau\rangle \subset D(G)$. Finalement $D(G) = K = \langle\tau\rangle = \langle\tau^2\rangle$. Dans ce cas, on a $G/D(G) \simeq \mathbb{Z}/2\mathbb{Z}$.

Si $n = 2m$ est pair, montrons que $D(G) = \langle\tau^2\rangle = \{1, \tau^2, \tau^4, \cdots, \tau^{n-2}\} = \{1, \tau^2, \tau^4, \cdots, \tau^{2(m-1)}\}$. On a déjà vu que $\langle\tau^2\rangle \subset D(G)$. Montrons que $\langle tau^2\rangle \triangleleft G$. Soit $y = \tau^{2a} \in \langle\tau^2\rangle$ et $x \in G$, on a $x = \tau^k$ ou $x = \tau^k\sigma$. On obtient dans le premier cas $xyx^{-1} = \tau^k\tau^{2a}\tau^{-k} = \tau^{k+2a-k} = \tau^{2a} = y \in \langle tau^2\rangle$. Dans le second cas, on a $xyx^{-1} = \tau^k\sigma\tau^{2a}\sigma^{-1}\tau^{-k} = \tau^k\tau^{2a(n-1)}\sigma\sigma^{-1}\tau^k = \tau^{k+2a(n-1)-k} = \tau^{2a(n-1)} \in \langle\tau^2\rangle$. Ainsi $\langle\tau^2\rangle \triangleleft G$. De plus $\mathrm{ord}(\tau^2) = \frac{n}{\mathrm{pgcd}(2,n)} = \frac{n}{2} = m$ donc $|\langle\tau^2\rangle| = m$. Ainsi le quotient $G/\langle\tau^2\rangle|$ est d'ordre $2n/m = 4$. Mais un groupe d'ordre 4 a soit un élément d'ordre 4 et est alors isomorphe à $\mathbb{Z}/4\mathbb{Z}$, soit n'a que des éléments d'ordre 2 et est isomorphe à un groupe de Klein. En particulier, un groupe d'ordre 4 est commutatif donc $G/\langle\tau^2\rangle$ est commutatif donc $D(G) \subset \langle\tau^2\rangle$. On obtient $D(G) = \langle\tau^2\rangle$. Il reste à déterminer $G/D(G) = G/\langle\tau^2\rangle$ qui est d'ordre 4. On peut facilement décrire $G/D(G) = \{[1], [\sigma], [\tau], [\tau\sigma]\}$. Mais on a $[1]^1 = [1]$, $[\tau]^2 = [\tau^2] = [1]$ (car on quotiente par $\langle\tau^2\rangle$), $[\sigma]^2 = [\sigma^2] = [1]$ et $[\tau\sigma]^2 = [\tau]^2[\sigma]^2 = [1]$ (car le groupe est commutatif. Ainsi tous les éléments sont d'ordre 2 et $G/D(G) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ est un groupe de Klein.

(xiv) On a $1 \cdot X = \mathrm{Id} \cdot X = X$ et pour $M, M' \in G$, on a $(MM') \cdot X = MM'X = M \cdot (M' \cdot X)$ par l'associativité du produit matriciel. On a donc bien une action de G sur $\mathbb{R}^2$.

(xv) Non l'action n'est pas transitive. L'orbit d'un vecteur $X \in \mathbb{R}^2$ est l'ensemble $G \cdot X = \{g \cdot X \mid g \in G\}$ donc $G \cdot X$ a au plus $2n$ éléments alors que $\mathbb{R}^2$ est infini donc aucune orbite ne peut être égale à $\mathbb{R}^2$ tout entier. Aussi il y a plusieures orbites, par exemple $G \cdot (0,0) = \{(0,0)\}$. Cette orbite n'a qu'un élément.

(xvi) Montrons que l'action est fidèle. Soit $g \in G$ tel que $g \cdot X = X$ pour tout $X \in \mathbb{R}^2$ alors par définition, g doit être l'application identité de $\mathbb{R}^2$ donc associé à la matrice identité donc $g = 1$. L'action est donc fidèle.

(xvii) On cherche les $X \in \mathbb{R}^2$ tels que $g \cdot X = X$ pour tout $g \in G$. On a déjà vu que $(0,0)$ est un point fixe. Montrons que c'est le seul. En effet, si $X = (x,y)$ est un point fixe, alors $\sigma \cdot X = X$ donc $(x,-y) = (x,y)$ donc $y = 0$. De plus, on a $\tau \cdot X = X$ donc $\tau \cdot (x,0) = (x,0)$ ce qui donne $\left(\cos\left(\frac{2\pi}{n}\right)x, \sin\left(\frac{2\pi}{n}\right)x\right) = (x,0)$ donc $x\left(\cos\left(\frac{2\pi}{n}\right) - 1\right) = 0$ et $x \sin\left(\frac{2\pi}{n}\right) = 0$. Mais pour $n \geq 3$, on a $\sin\left(\frac{2\pi}{n}\right) \neq 0$ donc $x = 0$ et $X = (0,0)$ est le seul point fixe.

(xviii) our rappel $G_{X_0} = \{g \in G \mid g \cdot X_0 = X_0\}$. On cherche les éléments g de G tels que $g \cdot (1,0) = (1,0)$. On voit que $\sigma \cdot X_0 = \sigma \cdot (1,0) = (1,0) = X_0$ donc $\sigma \in G_{X_0}$. Par ailleurs, on a $\tau^k \cdot X_0 = \left(\cos\left(\frac{2k\pi}{n}\right), \sin\left(\frac{2k\pi}{n}\right)\right)$. Ce vecteur est égal à X_0 si et seulement si $\cos\left(\frac{2k\pi}{n}\right) = 1$ et $\sin\left(\frac{2k\pi}{n}\right) = 0$ c'est-à-dire si et seulement si $\frac{2k\pi}{n} \equiv 0$ (modulo 2π donc si et seulement si k est un multiple de n donc si et seulement si $\tau^k = 1$. De même, on a $\tau^k\sigma \cdot X_0 = \tau^k \cdot X_0$ et donc $(\tau^k\sigma) \cdot X_0 = X_0$ si et seulement si $\tau^k = 1$ et donc si et seulement si $\tau^k\sigma = \sigma$. On obtient $G_{X_0} = \{1, \sigma\} = H$.

(xix) Par la formule des classes, on sait que $|G \cdot X_0| = [G/G_{X_0}] = [G : H] = |G|/|H| = 2n/2 = n$. On voit que les éléments $\tau^k \cdot X_0 = \left(\cos\left(\frac{2k\pi}{n}\right), \sin\left(\frac{2k\pi}{n}\right)\right)$ pour $k \in [0, n-1]$ sont deux-à-deux distincts donc ils forment l'orbite de X_0. Vu comme éléments du plan complexe, cette orbite est l'ensemble des racines n-ièmes de l'unité.

(xx) Comme $Y_0 = -X_0$, on voit que $\sigma \cdot Y_0 = \sigma(-X_0) = -\sigma(X_0) = -X_0 = Y_0$ donc $\sigma[X_0, Y_0] = [X_0, Y_0]$ et $\sigma \in G_{[X_0,Y_0]}$. Si $g \in G_{[X_0,Y_0]}$, alors comme g est linéaire, g doit envoyer X_0 sur un élément de la droite $\langle X_0 \rangle = (X_0, Y_0)$. Cherchons donc les $g \in G$ qui vérifient cette condition. On a $g = \tau^k$ ou $g = \tau^k\sigma$ pour $k \in [0, n-1]$ et donc dans les deux cas $g \cdot X_0 = \tau^k X_0 = \left(\cos\left(\frac{2k\pi}{n}\right), \sin\left(\frac{2k\pi}{n}\right)\right)$. Mais on a $\langle X_0 \rangle = \{(x,y) \in R^2 \mid y = 0\}$ donc on vuet que $\sim \left(\frac{2k\pi}{n}\right) = 0$ c'est-à-dire $\frac{2k\pi}{n} \equiv 0$ (modulo π).

SI n est impair, alors la seule possibilité est $k = 0$ et $G_{[X_0,Y_0]} = \{1, \sigma\} = H$.

Si $n = 2m$ est pair, alors on a deux possibilités : $k = 0$ et $k = m$. Pour $k = m$, on a

$$\tau^m = \begin{pmatrix} \cos\left(\frac{2\pi m}{n}\right) & -\sin\left(\frac{2\pi m}{n}\right) \\ \sin\left(\frac{2\pi m}{n}\right) & \cos\left(\frac{2\pi m}{n}\right) \end{pmatrix} = \begin{pmatrix} \cos(\pi) & -\sin(\pi) \\ \sin(\pi) & \cos(\pi) \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

■

Ainsi $\tau^m \cdot X_0 = Y_0$ et $\tau^m \cdot Y_0 = X_0$. Dons $\tau^m \cdot [X_0, Y_0] = [X_0, Y_0]$. Finalement, on a $G_{[X_0,Y_0]} = \{1, \sigma, \tau^m, \tau^m\sigma\}$.