

Groupes et géométrie, feuille 7

N. Perrin

À rendre le mercredi 25.03.2020

Correction le jeudi 26.03.2020

Exercice 1 ($3 \times 10 = 30$ Points) On rappelle la définition des matrices élémentaires de types I, II et III.

Type I. Soient $1 \leq p, q \leq n$ avec $p \neq q$ et $a \in \mathbb{R}$. On définit $T_{p,q}(a) = (t_{i,j}) \in M_n(\mathbb{R})$ par

$$t_{i,j} = \begin{cases} 1 & \text{si } i = j, \\ a & \text{si } (i,j) = (p,q), \\ 0 & \text{sinon.} \end{cases}$$

Type II. Soit $1 \leq p \leq n$ et soit $b \in \mathbb{R}^\times$. On définit $D_p(b) = (d_{i,j}) \in M_n(\mathbb{R})$ par

$$d_{i,j} = \begin{cases} 1 & \text{si } i = j \neq p, \\ b & \text{si } i = j = p, \\ 0 & \text{sinon.} \end{cases}$$

Type III. Soient $1 \leq p, q \leq n$. On définit $E_{p,q} = (e_{i,j}) \in M_n(\mathbb{R})$ par

$$e_{i,j} = \begin{cases} 1 & \text{si } q \neq i = j \neq p, \\ 1 & \text{si } (i,j) = (p,q), \\ 1 & \text{si } (i,j) = (q,p), \\ 0 & \text{sinon.} \end{cases}$$

On note G le sous-groupe de $\text{GL}_n(\mathbb{R})$ engendré par toutes les matrices élémentaires et H le sous-groupe de G engendré par les matrices élémentaires de type I et de type III : $G = \langle M \mid M \text{ matrice élémentaire de type I, II ou III} \rangle$ et $H = \langle M \mid M \text{ matrice élémentaire de type I ou III} \rangle$.

- (i) Montrer que $G = \text{GL}_n(\mathbb{R})$. [On pourra appliquer l'algorithme de Gauß].
- (ii) Montrer que pour tout élément $A \in H$, on a $\det(A) \in \{\pm 1\}$.
- (iii) Montrer que l'on a une bijection entre G/H et $\mathbb{R}_+^*$.

Solution. (i) On a clairement l'inclusion $G \subset \text{GL}_n(\mathbb{R})$. Montrons l'inclusion réciproque. Soit $M \in \text{GL}_n(\mathbb{R})$. Par l'algorithme de Gauss, il existe des matrices $T_1, \dots, T_r$ de type I et II telles que $MT_1 \cdots T_r = I_n$. On obtient donc $M = T_r^{-1} \cdots T_1^{-1} \in G$.

(ii) Si A est de type I, alors $\det(A) = 1$ alors que si A est de type III, on a $\det(A) = \pm 1$. Ainsi toute matrice de H est produit de matrices de déterminant 1 ou -1 d'où le résultat.

(iii) Considérons l'application $f : G \rightarrow \mathbb{R}_+^*$ définie par $f(M) = |\det(M)|$. C'est un morphisme de groupes. En effet, on a

$$f(MN) = |\det(MN)| = |\det(M) \det(N)| = |\det(M)| |\det(N)| = f(M)f(N).$$

Par ailleurs, comme $G = \text{GL}_n(\mathbb{R})$, cette application est surjective : pour un réel $\lambda \in \mathbb{R}_+^*$, prendre $M = \text{diag}(\lambda, 1, \dots, 1)$ la matrice diagonale ayant un λ et $n - 1$ fois 1 sur la diagonale. On a $f(M) = \lambda$. Pour conclure, il suffit de montrer que $H = \ker(f)$.

On commence par l'inclusion $H \subset \ker(f)$. On a vu que pour tout $M \in H$, on a $\det(M) = \pm 1$ donc $|\det(M)| = 1$ et $M \in \ker(f)$. Réciproquement, soit $M \in \ker(f)$. Alors $|\det(M)| = f(M) = 1$ et $\det(M) = \pm 1$. On veut montrer que $M \in H$. Comme H contient une matrice de déterminant -1 (la matrice $E_{1,2}$ par exemple, on peut, quitte à remplacer M par $ME_{1,2}$, supposer que $\det(M) = 1$. En appliquant l'algorithme de Gauss sans utiliser de matrice de type II, (donc seulement des matrices de type I et III), on voit qu'il existe des matrices $T_1, \dots, T_r$ de type I et III telles que

$$T_1 \cdots T_r M = \text{diag}(\lambda_1, \dots, \lambda_n)$$

où $\text{diag}(\lambda_1, \dots, \lambda_n)$ est la matrice diagonale ayant $\lambda_1, \dots, \lambda_n$ sur la diagonale. On peut donc supposer que M est diagonale de la forme

$$M = \text{diag}(\lambda_1, \dots, \lambda_n) \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}.$$

On a la formule suivante :

$$\begin{pmatrix} 1 & -\lambda_1 & | & \mathbf{0} \\ 0 & 1 & | & \mathbf{0} \\ \hline \mathbf{0} & & | & I_{n_2} \end{pmatrix} \begin{pmatrix} 1 & 0 & | & \mathbf{0} \\ \frac{1-\lambda_1}{\lambda_1} & 1 & | & \mathbf{0} \\ \hline \mathbf{0} & & | & I_{n_2} \end{pmatrix} \begin{pmatrix} 1 & 1 & | & \mathbf{0} \\ 0 & 1 & | & \mathbf{0} \\ \hline \mathbf{0} & & | & I_{n_2} \end{pmatrix} \begin{pmatrix} 1 & 0 & | & \mathbf{0} \\ \lambda_1 - 1 & 1 & | & \mathbf{0} \\ \hline \mathbf{0} & & | & I_{n_2} \end{pmatrix} \\ = \begin{pmatrix} \lambda_1 & 0 & | & \mathbf{0} \\ 0 & \frac{1}{\lambda_1} & | & \mathbf{0} \\ \hline \mathbf{0} & & | & I_{n_2} \end{pmatrix}.$$

Donc cette dernière matrice et son inverse sont dans H . Ainsi en multipliant par cet inverse, on peut remplacer $M = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$ par $M = \text{diag}(1, \lambda_1 \lambda_2, \lambda_3 \cdots, \lambda_n)$. Par récurrence, on voit qu'on peut remplacer M par $\text{diag}(1, \dots, 1, \lambda_1 \lambda_2 \cdots \lambda_n) = \text{diag}(1, \dots, 1, \det(M)) = I_n$ donc on a bien M dans H . ■

Exercice 2 ($5 \times 10 + 20 = 70$ Points) Soit $G = \mathfrak{A}_5 \subset \mathfrak{S}_5$ le groupe alterné.

(i) Décrire tous les éléments d'ordre 2 de G .

- (ii) Montrer que deux éléments d'ordre 2 de G sont conjugués dans G .
- (iii) Soit x un 5-cycle. Montrer que $x \in G$ et décrire les éléments de $\langle x \rangle$
- (iv) Montrer que tout 5-cycle est conjugué à un élément de $\langle x \rangle$.
- (v) Montrer que les 3-cycles sont tous conjugués dans G .
- (vi) Soit $H \triangleleft G$ avec $H \neq \{1\}$. Montrer que $H = G$.

Solution. (i) Par la décomposition en produit de cycles à support disjoints, les éléments d'ordre 2 de $\mathfrak{S}_n$ sont les produits de transpositions à support disjoint. Comme on cherche les éléments d'ordre 2 de $\mathfrak{A}_5$ on ne peut avoir que les produits de deux transpositions à support disjoint. Donc de la forme $\tau_{a,b}\tau_{c,d}$ avec $|\{a,b,c,d\}| = 4$. Il y en a $\binom{5}{4} \times 3 = 5 \times 3 = 15$ (choix des 4 éléments a, b, c et $d : \binom{5}{4}$ choix puis choix des trois découpages $\{a,b\} \amalg \{c,d\}$, $\{a,c\} \amalg \{b,d\}$ ou $\{a,d\} \amalg \{b,c\}$ de cet ensemble de 4 éléments : 3 choix). Voici la liste de ces éléments :

$$(21435), (21543), (21354), (34125), (35142), (32154), (43215), (45312), \\ (42513), (53241), (54321), (52431), (13254), (14523), (15432).$$

(ii) Deux éléments d'ordre 2 de G sont de la forme $\tau_{a,b}\tau_{c,d}$ et $\tau_{x,y}\tau_{u,v}$. On cherche donc un élément $\sigma \in G$ tel que $\sigma(\{a,b\}) = \{x,y\}$ et $\sigma(\{c,d\}) = \{u,v\}$. On commence par prendre l'unique $\sigma \in \mathfrak{S}_5$ tel que $\sigma(a) = x$, $\sigma(b) = y$, $\sigma(c) = u$ et $\sigma(d) = v$. Si $\sigma \in G = \mathfrak{A}_5$, on a fini, sinon, on remplace σ par $\sigma' = \sigma\tau_{a,b}$. On a alors $\sigma' \in \mathfrak{A}_5 = G$ et $\sigma'(a) = y$, $\sigma'(b) = x$, $\sigma'(c) = u$ et $\sigma'(d) = v$.

Un exemple, on prend $\tau_{1,2}\tau_{3,4}$ et $\tau_{2,3}\tau_{1,5}$. On prend σ tel que $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$ et $\sigma(4) = 5$. On a alors nécessairement $\sigma(5) = 4$. Ainsi $\sigma = (23154)$. De plus $\varepsilon(\sigma) = (-1)^3 = -1$ (il y a 3 inversions : $(1,2)$, $(1,3)$ et $(4,5)$). On prend alors $\sigma' = \sigma\tau_{1,2} = (23154)(21345) = (32154)$. On a $\sigma'(1) = 3$, $\sigma'(2) = 2$, $\sigma'(3) = 1$, $\sigma'(4) = 5$ et $\sigma'(5) = 4$. On a aussi $\varepsilon(\sigma') = (-1)^4 = 1$ (il y a 4 inversions : $(1,2)$, $(1,3)$, $(2,3)$ et $(4,5)$) donc $\sigma' \in \mathfrak{A}_5$. Enfin, on a $\sigma'\tau_{1,2}\tau_{3,4}(\sigma')^{-1} = \sigma'\tau_{1,2}(\sigma')^{-1}\sigma'\tau_{3,4}(\sigma')^{-1} = \tau_{\sigma'(1),\sigma'(2)}\tau_{\sigma'(3),\sigma'(4)} = \tau_{3,2}\tau_{1,5} = \tau_{2,3}\tau_{1,5}$.

(iii) Soit x un p -cycle. On sait que $\varepsilon(x) = (-1)^{p-1}$ (Cours Théorème 3.9.3). Ainsi pour un 5-cycle x , on a $\varepsilon(x) = (-1)^4 = 1$ et $x \in G$. Par ailleurs, un 5-cycle est d'ordre 5 (Cours Lemme 3.8.4) donc

$$\langle x \rangle = \{1, x, x^2, x^3, x^4\}.$$

(iv) Soit y un 5-cycle. On sait (Cours Proposition 3.8.7.(ii)) que les 5-cycles sont conjugués dans $\mathfrak{S}_5$. Il existe donc $\sigma \in \mathfrak{S}_5$ tel que $\sigma y \sigma^{-1} = x$. Le problème est que σ n'est pas nécessairement dans $G = \mathfrak{A}_5$. On va le modifier un peu.

Soyons plus précis. On écrit $x = [a_1, a_2, a_3, a_4, a_5]$ comme 5-cycle. On peut remarquer que $\{a_1, a_2, a_3, a_4, a_5\} = [1, 5]$. De même, on écrit $y = [b_1, b_2, b_3, b_4, b_5]$ comme 5-cycle. On a aussi $\{b_1, b_2, b_3, b_4, b_5\} = [1, 5]$. On peut prendre σ comme l'unique permutation telle que $\sigma(b_i) = a_i$ pour tout $i \in [1, 5]$. On a bien

$$\begin{aligned} \sigma y \sigma^{-1} &= \sigma[b_1, b_2, b_3, b_4, b_5] \sigma^{-1} = [\sigma(b_1), \sigma(b_2), \sigma(b_3), \sigma(b_4), \sigma(b_5)] \\ &= [a_1, a_2, a_3, a_4, a_5] = x \end{aligned}$$

Si $\sigma \in G = \mathfrak{A}_5$, on a terminé. Sinon, on remplace σ par $\sigma' = \sigma[b_2, b_3, b_5, b_4]$. Comme $[b_2, b_3, b_5, b_4]$ est un 4-cycle, on a $\varepsilon([b_2, b_3, b_5, b_4]) = -1$ donc $\sigma' \in G$. On

calcule maintenant

$$\begin{aligned}
\sigma'y(\sigma')^{-1} &= \sigma[b_2, b_3, b_5, b_4][b_1, b_2, b_3, b_4, b_5][b_2, b_3, b_5, b_4]^{-1}\sigma^{-1} \\
&= \sigma[b_1, b_3, b_5, b_2, b_4]\sigma \\
&= [a_1, a_3, a_5, a_2, a_4] = x^2 \in \langle x \rangle.
\end{aligned}$$

(v) Soient $x = [a_1, a_2, a_3]$ et $y = [b_1, b_2, b_3]$ deux 3-cycles. Il existe a_4, a_5, b_4, b_5 tels que

$$\{a_1, a_2, a_3, a_4, a_5\} = [1, 5] = \{b_1, b_2, b_3, b_4, b_5\}.$$

Soit σ la permutation telle que $\sigma(a_i) = b_i$ pour tout $i \in [1, 5]$. On a $\sigma x \sigma^{-1} = \sigma[a_1, a_2, a_3]\sigma^{-1} = [\sigma(a_1), \sigma(a_2), \sigma(a_3)] = [b_1, b_2, b_3] = y$. Si $\sigma \in G = \mathfrak{A}_5$, on a terminé. Sinon, on pose $\sigma' = \sigma\tau_{a_4, a_5}$. On a alors $\sigma' \in G$ et $\sigma'x(\sigma')^{-1} = \sigma'[a_1, a_2, a_3](\sigma')^{-1} = [\sigma'(a_1), \sigma'(a_2), \sigma'(a_3)] = [b_1, b_2, b_3] = y$.

(vi) Remarquons tout d'abord que $|G| = |\mathfrak{A}_5| = 5!/2 = 120/2 = 60$. Notons aussi que le nombre de 3-cycle de G est $2\binom{5}{3} = 20$, le nombre de 5-cycles est $4! = 24$ alors que le nombre d'éléments d'ordre 2 est 15 par (i). Ceci nous donne $20 + 24 + 15 = 59$ éléments. Avec le neutre, on a ainsi décrit tous les éléments de G .

Soit $H \triangleleft G$ tel que $H \neq \{1\}$. Si H contient un 3-cycle alors H contient tous les 3-cycles par (v) et comme G est engendré par les 3-cycles, on a $H = G$.

Si H contient un 5-cycle x , alors il contient $\langle x \rangle$ et tout 5-cycle est conjugué à un élément de $\langle x \rangle$ par (iv) donc H contient tous les 5-cycles. Mais $[12345][12435] = (35142) = \tau_{1,3}\tau_{2,5}$ donc H contient un élément d'ordre 2 et par (ii), le sous-groupe H doit contenir tous les éléments d'ordre 2. Le groupe H contient donc les 24 éléments d'ordre 5 et les 15 éléments d'ordre 2 donc au moins $24 + 15 = 39$ éléments. Comme $|H|$ divise $|G| = 60$, on doit avoir $|H| = 60$ et $H = G$.

Si H contient un élément d'ordre 2, alors il les contient tous par (ii). On a donc $\tau_{1,2}\tau_{4,5} \in H$ et $\tau_{2,3}\tau_{4,5} \in H$. On a alors $[123] = (23145) = \tau_{1,2}\tau_{4,5}\tau_{2,3}\tau_{4,5} \in H$. Donc H contient un 3-cycle et $H = G$. ■