UNIVERSITÉ DE RENNES 1

Compléments de cours d'algèbre

Le groupe des rotations rationnelles

Nous allons voir que le groupe $\mathrm{SO}_3(\mathbb{Q})$ n'est pas simple, contrairement au groupe $\mathrm{SO}_3(\mathbb{R})$ (la simplicité de ce dernier étant établie par exemple dans [2, théorème 6.1, p. 148] et [1, exercice 1.37, p. 67]). On pourra également remarquer que le groupe $\mathrm{SO}_3(\mathbb{C})$ est quant à lui isomorphe [1] à $\mathrm{PSL}_2(\mathbb{C})$ et se trouve donc être également simple.

Nous suivons les indications des exercices 3 et 4 p. 158 de [2] et montrons tout d'abord le résultat suivant.

Lemme 1. *Soit (x, y, z) un point de la sphère unité à coefficients dans $\mathbb{Q}$. Les coordonnées vérifient alors x, y et $z \in \mathbb{Z}_2$.*

Il convient de dire un mot sur l'ensemble $\mathbb{Z}_2$ auquel fait référence l'énoncé ci-dessus. Il est défini par :

$$\mathbb{Z}_2 := \left\{ \frac{p}{q} \in \mathbb{Q} \mid \mathrm{pgcd}(p, q) = 1 \text{ et } q \text{ est impair} \right\}.$$

Il s'agit d'un sous-anneau de $\mathbb{Q}$ et, de plus, si $x = \frac{p}{q} \in \mathbb{Z}_2$ avec p impair, alors $x^{-1} = \frac{q}{p} \in \mathbb{Z}_2$. L'idéal $\mathfrak{m} := 2\mathbb{Z}_2$ est donc un idéal maximal et c'est même l'unique idéal maximal de $\mathbb{Z}_2$ (car $\mathbb{Z}_2 \setminus \mathfrak{m} = \mathbb{Z}_2^\times$). On peut alors réduire modulo 2, voire modulo 2^r :

$$\mathbb{Z}_2/\mathfrak{m}^r \simeq \mathbb{Z}/2^r\mathbb{Z}.$$

En effet, si q est impair, q est inversible dans $\mathbb{Z}/2^r\mathbb{Z}$ et la quantité pq^{-1} est bien définie dans cet anneau.

Démonstration du lemme 1. On écrit x, y et z sous la forme :

$$x = \frac{p_1}{2^{\alpha_1} q_1}, \quad y = \frac{p_2}{2^{\alpha_2} q_2} \quad \text{et} \quad z = \frac{p_3}{2^{\alpha_3} q_3}$$

avec p_i et q_j impairs. Quitte à réordonner les éléments, on peut supposer que $\alpha_1 \geq \alpha_2 \geq \alpha_3$ et nous raisonnerons par l'absurde en supposant $\alpha_1 \geq 1$. L'équation $x^2 + y^2 + z^2 = 1$ se réécrit alors :

$$p_1^2 q_2^2 q_3^2 + 4^{\alpha_1 - \alpha_2} p_2^2 q_1^2 q_3^2 + 4^{\alpha_1 - \alpha_3} p_3^2 q_1^2 q_2^2 = 4^{\alpha_1} q_1^2 q_2^2 q_3^2. \tag{1}$$

Examinons les différentes possibilités qui s'offrent à nous.

— Si $\alpha_1 > \alpha_2$, tous les exposants des 4 sont strictement positifs dans (1) et la quantité $p_1^2 q_2^2 q_3^2$ serait alors pair.

1. Pour les courageux/courageuses, se reporter à [2, théorème 9.3, p. 195].

— Si $\alpha_1 = \alpha_2 > \alpha_3$, les congruences modulo 4 donnent $p_1^2q_2^2q_3^2 \equiv p_2^2q_1^2q_3^2 \equiv 1\,[4]$ alors que
$$p_1^2q_2^2q_3^2 + p_2^2q_1^2q_3^2 = 4^{\alpha_1}\,q_1^2q_2^2q_3^2 - 4^{\alpha_1-\alpha_3}p_3^2q_1^2q_2^2 \equiv 0\,[4].$$

— Si $\alpha_1 = \alpha_2 = \alpha_3 > 0$, on aurait :
$$[4]\,3 \equiv p_1^2q_2^2q_3^2 + p_2^2q_1^2q_3^2 + p_3^2q_1^2q_2^2 = 4^{\alpha_1}\,q_1^2q_2^2q_3^2 \equiv 0\,[4].$$

Finalement, la seule possibilité compatible avec (1) est $0 > \alpha_1 \geq \alpha_2 \geq \alpha_3 = 0$ et donc x, y et z sont dans $\mathbb{Z}_2$. □

Intéressons nous maintenant au groupe $O_3(\mathbb{Q})$. Comme les colonnes d'une matrice orthogonale sont des vecteurs orthonormés, les 3 coefficients de chaque colonne vérifient donc $x^2 + y^2 + z^2 = 1$ avec $(x, y, z) \in \mathbb{Q}^3$. Le lemme 1 permet d'affirmer que
$$O_3(\mathbb{Q}) \subset GL_3(\mathbb{Z}_2). \tag{2}$$

Nous pouvons alors considérer les réductions modulo $\mathfrak{m}^r$:
$$\pi_r : GL_3(\mathbb{Z}_2) \longrightarrow GL_3(\mathbb{Z}_2/\mathfrak{m}^r) \simeq GL_3(\mathbb{Z}/2^r\mathbb{Z}).$$

Les noyaux $N_r := \mathrm{Ker}(\pi_r)$ sont donc des sous-groupes d'indice fini de $GL_3(\mathbb{Z}_2)$ et vérifiant de plus $N_{r+1} \subset N_r$. On peut donc considérer
$$\forall\, r \geq 1,\ G_r := O_3(\mathbb{Q}) \cap N_r \lhd O_3(\mathbb{Q}). \tag{3}$$

En d'autres termes, une matrice orthogonale $A \in O_3(\mathbb{Q})$ est dans G_r si et seulement si $A = I_3 + 2^rB$ avec $B \in M_3(\mathbb{Z}_2)$. La condition $A \in O_3(\mathbb{Q})$ se retranscrit alors :
$$B + {}^tB = -2^r({}^tBB) \tag{4}$$

ou encore :
$$\forall\, i, j = 1 \ldots 3,\ B_{i,j} + B_{j,i} = -2^r(B_{1,i}B_{1,j} + B_{2,i}B_{2,j} + B_{3,i}B_{3,j}). \tag{5}$$

Remarquons ici qu'il est évident que
$$\bigcap_{r\geq 1} G_r = \{1\}.$$

Nous allons en fait constater que les sous-groupes G_r forment une suite strictement décroissantes : ce sont donc des sous-groupes normaux stricts de $O_3(\mathbb{Q})$.

Théorème 2. *Les quotients successifs de la suite $(G_r)_{r\geq 1}$ de sous-groupes de $O_3(\mathbb{Q})$ est donnée par :*

(i) $O_3(\mathbb{Q})/G_1 \simeq S_3$ (*le groupe symétrique sur 3 éléments*),

(ii) $G_1/G_2 \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 4}$ *et*

(iii) $\forall\, r \geq 2,\ G_r/G_{r+1} \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 3}$.

De plus, pour $r \geq 2$, $G_r \subset SO_3(\mathbb{Q})$. *Ce groupe n'est donc pas simple.*

Démonstration. Commençons par montrer la dernière assertion. Si $A = I_3 + 4B$ avec $B \in M_3(\mathbb{Z}_2)$ alors, en développant le déterminant, on constate aisément que $\det(A) = 1 + 4x$ avec $x \in \mathbb{Z}_2$. L'éventualité $\det(A) = -1$ impliquerait $x = -\frac{1}{2}$ qui n'est pas un élément de $\mathbb{Z}_2$ et donc $\det(A) = 1$.

Pour étudier les quotients successifs, nous allons réduire modulo 2 les différentes matrices qui se présentent à nous. Pour le premier point, considérons $\overline{A}$ la réduction modulo 2 d'un élément de $O_3(\mathbb{Q})$: il s'agit d'un élément du groupe

$$O_3(\mathbb{Z}_2/2\mathbb{Z}) := \left\{ P \in M_3(\mathbb{Z}_2/2\mathbb{Z}) \mid {}^tPP = I_3 \right\}.$$

Éluçidons d'abord la structure de ce groupe : il est constitué de matrices P à coefficients dans $\mathbb{Z}/2\mathbb{Z}$ dont les lignes et les colonnes sont des vecteurs *de norme* 1, au sens où la somme des coefficients au carré vaut 1. Comme $x^2 = x$ dans $\mathbb{Z}/2\mathbb{Z}$, la somme des coefficients (en ligne ou en colonne) vaut donc 1 et il n'y a que deux configurations possibles : les trois coefficients valent 1 ou deux coefficients valent 0 et le dernier vaut 1. Supposons alors que la première colonne soit uniquement constituée de 1 :

$$P = \begin{pmatrix} 1 & * & * \\ 1 & * & * \\ 1 & * & * \end{pmatrix}.$$

Nous constatons aisément que cela implique que les $*$ valent tous 0 ou tous 1 : nous aurions alors $\mathrm{rg}(P) = 1$ ce qui n'est pas possible dans $O_3(\mathbb{Z}/2\mathbb{Z})$. La matrice P a donc un unique 1 dans chaque ligne et chaque colonne : cela définit une permutation sur 3 éléments et nous avons donc bien $O_3(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$. De plus, comme les matrices de permutation sont aussi des éléments de $O_3(\mathbb{Q})$, la réduction modulo 2 fournit un morphisme

$$\pi : \begin{cases} O_3(\mathbb{Q}) & \longrightarrow & O_3(\mathbb{Z}/2\mathbb{Z}) \\ A & \longmapsto & \overline{A} \end{cases}$$

surjectif et dont le noyau est par définition G_1. Le point (i) est donc établi.

Pour étudier les quotients G_r/G_{r+1}, nous considérons cette fois la réduction modulo 2 de la matrice B (venant de (4)). En réduisant modulo 2 l'équation (4), nous constatons immédiatement que $\overline{B}$ est antisymétrique (ou symétrique !) mais nous pouvons obtenir un peu plus. En effet, l'équation (5) pour $i = j$ devient :

$$B_{i,i} = -2^{r-1}(B_{1,i}^2 + B_{2,i}^2 + B_{3,i}^2). \tag{6}$$

En particulier, si $r = 1$, nous en déduisons (en utilisant à nouveau que $x^2 = x = -x$ dans $\mathbb{Z}/2Z$ et le fait que $\overline{B}$ est symétrique) :

$$\overline{B}_{1,2} = \overline{B}_{1,3} = \overline{B}_{2,3} = \overline{B}_{2,1} = \overline{B}_{3,1} = \overline{B}_{3,2}. \tag{7}$$

Le morphisme

$$\pi_1 : \begin{cases} G_1 & \longrightarrow & M_3(\mathbb{Z}/2\mathbb{Z}) \\ A & \longmapsto & \frac{1}{2}(A - I_3) \bmod 2 \end{cases}$$

est à valeurs dans l'espace des matrices dont les coefficients non diagonaux sont tous égaux. De plus, les matrices des réflexions par rapport aux plans de coordonnées sont de la forme :

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3 + 2 \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Ceci montre que les matrices diagonales sont dans l'image de π_1. De plus, la réflexion par rapport au plan d'équation $(x + y + z = 0)$ n'est autre que

$$R = \begin{pmatrix} \frac{1}{3} & -\frac{2}{3} & -\frac{2}{3} \\ -\frac{2}{3} & \frac{1}{3} & -\frac{2}{3} \\ -\frac{2}{3} & -\frac{2}{3} & \frac{1}{3} \end{pmatrix} = I_3 + 2 \begin{pmatrix} -\frac{1}{3} & -\frac{1}{3} & -\frac{1}{3} \\ -\frac{1}{3} & -\frac{1}{3} & -\frac{1}{3} \\ -\frac{1}{3} & -\frac{1}{3} & -\frac{1}{3} \end{pmatrix}$$

et il s'ensuit que

$$\pi_1(R) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

et finalement l'image de π_1 est engendré par les matrices diagonales et la matrice qui n'a que des 1 : c'est un espace de dimension 4 sur $\mathbb{Z}/2\mathbb{Z}$. Comme on a évidemment $\mathrm{Ker}(\pi_1) = G_2$, ceci conclut la démonstration du point (ii).

Dans le cas $r \geq 2$, la condition (5) montre que $\overline{B}_{i,i} = 0$ pour $i = 1$, 2 ou 3. L'image du morphisme

$$\pi_r : \begin{cases} G_r & \longrightarrow & M_3(\mathbb{Z}/2\mathbb{Z}) \\ A & \longmapsto & \frac{1}{2^r}(A - I_3) \bmod 2 \end{cases}$$

est donc contenue dans les matrices symétriques de diagonale nulle. Pour montrer l'égalité, il faut exhiber des éléments particuliers de G_r. Comme $r \geq 2$ et que $G_r \subset SO_3(\mathbb{Q})$, il faut chercher une rotation. Pour être sûr de trouver une rotation rationnelle, il est commode de la chercher sous la forme $u = \tau_1 \circ \tau_2$ avec τ_i des réflexions par rapport à des plans dont les équations sont à coefficients dans $\mathbb{Q}$. Nous choisissons alors (en suivant l'indication de D. Perrin) les réflexions engendrées par $e_1 = (1, 0, 0)$ et $e_2 = (1, 2^{r-1}, 0)$. Comme tout se passe dans le plan $(z = 0)$, les calculs ne font intervenir que les deux premières coordonnées. En se rappelant que la matrice d'une réflexion engendrée par le vecteur (a, b) est donnée par

$$\tau = \frac{1}{a^2 + b^2} \begin{pmatrix} -a^2 + b^2 & 2ab \\ 2ab & a^2 - bb^2 \end{pmatrix}$$

et en faisant le produit de ces deux matrices pour $(a, b) = (1, 0)$ et $(1, 2^{r-1})$, nous obtenons que la matrice de $u \in SO_3(\mathbb{Q})$ est :

$$u = \begin{pmatrix} 2\lambda - 1 & -2^r\lambda & 0 \\ 2^r\lambda & 2\lambda - 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

avec $\lambda = \frac{1}{1+2^{2r-2}}$ et donc que

$$u - I_3 = \begin{pmatrix} 2\lambda - 2 & -2^r\lambda & 0 \\ 2^r\lambda & 2\lambda - 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} = 2^r \begin{pmatrix} -\frac{2^{r-1}}{1+2^{2r-2}} & -\frac{1}{1+2^{2r-2}} & 0 \\ \frac{1}{1+2^{2r-2}} & -\frac{2^{r-1}}{1+2^{2r}} & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

En réduisant modulo 2, nous obtenons finalement :

$$\pi_r(u) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

En effectuant le même raisonnement pour les paires de vecteurs $\left\{(1,0,0),(1,0,2^{r-1}\right\}$ et $\left\{(0,1,0),(0,1,2^{r-1}\right\}$, nous en déduisons que toutes les matrices symétriques avec des zéros sur la diagonale sont dans l'image de π_r et cela conclut la démonstration. □

Références

[1] S. Francinou, H. Gianella et S. Nicolas, *Oraux X–ENS, algèbre*, volume 3, Cassini, 2008.

[2] D. Perrin, *Cours d'algèbre*, Ellipses, 1996.