Quadrature nº 136 (2025) 30-38

$SO_3(\mathbb{Q})$ contient un sous-groupe libre, à l'aide des nombres 5-adiques

par Maria TRASHORRAS

Résumé.

Une preuve du fait que $SO_3(\mathbb{Q})$ contient un sous-groupe libre à deux générateurs, en utilisant les nombres 5-adiques pour pouvoir observer une dynamique de ping-pong sur l'action de certaines matrices de $SO_3(\mathbb{Q})$ sur l'ensemble des droites de $\mathbb{Q}_5^3$.

I Introduction

Nous allons ici nous intéresser à un problème de théorie géométrique des groupes : on cherche dans $SO_3(\mathbb{Q})$ un sous-groupe libre à deux générateurs. L'existence d'un tel sous-groupe est en fait un cas particulier de l'alternative de Tits. Ce théorème est un résultat important de théorie géométrique des groupes, démontré par le mathématicien franco-belge Jacques Tits en 1972.

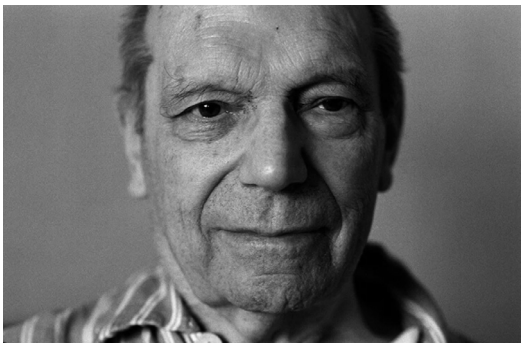

Figure 1. Jacques Tits (1930-2021).

Par ailleurs, l'existence d'un sous-groupe libre dans $SO_3(\mathbb{Q})$ est le point de départ d'une preuve d'une version faible du théorème de Banach-Tarski, dit « paradoxe de Banach-Tarski », qui affirme que la boule unité dans $\mathbb{R}^3$ est dédoublable. Notre résultat permet, lui, de montrer que la sphère unité est dédoublable, mais ce n'est pas l'objet de notre travail ici.

Nous nous appuierons sur une intuition géométrique assez simple de l'action des éléments de $SO_3(\mathbb{Q})$ diagonalisables dans $\mathbb{Q}_5$ avec une valeur propre de valeur absolue 5-adique strictement inférieure à 1. En effet, sous réserve de prouver l'existence de telles matrices, on observe alors une dynamique de ping-pong. Par ailleurs, de telles matrices ne peuvent se trouver qu'en se plaçant dans une extension de $\mathbb{Q}$. Les corps $\mathbb{R}$ et $\mathbb{C}$ ne conviennent pas puisque les rotations qui y sont diagonalisables ont des valeurs propres de module 1. On choisira donc de se placer dans un corps p-adique bien choisi.

Nous allons donc d'abord étudier une construction des anneaux puis des corps p-adiques. Nous reviendrons ensuite brièvement sur la notion de groupe libre, et notamment le lemme du ping-pong, avant de montrer que $SO_3(\mathbb{Q})$ contient bien un sous-groupe libre, selon une preuve qui suit notre intuition initiale.

II L'anneau des entiers p-adiques $\mathbb{Z}_p$

II.1 Construction et structure de $\mathbb{Z}_p$

Soit p un nombre premier quelconque.

La construction de $\mathbb{Z}_p$ suit celle proposée ici [1], à part les preuves de certains résultats, où la référence sera précisée.

Définition 1. *On définit $\mathbb{Z}_p$ comme l'ensemble des suites $(a_n)_{n\geqslant 0}$ vérifiant :*

▷ *pour tout* $n \in \mathbb{N}$, $a_n \in [\![0, p^{n+1}-1]\!]$;
▷ *pour tout* $n \in \mathbb{N}$, $a_{n+1} \equiv a_n \mod p^{n+1}$.

Proposition 2. *Pour tout* $a = (a_n)_{n\geqslant 0} \in \mathbb{Z}_p$, *il existe une unique suite* $(u_k)_{k\geqslant 0} \in [\![0, p-1]\!]^{\mathbb{N}}$ *telle que pour tout* $n \in \mathbb{N}$, $a_n = \sum_{k=0}^{n} u_k p^k$. *Réciproquement, pour tout* $(u_k)_{k\geqslant 0} \in [\![0, p-1]\!]^{\mathbb{N}}$, *la suite* $(a_n)_{n\geqslant 0} = (\sum_{k=0}^{n} u_k p^k)_{n\geqslant 0}$ *appartient à* $\mathbb{Z}_p$. *On appellera la suite* $(u_n)_{n\geqslant 0}$ *le développement de Hensel du nombre a.*

Démonstration. Soit $a = (a_n)_{n\geqslant 0} \in \mathbb{Z}_p$. On construit par récurrence la suite désirée.

▷ $n = 0$. $a_0 \in [\![0, p-1]\!]$, donc on a nécessairement $u_0 = a_0$.

▷ Soit $n \in \mathbb{N}$. Supposons construits $u_0, u_1, ..., u_n$. On a $a_{n+1} \equiv a_n \mod p^{n+1}$. Par théorème de la division euclidienne, il existe un unique $u_{n+1} \in \mathbb{N}$ tel que $a_{n+1} = u_{n+1}p^{n+1} + a_n$. De plus, $a_{n+1} \in [\![0, p^{n+1}]\!]$, et $a_n \leqslant a_{n+1}$. Donc $u_{n+1} = \frac{a_{n+1}-a_n}{p^{n+1}} \in [\![0, p-1]\!]$, et $a_{n+1} = \sum_{k=0}^{n+1} u_k p^k$ par hypothèse de récurrence. La récurrence est concluante.

▷ Réciproquement, soit $(u_k)_{k\geqslant 0} \in [\![0, p-1]\!]^{\mathbb{N}}$. Posons, pour tout $n \in \mathbb{N}$, $a_n = \sum_{k=0}^{n} u_k p^k$. Il est clair que pour tout $n \in \mathbb{N}$, $a_{n+1} \equiv a_n \mod p^{n+1}$, et que $a_n \in [\![0, p^{n+1}-1]\!]$. Donc $(a_n)_{n\geqslant 0} \in \mathbb{Z}_p$. □

Proposition 3. *On peut munir* $\mathbb{Z}_p$ *d'une structure d'anneau :*

▷ *Pour* $a = (a_n)_{n\geqslant 0}$ *et* $b = (b_n)_{n\geqslant 0}$ *dans* $\mathbb{Z}_p$, *pour tout* $n \in \mathbb{N}$, *on note* c_n *le reste de la division euclidienne de* $a_n + b_n$ *par* p^{n+1}. *La suite* $c = (c_n)_{n\geqslant 0}$ *est un élément de* $\mathbb{Z}_p$, *et on note* $a + b = c$, *ce qui définit une loi de composition interne* $+$ *sur* $\mathbb{Z}_p$. *On montre alors que* $(\mathbb{Z}_p, +)$ *est un groupe commutatif.*

▷ *Pour* $a = (a_n)_{n\geqslant 0}$ *et* $b = (b_n)_{n\geqslant 0}$ *dans* $\mathbb{Z}_p$, *pour tout* $n \in \mathbb{N}$, *on note* d_n *le reste de la division euclidienne de* $a_n \cdot b_n$ *par* p^{n+1}. *La suite* $d = (d_n)_{n\geqslant 0}$ *est un élément de* $\mathbb{Z}_p$, *et on note* $a \cdot b = d$, *ce qui définit une loi de composition interne commutative* $\cdot$ *sur* $\mathbb{Z}_p$. *On montre alors que* $(\mathbb{Z}_p, +, \cdot)$ *est un anneau commutatif.*

Proposition 4. *Il existe un morphisme injectif d'anneaux* $\theta : \mathbb{Z} \to \mathbb{Z}_p$.

Démonstration. Soit $x \in \mathbb{Z}$. Pour tout $n \in \mathbb{N}$, on pose x_n le reste de la division euclidienne de x par p^{n+1}. On montre d'abord que la suite $(x_n)_{n\geqslant 0}$ est un élément de $\mathbb{Z}_p$. On pose ensuite θ l'application qui à $x \in \mathbb{Z}$ associe la suite $\theta(x) = (x_n)_{n\geqslant 0}$. On montre que θ est un morphisme d'anneau en utilisant la définition de la somme et du produit dans $\mathbb{Z}_p$.

▷ Montrons que la suite ainsi définie est un élément de $\mathbb{Z}_p$. Il est clair que pour tout $n \in \mathbb{N}$, $x_n \in [\![0, p-1]\!]$. De plus, pour $n \in \mathbb{N}$, il existe $q, l \in \mathbb{Z}$ tels que $x = qp^{n+2} + x_{n+1} = lp^{n+1} + x_n$, d'où $x_{n+1} = p^{n+1}(l - pq) + x_n$, donc $x_{n+1} \equiv x_n \mod p^{n+1}$.

▷ Montrons que θ est un morphisme injectif.

En effet, par définition de la somme et du produit dans $\mathbb{Z}_p$, il est clair que θ est un morphisme d'anneaux. Pour l'injectivité, prenons $x, x' \in \mathbb{Z}$ tels que $\theta(x) = \theta(x')$. Soit $n_o \in \mathbb{N}$ tel que p^{n_0} est plus grand que $\max(|x|, |x'|)$. Soit $n \geqslant n_0$. Si x et x' sont positifs, on a $\theta(x)_n = x$ et $\theta(x')_n = x'$, d'où $x = x'$. Si $x \geqslant 0$ et $x' < 0$, on a $\theta(x)_n = x$ et $\theta(x')_n = p^{n+1} + x'$, donc $x = p^{n+1} + x'$ pour tout $n \geqslant n_0$, ce qui est impossible. On traite de même les deux derniers cas. Donc θ est injective. □

Par la suite, dans $\mathbb{Z}_p$, on notera $\mathbb{Z}$ à la place de $\theta(\mathbb{Z})$ pour alléger les notations.

II.2 Valeur absolue p-adique

On suivra ici, à peu de choses près, les travaux d'Yvette Amice [2].

Définition 5 (Valuation p-adique). *Pour tout* $a = (a_n)_{n\geqslant 0} \in \mathbb{Z}_p \setminus \{0\}$, *on définit la valuation p-adique de a comme* $v_p(a) = min\{n \in \mathbb{N} \, tel \, que \, a_n \neq 0\}$ *et on pose* $v_p(0) = +\infty$.

Remarque 6. *Pour tout* $a = (a_n)_{n\geqslant 0} \in \mathbb{Z}_p$, *en écrivant pour tout* $n \in \mathbb{N}$, $a_n = \sum_{k=0}^{n} u_k p^k$ *(proposition 1), cela revient à poser* $v_p(a) = min\{k \in \mathbb{N} \, tel \, que \, u_k \neq 0\}$.

Remarque 7. *Pour tout* $z \in \mathbb{Z}$, $v_p(\theta(z)) = v_p(z)$, *où* $v_p(z)$ *est la valuation p-adique usuelle de* $\mathbb{Z}$.

Proposition 8. *La valuation p-adique vérifie les propriétés suivantes :*

▷ *pour tout* $x \in \mathbb{Z}_p$, $v_p(x) = +\infty$ *si et seulement si* $x = 0$;

▷ *pour tous* $x, y \in \mathbb{Z}_p$, $v_p(x \cdot y) = v_p(x) + v_p(y)$;

▷ *pour tous* $x, y \in \mathbb{Z}_p$, $v_p(x + y) \geqslant min\{v_p(x), v_p(y)\}$, *et si* $v_p(x) \neq v_p(y)$, *alors* $v_p(x+y) = min\{v_p(x), v_p(y)\}$.

Démonstration. Le premier et le dernier point sont évidents par définition de la valuation p-adique et de la somme dans $\mathbb{Z}_p$. Pour montrer le second point, on utilise le fait que, pour $x = (x_i)_{i\geqslant 0}, y = (y_i)_{i\geqslant 0} \in \mathbb{Z}_p$, en posant $h = v_p(x)$ et $k = v_p(y)$, on a que $xy = x'y'p^{h+k}$ avec $x', y' \in \mathbb{Z}_p$ vérifiant $v_p(x') = v_p(y') = 0$. On a alors, en utilisant la définition de la valuation p-adique, que $v_p(xy) = v_p(x) + v_p(y)$. □

Remarque 9. *On remarque que* $\mathbb{Z}_p$ *est intègre.*

Définition 10 (Valeur absolue). *Une valeur absolue sur un anneau A est une application* $|.| : A \to \mathbb{R}_+$ *telle que :*

▷ *pour tout* x *dans* A, $|x| = 0 \implies x = 0$;
▷ *pour tout (x, y) dans* A^2, $|xy| = |x|\,|y|$;
▷ *pour tout* (x, y) *dans* A^2, $|x + y| \leq |x| + |y|$.

Si, de plus, pour tout $(x,y) \in A^2$, $|x+y| \leqslant \max\{|x|,|y|\}$, *cette valeur absolue est dite ultramétrique, ou non-archimédienne.*

Un corps K muni d'une valeur absolue $|\cdot|$ *est appelé un corps valué.*

Définition 11 (Valeur absolue p-adique)**.** *On définit la valeur absolue p-adique* $|.|_p : \mathbb{Z}_p \to \mathbb{R}_+$ *ainsi : pour tout* $a \in \mathbb{Z}_p$, $|a|_p = p^{-v_p(a)}$, *en considérant que* $p^{-\infty} = 0$.

Proposition 12. *La valeur absolue p-adique est une valeur absolue ultramétrique.*

Démonstration. Tout découle de la proposition **8**, et le fait que la valeur absolue p-adique soit ultramétrique entraîne l'inégalité triangulaire. □

Le diagramme ci-dessous montre les segments initiaux des éléments de $\mathbb{Z}_3$. Les entiers 3-adiques sont la continuation infinie de cet arbre vers la gauche. La valuation p-adique de la différence entre deux entiers 3-adiques est déterminée par la longueur de la branche de leur premier ancêtre commun. Plus cette branche est longue, plus les nombres sont proches.

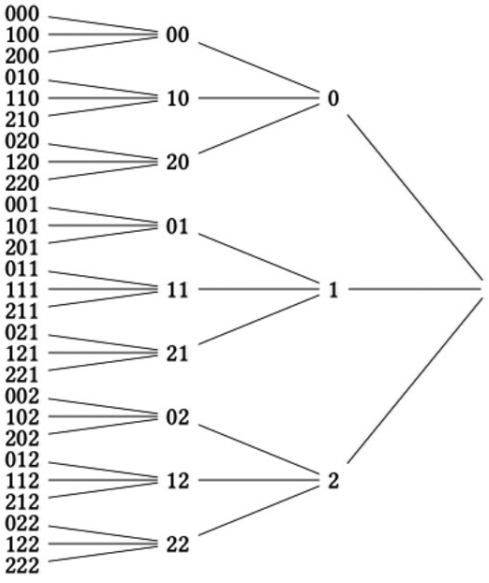

Figure 2. Représentation des nombres 3-adiques, tirée de [6].

Le dessin suivant donne une autre idée de comment « voir » les entiers 3-adiques. Chaque cercle contient trois sous-cercles principaux. Les entiers à l'intérieur d'un sous-cercle d'un cercle donné ont une distance 3-adique particulière par rapport aux entiers d'un autre sous-cercle de ce cercle. La valuation 3-adique de la différence entre deux nombres correspond au nombre de cercles qui contiennent les deux nombres considérés. Bien qu'il n'y ait pas de cercles plus grands que celui qui contient tous les autres pour $\mathbb{Z}_3$, les cercles peuvent devenir infiniment petits, car nous pouvons choisir des nombres qui diffèrent par des puissances de 3 de plus en plus grandes. De cette façon, les entiers p-adiques ne sont pas discrets même s'ils sont déconnectés. Par conséquent, une bonne image des entiers p-adiques serait de type fractal, comme l'est cette représentation avec des cercles.

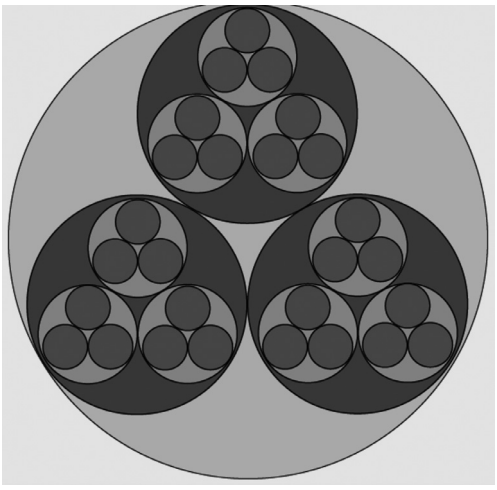

Figure 3. Visualisation des nombres 3-adiques, tirée de [8].

On trouvera plus de dessins pour visualiser ces nombres sur la page de Gérard Villemin [7].

Proposition 13. *L'ensemble des éléments inversibles de* $\mathbb{Z}_p$ *est* $\{x \in \mathbb{Z}_p \,||x|_p = 1\}$.

Démonstration. On suivra ici la démonstration proposée en [1].

Soit $a \in \mathbb{Z}_p$. Il suffit de montrer que a est inversible si et seulement si $a_0 \neq 0$. Le sens direct est clair. Supposons donc que $a_0 \neq 0$. Alors $\bar{a}_0$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$. Soit $\bar{b}_0$ un inverse de $\bar{a}_0$ tel que b_0 dans $[\![0, p-1]\!]$. On peut ensuite construire une suite $b = (b_n)_{n\geqslant 0} \in \mathbb{Z}_p$, inverse de a, par récurrence sur $n \in \mathbb{N}$. □

Exemple 14. *Dans* $\mathbb{Z}_3$, *cherchons l'inverse du nombre* $X = (0,1,7,16,70...)$, *qui s'écrit avec l'écriture sous forme de développement de Hensel* $X = (1,2,1,2,1...)$, *ou encore* $X = \ldots 212121$ *lorsque nous voulons imiter l'écriture décimale, comme dans le dessin après la proposition* **2**. *Pour cela, on pose la multiplication, comme dans les petites classes, en écrivant le nombre sous sa dernière forme et on trouve l'inverse de X, qui est* $X^{-1} = \ldots 10211$. *Pour la facilité de la lecture, nous avons mis deux étapes de la multiplication posée.*

$$
\begin{array}{cccccccc}
 & \cdots & 2 & 1 & 2 & 1 & 2 & 1 \\
\times & \cdots & \star & \star & \star & 2 & 1 & 1 \\
\hline
 & \cdots & 2 & 1 & 2 & 1 & 2 & 1 \\
 & \cdots & 1 & 2 & 1 & 2 & 1 & \\
 & \cdots & 2 & 0 & 1 & 2 & & \\
 & \cdots & \star & \star & \star & & & \\
 & \cdots & \star & \star & & & & \\
\hline
 & \cdots & 0 & 0 & 0 & 0 & 0 & 1
\end{array}
\quad \rightsquigarrow \quad
\begin{array}{cccccccc}
 & \cdots & 2 & 1 & 2 & 1 & 2 & 1 \\
\times & \cdots & \star & 1 & 0 & 2 & 1 & 1 \\
\hline
 & \cdots & 2 & 1 & 2 & 1 & 2 & 1 \\
 & \cdots & 1 & 2 & 1 & 2 & 1 & \\
 & \cdots & 2 & 0 & 1 & 2 & & \\
 & \cdots & 0 & 0 & 0 & & & \\
 & \cdots & 2 & 1 & & & & \\
\hline
 & \cdots & 0 & 0 & 0 & 0 & 0 & 1
\end{array}
$$

II.3 Le développement de Hensel

Nous reprenons les notations de la proposition **2**.

Maintenant que nous avons introduit des notions de topologie, nous pouvons donner plus de sens au développement de Hensel à travers la proposition suivante, en suivant la démonstration proposée en [4].

Proposition 15. *Pour tout $a \in \mathbb{Z}_p$, la série de terme général $(u_k p^k)_{k\geqslant 0}$ converge vers a dans $\mathbb{Z}_p$.*

Démonstration. Soit $\varepsilon > 0$, il existe $n_0 \in \mathbb{N}$ tel que $p^{-n_0} \leqslant \varepsilon$. En posant $a_n = \sum_{k=0}^{n} u_k p^k$ pour tout $n \in \mathbb{N}$, on a que, pour tout $n \geqslant n_0$, $v_p(\theta(a_n) - a) \geqslant n \geqslant n_0$, donc $|\theta(a_n) - a|_p \leqslant p^{-n_0} \leqslant \varepsilon$. Donc la série de terme général $(u_k p^k)_{k\geqslant 0}$ converge vers a dans $\mathbb{Z}_p$. □

Ce résultat donne une intuition de pourquoi $\mathbb{Q}_p$ peut aussi être construit comme le complété de $\mathbb{Q}$ pour la valeur absolue p-adique.

III Le corps des nombres p-adiques $\mathbb{Q}_p$

III.1 Construction de $\mathbb{Q}_p$

Soit p un nombre premier. On construit $\mathbb{Q}_p$ comme le corps des fractions de l'anneau intègre $\mathbb{Z}_p$.

Proposition 16 ($\mathbb{Q}$ se plonge dans $\mathbb{Q}_p$)**.** *Il existe un morphisme injectif de corps $\Theta : \mathbb{Q} \to \mathbb{Q}_p$.*

On suivra ici la démonstration proposée en [1].

Démonstration. Posons $\Theta : \mathbb{Q} \to \mathbb{Q}_p$ qui à $\frac{a}{b}$ associe la classe d'équivalence de $(\theta(a), \theta(b))$, avec θ l'application définie à la proposition **13**. Montrons que Θ est bien définie. Si $\frac{a}{b} = \frac{c}{d}$ avec $(a,c) \in \mathbb{Z}^2$ et $(b,d) \in (\mathbb{Z}\backslash\{0\})^2$, alors $ad = bc$, donc $\theta(a)\theta(d) = \theta(ad) = \theta(bc) = \theta(b)\theta(c)$. Donc $(\theta(a), \theta(b))$ et $(\theta(c), \theta(d))$ sont dans la même classe d'équivalence dans $\mathbb{Q}_p$. Donc Θ est bien défini. On montre que c'est un morphisme d'anneaux en utilisant que θ en est un, et qu'il est injectif par injectivité de θ (proposition **4**). □

III.2 Valeur absolue p-adique dans $\mathbb{Q}_p$

On suivra ici les travaux d'Yvette Amice [2].

Définition 17 (Valuation p-adique dans $\mathbb{Q}_p$)**.** *Pour tout $x = \frac{a}{b} \in \mathbb{Q}_p$, avec $(a,b) \in \mathbb{Z}_p \times (\mathbb{Z}_p\backslash\{0\})$, on définit $v_p(x) = v_p(a) - v_p(b)$.*

Cette application est bien définie : si $\frac{a}{b} = \frac{c}{d}$ avec $(a,b),(c,d) \in \mathbb{Z}_p \times (\mathbb{Z}_p\backslash\{0\})$. On a $ad = bc$ donc d'après la proposition **8**, $v_p(a) + v_p(d) = v_p(b) + v_p(c)$, donc $v_p(\frac{a}{b}) = v_p(\frac{c}{d})$.

Définition 18 (Valeur absolue p-adique)**.** *On définit la valeur absolue p-adique $|\cdot|_p : \mathbb{Q}_p \to \mathbb{R}_+$ en posant pour tout $a \in \mathbb{Q}_p$, $|a|_p = p^{-v_p(a)}$.*

Démonstration. La valuation p-adique vérifie toutes les propriétés de la proposition **8**. Par conséquent $|.|_p$ est une valeur absolue. □

Proposition 19 (Développement de Hensel)**.** *Tout élément $x \in \mathbb{Q}_p$ peut s'écrire sous la forme $x = \sum_{k=n_0}^{+\infty} u_k p^k$ avec $n_0 = v_p(x)$.*

On montre d'abord un lemme :

Lemme 20. *Pour tout $x \in \mathbb{Q}_p$, il existe un unique couple $(\alpha, u) \in \mathbb{Z} \times ({\mathbb{Z}_p}^{\times})$ tel que $x = p^{\alpha} u$, avec $\alpha = v_p(x)$.*

Démonstration. Soit $x = \frac{a}{b} \in \mathbb{Q}_p$ avec $a, b \in \mathbb{Z}_p$. Comme montré à la preuve de la proposition **4**, et grâce à la caractérisation des inversibles de $\mathbb{Z}_p$ établie à la proposition **16**, en posant $h = v_p(a)$ et $k = v_p(b)$, on obtient $a', b' \in {\mathbb{Z}_p}^{\times}$ tels que $a = p^h a'$ et $b = p^k b'$. Par construction de $\mathbb{Q}_p$, $x = p^{h-k} a' b'^{-1}$. On a donc l'existence. Si on avait $p^n u = p^m v$ avec $n, m \in \mathbb{Z}$ et $u, v \in {\mathbb{Z}_p}^{\times}$, on aurait $p^{n-m} = vu^{-1}$, donc $n - m = 0$, et $u = v$. On a donc aussi l'unicité. □

On peut maintenant prouver la proposition **19** :

Démonstration. Soit $x \in \mathbb{Q}_p$, il existe un unique couple $(n_0, u) \in \mathbb{Z} \times ({\mathbb{Z}_p}^{\times})$ tel que $x = p^{n_0} u$. D'après la proposition **15**, il existe une unique suite $(u_k)_{k\geqslant 0} \in [\![0, p-1]\!]^{\mathbb{N}}$ telle que $u = \sum_{k=0}^{+\infty} u'_k p^k$. Donc $x = \sum_{k=n_0}^{+\infty} u'_{k-n_0} p^k$. En posant ensuite pour tout $k \geqslant n_0$, $u_k = u'_{k-n_0}$, on obtient le développement désiré. □

Proposition 21. *Le corps $(\mathbb{Q}_p, |\cdot|_p)$ est complet.*

Démonstration. On suivra ici la démonstration de Svetlana Katok [4]. Soit $(a_k)_{k\geqslant 0}$ une suite de Cauchy de $\mathbb{Q}_p$. La suite $(a_n)_{n\geqslant 0}$ est de Cauchy donc bornée, donc il existe $n_0 \in \mathbb{Z}$ tel que pour tout $k \in \mathbb{N}$, $v_p(a_k) \geqslant n_0$. Donc pour tout $k \geqslant 0$, $a_k = \sum_{i=n_0}^{+\infty} u_i^{(k)} p^i$, d'après la proposition **19**. Soit $i \geqslant n_0$. La suite $(a_k)_{k\geqslant 0}$ est une suite de Cauchy, donc il existe k assez grand

pour que $v_p(a_k - a_{k+1}) \geqslant i+1$, donc $u_i^{(k)} = u_i^{(k+1)}$, donc pour tout $i \geqslant n_0$ la suite $(u_i^{(k)})_{k\geqslant 0}$ est stationnaire à la valeur u_i. Posons $a = \sum_{i\geqslant n_0} u_i p^i$. Soit $n \in \mathbb{N}, n \geqslant n_0$. Pour k assez grand, pour tout $i \leqslant n, u_i^{(k)} = u_i$, donc pour k assez grand, $v_p(a - a_k) \geqslant n$. □

Remarque 22. *On peut aussi montrer que $(\mathbb{Z}_p, |\cdot|_p)$ est complet, voir [1], question 47.*

Remarque 23. *À la différence avec l'anaylse réelle, dans $\mathbb{Q}_p$, une série est convergente, si, et seulement si, son terme général tend vers 0, voir [1], question 48.*

IV Application : $SO_3(\mathbb{Q})$ contient un sous-groupe libre

IV.1 Groupes libres et lemme du ping-pong

Nous suivrons ici la présentation proposée par J.S. Milne [5].

Définition 24 (Groupe libre). *Soit X un ensemble. Le groupe libre sur X, noté G, est le groupe formé des mots réduits sur $X \cup X^{-1}$, c'est-à-dire les mots sans facteur de la forme xx^{-1} .*

Plus précisément, on pose $X^{-1} := \{x^{-1}, x \in X\}$ un ensemble de symboles. On considère l'ensemble des mots sur $X \cup X^{-1}$ que l'on munit de l'opération de concaténation et de la classe d'équivalence suivante : deux mots w_1 et w_2 sont équivalents s'il existe une suite finie d'opérations élémentaires permettant de passer de w_1 à w_2. Une opération élémentaire est la suppression ou l'ajout de xx^{-1} dans un mot.

On peut montrer que l'ensemble des mots sur $X \cup X^{-1}$ quotienté par cette relation d'équivalence forme un groupe dont le mot vide est l'élément neutre, et que chaque classe d'équivalence admet un unique représentant ne contenant pas de facteur de la forme xx^{-1}. On appellera un tel représentant un mot réduit.

On remarque que X s'injecte canoniquement dans G, et on peut donc considérer que X est une partie génératrice de G.

Un groupe G est dit libre s'il existe $X \in G$ tel que G soit le groupe libre sur X.

On se donne $n \in \mathbb{N}^*$ et K un corps.

Nous utilisons ici la version du lemme du ping-pong proposée par Thomas Haettel [3].

Lemme 25 (Lemme du ping-pong). *Soit Γ un sous-groupe de $GL_n(K)$ engendré par deux éléments a et b. Supposons qu'il existe deux parties disjointes non-vides K_1 et K_2 de K^n telles que $\forall m \in \mathbb{Z}\backslash\{0\}$, $a^m \cdot K_2 \subset K_1$ et $b^m \cdot K_1 \subset K_2$. Alors Γ est libre de base $\{a,b\}$.*

Démonstration. Par l'absurde, supposons qu'il existe ω dans le groupe libre engendré par $\{a,b\}$ tel que ω vu dans Γ vaille 1. Alors ω admet une certaine écriture comme produit de a et de b. Si cette écriture commence et finit par le même élément, il n'est pas restrictif de supposer que ω commence et finit par a. On peut écrire $\omega = a^{n_1} b^{m_1} \ldots b^{m_p} a^{n_{p+1}}$. On choisit $x \in K_2$, ce qui nous donne que $\omega \cdot x \in K_1$, ce qui est absurde, car ω vu dans Γ vaut 1. Sinon, en conjuguant par une certaine puissance de a ou de b le mot ω, on se ramène à la situation précédente. □

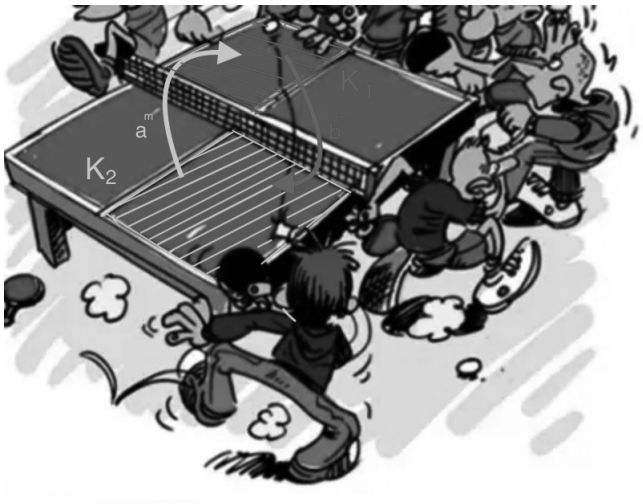

Figure 4. Pour s'amuser un peu avec ce lemme.

IV.2 $SO_3(\mathbb{Q})$ contient un sous-groupe libre

Cette dernière partie est entièrement personnelle et constitue le coeur de mon travail.

On pose $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{3}{5} & -\frac{4}{5} \\ 0 & \frac{4}{5} & \frac{3}{5} \end{pmatrix}$.

On a que $\chi_A = (X-1)(X^2 - \frac{6}{5}X + 1)$, et $A \in SO_3(\mathbb{Q})$.

La matrice A est l'une des matrices de $SO_3(\mathbb{Q})$ les plus simples auxquelles on puisse penser, puisqu'on connaît exactement les matrices de $SO_3(\mathbb{R})$, donc à fortiori les matrices de $SO_3(\mathbb{Q})$, et que $(3,4,5)$ est le triplet pythagoricien le plus élémentaire.

Montrons que ce polynôme admet des racines dans $\mathbb{Q}_5$. En fait, on remarque que ses racines complexes sont $\frac{3+4i}{5}$ et $\frac{3-4i}{5}$, il suffit donc de montrer que -1 admet une racine dans $\mathbb{Q}_5$. En effet, dans ce cas, en regardant χ_A comme un polynôme à coefficients dans $\mathbb{Q}_5$, il est scindé à racines simples et donc diagonalisable.

Proposition 26. *Il existe $l \in \mathbb{Q}_5$ tel que $l^2 = -1$.*

Ce résultat est une conséquence du lemme d'Hensel dont on pourra trouver la démonstration à [4].

Démonstration. On imite ici la méthode de Newton [1]. On pose $x_0 = 2 \in \mathbb{Z}_5^\times$, et une suite $(x_n)_{n\geqslant 0} \in \mathbb{Z}_5$ définie par $x_{n+1} = \frac{1}{2}(x_n - \frac{1}{x_n})$ pour tout $n \in \mathbb{N}$. Si on arrive à montrer que cette suite converge vers $l \in \mathbb{Q}_5$, on aura alors, d'après la relation de récurrence, que $l^2 = -1$. Montrons que la suite $(x_n)_{n\geqslant 0}$ est une suite de Cauchy. On montre par récurrence que pour tout $n \in \mathbb{N}, v_5(x_n) = 0$ et $v_5(x_{n+1} - x_n) = 2^n$. Cette propriété entraînera aisément que la suite $(x_n)_{n\geqslant 0}$ est de Cauchy. Le corps $\mathbb{Q}_5$ étant complet, on aura bien le résultat souhaité.

Pour l'initialisation, on calcule les premiers termes de la suite $(x_n)_{n\geq 0}$. On a $x_0 = 2, x_1 = \frac{3}{4}$, donc on a bien $v_5(x_0) = 0$ et $v_5(x_1 - x_0) = v_5(-\frac{5}{4}) = 1$. La récurrence est ainsi initialisée.

Soit $n \in \mathbb{N}$. Supposons que $v_5(x_n) = 0$ et $v_5(x_{n+1} - x_n) = 2^n$. On a $x_{n+2} - x_{n+1} = \frac{(x_n^2+1)^2}{2x_n(x_n^2-1)}$ et $x_{n+1} - x_n = \frac{-(x_n^2+1)}{2x_n}$, donc par hypothèse de récurrence, $v_5(x_n^2 + 1) = v_5(\frac{x_n^2+1}{x_n}) = 2^n$, d'où $v_5(x_{n+2} - x_{n+1}) = v_5(\frac{(x_n^2+1)^2}{2x_n(x_n^2-1)}) = 2v_5(x_n^2 + 1) - v_5(x_n^2 - 1)$ car $v_5(x_n) = 0$ par hypothèse de récurrence.

Posons $x_n^2 - 1 = 5^{s'}\frac{\alpha'}{\beta'}$ avec $\alpha', \beta' \in \mathbb{Z}$, non divisibles par 5. Comme $x_n^2 + 1 = 5^s\frac{\alpha}{\beta}$ avec $s \geq 1$ et $\alpha,\ \beta \in \mathbb{Z}$, non divisibles par 5, on obtient [2]

$$\begin{aligned} 2 = x_n^2 + 1 - (x_n^2 - 1) &= 5^{s'}(5^{s-s'}\frac{\alpha}{\beta} - \frac{\alpha'}{\beta'}) \\ &= 5^{s'}(\frac{5^{s-s'}\alpha\beta' - \beta\alpha'}{\beta\beta'}), \end{aligned}$$

donc $2\beta\beta' = 5^{s'}(5^{s-s'}\alpha\beta' - \beta\alpha')$, ce qui n'est possible que si $s' = 0$. En effet, si $s' > 0$, on a que 5 divise $2\beta\beta'$, et si $s' < 0$, on a que 5 divise $\beta\alpha'$ puisque dans ce cas $s - s' > 0$. Donc $v_5(x_{n+2} - x_{n+1}) = 2v_5(x_n^2 + 1) = 2^{n+1}$.

Par ailleurs, $v_5(x_{n+1}) = v_5(\frac{x_n^2-1}{x_n}) = v_5(x_n^2 - 1) - v_5(x_n) = 0$. La récurrence est concluante, on a donc bien $l \in \mathbb{Q}_5$ tel que $l^2 = -1$. On voit dans la preuve que pour tout n, $x_n \in \mathbb{Z}_5$, et puisque $\mathbb{Z}_5$ est aussi complet, on a même $l \in \mathbb{Z}_5$. □

Remarquons que $|2-l|_5|2+l|_5 = |5|_5 = \frac{1}{5}$. Fixons alors α la racine de -1 dans $\mathbb{Z}_5$ qui vérifie [3] $|2-\alpha| < 1$. Alors $|2-\alpha| = \frac{1}{5}$ et $|2+\alpha| = 1$ puisque $2 \pm \alpha \in \mathbb{Z}_5$. En posant $\lambda = \frac{3+4\alpha}{5} = \frac{2+\alpha}{2-\alpha}$, on a que $|\lambda| = 5$ et $\lambda^{-1} = \frac{3-4\alpha}{5} = \frac{2-\alpha}{2+\alpha}$, avec $|\lambda^{-1}| = \frac{1}{5}$.

1. Il s'agit d'approximer une racine de la fonction $f(x) = x^2 + 1$ en prenant la limite de la suite définie par $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} = x_n - \frac{x_n^2+1}{2x_n}$.

2. Si $s \geq s'$, sinon on écrit $-2 = x_n^2 - 1 - (x_n^2 + 1)$ et on poursuit de manière analogue.

3. Pour alléger les notations, on omettra d'indiquer à chaque fois le 5 dans la valeur absolue 5-adique.

C'est là le point-clé de la preuve : le fait que la valeur absolue de la valeur propre soit strictement supérieure à 1 est ce qui cause la dynamique de ping-pong que nous allons étudier. C'est pour arriver à ce résultat que nous nous sommes placés dans $\mathbb{Q}_5$, puisqu'en se plaçant dans $\mathbb{C}$, on aurait eu une valeur propre de valeur absolue 1.

Les racines de χ_A sont 1, λ et λ^{-1}, et donc χ_A est scindé à racines simples sur $\mathbb{Q}_5$. Cela signifie que A est diagonalisable dans $\mathscr{M}_3(\mathbb{Q}_5)$.

Notons e_1, v_A et u_A des vecteurs propres (de $\mathbb{Q}_5^3$) correspondant aux valeurs propres 1, λ et λ^{-1}. On a (pour la base canonique (e_1, e_2, e_3) de $\mathbb{Q}_5^3$) que v_A et u_A appartiennent au plan P_{23} engendré par e_2 et e_3.

Soit maintenant $B = \begin{pmatrix} \frac{3}{5} & -\frac{4}{5} & 0 \\ \frac{4}{5} & \frac{3}{5} & 0 \\ 0 & 0 & 1 \end{pmatrix}$. On a en fait choisi une matrice conjuguée à la matrice A, par une matrice de permutation des axes de coordonnées. Cela permet de s'économiser des calculs, puisque l'action de B sur les droites de $\mathbb{Q}_5^3$ sera donc la même que celle de A, mais « décalée ». La matrice B a donc les mêmes valeurs propres que A, et des vecteurs propres v_B, u_B et e_3 correspondant aux valeurs propres λ, λ^{-1} et 1, avec v_B et u_B qui appartiennent au plan P_{12} engendré par e_1 et e_2. Comme P_{23} et P_{12} se coupent en la droite engendrée par e_2, nécessairement les droites engendrées par v_A, u_A, v_B et u_B sont distinctes.

Du fait de la position relative dans $\mathbb{Q}_5^3$ des droites propres des matrices A et B, on peut observer dans l'action de A et de B sur l'ensemble des droites de $\mathbb{Q}_5^3$ une dynamique de ping-pong. Plus précisément, quitte à caractériser ces ensembles de manière confortable, ce que nous ferons plus tard, on peut remarquer qu'une puissance « assez grande » (en valeur absolue) de A envoie (pour une puissance positive) toutes les droites de $\mathbb{Q}_5^3$ qui ne sont pas dans le plan P_{1u_A} engendré par e_1 et u_A vers la droite D_{v_A} dirigée par v_A, et (pour une puissance négative) toutes les droites de $\mathbb{Q}_5^3$ qui ne sont pas dans le plan P_{1v_A} engendré par e_1 et v_A vers la droite D_{u_A} dirigée par u_A. De même l'application d'une puissance « assez grande » (en valeur absolue) de B envoie (pour une puissance positive) toutes les droites de $\mathbb{Q}_5^3$ qui ne sont pas dans le plan P_{3,u_B} engendré par e_3 et u_B vers la droite D_{v_B} dirigée par v_B et (pour une puissance négative) toutes les droites de $\mathbb{Q}_5^3$ qui ne sont pas dans le plan P_{3v_B} engendré par e_3 et v_B vers la droite D_{u_B} dirigée par u_B.

Il reste donc à caractériser les ensembles sur lesquels nous allons faire agir A et B pour rentrer dans les hypothèses du lemme du ping-pong de la manière la plus pratique possible. Ces ensembles doivent notamment être disjoints. On remarque de plus que la dynamique intuitive de A et de B se réalise sur les droites

vectorielles de $\mathbb{Q}_5^3$, et non pas sur les vecteurs. On notera donc par la suite $\mathbb{P}(\mathbb{Q}_5^3)$ l'espace des droites vectorielles de $\mathbb{Q}_5^3$. Une manière très simple de caractériser des voisinages disjoints d'objets distincts est de se placer sur un espace métrique, les espaces métriques étant séparés.

Puisque $\mathbb{Q}_5$ est un corps valué, on peut munir $\mathbb{Q}_5^3$ des normes suivantes :

$$||v||_A = \max(|v_1|, |v_2|, |v_3|)$$

pour (v_1, v_2, v_3), les coordonnées de v dans la base de vecteurs propres associés à la matrice A (e_1, v_A, u_A) de $\mathbb{Q}_5^3$, et

$$||v||_B = \max(|v_1|, |v_2|, |v_3|)$$

pour (v_1, v_2, v_3), les coordonnées de v dans la base de vecteurs propres associés à la matrice B (e_3, v_B, u_B) de $\mathbb{Q}_5^3$.

Définition 27. *On munit l'ensemble des droites de $\mathbb{Q}_5^3$ des distances d_A et d_B suivantes :*

$$d_A(D, D') = \inf\{||v - v'||_A;\ v \in D \text{ et } v' \in D'$$

avec $||v||_A = ||v'||_A = 1\}$, et

$$d_B(D, D') = \inf\{||v - v'||_B;\ v \in D \text{ et } v' \in D'$$

avec $||v||_B = ||v'||_B = 1\}$, pour D et D' deux droites de $\mathbb{Q}_5^3$.

Pour simplifier, on notera d dans la proposition suivante une distance quelconque parmi d_A et d_B, et $||.||$ une norme parmi $||.||_A$ et $||.||_B$.

Proposition 28. *Une distance ainsi définie est une distance sur l'ensemble des droites de $\mathbb{Q}_5^3$.*

Démonstration. On remarque tout d'abord que les vecteurs de norme 1 d'une droite D forment un compact de $\mathbb{Q}_5^3$, puisqu'il s'agit d'un ensemble borné (par définition) et fermé, comme intersection du fermé D et de la sphère $S = \{v \in \mathbb{Q}_5^3; ||v|| = 1\}$, qui est fermée également (puisque la norme est une application 1-lipschitzienne donc continue). L'application

$$\begin{array}{rccc} k: & (D \cap S) \times (D' \cap S) & \longrightarrow & \mathbb{R}^+ \\ & (v, v') & \mapsto & ||v - v'|| \end{array}$$

est continue et définie sur un compact, donc elle est bornée et atteint ses bornes. Par conséquent il existe $v \in D \cap S$ et $v' \in D' \cap S$ tels que $d(D, D') = ||v - v'||$.

Montrons alors que $d(D, D') = 0$ implique $D = D'$. Prenons pour cela $v \in D \cap S$ et $v' \in D' \cap S$ tels que $d(D, D') = ||v - v'|| = 0$. On a bien $v = v'$ donc $D = D'$. La réciproque est évidente, ainsi que la symétrie de d.

Pour montrer l'inégalité triangulaire sous la forme $d(D, D'') \leq d(D, D') + d(D', D'')$, fixons v et v' tels que $d(D, D') = ||v - v'||$, et v'' tel que $d(D', D'') = ||cv' - v''||$, pour c une constante de valeur absolue 1. On peut alors écrire $d(D', D'') = ||v' - \frac{1}{c}v''||$ et

$$\begin{aligned} d(D, D'') &\leq ||v - \frac{1}{c}v''|| \\ &\leq ||v - v'|| + ||v' - \frac{1}{c}v''|| \\ &= d(D, D') + d(D', D''). \end{aligned}$$ □

On peut désormais définir le voisinage d'une droite et le voisinage d'un plan.

Afin d'appliquer le lemme du ping-pong, on va définir les ensembles suivants, avec ε que l'on fixera plus loin :

$$\begin{aligned} P_{A^+} &= \{D \in \mathbb{P}(\mathbb{Q}_5^3) \mid d(D, P_{1u_A}) < \varepsilon;\ d \in \{d_A; d_B\}\} \\ P_{A^-} &= \{D \in \mathbb{P}(\mathbb{Q}_5^3) \mid d(D, P_{1v_A}) < \varepsilon;\ d \in \{d_A; d_B\}\} \\ P_{B^+} &= \{D \in \mathbb{P}(\mathbb{Q}_5^3) \mid d(D, P_{3u_B}) < \varepsilon;\ d \in \{d_A; d_B\}\} \\ P_{B^-} &= \{D \in \mathbb{P}(\mathbb{Q}_5^3) \mid d(D, P_{3v_B}) < \varepsilon;\ d \in \{d_A; d_B\}\} \\ T_{A^+} &= \{D \in \mathbb{P}(\mathbb{Q}_5^3) \mid d(D, D_{v_A}) < \varepsilon;\ d \in \{d_A; d_B\}\} \\ T_{A^-} &= \{D \in \mathbb{P}(\mathbb{Q}_5^3) \mid d(D, D_{u_A}) < \varepsilon;\ d \in \{d_A; d_B\}\} \\ T_{B^+} &= \{D \in \mathbb{P}(\mathbb{Q}_5^3) \mid d(D, D_{v_B}) < \varepsilon;\ d \in \{d_A; d_B\}\} \\ T_{B^-} &= \{D \in \mathbb{P}(\mathbb{Q}_5^3) \mid d(D, D_{u_B}) < \varepsilon;\ d \in \{d_A; d_B\}\} \end{aligned}$$

En choisissant μ comme le minimum des distances $d(D_{v_A}, P_{3u_B})$, $d(D_{v_A}, P_{3v_B})$, $d(D_{u_A}, P_{3u_B})$, $d(D_{u_A}, P_{3v_B})$, $d(D_{u_B}, P_{1v_A})$, $d(D_{u_B}, P_{1u_A})$, $d_A(D_{v_B}, P_{1v_A})$ et $d(D_{v_B}, P_{1u_A})$, pour $d \in \{d_A, d_B\}$, on aura pour $\varepsilon = \frac{1}{3}\min\{1, \mu\}$ les inclusions suivantes :

$$\begin{gathered} T_{A^+} \cup T_{A^-} \subset \mathbb{Q}_5^3 \setminus (P_{B^+} \cup P_{B^-}) \\ T_{A^+} \cup T_{A^-} \subset P_{A^+} \cup P_{A^-} \end{gathered}$$

ainsi que

$$\begin{gathered} T_{B^+} \cup T_{B^-} \subset \mathbb{Q}_5^3 \setminus (P_{A^+} \cup P_{A^-}) \\ T_{B^+} \cup T_{B^-} \subset P_{B^+} \cup P_{B^-}. \end{gathered}$$

Donc en posant $K_1 = T_{A^+} \cup T_{A^-}$ et $K_2 = T_{B^+} \cup T_{B^-}$, on a bien K_1 et K_2 disjoints. Il reste à caractériser K_1 et K_2 de manière confortable afin de mettre en évidence le fait que ces ensembles vérifient les hypothèses du lemme du ping-pong.

Lemme 29. *Soient $D_1 = \text{Vect}(e_1)$ et $D = \text{Vect}(v)$ les droites de $\mathbb{Q}_5^3$ engendrées par e_1 et v, avec v qui est de norme 1 et qui n'appartient pas au plan P_{23} engendré par e_2 et e_3. Soit ε un nombre réel strictement compris entre 0 et 1. On note d la distance induite par la norme max associée à la base (e_1, e_2, e_3). Si $v = xe_1 + ye_2 + ze_3$ alors $d(D_1, D) < \varepsilon$ si, et seulement si, $\max(|\frac{y}{x}|, |\frac{z}{x}|) < \varepsilon$.*

Démonstration. Sans restreindre la généralité on peut supposer pour l'implication directe que $d(D_1,D) = ||te_1 - v||$ pour t de valeur absolue 1, puisque la condition sur v est invariante par multiplication de v par une constante non nulle. On a $||v|| = \max(|x|,|y|,|z|) = 1$.

Puisque $||te_1 - v|| = \max(|x-t|,|y|,|z|) < \varepsilon < 1$, on obtient $|x| = 1$ et $|y| < \varepsilon$, $|z| < \varepsilon$, ce qui prouve que $\max(|\frac{y}{x}|,|\frac{z}{x}|) < \varepsilon$.

Réciproquement, si $\max(|\frac{y}{x}|,|\frac{z}{x}|) < \varepsilon$, on a $|y| < \varepsilon|x| < |x|$, et $|z| < \varepsilon|x| < |x|$, donc $|x| = 1$ et $|y| < \varepsilon$, $|z| < \varepsilon$. On a également $d(D_1,D) \leq ||te_1 - sv|| = \max(|t - sx|,|y|,|z|)$, pour t et s de valeur absolue 1. En choisissant $t = sx$ qui est de valeur absolue 1, on obtient $d(D_1,D) < \varepsilon$. □

Lemme 30. *Soit $P = P_{23}$ le plan engendré par e_2 et e_3, et $D = Vect(v)$ avec v unitaire pour la norme max associée à la base (e_1,e_2,e_3). Supposons $v = xe_1 + ye_2 + ze_3$. En notant d la distance induite par cette norme, on a que $d(D,P) > \varepsilon$ si, et seulement si, $\min(|\frac{x}{y}|,|\frac{x}{z}|) > \varepsilon$.*

Démonstration. Supposons que $d(D,P) > \varepsilon$. Autrement dit, on a, pour toute droite $D' \in P$, $d(D,D') > \varepsilon$. On a alors en particulier $d(D,Vect(ye_2 + ze_3)) > \varepsilon$, autrement dit

$$\inf_{|s|=|t|=1} (max\{|x|,|s-t||y|,|s-t||z|\}) > \varepsilon.$$

Donc pour tout $(s,t) \in \mathbb{Q}_5^2$ qui vérifie $|s| = |t| = 1$, on a $max\{|x|,|s-t||y|,|s-t||z|\} > \varepsilon$. En particulier, pour $s = t$, on a $|x| > \varepsilon$, et donc, v étant unitaire, $|y| \leq 1$ et $|z| \leq 1$, ce qui donne bien le résultat attendu.

Réciproquement, supposons que $\min(|\frac{x}{y}|,|\frac{x}{z}|) > \varepsilon$. On a alors $|x| > \varepsilon|y|$ et $|x| > \varepsilon|z|$. Montrons que $|x| > \varepsilon$, ce qui suffira pour conclure. Par hypothèse, v est unitaire, donc on a $max\{|x|,|y|,|z|\} = 1$. Si $|x| = 1$, puisqu'on a $\varepsilon < 1$, on a bien $|x| > \varepsilon$. Si $|y| = 1$, on a aussi $|x| > \varepsilon$. On traite de même le cas où $|z| = 1$. □

Montrons maintenant que K_1 et K_2 définis plus haut vérifient bien les hypothèses du lemme du ping-pong.

Soit $v \in K_2 = T_{B^+} \cup T_{B^-}$. Alors $v \notin P_{A^+} \cup P_{A^-}$, donc d'après le lemme **30**, en écrivant $v = xe_1 + yv_A + zu_A$ on a d'une part, puisque $v \notin P_{A^+}$, que $min\{\frac{|y|}{|x|},\frac{|y|}{|z|}\} > \varepsilon$. De plus, pour tout $n \in \mathbb{N}$, $A^n v = xe_1 + \lambda^n yv_A + \lambda^{-n} zu_A$. On a aussi $|\lambda| > 1$, donc il existe $n_0 \in \mathbb{N}$ tel que pour tout $n \geq n_0$, $\frac{1}{\varepsilon} < \varepsilon|\lambda|^n$. Puisqu'on a $|x| < \frac{|y|}{\varepsilon}$ et $|z| < \frac{|y|}{\varepsilon}$, on en déduit $|x| < \varepsilon|\lambda|^n|y|$ et $|z| < \varepsilon|\lambda|^n|y|$, donc d'après le lemme **29**, $A^n v \in T_{A^+}$ pour tout $n \geq n_0$.

D'autre part, puisque $v \notin P_{A^-}$, on a $min\{\frac{|z|}{|x|},\frac{|z|}{|y|}\} > \varepsilon$. Or $A^{-n}v = xe_1 + \lambda^{-n}yv_A + \lambda^n zu_A$ pour tout $n \in \mathbb{N}$. En raisonnant de même que sur A, on trouve $n_1 \in \mathbb{N}$ tel que pour tout $n \geq n_1$, $A^{-n}v \in T_{A^-}$. Ainsi, en choisissant $n_A = max\{n_0,n_1\}$, on a montré que pour tout $n \in \mathbb{Z}$ tel que $|n| \geq n_A$, $A^n \cdot K_2 \subset K_1$.

On montre de même, cette fois en décomposant les vecteurs dans la base de diagonalisation de B, qu'il existe $n_B \in \mathbb{N}$ tel que pour tout $n \in \mathbb{Z}$ avec $|n| \geq n_B$, $B^n \cdot K_1 \subset K_2$.

En posant $l = max\{n_A,n_B\}$, on a bien que $a = A^l$, $b = B^l$, K_1 et K_2 vérifient les hypothèses du lemme du ping-pong (lemme **25**), donc le sous-groupe H de $SO_3(\mathbb{Q}_5)$ engendré par A^l et B^l est libre. Mais A et B sont des matrices à coefficients dans $\mathbb{Q}$ que nous avons plongé dans $\mathbb{Q}_5$ (voir la proposition **16**). Le sous-groupe H n'est formé que par des matrices à coefficients dans $\mathbb{Q}$, donc est en fait un sous-groupe libre de $SO_3(\mathbb{Q})$.

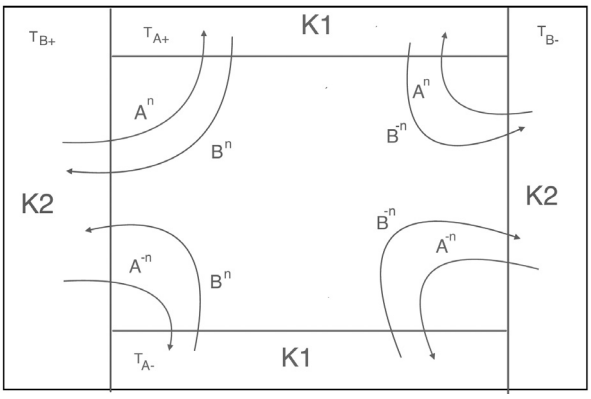

Figure 5. Illustration de la dynamique de ping-pong.

Notre groupe $SO_3(\mathbb{Q})$ contient donc bien un sous-groupe libre !

V Conclusion

Ce résultat nous amène vers de nombreuses autres questions. Dans quelle mesure notre démonstration se généralise-t-elle ? Toute matrice de $SO_3(\mathbb{Q})$ se diagonalise-t-elle dans un corps p-adique avec les bonnes propriétés ? Si c'était le cas, on obtiendrait d'autres sous-groupes libres de $SO_3(\mathbb{Q})$. Comment ces sous-groupes sont-ils reliés ?

VI Remerciements

Je tiens à remercier chaleureusement Serge Dupont qui a encadré ce projet et m'a encouragée à candidater, ainsi que Cornelia Druţu, Matteo Ruggiero et Georges Skandalis qui ont gentiment répondu à mes questions.

Références

[1] Sujet de la première épreuve de mathématiques à l'Agrégation interne de mathématiques de 2023.

[2] Yvette Amice, *Les nombres p-adiques*, Presses universitaires de France, 1975.

[3] Thomas Haettel, *Introduction à la théorie géométrique des groupes*, Cours de Master 2, 2016-2017, Université de Montpellier, https://imag.umontpellier.fr/~haettel/TGG.pdf

[4] Svetlana Katok, *p-adic analysis compared with real*, American Mathematical Society, 2007.

[5] J.S Milne, *Group Theory*, Cours de première année, 2021, https://www.jmilne.org/math/CourseNotes/GT.pdf

[6] Robert Y. Lewis, *A formal Proof of Hensel's Lemma over the p-adic integers*, 2019, https://www.semanticscholar.org/reader/a6abfbd927012f22b1363db90280a33ec4a05f40

[7] Gérard Villemin, http://villemin.gerard.free.fr/NombrCar/PadiqueT.htm

[8] Evelyn Lamb, *The Numbers behind a Fields Medalist's Math*, 2018. https://www.scientificamerican.com/blog/roots-of-unity/the-numbers-behind-a-fields-medalists-math/