Le paradoxe Banach-Tarski

Le but de ce papier est de démontrer le résultat suivant :

Paradoxe. *Si $\mathcal{B}$ et $\mathcal{B}'$ sont deux boules, n'ayant pas nécessairement la même taille, il est possible de découper $\mathcal{B}$ en un nombre fini de morceaux, et réarranger ces morceaux (par des isométries directes) de façon à ce qu'ils forment $\mathcal{B}'$.*

Dans une version fantaisiste, il est possible de découper un petit pois en morceaux et réarranger ces morceaux pour obtenir une boule de la taille du soleil.

Les connaissances mathématiques requises sont assez limitées : un bon élève de math. sup. devrait pouvoir lire cette démonstration.

Pour commencer, je vais faire quatre remarques afin de rendre le résultat moins paradoxal, et d'expliquer un peu l'"astuce" utilisée.

- En premier lieu, le Paradoxe utilise l'Axiome du Choix, qui, bien qu'affirmant quelque chose d'intuitivement évident (à savoir que pour tout ensemble E, si on appelle $\mathcal{P}(E)$ l'ensemble des parties de E, il existe une application $\varphi\colon \mathcal{P}(E) \setminus \{\emptyset\} \to E$ telle que pour tout $X \in \mathcal{P}(E) \setminus \{\emptyset\}$ on ait $\varphi(X) \in X$, c'est-à-dire une application φ qui "choisit" un élément de chaque partie de E), n'est ni démontrable (Cohen) ni réfutable (Gödel). Et certaines de ses conséquences sont horriblement gênantes (comme le paradoxe de Banach-Tarski, justement, ou la possibilité de "bien-ordonner" les réels, c'est-à-dire de les ordonner de manière que chaque sous-ensemble de $\mathbb{R}$ ait un plus petit élément). Certains mathématiciens ont d'ailleurs choisi de le refuser, comme Henri Lebesgue.
- Deuxièmement, il est totalement impossible de réaliser la "décomposition paradoxale de la boule" physiquement, ni même de l'imaginer. Par comparaison à la forme des morceaux utilisés, l'ensemble des points rationnels de l'espace est très agréable et très facile à se représenter.
- Troisièmement, il faut signaler que le raisonnement suivant ne tient pas : "Le volume de la boule de départ doit être égal à la somme des volumes des morceaux, qui doit être égal au volume de la boule d'arrivée". En effet, les morceaux ont une forme *si étrange* qu'on ne peut même pas *parler* de leur volume. Ils sont dits *non-mesurables*. Les fonctions qu'il faudrait intégrer pour déterminer leur volume ne sont, justement, pas intégrable, ni au sens (classique) de Riemann, ni au sens (généralisé) de Lebesgue. La fonction caractéristique des rationnels (qui vaut 1 sur les rationnels et 0 ailleurs) est intégrable au sens de Lebesgue (et son intégrale vaut 0) mais non au sens de Riemann. Un exemple de fonction non-mesurable serait une fonction f (qui existe, si, si) qui prend *toutes* les valeurs réelles sur n'importe quel intervalle, aussi petit soit-il, non-vide et non réduit à un point. Ce genre de monstres mathématiques, que certaines écoles (Brouwer, Borel, Kronecker, Poincaré, etc.) ont tenté d'éliminer peuplent malheureusement l'univers platonique...
- Enfin, on peut avoir une petite idée de la méthode en considérant l'exemple suivant qui est plus simple : il est possible de découper la boule-unité B en *deux* morceaux, A_0 et A_1, et de trouver un déplacement φ tel que $A_0 \cup \varphi(A_1)$ soit la boule unité privée, disons, d'un point. Autrement dit, en déplaçant une des parties de la boule, on a retiré un point. Pour cela, soit O le centre de la boule B, et I un point tel que $OI = \frac{1}{2}$. On appelle φ une rotation de centre I et d'un angle θ tel que θ/π soit irrationnel. Alors $O_0 = O$, $O_1 = \varphi(O)$, $O_2 = \varphi(O_1)$, etc., sont tous distincts (car si on avait $O_m = O_n$ avec $m > n$ alors on aurait $O_{m-n} = O_0$, donc $(m-n)\theta = 2k\pi$, ce qui contredit l'irrationnalité de θ/π). On appelle A_1 l'ensemble de tous ces points (il est d'ailleurs dénombrable) : $A_1 = \{O_i \mid i \in \mathbb{N}\}$. On a clairement $\varphi(A_1) = \{O_1, O_2, \ldots\} = A_1 \setminus \{O\}$. Et on prend pour A_0 le complémentaire de A_1 dans la boule. Ceci vérifie bien ce qui était annoncé. Et il est assez facile de voir que ce même raisonnement permet de faire disparaître un segment ou même une partie de plan (disons, un disque). Alors, on peut bien supposer que le même genre d'astuces marchera pour faire apparaître un petit volume... Certes, il y a bien des différences fondamentales, et notamment justement la question de la mesurabilité (A_1 est mesurable et de mesure nulle), mais l'idée y est.

Voici un bref plan de la démonstration :

- ○ On commence par donner quelques définitions, comme celle d'équidécomposabilité dans l'espace qui traduit le fait que deux ensembles peuvent être décomposés en morceaux isométriques, ou, plus précisément, qu'on peut découper l'un en morceaux (en nombre fini), déplacer les morceaux, et obtenir l'autre. Le problème est alors de montrer que deux boules quelconques sont équidécomposables, ou encore qu'une boule est équidécomposable à deux boules. Ou encore, qu'il existe deux parties disjointes de la boule, chacune équidécomposable à la boule entière. Pour montrer ces équivalences, on utilise un théorème fondamental, le théorème de Banach-Schröder-Cantor-Bernstein-Zermelo-Tarski (ou tout sous-ensemble de ces noms), qui dit que si A est équidécomposable à une partie de B et B à une partie de A, alors A et B sont équidécomposables. On définit aussi une partie "paradoxale" de l'espace comme une partie qui peut se décomposer en deux sous-ensembles disjoints chacun équidécomposable au tout (c'est ce qu'on veut montrer de la boule).

- Ensuite, on montre le théorème de Hausdorff, qui affirme qu'il y a deux rotations, ϕ et ρ de l'espace qui engendrent un "groupe libre", c'est-à-dire qu'aucun des déplacements ϕ, $\phi\rho$, $\phi\rho\rho$, $\phi\rho^{-1}\phi^{-1}$, $\phi\phi\phi\rho^{-1}\rho^{-1}$, ou n'importe quoi d'autre dans le genre, n'est l'identité. Ceci se fait par des moyens d'arithmétique (oui!) élémentaire.
- On déduit du théorème de Hausdorff, en utilisant l'Axiome du Choix, et une méthode qui se rapproche de celle que j'ai mentionnée dans mon petit exemple ci-dessus, que la sphère-unité, privée d'un nombre dénombrable de points, est paradoxale.
- Enfin, on rajoute un peu de vernis au tout : on élimine le problème du nombre dénombrable de points à retirer, puis on passe de la sphère à la boule, et on généralise au plus haut point. Cette dernière partie est, d'ailleurs, la plus amusante.

Il est à noter que *cinq* morceaux suffisent à transformer une boule en deux boules, et quatre pour une sphère en deux sphères (nous ne montrerons pas cette borne inférieure, qui est du reste la meilleure possible). Deuxièmement, le Paradoxe n'est pas valable dans le plan, ni dans la droite (c'est le théorème de Hausdorff qui cesse d'être valable) ; il l'est dans toutes les dimensions supérieures à 3. Troisièmement, il existe un petit livre de S. Wagon appelé "The Banach-Tarski Paradox", qui explique tout ceci très bien ; c'est d'ailleurs ma source.

Mais venons-en au cœur de la matière en cours. Je commence par donner quelques définitions, certaines extrêmement classiques et naturellement connues, mais cela ne fait jamais de mal de les réécrire.

Un ensemble D est dit *(au plus) dénombrable* ss'il existe une surjection $\mathbb{N} \to D$, ou, ce qui revient au même, une injection $D \to \mathbb{N}$. Ainsi, $\mathbb{N}$ est dénombrable. Tout sous-ensemble d'un ensemble dénombrable est dénombrable. L'union d'une famille dénombrable d'ensembles dénombrables est dénombrable (on se ramène à montrer que $\mathbb{N}^2$ est dénombrable, et c'est bien le cas car $(m, r) \mapsto 2^r(2m+1)$ définit une injection de $\mathbb{N}^2$ dans $\mathbb{N}$).

Un *groupe* est un ensemble G muni d'une loi $\star$ de composition interne associative et possédant un élément neutre (i.e. un élément e tel que $e \star a = a \star e = a$ pour tout $a \in G$), et dans lequel tout élément admet un symétrique (i.e. pour tout a il existe a' tel que $a \star a' = a' \star a = e$). Dans la suite, on notera ab plutôt que $a \star b$ l'image du couple (a, b) par $\star$, et 1 l'élément neutre, si cela ne crée pas d'ambiguïtés. Et a^n désignera $a \star a \star \cdots \star a$ (n fois), a^{-1} le symétrique de a, et $a^{-n} = (a^n)^{-1}$.

On dit qu'un groupe G *opère* sur un ensemble E si on se donne une application $\alpha: G \times E \to E$, par laquelle l'image d'un couple (g, x) (avec $g \in G$ et $x \in E$) sera notée gx, vérifiant d'une part $1x = x$ pour tout $x \in E$ et d'autre part $(gg')x = g(g'x)$ pour tous g et g' de G et x de E. On note alors que chaque application $\alpha_g: E \to E, x \mapsto gx$ est bijective de réciproque $\alpha_{g^{-1}}$. Par exemple, le groupe (noté $SO(3)$) des rotations de centre 0 de $\mathbb{R}^3$ opère sur $\mathbb{R}^3$. Le groupe des isométries, des déplacements, des similitudes, opère sur l'espace affine de dimension 3. Le groupe $\mathfrak{S}(E)$ de toutes les bijections de E sur E, où E est un ensemble quelconque, opère sur E. Un exemple plus important est le suivant : tout groupe opère sur lui-même "par translation" si l'application α est justement la loi de composition interne, en autres mots si gx a le même sens comme opération dans le groupe ou comme opération de l'élément g du groupe sur l'élément x de l'ensemble correspondant.

On appelle *groupe non-abélien libre de rang* 2 l'ensemble des chaînes de caractères (éventuellement vides) constitués des quatres symboles a, b, a^{-1} et b^{-1} dans lesquelles les symboles a et a^{-1}, ou b et b^{-1} ne sont jamais côte à côte. Par exemple, aaa ou $ababab^{-1}$ ou $aba^{-1}b^{-1}$, etc. La chaîne vide sera notée 1 par commodité. La loi de composition est celle qui consiste à écrire deux chaînes A et B côte à côte, puis à retirer toutes les occurrences de aa^{-1}, $a^{-1}a$, bb^{-1} ou $b^{-1}b$. Par exemple, $(aabbab^{-1})(ba^{-1}bba) = aabbbba$. On notera évidemment, comme dans tout groupe, $a^2 = aa$, $a^3 = aaa$, etc. Il est clair que ce groupe, noté $C_\infty * C_\infty$, est infini, puisque l'application $n \mapsto a^n$ est injective de $\mathbb{N}$ dans $C_\infty * C_\infty$.

Si E est un ensemble et G un groupe opérant sur E, dit que deux sous-ensembles A et B de E sont G-

équidécomposables ss'il existe une partition $(A_i)_{1\leq i\leq n}$ de A (c'est-à-dire une suite finie $(A_i)_{1\leq i\leq n}$ de parties non-vides de E deux-à-deux disjointes dont l'union soit A) et une partition $(B_i)_{1\leq i\leq n}$ de B toutes deux finies et ayant le même nombre n de morceaux, et n éléments de G, $(g_i)_{1\leq i\leq n}$ tels que $B_i = g_iA_i$ pour tout $1 \leq i \leq n$, en désignant naturellement par g_iA_i l'ensemble

$$g_iA_i = \{g_ix \mid x \in A_i\}$$

On notera $A \sim B$. Si $A \sim B'$ où $B' \subseteq B$, on dira que A est *subdécomposable* à B, et on notera $A \preceq B$, ou $B \succeq A$.

Un ensemble $A \subseteq E$ est dit *G-paradoxal* ss'il existe A' et A'' deux parties de A avec $A' \cap A'' = \emptyset$ telles que $A \sim A'$ et $A \sim A''$.

On omettra de mentionner le groupe G s'il est évident, ou bien s'il s'agit du groupe des déplacements de l'espace. Ainsi, nous désirons prouver que la boule est paradoxale, à partir de quoi on pourra prouver que deux boules quelconques sont équidécomposables.

On peut à présent citer le premier résultat qui sera l'une des pierres essentielles de la démonstration du Paradoxe :

Proposition. *Si G désigne le groupe $C_\infty * C_\infty$ non-abélien libre de rang 2, alors G est paradoxal quand il opère sur lui-même par translation.*

Démonstration : Soit A' l'ensemble de toutes les chaînes de G commençant par a, A'' par a^{-1}, B' par b et B'' par b^{-1}. Alors $a^{-1}A'$ est l'ensemble des chaînes ne commençant pas par a^{-1} (puisqu'un élément de A' ne peut pas avoir un a^{-1} juste après le a), donc $a^{-1}A' \cup A'' = G$. On pose $A = A' \cup A''$, nous venons de montrer $A \sim G$. De même, si on pose $B = B' \cup B''$, on a $B \sim G$. Comme $A \cap B = \emptyset$, on a montré que G est paradoxal.

On peut presque dire que cette proposition est l'étape essentielle de la démonstration et que le reste n'en est que commentaire.

Nous procédons à présent à l'étude du théorème de BSCBZT (Banach-Schröder-Cantor-Bernstein-Zermelo-Tarski). Il s'agit de montrer :

Théorème de BSCBZT. *Si $A \preceq B$ et $A \succeq B$ alors $A \sim B$.*

Avant de commencer la démonstration, quelques remarques s'imposent. Tout d'abord, ce théorème est parfaitement naturel, puisque après tout $A \preceq B$ signifie quelque chose comme "A est plus petit que B". Mais il n'est pas trivial : il va après tout falloir mettre en évidence une manière de découper A en petits morceaux pour obtenir exactement B.

Le résultat, naturellement, ne dépend pas de l'ensemble E dans lequel on se place, ni du groupe G qui opère dessus.

Ce théorème est fortement lié à un résultat classique de la Théorie des Ensembles :

Théorème de SCBZ. *S'il existe une bijection de A sur une partie de B et une bijection de B sur une partie de A, alors il existe une bijection de A sur B.*

(Il est toutefois à noter que SCBZ n'est pas un corollaire immédiat de BSCBZT. Nous démontrerons les deux ensemble.)

On a aussi le corollaire immédiat, qui pourtant utilise l'Axiome du Choix, contrairement aux deux résultats ci-dessus :

Corollaire. *S'il existe une injection de A vers B et une surjection de A sur B, alors il existe une bijection entre A et B.*

Démonstration (du corollaire) : Soit f l'injection de A vers B, et B' son image. Soit g la surjection de A sur B : on utilise l'axiome du choix pour produire une partie A' de A telle que g restreinte à A' soit bijective (il faut pour cela "choisir" un antécédent et un seul de chaque élément de B). Alors on a une bijection de A sur une partie (B') de B et une bijection de B sur une partie (A') de A. Le théorème de SCBZ donne donc une bijection entre A et B.

Remettons les choses en place. Dans le cas de BSCBZT, nous avons une relation $\sim$ (d'équidécomposabilité), et dans le cas de SCBZ, on lui donne le sens d'existence d'une bijection ($A \sim B$ ss'il existe une bijection entre A et B). $\sim$ est dans les deux cas une relation d'équivalence, c'est-à-dire qu'elle est réflexive, symétrique et transitive (tout ceci est évident, sauf peut-être la transitivité dans le cas de BSCBZT, mais même cela n'est pas très dur à montrer).

Par ailleurs, on a défini une relation $\preceq$ par $A \preceq B$ ssi $A \sim B'$ où $B' \subseteq B$. Dans le cas de SCBZ, $\preceq$ signifie qu'il existe une bijection sur une partie ($A \preceq B$ signifie qu'il existe une bijection de A sur une partie de B).

Les deux propriétés de $\sim$ qu'on utilisera dans la démonstration sont :

a) Si $A \sim B$, alors il existe une bijection g de A sur B telle que $C \sim g(C)$ pour tout $C \subseteq A$. (Pour SCBZ, c'est trivial ; pour BSCBZT, cela signifie seulement qu'on peut décomposer une partie de A en son image dans B, et c'est évident...)

b) Si $A_1 \cap A_2 = B_1 \cap B_2 = \emptyset$ et $A_1 \sim B_1$ et $A_2 \sim B_2$, alors $A_1 \cup A_2 \sim B_1 \cup B_2$. (Dans les deux cas, c'est plutôt évident...)

Si on a $A \sim B'$ avec $B' \subseteq B$ et $A' \sim B$ avec $A' \subseteq A$, on cherche en fait à envoyer tous les éléments de A sur tous les éléments de B (en donnant au verbe "envoyer" un sens assez vague qui soit valable tant dans BSCBZT que dans SCBZ ; le mieux est d'essayer d'imaginer seulement ce second cas). Les éléments de $A \setminus A'$ ne peuvent clairement être envoyés que sur B' en utilisant la bijection fournie par $A \sim B'$. Plus précisément, si on appelle f la bijection donnée par la propriété a) appliquée à $A \sim B'$, il faut clairement envoyer $A \setminus A'$ sur $f(A \setminus A') = B' \setminus f(A')$. Si on appelle g la bijection correspondant à $A' \sim B$, on a la possibilité d'utiliser f ou g sur les éléments de A'. Ni l'une ni l'autre ne convient, puisque si on prend f, certains éléments de B (ceux de $B \setminus B'$) n'auront pas d'antécédent, et si on prend g, les éléments de $B' \setminus f(A')$ auront deux antécédents. Toute l'astuce du théorème consiste à "bricoler" notre bijection finale en utilisant f par endroits et g par endroits. Procédons à présent à la démonstration rigoureuse.

Démonstration : On pose $C_0 = A \setminus A'$, et par récurrence $C_{k+1} = g^{-1} \circ f(C_k)$. Alors on a $f(C_k) = g(C_{k+1})$, comme on le vérifie aussitôt. On pose $C = \bigcup_{k \in \mathbb{N}} C_k$. Alors, puisque $C_0 \cap A' = \emptyset$ et $C_k \subseteq A'$ pour $k \geq 1$, on a $C \cap A' = C \setminus C_0$. Or $f(C) = g\left(\bigcup_{k \in \mathbb{N}} C_{k+1}\right) = g(C \setminus C_0) = g(A' \cap C)$.

Par ailleurs, on peut vérifier $g(A \setminus C) = B \setminus f(C)$ (Si $x \in A \setminus C$, $x \in A'$ donc $g(x)$ existe, $g(x) \in B$ et $g(x) \notin f(C)$ car $f(C) = g(A' \cap C)$. On vient de montrer $g(A \setminus C) \subseteq B \setminus f(C)$, et on montre de manière semblable l'inclusion contraire.)

Le fait que $f(C) = g(A' \cap C)$ montre $C \sim g(A' \cap C)$, et le fait que $g(A \setminus C) = B \setminus f(C)$ montre $A \setminus C \sim B \setminus f(C) = B \setminus g(A' \cap C)$. On applique la propriété b), et on trouve $A \sim B$. Ce qu'il fallait démontrer.

Pour récapituler, on a pris l'ensemble C sur lequel on *doit* utiliser f, et on a utilisé g sur son complémentaire.

Dans le cas qui nous intéresse, on a des applications immédiates. On avait par exemple défini un ensemble A comme paradoxal ss'il existe deux parties, A' et A'' de A, disjointes, telles que $A' \sim A$ et $A'' \sim A$. On peut se demander s'il est possible de rajouter la condition supplémentaire $A' \cup A'' = A$. Le théorème de BSCBZT répond affirmativement à cette question. En effet, on a $A \setminus A' \preceq A$ trivialement, et $A \setminus A' \succeq A'' \sim A$ donc $A \setminus A' \succeq A$. Alors BSCBZT donne $A \setminus A' \sim A$. Et on n'a qu'à remplacer A'' par $A \setminus A'$, ce qui donne bien $A' \cup A'' = A$ et $A' \cap A'' = \emptyset$.

Le même théorème nous permettra, une fois démontré qu'une boule est paradoxale, de conclure que deux boules quelconques sont équidécomposables. En effet, si on note $\mathcal{B}$ la boule-unité, et $\mathcal{B}'$ une autre boule, disons plus grande, on a clairement $\mathcal{B} \preceq \mathcal{B}'$. Mais d'autre part, si on note $n\mathcal{B}$ un ensemble constitué de n boules-unité, disons côte-à-cote, on aura montré $n\mathcal{B} \sim \mathcal{B}$. Et il est clair qu'en prenant n assez grand, on aura $\mathcal{B}' \preceq n\mathcal{B}$, donc $\mathcal{B}' \preceq \mathcal{B}$. Le théorème de BSCBZT donnera alors $\mathcal{B}' \sim \mathcal{B}$.

Maintenant, il n'y a plus qu'à montrer $\mathcal{B} \sim 2\mathcal{B}$!

En fait, ce que je démontre à présent est bien la partie la moins intéressante du Paradoxe ; ce n'est ni la plus technique, ni la plus astucieuse, ni celle qui utilise l'Axiome du Choix. Il s'agit simplement de montrer que deux rotations de l'espace engendrent un groupe non-abélien libre de rang 2.

Pour cela, on considère les rotations ϕ et ρ (dont les axes passent par l'origine) déterminées par les matrices :

$$\phi^{\pm 1} = \begin{pmatrix} \frac{1}{3} & \mp\frac{2\sqrt{2}}{3} & 0 \\ \pm\frac{2\sqrt{2}}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

et

$$\rho^{\pm 1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & \mp\frac{2\sqrt{2}}{3} \\ 0 & \pm\frac{2\sqrt{2}}{3} & \frac{1}{3} \end{pmatrix}$$

(C'est parce que les axes passent par l'origine que les rotations n'ont qu'une composante linéaire et pas de terme constant qui correspondrait à une translation.)

Il est à la charge de tous ceux qui ne le croiraient pas de vérifier que ϕ et ρ sont bien des rotations, et que ϕ^{-1} et ρ^{-1} en sont bien les inverses respectives. Il est assez clair que ϕ est une rotation d'angle arccos $\frac{1}{3}$ autour de (Oz) et ρ de même angle autour de (Ox).

Nous voulons montrer que le groupe engendré par ces rotations, c'est-à-dire le groupe de tous les déplacements qui peuvent s'écrire comme une composée d'un nombre quelconque de ϕ, ϕ^{-1}, ρ et ρ^{-1}, est un groupe non-abélien libre de rang 2. Cela semble plus compliqué que ce ne l'est en réalité. Pour y arriver, on suppose que w est un "mot" de ϕ, ϕ^{-1}, ρ et ρ^{-1} (c'est-à-dire une suite finie quelconque de ces symboles), non-triviale (non-vide) et réduite (c'est-à-dire dans laquelle suite on ne trouve jamais $\phi\phi^{-1}$, $\phi^{-1}\phi$, $\rho\rho^{-1}$ ou $\rho^{-1}\rho$). Il est clair que w peut être interprété comme une rotation, dont nous voulons montrer qu'elle n'est pas l'identité ; attention toutefois, il ne faut pas définir w comme une rotation dès le départ, sans quoi on n'a rien à montrer !

Tout d'abord, si w se termine par ρ ou ρ^{-1}, on considère $w' = \phi^{-1}w\phi$ (naturellement, si w commençait par ϕ, il faut supprimer le $\phi^{-1}\phi$ initial de w'). Montrer que $w \neq 1$ (1 est l'identité) revient à montrer $w' \neq 1$. On peut donc se limiter à l'étude des cas où w se termine par ϕ ou ϕ^{-1}.

Nous affirmons tout d'abord que $w(1,0,0)$ est de la forme $\left(\frac{a}{3^k}, \frac{b\sqrt{2}}{3^k}, \frac{c}{3^k}\right)$, où a, b et c sont des entiers et k un naturel. Ceci se fait par récurrence sur la longueur de w, en autres mots on montre que c'est le cas si w est de longueur 1 (c'est-à-dire, moyennant la supposition faite plus haut, si $w = \phi^{\pm 1}$) et que si on compose w à gauche par une des quatre rotations on cela reste vrai. Si $w = \phi^{\pm 1}$, $w(1,0,0) = (1, \pm 2\sqrt{2}, 0)/3$ a bien la forme voulue. Si $w = \phi^{\pm 1}w'$ où $w'(1,0,0) = (a', b'\sqrt{2}, c')/3^{k-1}$, on trouve $w(1,0,0) = (a, b\sqrt{2}, c)/3^k$ où $a = a' \mp 4b'$, $b = b' \pm 2a'$ et $c = 3c'$, donc w vérifie bien la propriété. Si $w = \rho^{\pm 1}w'$ où $w'(1,0,0) = (a', b'\sqrt{2}, c')/3^{k-1}$, on trouve $w(1,0,0) = (a, b\sqrt{2}, c)/3^k$ où $a = 3a'$, $b = b' \mp 2c'$ et $c = c' \pm 4b'$, donc w vérifie bien la propriété. On a donc montré par récurrence que $w(1,0,0) = (a, b\sqrt{2}, c)/3^k$.

Nous montrons à présent que (si w est non-trivial), b n'est jamais divisible par 3. On procède de nouveau par récurrence mais en ajoutant deux symboles à la fois.

Pour démarrer la récurrence, il faut montrer la propriété si w est de longueur 1 ou 2, c'est-à-dire si w vaut $\phi^{\pm 1}$, $\rho\phi^{\pm 1}$, $\rho^{-1}\phi^{\pm 1}$ ou $\phi^{\pm 2}$: dans le premier des cas, $b = \pm 2$ donc c'est vrai. Dans le second et le troisième, $b = \pm 2$, donc c'est encore vrai. Dans le quatrième, $b = \pm 4$, donc c'est toujours vrai.

Ensuite, on étudie les différents cas $w = \phi^{\pm 1}\rho^{\pm 1}v$, $w = \phi^{\pm 1}\rho^{\mp 1}v$, $w = \rho^{\pm 1}\phi^{\pm 1}v$ et $w = \rho^{\pm 1}\phi^{\mp 1}v$, où v est un mot vérifiant l'hypothèse de récurrence, i.e. $v(1,0,0) = (a'', b''\sqrt{2}, c'')/3^{k-2}$ avec b'' non-divisible par 3. Nous traitons seulement le premier de ces cas, les autres procédant de même. On a $\rho^{\pm 1}v(1,0,0) = (a', b'\sqrt{2}, c')/3^{k-1}$ avec $a' = 3a$, donc a' est multiple de 3. Et $w(1,0,0) = (a, b\sqrt{2}, c)/3^k$ avec $b = b' \pm 2a'$. Cependant, l'hypothèse de récurrence ne s'applique pas seulement à v mais aussi à $\rho^{\pm 1}v$, donc b' n'est pas multiple de 3. Donc b non plus, car $2a'$ est un multiple de 3.

Les deux cas restant à traiter sont $w = \phi^{\pm 2}v$ et $w = \rho^{\pm 2}v$. Nous considérons le premier. On écrit $v(1,0,0) = (a'', b''\sqrt{2}, c'')/3^{k-2}$, $\phi^{\pm 1}v(1,0,0) = (a', b'\sqrt{2}, c')/3^{k-1}$ et $w(1,0,0) = (a, b\sqrt{2}, c)/3^k$. Alors on vérifie $b = 2b' - 9b''$, donc, b' n'étant pas divisible par 3, b non plus.

On a donc montré $w(1,0,0) = (a, b\sqrt{2}, c)/3^k$ où b n'est pas multiple de 3, donc en particulier $b \neq 0$, donc $w(1,0,0) \neq (1,0,0)$. Donc w n'est pas l'identité. Ce qui est le résultat recherché : *tout* mot réduit non-trivial de $\phi^{\pm 1}$ et $\rho^{\pm 1}$ est différent de l'identité, donc le groupe engendré par ces quatre rotations est le (est isomorphe au) groupe non-abélien libre de rang 2.

A ce moment, d'après la proposition énoncée précedemment, le groupe G de déplacements engendré par ϕ et ρ est paradoxal. Nous expliquons maintenant comment utiliser le fameux Axiome du Choix pour démontrer le paradoxe de Hausdorff, duquel on déduit facilement le paradoxe de Banach-Tarski.

Pour récapituler ce que nous avions fait, nous avions montré que deux rotations ϕ et ρ d'axes passant par l'origine engendraient un groupe non-abélien libre de rang 2, que nous notons G. En particulier, si on note A' l'ensemble de tous les éléments de G qui commencent par ϕ ("commencent" lorsqu'on les écrit comme une chaîne de caractères ; en fait, le ϕ est la dernière rotation effectuée), A'' l'ensemble de ceux qui commencent par ϕ^{-1}, B' par ρ et B'' par ρ^{-1}, on a $G = A' \cup A'' \cup B' \cup B'' \cup \{1\} = \phi^{-1}A' \cup A'' = \rho^{-1}B' \cup B''$. C'est-à-dire que G est paradoxal ; nous allons utiliser cela pour démontrer que, à "peu de choses" près, la sphère est paradoxale.

Le groupe G est un groupe de rotations d'axes passant par l'origine O, et on peut donc le considérer comme opérant sur la sphère-unité que nous noterons S. Or une rotation (différente de l'identité) admet deux points fixes sur S ; on appellera D l'ensemble des points laissés fixes par un élément de G différent de l'identité.

On peut facilement voir que G est dénombrable : une manière de procéder est de remplacer ϕ par 1, ϕ^{-1} par 2, ρ par 3 et ρ^{-1} par 4 ; alors chaque élément de G se voit associer un entier naturel de manière unique, ce qui montre que G est dénombrable. D l'est donc aussi.

On appellera *orbite* (par G) de $x \in S$ l'ensemble $G(x)$ des images de x par tous les éléments de G, c'est-à-dire $Or(x) = \{y \in S \mid \exists g \in G(x = gy)\}$. Si $x \notin D$, et si g et g' sont des éléments distincts de G, on a $g^{-1}g'x \neq x$ (car $x \notin D$) donc $gx \neq g'x$, c'est-à-dire que l'application "canonique" $g \mapsto gx$ de G vers $Or(x)$ est bijective (alors que si $x \in D$ elle est seulement surjective). Cette dernière remarque sera appellée la remarque 1, quand j'en aurai besoin plus tard.

Soit $\mathcal{O}$ l'ensemble de toutes les orbites par G dans $S \setminus D$; il est à noter que tous les éléments de $\mathcal{O}$ sont non-vides et que deux éléments distincts de $\mathcal{O}$ sont disjoints. Soit $0_\sharp$ un ensemble qui contient (qui "choisit") un élément et un seul de chacun des éléments de $\mathcal{O}$, autrement dit, $0_\sharp$ contient un élément de chaque G-orbite dans $S \setminus D$. (C'est à ce niveau qu'on utilise l'Axiome du Choix, mais il est inutile de s'apesantir dessus pour l'instant.)

On considère à présent $A'_\sharp = A'(0_\sharp)$, c'est-à-dire l'ensemble des éléments de $S \setminus D$ de la forme gx où $g \in A'$ et $x \in 0_\sharp$. On pose de même $A''_\sharp = A''(0_\sharp)$, $B'_\sharp = B'(0_\sharp)$ et $B''_\sharp = B''(0_\sharp)$. Alors premièrement $A'_\sharp$, $A''_\sharp$, $B'_\sharp$ et $B''_\sharp$ sont deux-à-deux disjoints car A', A'', B' et B'' le sont et par la remarque 1 (et aussi parce que deux éléments distincts de $0_\sharp$ sont dans deux orbites disjointes). En effet, supposons $x \in A'_\sharp$ et $x \in A''_\sharp$; alors $x = gy$ avec $g \in A'$ et $x = g'y'$ avec $g' \in A''$; donc $y = g'^{-1}gy'$ donc y est dans l'orbite de y' donc $y = y'$, et alors $y = g'^{-1}gy$, et on en déduit $g = g'$ car $y \notin D$.

On pose alors $A_\sharp = A'_\sharp \cup A''_\sharp$ et $B_\sharp = B'_\sharp \cup B''_\sharp$: on a $A_\sharp \cap B_\sharp = \emptyset$. Mais $\phi^{-1}A'_\sharp \cup A''_\sharp = S \setminus D$ car $\phi^{-1}A' \cup A'' = G$ et de même $\rho^{-1}B'_\sharp \cup B''_\sharp = S \setminus D$. Ceci montre que $A \sim B \sim S \setminus D$. Mais alors $S \setminus D$ est paradoxal ! C'est le paradoxe de Hausdorff : on a deux parties disjointes $A_\sharp$ et $B_\sharp$ de $S \setminus D$, telles qu'en découpant chacune en deux morceaux et en faisant tourner l'un de ces morceaux, on retrouve $S \setminus D$.

Maintenant, il n'est plus difficile de terminer la démonstration. Le plus important est de retirer ce D qui nous gêne. Pour cela, ce n'est guère difficile : soit P un point quelconque de $S \setminus D$ (il en existe un car D est dénombrable et S ne l'est pas), et soit P' son symétrique par rapport à O. On appelle ϱ_θ la rotation d'axe orienté $(P'P)$ et d'angle θ. Pour chaque M de D, soit $\mathcal{A}(M)$ l'ensemble des angles θ tels que $\varrho_\theta(M) \in D$: cet ensemble est dénombrable car D l'est. Donc l'union de tous les $\mathcal{A}(M)$ pour M décrivant D est aussi dénombrable. Et on peut alors prendre θ_0 qui ne soit pas dans aucun de ces $\mathcal{A}(M)$. Alors on pose $\varrho = \varrho_{\theta_0}$: on a $\varrho(M) \notin D$ pour tout $M \in D$, donc $\varrho(D) \subseteq S \setminus D$. On pose alors $E = D \cup \varrho(D) \cup \varrho^2(D) \cup \cdots$: on a $\varrho(E) = E \setminus D$, donc $E \sim E \setminus D$, et, en ajoutant $S \setminus E$ de part et d'autre, $S \sim S \setminus D$. Mais comme on a $A_\sharp \sim S \setminus D$, on a $A_\sharp \sim S$ et de même $B_\sharp \sim S$. Donc S est paradoxale.

Passer de la sphère à la boule est très simple : il suffit de remplacer chaque point M de la sphère par le segment $]OM]$ ouvert en O et fermé en M, ce qui donne le fait que la boule fermée privée de O est paradoxale. Pour rajouter le point O, il n'y a plus qu'à utiliser la remarque que j'ai faite avant la démonstration (la quatrième remarque précédée de $\bullet$).

On a donc montré qu'une boule est paradoxale : on peut la découper en un nombre fini de morceaux, déplacer ces morceaux, et obtenir deux boules de même taille.

Maintenant, soient $\mathcal{A}$ et $\mathcal{B}$ deux parties quelconques de l'espace, bornées et d'intérieur non-vide, c'est-à-dire que $\mathcal{A}$ est contenu dans une boule $B_\mathcal{A}$ ($\mathcal{A}$ est borné) et contient une boule $b_\mathcal{A}$ ($\mathcal{A}$ est d'intérieur non-vide) ; et de même pour $\mathcal{B}$. Il est clair que l'on peut recouvrir $\mathcal{B}$ par un ensemble E constitué d'un nombre suffisant de copies de $b_\mathcal{A}$; comme $b_\mathcal{A}$ est une boule donc est paradoxale, on a $b_\mathcal{A} \sim E$; et d'autre part, $\mathcal{B} \preceq E$, et $b_\mathcal{A} \preceq \mathcal{A}$. Donc $\mathcal{B} \preceq \mathcal{A}$. Et de même $\mathcal{A} \preceq \mathcal{B}$. Alors, BSCBZT donne $\mathcal{A} \sim \mathcal{B}$. C'est-à-dire que deux ensembles bornés d'intérieur non-vide quelconques de l'espace sont équidécomposables.

En fait, on a fait mieux : donné un nombre fini $(\mathcal{A}_i)_{1 \leq i \leq n}$ de parties bornées d'intérieur vide de l'espace, il existe un "puzzle" dont les morceaux peuvent être arrangés pour donner chacun des $(\mathcal{A}_i)$.

En revanche, il faut noter que dans le plan, ce genre de choses antipathiques n'arrive pas. Banach a montré le résultat suivant :

Théorème. *Si $\mathbb{P}$ désigne le plan euclidien, il existe une application $\mu\colon \mathcal{P}(\mathbb{P}) \to [0; +\infty]$ définie sur* toutes *les parties du plan, telle que si $(A_i)_{1\leq i\leq n}$ sont des parties disjointes du plan alors $\mu\left(\bigcup_{1\leq i\leq n} A_i\right) = \sum_{1\leq i\leq n} \mu(A_i)$, que si A est une partie du plan et φ une isométrie alors $\mu(A) = \mu(\varphi(A))$, et enfin que si C est un carré de côté 1, alors $\mu(C) = 1$.*

En autres mots, il existe une façon de mesurer (de définir l'aire de) *toutes* les parties du plan, ce qui empêche que le paradoxe de Banach-Tarski ne se produise dans le plan. Il en va de même de la droite.

J'ai également mentionné l'Axiome du Choix, dont voici un énoncé :

Axiome du Choix. *Si $\mathcal{C}$ est un ensemble dont les éléments sont non-vides et deux-à-deux disjoints, alors il existe une application φ sur $\mathcal{C}$ (à valeurs dans l'union de tous les éléments de $\mathcal{C}$) telle que pour tout $x \in \mathcal{C}$ on ait $\varphi(x) \in x$.*

En autres mots, φ "choisit" un élément de chacun des éléments de $\mathcal{C}$. Cet énoncé équivaut à celui que j'ai cité dans ma première lettre. Bien qu'intuitivement "évident", cet axiome ne peut être ni démontré ni réfuté. Il est utilisé à peu près partout en mathématiques, ne serait-ce que pour montrer qu'une union dénombrable d'ensembles dénombrables est dénombrable, ou pour montrer que tout espace vectoriel admet une base, ou encore pour montrer qu'un produit d'espaces topologiques compacts est compact (théorème de Tychonoff). Le paradoxe de Banach-Tarski ne *peut pas* être démontré sans l'aide de l'Axiome du Choix, cela a été démontré.