

Appendix G

The Banach–Tarski Paradox

The usual informal statement of the Banach–Tarski paradox is as follows:

A pea can be divided into a finite number of pieces, and these pieces, after being moved by rigid motions, can be reassembled in such a way as to produce the sun.

For a more precise statement, let us replace the pea and the sun with subsets P and S of \mathbb{R}^3 that are bounded and have nonempty interiors. Then the Banach–Tarski paradox says that there exist a positive integer n , disjoint subsets A_1, A_2, \dots, A_n of P , and disjoint subsets B_1, B_2, \dots, B_n of S such that

- (a) $P = A_1 \cup A_2 \cup \dots \cup A_n$,
- (b) $S = B_1 \cup B_2 \cup \dots \cup B_n$, and
- (c) for each i there is a rigid motion of \mathbb{R}^3 that maps A_i onto B_i .

There are a couple of things to note here. First, this paradox depends on the axiom of choice, and so the sets A_1, \dots and B_1, \dots are produced in a very nonconstructive way. Second, the Banach–Tarski paradox implies that there is no way to extend Lebesgue measure to the collection of all subsets of \mathbb{R}^3 in such a way that the extension is invariant under rigid motions and is at least finitely additive.

Let us turn to the mathematical concepts that we need for a proof of the Banach–Tarski paradox. Let G be a group and let X be a nonempty set. Suppose (for definiteness) that the group operation on G is written multiplicatively and that e is the identity element of G . An *action* of G on X is a mapping $(g, x) \mapsto g \cdot x$ of $G \times X$ to X that satisfies

- (a) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ and
- (b) $e \cdot x = x$

for all g_1, g_2 in G and all x in X . We often abbreviate $g \cdot x$ with gx . One sometimes says that G *acts* on X when we are dealing with an action of G on X .

If G acts on X , if $g \in G$, and if A is a subset of X , then gA or $g \cdot A$ is the set $\{y \in X : y = g \cdot a \text{ for some } a \text{ in } A\}$. Likewise, if H is a subset of G and A is a subset of X , then $H \cdot A$ is the set $\{y \in X : y = h \cdot a \text{ for some } h \text{ in } H \text{ and some } a \text{ in } A\}$.

G.1. (Examples)

- (a) Let d be a positive integer and let G be a subgroup of the group of all invertible d by d matrices. For S in G and x in \mathbb{R}^d let Sx be the usual product of the matrix S and the vector x , where x is regarded as a column vector. Then $(S, x) \mapsto Sx$ gives an action of G on \mathbb{R}^d .
- (b) Recall that a d by d matrix $S = (s_{ij})$ is *orthogonal* if its columns are orthogonal to one another and have norm 1 (with respect to the usual Euclidean norm $\|\cdot\|_2$). In other words, S is orthogonal if $\sum_i s_{ij} s_{ik}$ is 1 if $j = k$ and is 0 if $j \neq k$. The set of all d by d orthogonal matrices with determinant 1 is a group, which is called the *special orthogonal group* and is denoted by $SO(d)$. Such groups are, of course, groups of the sort described in the previous example.
- (c) Now let G_3 be the set of all rigid motions $T: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ of the form $T(x) = Sx + b$, where $S \in SO(3)$ and $b \in \mathbb{R}^3$. Thus G_3 is a group; it acts on \mathbb{R}^3 by $(T, x) \mapsto T(x)$.
- (d) Let G be an arbitrary group. Then $(g, g') \mapsto g \cdot g'$, where \cdot is the group operation of G , gives an action of G on G .

Equidecomposability

Now suppose that G acts on the set X and that A and B are subsets of X . Then A and B are called *G -equidecomposable* (or simply *equidecomposable*), or A is said to be *G -equidecomposable with B* if there exist a positive integer n , disjoint subsets A_1, \dots, A_n of A , disjoint subsets B_1, \dots, B_n of B , and elements g_1, \dots, g_n of G such that

- (a) $A = A_1 \cup A_2 \cup \dots \cup A_n$,
- (b) $B = B_1 \cup B_2 \cup \dots \cup B_n$, and
- (c) $B_i = g_i \cdot A_i$ holds for each i .

Thus A and B are G -equidecomposable if and only if there is a bijection $f: A \rightarrow B$ that is *defined piecewise*¹ by the action of G on X —that is, for which there are disjoint subsets A_1, \dots, A_n of A that satisfy $A = A_1 \cup A_2 \cup \dots \cup A_n$ and elements g_1, \dots, g_n of G such that f is given by $f(x) = g_i \cdot x$ if $x \in A_i$, for $i = 1, \dots, n$.

It is easy to check that if $g: A \rightarrow B$ and $f: B \rightarrow C$ are bijections that are defined piecewise by the action of G on X (see the preceding paragraph), then $f \circ g: A \rightarrow C$ is also a piecewise defined bijection. Since the identity map (from a subset A of X to itself) is such a piecewise defined bijection, as are the inverses of such bijections, it follows that the relation of G -equidecomposability is an equivalence relation.

Recall the Schröder–Bernstein theorem from set theory: if the set A has the same cardinality as some subset of the set B , and if B has the same cardinality as some subset of A , then A and B have the same cardinality. In other words, if there is a

¹This is perhaps not entirely standard terminology.

- (b) Use part (a) to show that if T is an orthogonal operator on \mathbb{R}^3 that has determinant 1 and has 1 among its eigenvalues, then there is an orthonormal basis of \mathbb{R}^3 with respect to which T has matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \theta & -\sin \theta \\ 0 & \sin \theta & \cos \theta \end{pmatrix},$$

where θ is a real number. Conclude that T is a rotation through an angle of θ about some line through the origin.

6. The preceding exercises outline a proof that every matrix in $SO(3)$ gives a rotation of \mathbb{R}^3 about some line through the origin. Prove the converse: every rotation of \mathbb{R}^3 about a line through the origin corresponds to a matrix in $SO(3)$.

Notes

The fundamental paper by Banach and Tarski is [2]. The book by Wagon [122] is very thorough and rather up-to-date.

1. Let V be a subspace of \mathbb{R}^d (possibly equal to \mathbb{R}^d), let $\{e_i\}$ be an orthonormal basis⁴ of V , and let A be the matrix of T with respect to $\{e_i\}$. Show that the conditions
 - (i) $(Tx, Ty) = (x, y)$ holds for all x, y in V ,
 - (ii) A is an orthogonal matrix, and
 - (iii) $A^T A = I$
 are equivalent. Thus we can call the operator T *orthogonal* if its matrix with respect to some (and also every) orthonormal basis of V is an orthogonal matrix.
2. Suppose that T is an orthogonal operator on \mathbb{R}^3 .
 - (a) Show that $\det(T)$ is 1 or -1 .
 - (b) Show that T has at least one real eigenvalue. (Hint: The characteristic polynomial of T is a cubic polynomial.)
 - (c) Show that every real eigenvalue of T has absolute value 1.
3. Let T be an orthogonal operator on \mathbb{R}^3 , let λ be a real eigenvalue of T , and let x be an eigenvector of T that corresponds to the eigenvalue λ .
 - (a) Let x^\perp be the set of all vectors y in \mathbb{R}^3 that are *orthogonal* to x (i.e., the set of all y such that $(x, y) = 0$). Show that x^\perp is a linear subspace of \mathbb{R}^3 that is invariant under T , in the sense that $T(y) \in x^\perp$ whenever $y \in x^\perp$.
 - (b) Let T_{x^\perp} be the restriction of T to x^\perp . Show that the determinants of T and T_{x^\perp} are related by $\det(T) = \lambda \det(T_{x^\perp})$.
- 4.(a) Let S be an orthogonal operator on \mathbb{R}^2 , or on a two-dimensional subspace of \mathbb{R}^3 , and suppose that $\det(S) = -1$. Show that 1 and -1 are both eigenvalues of S . (Hint: This can be proved using elementary calculations involving the matrix of S ; no big theorems are needed.)
 - (b) Use part (a) to show that if T is an orthogonal operator on \mathbb{R}^3 that has determinant 1 and has -1 among its eigenvalues, then the eigenvalues of T are -1 (with multiplicity 2) and 1 (with multiplicity 1).
 - (c) Conclude that if T is an orthogonal operator on \mathbb{R}^3 that has determinant 1 and has -1 among its eigenvalues, then T is a rotation through an angle of π about some line through the origin.
- 5.(a) Let S be an orthogonal operator on \mathbb{R}^2 , or on a two-dimensional subspace of \mathbb{R}^3 , and suppose that $\det(S) = 1$. Show that for any orthonormal basis of the two-dimensional space, there are real numbers a and b such that $a^2 + b^2 = 1$ and such that the matrix of S with respect to that basis is $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ and hence has the form $\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$ for some real number θ .

⁴An *orthonormal basis* for a finite-dimensional inner product space V is a basis $\{e_i\}$ of V such that $(e_i, e_j) = 0$ if $i \neq j$ and $(e_i, e_j) = 1$ if $i = j$.

bijection from A onto a subset of B and a bijection from B onto a subset of A , then there is a bijection from A onto B (see A.7 in Appendix A).

The following proposition gives an analogous result for G -equidecomposability.

G.2. (Proposition) *Suppose that the group G acts on the set X and that A and B are subsets of X . If A is G -equidecomposable with a subset of B and if B is G -equidecomposable with a subset of A , then A and B are G -equidecomposable with one another.*

Proof. Suppose that A and B are as in the statement of the proposition. Then there are injections $f: A \rightarrow B$ and $g: B \rightarrow A$ that are defined piecewise by the action of G on X . Let us look at how elements of A and B arise as images of elements of B and A under the functions g and f . As is rather standard in proving versions of the Schröder–Bernstein theorem, we express this in terms of ancestors. Consider an element a of A . We call an element b of B a *parent* of a if $a = g(b)$, and an element a' of A a *grandparent* of a if $a = g(f(a'))$. We continue in this way, considering great-grandparents, We view the parents, grandparents, ..., as *ancestors*. In a similar way, we define the ancestors of the elements of B . For example, the ancestors of b are the elements of the sequence $f^{-1}(b), g^{-1}(f^{-1}(b)), f^{-1}(g^{-1}(f^{-1}(b))), \dots$. Since f and g are injective but not necessarily surjective, these sequences may be of any length, containing 0, 1, 2, ..., or even infinitely many terms. Let us define subsets A_e , A_o , and A_∞ of A to be the sets of elements of A for which the corresponding sequence is of even length, of odd length, or infinitely long. We define subsets B_e , B_o , and B_∞ of B similarly. It is not difficult to check that f maps A_e onto B_o and A_∞ onto B_∞ , and that g maps B_e onto A_o . It follows that we can define a bijection $h: A \rightarrow B$ by

$$h(x) = \begin{cases} f(x) & \text{if } x \in A_e \text{ or } x \in A_\infty, \text{ and} \\ g^{-1}(x) & \text{if } x \in A_o. \end{cases}$$

Since f and g are injective and defined piecewise by the action of G , h is also defined piecewise by the action of G , and the proof is complete. \square

Finally, here is a precise version of the Banach–Tarski paradox; we prove it below.

G.3. (Theorem—the Banach–Tarski paradox) *Let A and B be subsets of \mathbb{R}^3 that are bounded and have nonempty interiors, and let G_3 be the group of rigid motions discussed in Example G.1(c). Then A and B are G_3 -equidecomposable.*

Note that the Banach–Tarski paradox says that if $\{A_i\}$ and $\{B_i\}$ are the sets into which A and B are decomposed, then each A_i can be mapped onto the corresponding set B_i using a rigid motion from G_3 . It does not say that the pieces A_i into which A is decomposed can be moved along continuous paths, eventually becoming the corresponding pieces B_i and never colliding with the other pieces. It was long an open problem whether such a continuous decomposition is possible. However, Wilson [129] has recently proved that such decompositions are possible.

In particular, he proves that there are continuous maps $t \mapsto g_t^i$ from $[0, 1]$ to G_3 such that

- (a) $g_0^i \cdot A_i = A_i$ for all i ,
- (b) $g_1^i \cdot A_i = B_i$ for all i , and
- (c) $g_t^i \cdot A_i \cap g_t^j \cdot A_j = \emptyset$ for all t in $[0, 1]$ and all i and j for which $i \neq j$.

Paradoxical Sets

Suppose that the group G acts on the set X . A subset A of X is *G-paradoxical*, or simply *paradoxical*, if it is equal to $A_1 \cup A_2$ for some pair A_1, A_2 of disjoint subsets of A , each of which is G -equidecomposable with A .

The following consequence of the Schröder–Bernstein-like theorem above makes it slightly easier to prove that a set is paradoxical: we can show that a set A is paradoxical by producing disjoint subsets A_1 and A_2 of A that are equidecomposable with A ; we do not need to check that $A = A_1 \cup A_2$.

G.4. (Corollary) *Suppose that the group G acts on the set X . A subset A of X is G -paradoxical if it includes disjoint subsets A_1 and A_2 , each of which is G -equidecomposable with A .*

Proof. Suppose that A, A_1 , and A_2 are as in the statement of the corollary. Then $A - A_1$ is equidecomposable with a subset of A (it is a subset of A), and A is equidecomposable with a subset of $A - A_1$, namely with A_2 . Thus Proposition G.2 implies that A and $A - A_1$ are equidecomposable, and so A_1 and $A - A_1$ form the required partition of A . \square

It is a consequence of the Banach–Tarski paradox that

$$\text{the ball } \{x \in \mathbb{R}^3 : \|x\| \leq 1\} \text{ is } G_3\text{-paradoxical} \quad (1)$$

(if we divide the ball into two pieces by cutting it with a plane through the origin, then the Banach–Tarski paradox says that the ball is equidecomposable with each of the two pieces).

Let us check that we can also derive the Banach–Tarski paradox from (1). So suppose that (1) holds. Certainly if some closed ball is G_3 -paradoxical, then so are all closed balls (two sets that are equidecomposable are still equidecomposable if they are translated or if both are scaled by the same constant). Let A and B be the sets in the statement of the Banach–Tarski paradox, let B_0 be a closed ball included in A , and let r be the radius of B_0 . Let B_1, B_2, \dots be disjoint closed balls, each with radius r . Since B_0 is the union of a pair of disjoint sets, each of which is equidecomposable with B_0 , it follows that B_0 is equidecomposable with $B_1 \cup B_2$. By repeating that argument we can conclude that B_0 is equidecomposable with $B_1 \cup B_2 \cup B_3$, and eventually that it is equidecomposable with $B_1 \cup B_2 \cup \dots \cup B_n$ for an arbitrary n . Since the set B in the statement of the Banach–Tarski paradox is bounded, we can

Since S and $S - D$ are equidecomposable, while $S - D$ is paradoxical, it follows from Corollary G.4 that S is paradoxical. \square

G.10. (Proposition) *The ball B with its center removed, $\{x \in \mathbb{R}^3 : 0 < \|x\| \leq 1\}$, is $SO(3)$ -paradoxical.*

Proof. For each subset E of S let $c(E)$ be the conical piece of the ball B defined by

$$c(E) = \{x \in \mathbb{R}^3 : x = ts \text{ for some } t \text{ in } (0, 1] \text{ and some } s \text{ in } E\}.$$

Thus, for example, $c(S)$ is the ball B with its center removed. We know from Proposition G.9 that the sphere S is $SO(3)$ -paradoxical. If $S = C \cup D$ is a partition of S into sets that are $SO(3)$ -equidecomposable with S , then $c(S) = c(C) \cup c(D)$ is a partition of $c(S)$ into sets that are $SO(3)$ -equidecomposable with $c(S)$; to see this, for instance, in the case of $c(S)$ and $c(C)$, take a bijection $f: S \rightarrow C$ that is piecewise defined by the group action, and note that $tx \mapsto tf(x)$ gives a bijection from $c(S)$ to $c(C)$ that is piecewise defined by the group action. Since $c(S)$ is the ball with its center removed, the proof is complete. \square

Now we can complete the proof of (1) and hence of the Banach–Tarski paradox:

G.11. (Theorem) *The ball B is G_3 -paradoxical, where G_3 is the group of isometries defined in Example G.1(c).*

Proof. Let L be a line in \mathbb{R}^3 that does not pass through the origin 0 but lies close enough to it that none of the rotations about L map 0 to a point outside the ball B (note that the rotations about L belong to G_3 but not to $SO(3)$). Let ρ_0 be a rotation about L through an angle θ , where $\theta/2\pi$ is irrational, in which case the points $0, \rho_0(0), \rho_0^2(0), \dots$ are distinct. Let $D^0 = \{0\} \cup \{\rho_0^n(0) : n \geq 1\}$ and $D^1 = \{\rho_0^n(0) : n \geq 1\}$. Then $B = (B - D^0) \cup D^0$ and $B - \{0\} = (B - D^0) \cup D^1$, and we can modify the last part of the proof of Proposition G.9 to conclude first that B is G_3 -equidecomposable with $B - \{0\}$ and then, since $B - \{0\}$ is $SO(3)$ -paradoxical (Proposition G.10), that B is G_3 -paradoxical. \square

Exercises

Some of the linear algebra needed for this section is developed in the following exercises. In particular, these exercises give a proof that the rotations of \mathbb{R}^3 about lines through the origin are exactly the actions on \mathbb{R}^3 induced by the elements of $SO(3)$.

equidecomposable with A , we can choose a partition G_1, G_2, \dots, G_n of G , a partition A_1, A_2, \dots, A_n of A , and elements g_1, g_2, \dots, g_n of G such that $A_i = g_i \cdot G_i$ for each i . Then the sets $G_1 \cdot C, G_2 \cdot C, \dots, G_n \cdot C$ form a partition of X , the sets $A_1 \cdot C, A_2 \cdot C, \dots, A_n \cdot C$ form a partition of $A \cdot C$, and $A_i \cdot C = g_i \cdot (G_i \cdot C)$ holds for each i . In other words, X and $A \cdot C$ are equidecomposable. A similar argument shows that X and $B \cdot C$ are equidecomposable, and so X is G -paradoxical. \square

Let S be the unit sphere $\{x \in \mathbb{R}^3 : \|x\| = 1\}$, and let B be the unit ball $\{x \in \mathbb{R}^3 : \|x\| \leq 1\}$.

G.8. (Proposition) *Let F be a subgroup of $SO(3)$ that is free on two generators. Then there is a countable subset D of the sphere S such that $S - D$ is F -paradoxical and hence $SO(3)$ -paradoxical.*

Proof. The elements of F , since they belong to $SO(3)$, are distance-preserving as operators on \mathbb{R}^3 ; hence we can view them as acting on the sphere S . Each element of F (other than the identity element) is a nontrivial rotation about a line through the origin (see the remarks just before the statement of Proposition G.7) and so has exactly two fixed points on S . Let D be the collection of all fixed points on S of elements of F other than e . Since the group F is countable, D is also countable.

The elements of F have no fixed points in $S - D$, and $S - D$ is closed under the action of elements of F (for if $x \in S - D$, $f \in F$, and $fx \in D$, then fx would be a fixed point of some nontrivial element f' of F , from which it would follow that $f^{-1}f'fx = x$ and hence that $f^{-1}f'f = e$, which contradicts the assumption that $f' \neq e$). It now follows from Proposition G.7 that $S - D$ is F -paradoxical. Since F is a subgroup of $SO(3)$, $S - D$ is also $SO(3)$ -paradoxical. \square

G.9. (Proposition) *The sphere S is $SO(3)$ -paradoxical.*

Proof. Let F be a subgroup of $SO(3)$ that is free on two generators, and let D be a countable subset of S such that $S - D$ is F -paradoxical (see Proposition G.8). We begin the proof by constructing an element ρ_0 of $SO(3)$ such that the sets $D, \rho_0(D), \rho_0^2(D), \dots$ are disjoint. First we choose as axis for ρ_0 a line L that passes through the origin but through none of the points in D . We can describe the nontrivial rotations with axis L in terms of values (i.e., angles) in the interval $(0, 2\pi)$. For each pair of points x, y in $S - D$ there is at most one rotation about L that takes x to y . Thus there are only countably many rotations ρ about L for which $D \cap \rho(D)$ is nonempty. A similar argument shows that for each n there are at most countably many rotations ρ for which $D \cap \rho^n(D)$ is nonempty. Since there are uncountably many rotations about L , we can choose a rotation ρ_0 such that for every n the sets D and $\rho_0^n(D)$ are disjoint. It follows that for all k and n the sets $\rho_0^k(D)$ and $\rho_0^{k+n}(D)$ are disjoint, and hence that the sequence $D, \rho_0(D), \rho_0^2(D), \dots$ consists of disjoint sets.

Claim. The sets S and $S - D$ are $SO(3)$ -equidecomposable.

Let $D^{1,\infty} = \bigcup_{i=1}^{\infty} \rho_0^i(D)$ and let $D^{0,\infty} = \bigcup_{i=0}^{\infty} \rho_0^i(D) = D \cup D^{1,\infty}$. Then $S = (S - D^{0,\infty}) \cup D^{0,\infty}$ and $S - D = (S - D^{0,\infty}) \cup D^{1,\infty}$. Since $D^{1,\infty} = \rho_0 \cdot D^{0,\infty}$, it follows that S and $S - D$ are $SO(3)$ -equidecomposable, and the claim is established.

choose n large enough that B can be covered with n closed balls of radius r . This implies that B is equidecomposable with a subset of $B_1 \cup B_2 \cup \dots \cup B_n$, and hence with a subset of B_0 , which is itself a subset of A . A similar argument tells us that A is equidecomposable with a subset of B , and then Proposition G.2 implies that A and B are equidecomposable. Thus the Banach–Tarski paradox follows from (1).

We will prove the Banach–Tarski paradox by proving (1). We need to gather some more tools.

Generators and Free Groups

Let G be a group, let S be a set of elements of G , and let $S^{-1} = \{u \in G : u = v^{-1} \text{ for some } v \text{ in } S\}$. The smallest subgroup of G that includes S is called the subgroup *generated by* S . The subgroup of G generated by S has a more constructive description; namely it consists of the elements of G that are represented² by a *word* of the form

$$s_1 s_2 \cdots s_n,$$

where n is a nonnegative integer and s_1, \dots, s_n are elements of $S \cup S^{-1}$.

Now suppose that S generates G and that $S \cap S^{-1} = \emptyset$. Note that if $s \in S$, then the words $ss^{-1}, ss^{-1}ss^{-1}, ss^{-1}ss^{-1}ss^{-1}, \dots$ all represent the same element of G , namely e . Furthermore, a word can be modified by repeatedly removing substrings of the form ss^{-1} or $s^{-1}s$, where $s \in S$, without changing the element of G represented by the word. We can continue this process until we reach a word in which no element of S appears adjacent to its inverse. A word in which no element of S appears adjacent to its inverse is called a *reduced* word.

Let us continue to assume that $S \cap S^{-1} = \emptyset$. The group G is said to be *free* on S , or to be *freely generated* by S , if S generates G and each element of G can be represented in only one way by a reduced word over S . If G is free on S and if S has n elements, then one sometimes says that G is free on n generators.

G.5. (Proposition) *Let F be a free group on two generators. Then the set F is paradoxical under the action of the group F on it.*

Proof. Suppose that F is freely generated by σ and τ and that e is the identity element of F . Let F_σ be the set of all elements of F that can be represented with reduced words that begin with σ , and define $F_{\sigma^{-1}}, F_\tau$, and $F_{\tau^{-1}}$ analogously. The sets $\{e\}, F_\sigma, F_{\sigma^{-1}}, F_\tau$, and $F_{\tau^{-1}}$ then form a partition of the set F . We can check that F and $F_\sigma \cup F_{\sigma^{-1}}$ are F -equidecomposable by writing $F = F_\sigma \cup (\{e\} \cup F_{\sigma^{-1}} \cup F_\tau \cup F_{\tau^{-1}})$ and noting that $F_\sigma = e \cdot F_\sigma$ and $F_{\sigma^{-1}} = \sigma^{-1} \cdot (\{e\} \cup F_{\sigma^{-1}} \cup F_\tau \cup F_{\tau^{-1}})$. A similar argument shows that F is also F -equidecomposable with $F_\tau \cup F_{\tau^{-1}}$. Since F is F -

²The word $s_1 s_2 \cdots s_n$ is the sequence $\{s_i\}_{i=1}^n$, and the element of G represented by the word is the group-theoretic product of s_1, s_2, \dots, s_n . The empty word, where $n = 0$, gives the identity element of G .

equidecomposable with $F_\sigma \cup F_{\sigma^{-1}}$ and with $F_\tau \cup F_{\tau^{-1}}$, it follows from Corollary G.4 that F is F -paradoxical. \square

G.6. (Proposition) *The special orthogonal group $SO(3)$ has a subgroup that is free on two generators.*

Proof. Let us begin with the question of how we might check that suitably chosen elements σ and τ of $SO(3)$ freely generate a subgroup of $SO(3)$. We need to show that distinct reduced words w_1 and w_2 in $\sigma, \sigma^{-1}, \tau$, and τ^{-1} represent distinct elements of $SO(3)$. So assume that w_1 and w_2 are distinct reduced words that represent the same element of $SO(3)$. We can assume that they do not begin (on the left) with the same element, since otherwise we can remove elements from the left until w_1 and w_2 no longer begin with equal elements (this does not change whether the elements of $SO(3)$ represented by w_1 and w_2 are equal or different). So we can assume that either w_1 and w_2 begin with different ones of $\sigma, \sigma^{-1}, \tau$, and τ^{-1} , or else one of w_1 and w_2 is the empty word and the other is not. Our job is to choose σ and τ in such a way that we can conclude that the elements of G represented by such w_1 and w_2 are necessarily distinct.

Suppose that we can find an element u of \mathbb{R}^3 , plus disjoint subsets S_+, S_-, T_+ , and T_- of \mathbb{R}^3 (none of which contains u), such that operating on u by the element of G represented by a non-null reduced word w gives an element of S_+, S_-, T_+ , or T_- , according as the left-hand element of w is $\sigma, \sigma^{-1}, \tau$, or τ^{-1} . If we can find such an element u and sets S_+, S_-, T_+ , and T_- , and if w_1 and w_2 are distinct reduced words as described in the preceding paragraph, then operating on u by the group elements represented by w_1 and w_2 will give different elements of \mathbb{R}^3 , and we will have a proof that w_1 and w_2 represent different elements of $SO(3)$.

The argument just outlined will work if we can verify that our choices of σ, τ, u , S_+, S_-, T_+ , and T_- (with the choices still to be made) satisfy

$$\begin{aligned}\sigma(S_+ \cup T_+ \cup T_- \cup \{u\}) &\subseteq S_+, \\ \sigma^{-1}(S_- \cup T_+ \cup T_- \cup \{u\}) &\subseteq S_-, \\ \tau(S_+ \cup S_- \cup T_+ \cup \{u\}) &\subseteq T_+, \text{ and} \\ \tau^{-1}(S_+ \cup S_- \cup T_- \cup \{u\}) &\subseteq T_-. \end{aligned}$$

Now let us define elements σ and τ of $SO(3)$ by

$$\sigma = \begin{pmatrix} 3/5 & 4/5 & 0 \\ -4/5 & 3/5 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } \tau = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3/5 & -4/5 \\ 0 & 4/5 & 3/5 \end{pmatrix},$$

an element u of \mathbb{R}^3 by $u = (0, 1, 0)^t$, and subsets S_+, S_-, T_+ , and T_- of \mathbb{R}^3 by

$$S_+ = \left\{ \frac{1}{5^k} (x, y, z)^t : k \geq 1, x = 3y \bmod 5, x \neq 0 \bmod 5, \text{ and } z = 0 \bmod 5 \right\},$$

$$S_- = \left\{ \frac{1}{5^k} (x, y, z)^t : k \geq 1, x = -3y \bmod 5, x \neq 0 \bmod 5, \text{ and } z = 0 \bmod 5 \right\},$$

$$T_+ = \left\{ \frac{1}{5^k} (x, y, z)^t : k \geq 1, z = 3y \bmod 5, z \neq 0 \bmod 5, \text{ and } x = 0 \bmod 5 \right\}, \text{ and}$$

$$T_- = \left\{ \frac{1}{5^k} (x, y, z)^t : k \geq 1, z = -3y \bmod 5, z \neq 0 \bmod 5, \text{ and } x = 0 \bmod 5 \right\}$$

(in these definitions k , x , y , and z are integers; furthermore, the t 's on the vectors here indicate transposes, and so we are dealing with column vectors, rather than with the row vectors that are listed). It is now a routine calculation, which is left to the reader, to show that the sets S_+ , S_- , T_+ , and T_- are disjoint, that they do not contain u , and that the inclusions specified above indeed hold. With that we have shown that σ and τ freely generate a subgroup of $SO(3)$, and the proof of the proposition is complete. \square

Details for the Banach–Tarski Paradox

The following proposition will let us use the free group on two generators that we just constructed to get some paradoxical subsets of \mathbb{R}^3 . It is here that the axiom of choice is used.

We will be using the fact that every element of $SO(3)$, when interpreted as an action on \mathbb{R}^3 , is a rotation about a line through the origin,³ and the fact that each such rotation is given by an element of $SO(3)$. For proofs of these results, see the exercises at the end of this appendix.

G.7. (Proposition) *Let G be a group for which the action of G on G is paradoxical, let $(g, x) \mapsto g \cdot x$ be an action of G on a set X , and suppose that this action has no nontrivial fixed points (in other words, suppose that if $g \cdot x = x$ holds for some g and x , then $g = e$). Then the action of G on X is paradoxical.*

Proof. Let x be an element of X , and let $o(x)$ be the orbit of x under the action of G . That is, $o(x) = \{g \cdot x : g \in G\}$. Define a relation \sim on X by letting $x \sim y$ hold if and only if $y = g \cdot x$ for some g in G . It is easy to check that \sim is an equivalence relation and that the equivalence classes of \sim are the orbits of the action of G on X . Use the axiom of choice to create a set C that contains one point from each orbit. We'll use the set C to show that X is G -paradoxical.

Since G is G -paradoxical, there is a partition $A \cup B$ of G such that G is G -equidecomposable with A and with B . Then $X = G \cdot C$, and the sets $A \cdot C$ and $B \cdot C$ form a partition of X (to check the disjointness of $A \cdot C$ and $B \cdot C$, use the assumption that the action of G on X has no fixed points, together with the fact that C contains exactly one element from each equivalence class under \sim). Since G is

³The identity element of $SO(3)$ may seem to be an exception. However, its action on \mathbb{R}^3 can be viewed as a rotation through the angle 0 about an arbitrary line through the origin.