Free Groups and Rotations

Steve Ziskind

April 17, 2026

References

[1] Anders Kaseorg, "The Banach-Tarski Paradox"

[2] Steve Ziskind, "The Banach-Shröder-Bernstein Theorem"

1 Free Groups

A **group** is an algebraic structure consisting of a pair of objects: the set of group elements (G) and a binary operation ($\cdot$) on them, that satisfy these rules:

* associativity $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
* there is an identity element e: $a \cdot e = e \cdot a = a$
* every element has an inverse: $\forall a \exists b = a^{-1}$ for which $a \cdot b = b \cdot a = e$

We will be most interested in the group of rotations of $\mathbb{R}^3$, which can be represented by special 3x3 matrices with ordinary matrix multiplication as the operation. The unit diagonal matrix is the identity.

Given any 2 distinct non-identity elements from a group, σ and τ, we can form all finite words using these letters and their inverses, with the extra rule that any letter adjacent to its inverse collapses to e. An example might be $\tau\sigma\sigma\tau^{-1}\sigma$. With concatenation as the operation, these words form a group called the **Free Group on 2 Generators**.

A key step in proving the Banach-Tarski Paradox will be to show that this set of words can be nicely split into two copies, each having the same size and character as the full set. More specifically, we need a definition.

If a group G acts on a set X, we say that subsets $A, B \subseteq X$ are **G-equidecomposable** if each can be split into the same finite number of pieces, each of which from A can be matched with one from B via a member of G. i.e. each $B_i = g_i A_i$.

For Banach-Tarski the set X will be a 3-D sphere and G will be a group of rotations. But we will stay abstract for the moment.

Word-Splitting Theorem: Let F denote the free group on 2 letters, and define G as the group $F \times \{1, -1\}$ (i.e. each member of G consists of a word and ± 1). Then G is G-equidecomposable with $F \times \{1\}$ and also with $F \times \{-1\}$.

The proof will use a basic set theory fact known as the Banach-Schröder-Bernstein (BSB) Theorem.

BSB Theorem: If a group G acts on a set X, and if each of two subsets $A, B \subseteq X$ is G-equidecomposable to a subset of the other, then A is G-equidecomposable to B.

Without the prefix Banach, this is an obvious fact, but tricky to prove. The proof in (2) includes the property of group action when α and β are group members.

Word-Splitting proof: We will exhibit maps between 4 subsets of G and of $F \times \{1\}$, and then invoke BSB. One direction is obvious: from $F \times \{1\}$ into G we just use the identity injection. The other direction is not so obvious.

With σ and τ as the two generators of words in F, let $W(\rho)$ denote all words beginning with each of those generators or their inverses. Each member of G belongs to one of these:

$$G_1 = W(\sigma) \times \{1\}$$
$$G_2 = (F \setminus W(\sigma)) \times \{1\}$$
$$G_3 = W(\tau) \times \{-1\}$$
$$G_4 = (F \setminus W(\tau)) \times \{-1\}$$

Now break $F \times \{1\}$ into these corresponding four sets:

$$F_1 = (\epsilon, 1)G_1 \qquad = W(\sigma) \times \{1\}$$
$$F_2 = (\sigma^{-1}, 1)G_2 \qquad = W(\sigma^{-1}) \times \{1\}$$

$$F_3 = (\epsilon, -1)G_3 \qquad = W(\tau) \times \{1\}$$
$$F_4 = (\tau^{-1}, -1)G_4 \qquad = W(\tau^{-1}) \times \{1\}$$

We now have (cleverly) mapped all of G to $F \times \{1\}$. Invoking BSB, the Word-Splitting theorem is proved.

2 Rotations

Theorem: There are rotations (ϕ, ρ) of $\mathbb{R}^3$ that are independent. That is, no non-trivial word using them and their inverses equals the identity rotation. Thus they generate the free group F on 2 generators.

Proof: It seems obvious that nearly any two rotations about different axes will do. Unfortunately, Kaseorg's proof (1) seems erroneous. QED

As a corollary, the Word-Splitting Theorem becomes the Rotation-Splitting Theorem.