The Axiom of Choice is clearly true, the Well-Ordering Principle clearly false, and no one can tell about Zorn's Lemma.

– *Unknown*

# 1 The Axiom of Choice

**Defn:** **The Axiom of Choice:** Let $\mathcal{D}$ be a collection of disjoint sets. Then there is a set $X$ so that for every set $D \in \mathcal{D}$, $|X \cap D| = 1$. In other words, we can pick exactly one element from each set in $\mathcal{D}$.

**Ex:** Recall the Cartesian product:

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}$$

This works, because we're picking one thing from $X$, and one thing from $Y$.
How about, instead, an infinite product?

$$\prod_{i=1}^{\infty} X_i = \{(x_1, x_2, \ldots) \mid x_i \in X_i \forall i\}$$

Without the axiom of choice, this set might be empty.
Let $f : X \to Y$ be a surjective function. A **right inverse** for $f$ is a function $g : Y \to X$ so that $f \circ g(x) = x$. How would we find such a function? We should have $g(y) \in \{x \in X \mid f(x) = y\} = f^{-1}(\{y\})$. Okay... but how do we pick one element from this possibly infinite set? Axiom of Choice says it can be done. Constructing $g$ requires choosing one element from each set $f^{-1}(\{y\})$. Oh noes.

**Theorem:** If $R$ is a ring with identity, and $I$ is an ideal, then there is a maximal ideal $M$ with $I \subseteq M$.

**Proof:** In some way, this makes sense. Given any ideal, we can just keep adding stuff to it, and as long as it doesn't become the whole ring, keep adding more stuff. However, it is not clear that this process will ever terminate. We need the Axiom of Choice in order to make this concrete. ∎

But the axiom of choice also gives us some absolutely crazy stuff.

## 1.1 The Banach-Tarski Paradox

Let's take a sphere. Then we'll cut it up in to a few sets, and move those sets around in space (without stretching them - just sliding). What we're left with is two spheres of exactly the same size as the original.

The page `en.wikipedia.org/wiki/Banach_Tarski` is a very good reference.

A sketch of the proof is as follows: Consider $[0, 1)$. Choose as many elements as possible from this interval so that no two of them differ by a rational number. This means things from different cosets of $\mathbb{Q}$ in $\mathbb{C}$. Call this set $X$. Now, consider the translates of $X$:

$$X + \frac{m}{n} = \{x + \frac{m}{n} (\mod 1) \mid x \in X, \frac{m}{n} \in \mathbb{Q}\}.$$

These sets are disjoint. The proof of the Banach Tarski paradox does essentially this to the points on the surface of the sphere, then uses four such translates to create the two new spheres.

## 1.2 Zorn's Lemma

**Defn:** A **partially ordered set** (poset) is a set with a relation $\leq$ which is reflexive, transitive, and antisymmetric. A subset of a poset is **linearly ordered** if any two elements of it are comparable.

**Ex:** The positive integers with relation "$a$ divides $b$".

**Defn:** **Zorn's Lemma:** If $S$ is a nonempty partially ordered set such that every linearly ordered subset has an upper bound in $S$, then $S$ contains a maximal element.

**Ex:** In the example above, with the positive integers and division, we don't satisfy Zorn's Lemma. But if we invert the relation, so that, say $2 > 4$, then we satisfy Zorn's Lemma with the element 1.

**Note:** This is entirely equivalent to the Axiom of Choice – if we have one, we can prove the other.

## 1.3 Back to Ring Theory

Recall the Theorem from the beginning of the lecture.

**Recall:** If $R$ is a ring with identity, and $I$ is an ideal, then there is a maximal ideal $M$ with $I \subseteq M$.

**Proof:** We can now prove this with Zorn's Lemma. Let $I$ be an ideal of $R$. Let $S = \{\text{ideals } J \subset R \mid I \subseteq J\}$, ordered by containment. Let $X$ be a linearly ordered subset of $S$. Take the union of the ideals in $X$, call it $A$. Why is $A$ an ideal? Pick $a_1, a_2 \in A$. Then $a_1 \in x_1 \in X$ and $a_2 \in x_2 \in X$. Since $X$ is linearly ordered, assume (WLOG) that $x_1 \subseteq x_2$. Then $a_1 - a_2 \in x_2 \in A$, and $a_1 r \in x_2 \in A$ for any $r \in R$. Why is $A$ proper? No $x \in X$ contains the identity, so neither does $A$. Thus, this linearly ordered subset $X$ has an upper bound $A \in S$. So we get to apply Zorn's Lemma, and say that $S$ contains a maximal element $M$. Begin a maximal element means that no proper ideals of $R$ contain $M$, which is our definition of a maximal ideal. ■