Week 2

This week, we covered operations on sets and cardinality.

Definition 0.1 (Correspondence)**.** *A correspondence between two sets A and B is a set S contained in $A \times B = \{(a,b)|a \in A, b \in B\}$. A correspondence from A to A is called a relation.*

Definition 0.2 (Equivalence Relation)**.** *An equivalence relation is a relation R on A satisfying the following:*

Reflexivity *For all $a \in A$, $(a,a) \in R$*

Symmetry *If $(a,b) \in R$ then $(b,a) \in R$.*

Transitivity *If $(a,b) \in R$ and $(b,c) \in R$ then $(a,c) \in R$.*

We often denote $(a,b) \in R$ by aRb.

Definition 0.3 (Function)**.** *A function $f : A \to B$ is a correspondence from A to B such that for each $a \in A$, there exists a unique $b \in B$ such that $(a,b) \in f$. We denote $(a,b) \in f$ by $f(a) = b$.*

Definition 0.4 (Injective, Surjective, Bijective)**.** *A function is said to be injective if $f(a) = f(a')$ implies that $a = a'$.*

A function is said to be surjective if for all $b \in B$, there exists $a \in A$ such that $f(a) = b$.

A function is said to be bijective if it is injective and surjective.

Definition 0.5 (Equivalence)**.** *We say that two sets A and B are equivalent, written $A \sim B$ if and only if there exists a function $f : A \to B$ which is a bijection.*

Now, on finite sets, this amounts to them having the same size (see first homework)

Definition 0.6 (Composition of functions)**.** *If $f : A \to B$ and $g : B \to C$ are functions, we define $g \circ f$ by $g \circ f(a) = g(f(a))$.*

Lemma 0.1. *Let $f : A \to B$ be a bijection. Then there exists a function $g : B \to A$ such that $g \circ f(a) = a$ and $f \circ g(b) = b$ for all $a \in A$ and $b \in B$. We call g the inverse of f and denote it by f^{-1}.*

Proof. Define a correspondence g from B to A by $(a,b) \in f$ if and only if $(b,a) \in g$. We will show that g is a function. As f is surjective, for every $b \in B$, there exists $a \in A$ with $f(a) = b$. Thus, for any $b \in B$, there exists some $a \in A$ with $(b,a) \in g$. To see that it is unique, we note that f is injective, and so we have $f(a) = f(a')$ implies $a = a'$. Specifically, that means that if $(b,a) \in g$ and $(b,a') \in g$ then $a = a'$. Thus, for any $b \in B$, there exists a unique $a \in A$ such that $(b,a) \in g$. So g is a function.

To see that the compositions work out, fix $a \in A$. then $g(f(a)) = a$ because $(a, f(a)) \in f$ and $(f(a), a) \in g$. The same argument works for the other composition. $\square$

Proposition 0.2. $\sim$ *is an equivalence relation.*

Proof. For any set A, we have $1_A : A \to A$ the function which has $1_A(a) = a$ for all $a \in A$. This is a bijection $A \to A$, and so $\sim$ is reflexive.

If $f : A \to B$ is a bijection, then $f^{-1} : B \to A$ is also a bijection, and so $\sim$ is symmetric.

If $f : A \to B$ and $g : B \to C$ are bijections, then $g \circ f : A \to C$ is a bijection, and so $\sim$ is transitive. $\square$

So now we have an equivalence relation on sets. Given a set A, we'll call $|A|$ the collection of all sets equivalent to A. We call $|A|$ the cardinal number of A. For finite sets, we use numbers. So $|\{a,b\}| = 2$. This is justified by the fact that the arithmetic we will describe shortly is exactly the usual arithmetic for natural numbers when restricted to finite sets, as you are to prove in your homework.

Now for a couple of examples

Example 0.1. *We will show that $\mathbb{N} \sim \mathbb{Z}$. Any function $f : \mathbb{N} \to A$ for any set A can be thought of as a sequence, or a listing. So, to describe f, we must merely list the elements of A. For $A = \mathbb{Z}$, we can take f to be the list $0, 1, -1, 2, -2, 3, -3, \ldots, n, -n, \ldots$. This function is surjective and injective, and so is a bijection, and demonstrates that $\mathbb{N} \sim \mathbb{Z}$.*

Example 0.2. *We will also show that $\mathbb{N} \not\sim \mathbb{R}$. We'll actually do it by showing that $\mathbb{N} \not\sim [0,1] \subset \mathbb{R}$. Every element of $[0,1]$ can be written as $\sum_{i=1}^{\infty} \frac{a_i}{10^i}$. Now, assume, for contradiction, that there is a bijection $\mathbb{N} \to [0,1]$. Then the number j is sent to $x_j = \sum_{i=1}^{\infty} \frac{a_{ij}}{10^i}$. We now construct a number $x \in [0,1]$ not on the list. Let $x = \sum_{i=1}^{\infty} \frac{a_{ii}+1}{10^i}$ with the convention that $9 + 1 = 0$ rather than 10. Now, x can't be on the list, because it differs with every element of the list in some position. Thus, we didn't have a bijection in the first place, and $\mathbb{N} \not\sim \mathbb{R}$.*

As a convention, we say that if there's an injection $f : A \to B$ that $|A| \leq |B|$. If there's an injection but no bijection, then we say $|A| < |B|$. So the above example in fact says that $|\mathbb{N}| < |[0,1]| \leq |\mathbb{R}|$, and so $|\mathbb{N}| < |\mathbb{R}|$.

Definition 0.7 (Power Set). *Given a set A, define $\mathcal{P}(A)$ to be the set of all subsets of A. Call this the power set of A.*

Theorem 0.3. *For any set A, $|A| < |\mathcal{P}(A)|$.*

Proof. That $|A| \leq |\mathcal{P}(A)|$ follows from the existence of the injection $A \to \mathcal{P}(A)$ given by $a \in A$ maps to $\{a\} \subset A$.

To see that there is no bijection, we assume one exists for contradiction. Let $f : A \to \mathcal{P}(A)$ be a bijection. Then, in particular, it is surjective. So any subset of A that we can describe is in the image. Look at $B = \{a \in A | a \notin f(a)\} \subset A$. Now, there must be an element of A sent to B, and we'll denote it by a_0. Here is where we encounter the problem: can a_0 be in B?

If $a_0 \in B$, then $a_0 \in f(a_0)$ and so $a_0 \notin B$, which is a contradiction. Similarly, if $a_0 \notin B$, then $a_0 \notin f(a_0)$, and so by the definition of B, we have $a_0 \in B$, which is also a contradiction.

So, if we assume that there is a bijection, there is a contradiction, so such a function cannot exist, and $|A| \not\sim |\mathcal{P}(A)|$. □

Though we won't be using it later, we state the following theorem without proof because it's important to know in general:

Theorem 0.4 (Cantor-Schroeder-Bernstein)**.** *Let A and B be sets. If $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$.*

All this says is that instead of looking for bijections, we can just look for injections both ways. The proof actually uses them to construct a bijection, but we won't go into detail there, because it's rather complicated and not relevant at the moment.

Definition 0.8 (Operations on Sets and Cardinal Numbers)**.** *Given two sets A, B, we define the following: $A \times B = \{(a, b) | a \in A, b \in B\}$ the Cartesian product, $A \coprod B = (A \times \{0\}) \cup (B \times \{1\})$ and B^A =the set of all functions $f : A \to B$.*

We define $|A||B| = |A \times B|$, $|A| + |B| = |A \coprod B|$ and $|B|^{|A|} = |B^A|$.

Note that the power set of A can be identified with $\{0, 1\}^A$, and has cardinality $2^{|A|}$.

Definition 0.9 (Partial Ordering)**.** *A partial order on a set A is a relation $\leq$ on A that is reflexive, transitive and antisymmetric (ie, if $a \leq b$ and $b \leq a$ then $a = b$).*

We call a set with a partial ordering a poset. (Partiall Ordered SET)

Definition 0.10 (Total Order)**.** *A partial ordering is a total ordering if for any $a, b \in A$ we have $a \leq b$ or $b \leq a$. A subset of a poset if called a chain if the ordering restricts to a total order on it.*

Example 0.3. *The usual order on the natural numbers is a linear ordering. However, the poset of subsets of a given set ordered by inclusion is not, as for $\{1, 2, 3\}$, neither $\{1, 2\}$ or $\{2, 3\}$ contains the other.*

Definition 0.11 (Well Ordering). *A total ordering on S is a well ordering if every subset of S has a least element.*

Theorem 0.5. *The following are equivalent:*

Axiom of Choice *Given any collection fo nonempty sets A_b indexed by $b \in B$, there exists a function $f : B \to \cup A_b$ such that $f(b) \in A_b$ for all $b \in B$.*

Given any collection of nonempty sets, their product is nonempty.

Well-Ordering Principle *Given a set S, there exists a partial ordering $\leq$ on S which is a well ordering.*

Zorn's Lemma *Given a poset S, if every chain has an upper bound (that is, an element x with $a \leq x$ for all a in the chain) then there exists a maximal element of S. (We say a is maximal if $a \leq x$ implies that $a = x$.)*

Most mathematicians just take the equivalent statements above to hold, though there is some disagreement. For our purposes, we will assume them.

Theorem 0.6. *If A, B are sets, $|A| \leq |B|$, then $|A| + |B| = |B|$.*

Proof. It is simple to check that $|B| \leq |A| + |B| \leq |B| + |B|$, and so it is enough to check that $|B| = |B| + |B|$ for infinite sets. We will proceed using Zorn's Lemma to construct a bijection between B and $B \coprod B = B \times \{0, 1\}$.

Look at pairs (X, f) with $X \subset B$ and $f : X \times \{0, 1\} \to X$ a bijection. First, we must check that such things exist. Now, every infinite set has a subset that is equivalent to $\mathbb{N}$ (Exercise), so we take $C \subset B$ to be such a subset. Then, as $\mathbb{N} \times \{0, 1\}$ is equivalent to $\mathbb{N}$, (To see it, sent $\mathbb{N} \times \{0\}$ to the even natural numbers and $\mathbb{N} \times \{1\}$ to the odd natural numbers) we have $C \times \{0, 1\} \to C$ a bijection. So there exist pairs like this.

Now, we order them to get a poset as follows: $(X, f) \leq (Y, g)$ if and only if $X \subseteq Y$ and $g|_X = f$. That is, for all $x \in X$, $g(x) = f(x)$. That this is a partiall ordering is left as an exercise. Now take any chain with elements (X_α, f_α). Then it has an upper bound given by $X = \cup X_\alpha$ and $f = \cup f_\alpha$. Here is one of the rare times we recall that a function is a set. Now, f will be a function, because once an element of X is assigned a value, it must have the same value forever after. Now, Zorn's Lemma implies the existence of (C, g), a maximal element. Because g is a bijection $C \times \{0, 1\} \to C$, we note that $|C| = |C| + |C|$.

We will now show that $|C| = |B|$. If $B \setminus C$ is infinite, then it would contain $X \subset B \setminus C$ equivalent to $\mathbb{N}$. Then we can take $h : X \times \{0, 1\} \to X$ a bijection, and have $X \cup C$ with $f \cup h$ a bijection from $(X \cup C) \times \{0, 1\} \to X \cup C$. This, however, contradicts C being maximal, and so can't happen. Thus, $B \setminus C$ is finite. So then $B = C \cup (B \setminus C)$, and so $|B| = |C| + |B \setminus C| = |C| + n$ for some finite n. As an exercise, show that for any infinite set, adding a finite number doesn't change the cardinality.

With that, we are done, $|C| + n = |C| = |B|$, and $|C| + |C| = |C|$, so $|B| + |B| = |B|$ and $|A| + |B| = |B|$. ∎

Theorem 0.7. *If A, B are sets, $A \neq \emptyset, B$ infinite and $|A| \leq |B|$, then $|A||B| = |B|$.*

Proof. Here $|B| \leq |A||B| \leq |B||B|$, so all we must show is that $|B||B| = |B|$.

We will again use Zorn's lemma. Look at pairs (X, f) with $f : X \times X \to X$ a bijection. We note that this is nonempty, because there is a subset $D \subset B$ with $D \sim \mathbb{N}$, and $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ given by $(m, n) \mapsto 2^m(2n+1)$ is a bijection. Applying Zorn's lemma in the same way as above gives a maximal element (C, g) with $|C||C| = |C|$.

Now, for contradiction, we suppose that $|B \backslash C| > |C|$. Then there is a subset $D \subset B \backslash C$ such that $D \sim C$. Now, $D \sim C \sim C \times C \sim C \times D \sim D \times C \sim\sim D \times D$, and all of these sets are disjoint.

This tells us that $|(C \cup D) \times (C \cup D)| = |C \times C| + |D \times D| + |C \times D| + |D \times C| = |C| + |C| + |D| + |D| = |C| + |D| = |C \cup D|$, and so there's a bijection $(C \cup D) \times (C \cup D) \to (C \cup D)$, which contradicts the maximality of C. Thus, $|B \setminus C| \leq |C|$, and so $|B| = |C| + |B \setminus C| = |C|$, by the previous. $\square$