Set Theoretical Preliminaries

Let's start out with a brief collection of notation, terminology, and results concerning *set theory*, the underpinning of just about everything we'll do this semester.

You likely learned everything discussed below in some sort of "intro to proofs" class, but it doesn't hurt to review!

For us, a *set* will simply refer to a (finite or infinite) collection of objects of some kind, called the *elements* of the set. If s is an element of the set S, we denote this by $s \in S$. A *subset* of the set T is any collection of objects satisfying $s \in T \Rightarrow s \in S$: everything in T is also in S. This relationship is denoted by $T \subseteq S$; if T is *not* a subset of S, we indicate this by $T \nsubseteq S$.

If we choose to indicate a set by listing out its elements, we enclose the set's elements in "curly brackets": $S = \{s_1, s_2, s_2, ...\}$.

Examples. Let $S = \{1, 2, a, \pi, \heartsuit\}$. Then $1 \in S$ and $\heartsuit \in S$, and $T = \{\pi, a\}$ is a subset of S, so $T \subseteq S$, but $U = \{\heartsuit, \spadesuit\}$ is *not* a subset of S, so $U \nsubseteq S$.

Notice, as in the above example, it doesn't matter in what order we list the elements of a set: order is unimportant.

Given a set S, we may specify a subset T of elements satisfying some particular property P; this newly-specified subset is written as follows:

$$T = \{s \in S \mid s \text{ satisfies } P\},$$

read "T is the set of s in S such that s satisfies property P."

Examples. $C = \{n \in \mathbb{N} \mid n \geq 2 \text{ and } n \text{ is not prime}\}$ is the set of composite numbers. $[-1, 1] = \{r \in \mathbb{R} \mid -1 \leq r \text{ and } r \leq 1\}$ is the closed interval consisting of all real numbers between -1 and 1, inclusive.

As in the above examples, $\mathbb{N} = \{1, 2, 3, ...\}$ is the set of *natural numbers* and $\mathbb{R}$ is the set of *real numbers*. Similarly, $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ is the set of *integers*, and $\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\}$ is the set of *rational numbers*.

If S is a finite set, the *cardinality* of S, denoted $|S|$, is the number of elements in S. Strictly speaking, in this case either S is has no elements, and is thus the *empty set* (denoted $\emptyset$), or there is a *bijection* (a *one-to-one* and *onto* function) between S and the set $[n] = \{1, 2, 3, ..., n\}$ for some $n \in \mathbb{N}$. The cardinality of an infinite set is harder to pin down, but usually we will be concerned only with *countably infinite* sets, whose cardinality is the same as that of $\mathbb{N}$.

We're allowed to form sets whose elements are themselves sets. The most useful such set is the powerset of a given set. If S is given to us, the *powerset* $\mathcal{P}(S)$ is the set of all subsets of S. If S is finite, $|S| = n$ implies $|\mathcal{P}(S)| = 2^n$.

Examples. $\mathcal{P}(\emptyset) = \{\emptyset\}$, the (nonempty!) set whose single element is the empty set. $\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

There are other useful ways of constructing new sets from old ones. Given two sets S and T, the *union* $S \cup T$ and the intersection $S \cap T$ are defined as follows:

$$S \cup T = \{s \mid s \in S \text{ or } s \in T\}, \text{ and } S \cap T = \{s \mid s \in S \text{ and } s \in T\}.$$

We may "repeat" the union operation or the intersection operation, both of which are commutative and associative, so that the order in which the operation is performed is unimportant. Thus, for instance,

$$S_1 \cup S_2 \cup S_3 \cup S_4 = S_3 \cup S_1 \cup S_4 \cup S_2,$$

both sets comprising elements which lie in at least one of the sets S_1, S_2, S_3, or S_4.

The union of a collection of sets $\{S_1, ..., S_n\}$ is often denoted by $\bigcup_{i=1}^{n} S_i$; the intersection $\bigcap_{i=1}^{n} S_i$ is defined similarly.

Examples. If $S_1 = \{1, 5, 6, 7\}$, $S_2 = \{1, 3, 5\}$, and $S_3 = \{5, 8\}$, then $\bigcup_{i=1}^{3} S_i = \{1, 3, 5, 6, 7, 8\}$ and $\bigcap_{i=1}^{3} S_i = \{5\}$.

You should be familiar with the following distributive laws for unions and intersections: if S, T, and U are sets, then

$$S \cup (T \cap U) = (S \cup T) \cap (S \cup U) \text{ and } S \cap (T \cup U) = (S \cap T) \cup (S \cap U).$$

The *Cartesian product* of two sets S and T is the collection

$$S \times T = \{(s, t) \mid s \in S \text{ and } t \in T\}$$

of *ordered pairs* whose first *coordinate* lies in S and whose second lies in T. Notice that in an order pair, the order *is* important, so that (s, t) and (t, s) are two totally different objects! (Compare this with $\{s, t\} = \{t, s\}$.) The distinction between sets and ordered pairs will be a crucial one when we define undirected and directed graphs.

Examples. If $S = \{a, b\}$ and $T = \{1, 2, 3\}$, then

$$S \times T = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$$

and

$$T \times S = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

Notice that $|S \times T| = |S| \cdot |T|$ whenever both S and T are finite.

(This next definition is likely unfamiliar to many of you.) A *multiset* M is a collection of objects in which order is unimportant, but the objects in M are allowed to repeat. (Of course, repetition is not allowed in sets.) If $m \in M$, the *multiplicity* of the element m in M is equal to the number of times m appears in M. If there are only finitely many distinct elements in M and every element $m \in M$ has finite multiplicity in M, we say that M is finite, and its cardinality $|M|$ is the number of elements it contains, counting multiplicities.

Examples. Let $M = \{1, 1, 1, 1, 6, \pi, \pi, \pi\} = \{1, 1, \pi, 6, \pi, 1, \pi, 1\}$. Then the multiplicity of 1 is 4, that of 6 is 1, and that of π is 3. This multiset is finite, and $|M| = 8$. If $E = \{(v, w), (v, w), (v, w), ...\}$, then the multiset E is infinite, since the multiplicity of the ordered pair (v, w) in E is infinite.

Exercises. Before meeting up again tomorrow, please work together to find solutions to the following problems, and be prepared to present your solutions in seminar.

1. Prove one of the distributive laws for union and intersection given above.

2. Let $S \subseteq U$, where U is a *universal* set containing all elements of interest to us. The *complement of* S in U, denoted S^c, is the set $\{u \in U \mid u \notin S\}$. Prove the following *DeMorgan Laws* carefully: if $S, T \subseteq U$, then $(S \cup T)^c = S^c \cap T^c$ and $(S \cap T)^c = S^c \cup T^c$.

3. A function $f : S \to T$ from the set S to the set T is called an *injection* if it is one-to-one: $f(s_1) = f(s_2) \Rightarrow s_1 = s_2$. The function f is called a *surjection* if it is onto: for every $t \in T$ there exists an $s \in S$ such that $f(s) = t$. A *bijection* is a function f that is both injective and surjective.

   (a) Prove that the composition of two injections is an injection. (Recall that if $f : S \to T$ and $g : T \to U$, then $g \circ f : S \to U$ is the *composition* of g with f, defined by $(g \circ f)(s) = g(f(s))$.)

   (b) Prove that the composition of two surjections is a surjection.

   (c) Prove that the composition of two bijections is a bijection.

4. We say that two sets S and T have the same cardinality if there is a bijection f from S to T. Prove that having the same cardinality is an equivalence relation. That is, prove that it this property is *reflexive*, *symmetric*, and *transitive*.

5. Let S be a set (finite or infinite). Let $X = \{0, 1\}^S = \{f \mid f : S \to \{0, 1\}\}$ be the collection of functions from S to the two-element set $\{0, 1\}$. Show that $\mathcal{P}(S)$ and X have the same cardinality by coming up with an *explicit* bijection from $\mathcal{P}(S)$ to X.

6. Prove that the set of natural numbers, $\mathbb{N}$, has the same cardinality as the set of integers, $\mathbb{Z}$, by coming up with an *explicit* bijection from $\mathbb{N}$ to $\mathbb{Z}$.

7. Let S be a given set, finite or infinite. Suppose that $f : S \to \mathcal{P}(S)$ is a bijection. Since the set $A = \{s \in S \mid s \notin f(s)\}$ is a valid subset of S, it's an element in the powerset $\mathcal{P}(S)$. Explain how this set allows us to derive a contradiction, showing that f cannot possibly be a bijection. (*Hint:* since $A \in \mathcal{P}(S)$, there is some $s \in S$ such that...) What does this say about the cardinalities of S and $\mathcal{P}(S)$, relative to one another?

8. Explain how the previous exercise allows us to create infinitely many different sizes of infinite sets.