Purpose: A review of some prerequisite information for taking a course on abstract algebra. Most of this will be reviewed during the first lecture, but it is still recommended that you try to work through it and understand it before class.

Sets

Because we are not taking a class on set theory, we will not go through a rigorous treatment of what a set is. Instead, we rely on our intuition here. What we mean by a *set* is just a "collection of things." A set is just a basket, and the *elements* of the set are just the things in the basket. So, we can define a set of integers, or a set of cats, or even a set of sets. Sets are written with curly brackets $\{$, so we can represent the set of integers between 0 and 5 in writing by $\{1, 2, 3, 4\}$. As a more complicated example, the set whose elements are the sets $\{1, 2, 3\}$, $\{dog, cat, horse\}$, and $\{\&, *, !\}$ can be written as

$$\{\{1, 2, 3\}, \{dog, cat, horse\}, \{\&, *, !\}\}$$

A set is completely defined by its elements, so the sets $\{1, 2, 3\}$ and $\{2, 1, 3\}$ are the same, and we write $\{1, 2, 3\} = \{2, 1, 3\}$. Similarly, $\{1, 1, 2, 3\} = \{1, 2, 3\}$. A special set is the *null set*, which is the set with nothing in it. The null set is represented by the symbol $\varnothing$. Note that $\varnothing \neq \{\varnothing\}$; the left is the null set, and the right is the set containing the null set.

In general, we will denote a set by a normal capital letter (although sometimes different symbols might be used). So, if we write $A = \{1, 2, 3\}$, and then later on we write A, we are referring to the set consisting of the elements 1, 2, and 3. Some special and often used sets are given standard symbols, and are listed here:

$\mathbb{R}$ - the set of real numbers.
$\mathbb{Z}$ - the set of integers.
$\mathbb{C}$ - the set of complex numbers.
$\mathbb{Q}$ - the set of rational numbers.
$\mathbb{N}$ - the set of natural numbers.

We can refer to specific elements of a set by the symbol $\in$. So, if $A = \{1, 2, 3\}$, then we can say $2 \in A$ or $1 \in A$. We can also say that $5 \notin A$ or $dog \notin A$. So, we can say, for example, that $\pi \in \mathbb{R}$ and $\pi \in \mathbb{C}$, but $\pi \notin \mathbb{Q}$.

Before we move on, it's important to introduce some new symbols that we will be frequently using. The symbol $\forall$ means "for all" and the symbol $\exists$ means "there exists." Also, the symbol ! in some contexts means "unique" (you may be used to ! denoting a factorial). Hence, the statement "$\forall x \in A, \exists y \in B$ s.t. $x = y$" can be read as "for every element x in the set A, there exists an element y in set B such that x and y are equal." Two sets A, B for which this statement is true are $A = \{1, 2, 4\}$ and $B = \{1, 2, 4\}$. Two sets A, B for which this statement is not true are $A = \{1, 2, 4, 5\}$ and $B = \{\varnothing, 1, 2, 4\}$ (can you see why?). Note that the words "such that" are often shortened in mathematical writing to *s.t.*.

Now, we can continue with our development of set theoretical language. A set A is a *subset* of the set B if $\forall x \in A$, $x \in B$. When this happens, we write $A \subset B$. Hence, $\{1, 2, 3\} \subset \{1, 2, 3, 4\}$. By default, $\varnothing \subset A$ for all sets A. This is because the statement above that defines what a *subset* is holds true, as there are no elements in A in order to test against the condition. This is known as a statement that is

vacuously true. Another vacuously true statement would be "All unicorns are pink," as there doesn't exist any unicorn with which to test this statement (yes, I know, very sad).

Hence, we can say that

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

Often we will use the symbol $\subsetneq$, to denote a set that is a subset of another set but is not equal to that other set. Note that two sets are equal if and only if each set is a subset of the other set.

As a final term for this section, if $A \subset B$, we denote A^c or $A - B$ as the set of elements that are in B but not in A.

Exercise 1: Consider the following sets:
A =the set of all cats.
B =the set of all animals.
C =the set of all animals with four legs.
$D = \varnothing$
E =the set of all black cats and the set of all dogs.
Which one of these sets are subsets of the others?

Intersections and Unions of Sets

Two operations we can perform between different sets are *intersections* and *unions*. We define the *intersection* of A and B, denoted $A \cap B$, as the following: $x \in A \cap B$ if and only if $x \in A$ and $x \in B$. We define the *union* of A and B, denoted $A \cup B$, as the following: $x \in A \cup B$ if and only if $x \in A$ or $x \in B$. Hence, if $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$, then $A \cap B = \{2, 3\}$ and $A \cup B = \{1, 2, 3, 4\}$. If two sets have no elements in common, then their intersection is the null set.

Two standard results in set theory are the De Morgan Laws, which tell us what happens when we take the complement of an intersection or a union. Namely,

De Morgan Laws

Given n sets $A_1, ..., A_n$, we have that

$$(A_1 \cup ... \cup A_n)^c = A_1^c \cap ... \cap A_n^c$$

and

$$(A_1 \cap ... \cap A_n)^c = A_1^c \cup ... \cup A_n^c$$

Proof: Suppose $x \in (A_1 \cup ... \cup A_n)^c$. This means that $x \notin A_1 \cup ... \cup A_n$, and hence x is not in any of the sets $A_1, ..., A_n$. We conclude that $x \in A_i^c$ for $i = 1, ..., n$, and hence $x \in A_1^c \cap ... \cap A_n^c$. Now, we have just shown that $(A_1 \cup \ldots \cup A_n)^c \subset A_1^c \cap \ldots \cap A_n^c$. To show that these two sets are equal, we must prove the opposite inclusion, or that $A_1^c \cap \ldots \cap A_n^c \subset (A_1 \cup \ldots \cup A_n)^c$. Hence, assume that $x \in A_1^c \cap \ldots \cap A_n^c$. This implies that x is not in any of the sets $A_1, ..., A_n$. Therefore, $x \notin A_1 \cup \ldots \cup A_n$, and therefore $x \in (A_1 \cup \ldots \cup A_n)^c$, and we have proven the first De Morgan Law. The second De Morgan Law follows by similar reasoning (see if you can do this proof!). □

Make sure you can follow this proof, and understand how every statement logically is true. Proofwriting is essentially being able to put down a logical sequence of ideas that leads to a desired conclusion. It takes practice to become proficient at writing proofs, and this class will give you lots of practice. Note that I used the fact that to prove $A = B$, we can just as well prove that $A \subset B$ and $B \subset A$.

The two set-theoretical identities we just proved gives us some insight into how to prove certain types of statements. For example, say we have two statements, S_1 and S_2. If we want to prove that both S_1 and S_2 are true, then we essentially want to show that $S_1 \cap S_2$ is true. If we want to prove that $S_1 \cap S_2$ is not true, then by the just proven result, we have to prove that $S_1^c \cup S_2^c$ is true; that is, that either S_1 is not true or S_2 is not true. This is pretty intuitive if you think about it, but we've now found and proven a method to "negate" statements, or change a statement into its complement. We will find use for logical negation in many proofs.

Maps Between Sets

In high school, you learned about *functions*, which were entities that took in a number and produced one (and only one) number. A map between sets is very similar. For notation, we denote a map f between sets A and B as $f : A \to B$. This function f takes an element of A and assigns it one (and only one) element of B. For any $a \in A$, we denote the element of B that f assigns a to as $f(a)$. Hence, f is fully defined if we know for any $a \in A$, what the value of $f(a)$ is. As an example, consider $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$, and the map $f : A \to B$ such that $f(x) = x - 1$ (which means that $f(3) = 2$ and so forth). Note that if we said that $f(1) = 8$, this would not be well defined, since $8 \notin B$.

For a map $f : A \to B$, we call A the *domain* of f, and B the *codomain*. We call the *image* of f, often denoted as $\text{Im}(f)$ or $f(A)$, as the subset $B_0 \subset B$ such that $\exists a \in A$ such that $f(a) \in B_0$. In simpler terms, the image of f are all the elements of B that are "hit" by f.

Given any $C \subset B$, we define the *inverse image* of C as the subset $f^{-1}(C) \subset A$ such that given $x \in f^{-1}(C), f(x) \in C$. For example, given $g : \mathbb{Z} \to \mathbb{Z}$ such that $g(x) = x + 1$, then if we denote A as all even integers, $f^{-1}(A)$ is precisely the set of all odd integers. If $f(A) = B$, then we say that f is *surjective*. If $f(a) = f(b)$ implies that $a = b$ for all $a, b \in A$, then we say that f is *injective* (which is a fancier word for "one-to-one"). In simpler terms, a map is injective if everything in the function's image is only hit once. If a map is both injective and surjective, then it is *bijective*. The map g defined above is bijective. The map $h : \mathbb{Z} \to \mathbb{Z}$ such that $h(x) = 3x$ is injective but not surjective. Saying that a map is bijective is the same as saying that there exists an inverse for that function.

Proofwriting and Proof Strategies

For this final section, we will go over some general proofwriting strategies that you should know for this course. A proof is just, simply, a sequence of statements that are all logically sound, which leads to some desired result. As beginning proofwriters, it is often easier to organize your proofs by going back to the definitions. For example, to prove that $A \subset B$, we recall that $A \subset B$ means that $\forall x \in A, x \in B$ and then prove that defining statement.

First, a short blurb about what some things you may be asked to prove actually mean. If we want to prove a statement "A if B," this means that we assume B and then show that A is true. If we want to prove a statement "A only if B" then this means that we should assume A is true, and show that B is true. The statements "A if B" and "A only if B" are called converses.

Now, there are a couple of mathematical methods that sometimes give a nice way to do proofs. The three that we will be covering in this section are proof by induction, proof by contrapositive, and proof by contradiction.

First, induction. Suppose that we had a statement A that we wish to show is true for all the positive integers (i.e. the natural numbers). A lot of statements we hope to be true come in this flavor. Consider the following strategy.

(1) Show that A is true for the integer 1.
(2) Show that if A is true for the integer i, then A is also true for the integer $i+1$.

These two statements form the proof strategy known as *induction*. The first half of (2), where we assume that A is true for the integer i, is known as the *inductive hypothesis*. Now, the reason we are done with the proof is that because we know that A is true for 1, it must be true for 2 as well because of (2) above. Similarly, it must be true for 3, and 4, and so on and so forth. Hence, A must be true for all positive integers.

Example: Suppose that there are $n > 1$ people in a room, and every person shakes hands with every other person. Show that there are $\frac{n^2-n}{2}$ handshakes.

Proof: This is obvious for $n = 2$, which is our base case (in this case, we only care about integers greater than 1, so we start at $n = 2$), since there would be 1 handshake in this case. Now, go to the case where we have $n = k$ people. By inductive hypotheesis, there are $(k^2 - k)/2$ handshakes. For the case $n = k + 1$, we will have precisely k more handshakes, since the $k + 1$st person must shake hands with the k people already present. Hence, the number of handshakes is then

$$\frac{k^2 - k}{2} + k = \frac{k^2 + k}{2} = \frac{k^2 + 2k + 1 - k - 1}{2} = \frac{(k+1)^2 - (k+1)}{2}$$

and we are done by induction. □

The second method that we will discuss is contrapositive. Suppose that we would like to prove the statement "if A, then B." By the contrapositive method, we would instead prove the statement "if not B, then not A." It turns out that these two statements are equivalent. I will not prove their logical equivalence here (you can do so easily with some well-drawn diagrams), but will demonstrate the use of this method.

Example: If n is a positive integer such that n mod 4 is 2 or 3, then n is not a perfect square (n mod k is precisely the integer remainder when we divide n by k).

Proof: We go by contrapositive. We therefore prove the statement: If n is a perfect square, then n mod 4 is 0 or 1. This is fairly easy to prove. For n even, we know that $m = \sqrt{n}$ must be even, and hence $m = 2k \Rightarrow n = 4k^2 = 0$ mod 4. For n odd, we know that m must be odd, and hence

$m = 2k + 1 \Rightarrow n = 4k^2 + 4k + 1 = 1 \bmod 4$. Hence, we are done by contrapositive. □

The last method that is used a lot by mathematicians is proof by *contradiction*. Suppose we would like to prove the statement "if A, then B." If we would like to prove this by contradiction, then we first assume A is true but B is false, and show that this set of conditions leads to something silly being true. This is best shown by example, and we offer a classic one:

Example: Show that $\sqrt{2}$ is not rational.

Proof: Assume that $\sqrt{2}$ is rational. Then, we write $\sqrt{2} = p/q$, where p and q are integers and we assume that p and q have no common factors (in other words, we reduce the fraction p/q to its most simple form, which is always possible). We then see that $2q^2 = p^2$, which shows us that p^2 is divisible by 2. However, if p^2 is divisible by 2, then p is divisible by 2 (why?). We thus write $p = 2k$, and we have $2q^2 = 4k^2 \Rightarrow q^2 = 2k^2$. By the same logic, q^2 is divisible by 2 and hence q is divisible by 2. However, we've shown that both p and q are divisible by 2, contradicting our previous assumption that p and q had no common factors. □

Read this proof carefully and make sure you understand where the contradiction came in. Essentially, if $\sqrt{2}$ were rational, we could never express its fraction in lowest reduced form, which makes no sense considering the properties of rational numbers.

These are some of the basic concepts you should be comfortable with as we go through this course. Don't sweat if some (or a lot) of this seems unfamiliar or difficult at the moment - mathematics takes experience, and once you get used to these ideas they will feel much more natural. Enjoy the class!