Supplemental handout - Some basic set theory.

- As you should now be aware, this course deals quite often with *sets*. A set is any collection of objects, e.g. $\{1, 2, 3, 4, 5\}$ is a set of numbers. A vector space is a set of vectors; so is a basis.

- Hopefully, most of you have seen some set notation in earlier courses, but if not, here is a very brief review. (For a really thorough review of set theory, see the Math M112 or Philosophy 134 course).

- Set theory, by itself, is not all that exciting or interesting. However, almost every other branch of mathematics (and algebra, in particular) relies on set theory as its foundation, so it is important to get at least some grounding in set theory before doing other advanced areas of mathematics.

- A *set* S is a collection of objects. If x is an object, we say that x *is an element of* S or $x \in S$ if x lies in the collection; otherwise we say that $x \notin S$. For instance, $3 \in \{1, 2, 3, 4, 5\}$ but $7 \notin \{1, 2, 3, 4, 5\}$.

- One very common way to define a set is to take all the elements of some bigger set which obey a certain property: the set

  $$\{x \in X : x \text{ obeys property} P\}$$

  denotes all the elements x in X which obey a certain property P. For instance,

  $$\{x \in \mathbf{R} : 2 < x < 3\}$$

  denotes all the real numbers strictly between 2 and 3. Sometimes we abbreviate the above notation, e.g. $\{x : 2 < x < 3\}$ or even $\{2 < x < 3\}$, although too much abbreviation often becomes confusing.

- Another way to make sets is to take all the elements x obeying a certain property P, and then apply a function f to each such element:

  $$\{f(x) : x \in X, x \text{ obeys property} P\}.$$

  For instance, the set

  $$\{x + 1 : x \in \mathbf{R}, 2 < x < 3\}$$

denotes all the numbers of the form $x + 1$, where x is a real number strictly between 2 and 3; this is the same set as $\{y \in \mathbf{R} : 3 < y < 4\}$ (as one can see by making a substitution $y := x + 1$).

- A special example of a set is the *empty set* $\emptyset$, also denoted $\{\}$. This set contains no elements, i.e. $x \notin \emptyset$ for all x. All other sets contain at least one element.

- Two sets are *equal*, $S_1 = S_2$, if they have exactly the same elements; every element of S_1 is an element of S_2 and vice versa. Thus, for instance, $\{1, 2, 3, 4, 5\}$ and $\{3, 4, 2, 1, 5\}$ are the same set, since they contain exactly the same elements. If one wants to prove that two sets S_1, S_2 are equal, one has to show two things:

- (a) Every element x of S_1, also belongs to S_2 (i.e. $S_1 \subseteq S_2$);

- (b) Every element x of S_2, also belongs to S_1 (i.e. $S_2 \subseteq S_1$).

- To put it another way, $S_1 = S_2$ if and only if

$$x \in S_1 \iff x \in S_2$$

for all objects x.

- Thus, for instance, if one wants to show

$$\{(x, y, z) \in \mathbf{R}^3 : x + y + z = 0\} = \mathrm{span}\{(1, 0, -1), (1, -1, 0)\},$$

one has to show two things:

- (a) Every element (x, y, z) in $\mathbf{R}^3$ with $x + y + z = 0$, can be written as a linear combination of $(1, 0, -1)$ and $(1, -1, 0)$.

- (b) Every vector (x, y, z) which is a linear combination of $(1, 0, -1)$ and $(1, -1, 0)$, is in $\mathbf{R}^3$ and satisfies the property $x + y + z = 0$.

- A set S_1 is a *subset* of S_2, denoted $S_1 \subseteq S_2$, if every element of S_1 is also an element of S_2:

$$\text{For any } x, \quad x \in S_1 \quad \Rightarrow \quad x \in S_2.$$

Thus for instance $\{1, 2, 4\} \subseteq \{1, 2, 3, 4, 5\}$. Note that every set is considered a subset of itself. We say that S_1 is a *proper subset* of S_2, denoted $S_1 \subsetneq S_2$, if $S_1 \subseteq S_2$ and $S_1 \neq S_2$.

- Given any two sets S_1, S_2, the *union* $S_1 \cup S_2$ of the two sets consists of all the elements which belong to S_1 or S_2 or both. In other words, for all objects x,

  $$x \in S_1 \cup S_2 \iff x \in S_1 \text{ or } x \in S_2.$$

  (In mathematics, "or" refers to *inclusive* or: "X or Y is true" means that "either X is true, or Y is true, or both are true".)

- Meanwhile, the *intersection* $S_1 \cap S_2$ of two sets consists of all the elements which belong to both S_1 and S_2. Thus, for all objects x,

  $$x \in S_1 \cap S_2 \iff x \in S_1 \text{ and } x \in S_2.$$

  Thus for instance, $\{1,2,4\} \cup \{2,3,4\} = \{1,2,3,4\}$, and $\{1,2,4\} \cap \{2,3,4\} = \{2,4\}$. Some more examples: $\{1,2\} \cap \{3,4\} = \emptyset$, $\{2,3\} \cup \emptyset = \{2,3\}$, and $\{2,3\} \cap \emptyset = \emptyset$.

- By the way, one should be careful with the English word "and": rather confusingly, it can mean either union or intersection, depending on context. For instance, if one talks about a set of "boys and girls", one means the *union* of a set of boys with a set of girls, but if one talks about the set of people who are single and male, then one means the *intersection* of the set of single people with the set of male people. (Can you work out the rule of grammar that determines when "and" means union and when "and" means intersection?). One reason we resort to mathematical symbols instead of English is that mathematical symbols always have a precise and unambiguous meaning.

- Note, by the way, that the *union* $V \cup W$ of two vector spaces is not the same thing as the *sum* $V + W$ of two vector spaces; thus Q7 and Q8 of Assignment 1 are referring to two very different things.

- Given two sets A and B, we define the set $A - B$ or $A \backslash B$ to be the set A with any elements of B removed:

  $$A - B := \{x \in A : x \notin B\};$$

  for instance, $\{1,2,3,4\} \backslash \{2,4,6\} = \{1,3\}$. In many cases B will be a subset of A, but not necessarily.

- One has to keep the concept of a set distinct from the elements of that set; for instance, the line $\{(t,t,t) : t \in \mathbf{R}\}$ is not the same thing as the point (t,t,t). To make this more plain, the following two sets are equal:
$$\{(t,t,t) : t \in \mathbf{R}\} = \{(2t,2t,2t) : t \in \mathbf{R}\}$$
(see below), while the following two points are in general not equal:
$$(t,t,t) \neq (2t,2t,2t).$$
Thus, it is a good idea to remember to put those curly braces $\{\}$ in when you talk about sets, lest you accidentally confuse a set with its elements.

- Another example: the sets
$$\{t+1 : t = 1,2,3,4\} \text{ and } \{6-t : t = 1,2,3,4\}$$
are both equal - in fact, they both describe the set $\{2,3,4,5\}$ - even though $t+1$ and $6-t$ are never equal to each other for $t = 1,2,3,4$.

- How does one show that the two sets $\{(t,t,t) : t \in \mathbf{R}\}$ and $\{(2t,2t,2t) : t \in \mathbf{R}\}$ are equal? As we saw, this is not simply a matter of equating the two expressions inside the braces. Well, the first thing to note is that the letter t is being used to denote two different things here. When that happens, it is often helpful to change one of the letters to reduce confusion; for instance one can rewrite $\{(t,t,t) : t \in \mathbf{R}\}$ as $\{(s,s,s) : s \in \mathbf{R}\}$. Clearly this describes the same set. So now we want to show that the two sets
$$\{(s,s,s) : s \in \mathbf{R}\} \text{ and } \{(2t,2t,2t) : t \in \mathbf{R}\}$$
are equal.

- Remember, to show two sets S_1, S_2 are equal, we need to show that every element of S_1 is an element of S_2 and conversely. Applying this to our particular situation, we see that we have to show two things:

- (a) Every point of the form (s,s,s) for some $s \in \mathbf{R}$, is also of the form $(2t,2t,2t)$ for some $t \in \mathbf{R}$.

- (b) Every point of the form $(2t, 2t, 2t)$ for some $t \in \mathbf{R}$, is also of the form (s, s, s) for some $s \in \mathbf{R}$.

- To see (a), just observe that $(s, s, s) = (2(s/2), 2(s/2), 2(s/2))$, so we can write (s, s, s) in the form $(2t, 2t, 2t)$ by setting $t := s/2$. (Note that we are allowed to set t to be whatever we want, so long as it is real, since we only specified "for *some* $t \in \mathbf{R}$", as opposed to, say, "for *all* $t \in \mathbf{R}$"). Similarly to show (b), observe that we can write $(2t, 2t, 2t)$ in the form (s, s, s) by setting $s := 2t$. [Note how confusing (a) and (b) would be if we did not change t to s at the very beginning!]

* * * * *

Images and inverse images

- Now we introduce the concept of a *function*. A function $f : X \to Y$ from one set X to another set Y is an object which assigns to each element x in X, an element $f(x)$ in Y. A very basic property of functions is that if $x = x'$, then $f(x) = f(x')$: functions preserve equality.

- X is sometimes called the *domain* of f, and Y is called the *range*.

- Two functions $f : X \to Y$, $g : X \to Y$ are said to be *equal*, $f = g$, if and only if $f(x) = g(x)$ for *all* $x \in X$. (If $f(x)$ and $g(x)$ agree for some values of x, but not others, then we do not consider f and g to be equal). For instance, the functions $x^2 + 2x + 1$ and $(x + 1)^2$ are equal on the domain $\mathbf{R}$. The functions x and $|x|$ are equal on the positive real axis, but are not equal on $\mathbf{R}$.

- If $f : X \to Y$ is a function from X to Y, and S is a set in X, we define $f(S)$ to be the set
$$f(S) := \{f(x) : x \in S\};$$
this set is a subset of Y, and is sometimes called the *image* of S under the map f. For instance, if $f : \mathbf{R} \to \mathbf{R}$ is the map $f(x) = 2x$, then
$$f(\{1, 2, 3\}) = \{2, 4, 6\}.$$
Thus to compute $f(S)$, we take every element x of S, and apply f to each element individually, and then put all the resulting objects together to form a new set.

- In the above example, the image had the same size as the original set. But sometimes the image can be smaller, because f is not *one-to-one*. For instance, if $f : \mathbf{R} \to \mathbf{R}$ is the map $f(x) = x^2$, then

$$f(\{-1, 0, 1, 2\}) = \{0, 1, 4\}.$$

- Note that

$$f(x) \in f(S) \iff x \in S.$$

- If U is a subset of Y, we define the set $f^{-1}(U)$ to be the set

$$f^{-1}(U) := \{x \in X : f(x) \in U\}.$$

  In other words, $f^{-1}(U)$ consists of all the stuff in X which maps into U. Thus for instance, if $f : \mathbf{R} \to \mathbf{R}$ is the map $f(x) = 2x$, then

$$f^{-1}(\{2, 4, 6\}) = \{1, 2, 3\},$$

  while if $f : \mathbf{R} \to \mathbf{R}$ is the map $f(x) = x^2$, then

$$f^{-1}(\{0, 1, 4\}) = \{-2, -1, 0, 1, 2\}.$$

  We call $f^{-1}(U)$ the *inverse image* of U. Note that f does not have to be invertible in order for $f^{-1}(U)$ to make sense. Also note that images and inverse images do not quite invert each other: in the example of $f(x) = x^2$, note that $f^{-1}(f(\{-1, 0, 1, 2\}))$ did not quite cancel to $\{-1, 0, 1, 2\}$. (In general, what can one say about $f^{-1}(f(S))$ and S? What about $f(f^{-1}(U))$ and U?)

- Note that

$$f(x) \in U \iff x \in f^{-1}(U).$$

- A function f is *one-to-one* if different elements map to different elements:

$$x \neq x' \quad \Rightarrow \quad f(x) \neq f(x').$$

  Thus for instance, the map $f(x) = x^2$ from $\mathbf{R}$ to $\mathbf{R}$ is not one-to-one because the distinct elements -1, 1 map to the same element 1. Equivalently, a function is one-to-one if

$$f(x) = f(x') \quad \Rightarrow \quad x = x'.$$

  One-to-one functions are also called *injective*.

- A function f is *onto* if $f(X) = Y$, i.e. every element in Y comes from applying f to some element in X:

$$\text{For every } y \in Y, \text{ there exists } x \in X \text{ such that } f(x) = y.$$

For instance, the function $f(x) = x^2$ from $\mathbf{R}$ to $\mathbf{R}$ is not onto because the negative numbers are not in the image of f. Onto functions are also called *surjective*.

- Functions $f : X \to Y$ which are both one-to-one and onto are also called *bijective* or *invertible*. If f is bijective, then for every $y \in Y$, there is exactly one x such that $f(x) = y$ (there is at least one because of surjectivity, and at most one because of injectivity). This value of x is sometimes denoted $f^{-1}(y)$; thus f^{-1} is a map from $Y \to X$. We have the cancellation laws $f^{-1}(f(x)) = x$ for all $x \in X$ and $f(f^{-1}(y)) = y$ for all $y \in Y$ (why?).

- The notions of spanning and linear independence are similar to the notions of surjection and injection respectively, while the notion of basis is similar to that of bijection. This can be made precise. Given any collection $v_1, \ldots, v_n$ of vectors in a vector space V, one can consider the map $T : \mathbf{R}^n \to V$ defined by

$$T(a_1, \ldots, a_n) := a_1 v_1 + \ldots + a_n v_n.$$

Now observe that

- (a) T is surjective if and only if the vectors $\{v_1, \ldots, v_n\}$ span V (why?);

- (b) T is injective if and only if the vectors $\{v_1, \ldots, v_n\}$ are linearly independent (why?);

- (c) T is bijective if and only if the vectors $\{v_1, \ldots, v_n\}$ are a basis (why?).

- We will return to these points in the Week 3 notes.

* * * * *

Proofs in set theory

- Here we give some examples of proofs in set theory. The concepts given above are not very deep, and one can understand most things with diagrams (Venn diagrams to understand unions and intersections, and pictures of an arrow from one space to another space to understand functions). Of course, at the end of the day we want a rigorous proof. Despite the fact that most statements in set theory are intuitively obvious, writing a proof requires thinking clearly and unfolding all the definitions methodically. Here is an example:

- **Question:** Let A, B be two subsets of a set X, and let $f : X \to Y$ be a function. Show that $f(A \cap B) \subseteq f(A) \cap f(B)$.

- Before we go to the proof, try drawing a picture of what's going on here.

- **Proof** We have to show that every element of $f(A \cap B)$ is also an element of $f(A) \cap f(B)$. So, let's pick an element $y \in f(A \cap B)$, and try to show that y is also in $f(A) \cap f(B)$. This is the same as showing that y is in $f(A)$ and that y is in $f(B)$.

- Let's first try to show that y is in $f(A)$. Since $y \in f(A \cap B)$, we know from the definition of image that $y = f(x)$ for some $x \in A \cap B$. Since $x \in A \cap B$, we certainly have $x \in A$. But then $y = f(x)$ is in $f(A)$, just from the definition of image again. Similarly y is in $f(B)$, and so y is in $f(A) \cap f(B)$ as desired. $\square$.

- If you are uncomfortable with this type of proof, you might want to try some examples. In the following examples, A, B, C are subsets of a set X, $f : X \to Y$ is a function from X to Y (not necessarily injective, surjective, or invertible), and U, V are subsets of Y.

- (a) Show that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

- (b) Show that $A \subseteq B$ if and only if $A \cup B = B$ and $A \cap B = A$.

- (c) Show that $A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$, and $\emptyset \subseteq A$.

- (d) Show that $(A \backslash B) \cup B = A$, and $(A \backslash B) \cap B = \emptyset$.

- (e) Show that $f(A \cup B) = f(A) \cup f(B)$ and that $f(A) \backslash f(B) \subseteq f(A \backslash B)$.

- (f) Show that $f^{-1}(U \cup V) = f^{-1}(U) \cup f^{-1}(V)$, that $f^{-1}(U \cap V) = f^{-1}(U) \cap f^{-1}(V)$, and that $f^{-1}(U \backslash V) = f^{-1}(U) \backslash f^{-1}(V)$.

- (g) Show that $f(f^{-1}(S)) = S$ for every $S \subseteq Y$ if and only if f is surjective.

- (h) Show that $f^{-1}(f(S)) = S$ for every $S \subseteq X$ if and only if f is injective.

- Note: These exercises are not for course credit! They are just to give you some practice as to how to do the type of proofs which will appear in this course.