MATH 22

Lecture I: 9/30/2003

SETS

A set of phrases learn't by rote . . .

—Jonathan Swift

The union of the mathematician with the poet . . . this surely is the ideal.

—William James, *Collected Essays and Reviews,* ch. 11

Administrivia

- http://denenberg.com/LectureI.pdf
- Anything to discuss from the exam?
- Next exam: Monday 10/27, covers Ch 3, 5, and 4.1

Today: Elementary set theory.

Sets

Although we informally talk about a set as being a collection of objects, this isn't much of a definition. (Because then what's the definition of "collection"?) The notions *set* and *element of a set* are left undefined.

The term *member* is a synonym for "element".

Notation: We write $x \in S$ to mean that object x is an element of set S, $x \notin S$ to mean that object x is *not* an element of set S. We can specify a set in several ways. The following all specify the same set:

$$S = \{\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\ \}$$
$$S = \{\ 1,\ 8,\ 7,\ 6,\ 6,\ 5,\ 4,\ 3,\ 2,\ 1,\ 9,\ 7\ \}$$
$$S = \{\ \text{the positive integers less than } 10\ \}$$
$$S = \{\ x \mid x \in \underline{\boldsymbol{Z}} \ \text{ and } \ 1 \leq x \leq 9\ \}$$
$$S = \{\ x \in \underline{\boldsymbol{Z}} \mid 1 \leq x < 10\ \}$$

(The vertical bar is read "such that". $\underline{\boldsymbol{Z}}$ is the integers since I don't have the right font; similarly $\underline{\boldsymbol{Q}}$, $\underline{\boldsymbol{N}}$, $\underline{\boldsymbol{R}}$, …)

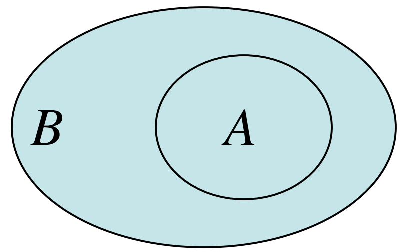
Two sets are *equal* (informally) if they have the same members. That is, if A and B are sets we have

$$A = B \quad \Leftrightarrow \quad (\forall x)\ x \in A \equiv x \in B$$

We'll see a more practical and rigorous definition later.

Subsets, Proper & not

Definition: If A and B are sets, and every element of A is also an element of B, then we say that A is a *subset* of B and we write $A \square B$.



Here's the picture:

Notice that according to our definition A can be a subset of B even if B has no other elements. (That is, the area inside B but outside A might be empty.) But if $A \square B$ and B has at least one element not in A, we say that A is a *proper subset* of B and we write $A \square B$.

Theorem:

If $A \square B$, then $A \square B$

If $A \square B$ and $B \square C$, then $A \square C$

If $A \square B$ and $B \square C$, then $A \square C$

If $A \square B$ and $B \square C$, then $A \square C$

If $A \square B$ and $B \square C$, then $A \square C$

The proofs are basically by picture. Formal proofs are in the text. (The first is trivially by Conjunctive Simplification.)

Element vs Subset

It's sometimes easy to confuse "x is an element of S", that is, $x \in S$, with "A is a subset of S", that is, $A \subseteq S$. This is especially true when S has sets as elements!

Example:

Let N be the set $\{ 1, 2, 3, 4 \}$. Then we have $1 \in N$, and $\{1\} \subseteq N$, but it's not true that $\{1\} \in N$ or that $1 \subseteq N$. We also have $\{ 1, 2 \} \subseteq N$ and $N \subseteq N$. No trouble here.

But now let

$$M = \{ 1, 2, 3, 4, \{1, 2\}, \{ 3, 7 \}, \{ \{ 1 \} \} \}$$

Note that M has seven elements. Now it's true both that $\{ 1, 2 \} \in M$ and also $\{ 1, 2 \} \subseteq M$! It is still not true that $\{ 1 \} \in M$ (why?). And none of the following are true: $7 \in M$, $\{ 7 \} \subseteq M$, $\{ 3, 7 \} \subseteq M$.

Notice that if $X \subseteq Y$ then X *must* be a set, but if $X \in Y$ then X may or may not be a set. Y must be a set in both cases!

(The word *contains* can be especially confusing. Does "A contains B" mean $B \in A$ or does it mean $B \subseteq A$? Usually the former, but avoid the word if there's any chance of ambiguity!)

Equality again

Now we're ready for a useful definition of equality:

Two sets A and B are *equal* if $A \subseteq B$ and $B \subseteq A$.

Why is this useful? Because it gives us a way to test equality that doesn't involve testing all the elements in some unspecified universe. We just need to test each element of A to see that it's in B, and each element of B to see that it's in A. If both are true, then $A = B$.

Typical proof that two sets A and B are equal:

(a) Suppose $a \in A$. Then . . .<stuff>. . . so $a \in B$.

(b) Now suppose $b \in B$. Then . . .<stuff>. . . so $b \in A$.

It follows that $A = B$.

Furthermore, we'll often be able to prove either $A \subseteq B$ or $B \subseteq A$ or both in some more direct way.

The Empty Set

Just for fun, we'll tackle this topic with classical rigor.

Definition: An *empty set* is a set with no elements.
(Grimaldi begs the question by defining "the" empty set. How does he know there's only one?)

Lemma: If S is an empty set, then $S \subseteq X$ for any set X.
Proof: We must prove that for all $x \in S$, $x \in X$. But this is easy, since there are no $x \in S$, so we're done.

Theorem: All empty sets are equal.
Proof: Let S_1 and S_2 be empty sets. Since S_1 is empty, $S_1 \subseteq S_2$ by the Lemma. Since S_2 is empty, $S_2 \subseteq S_1$ also by the Lemma. These two inclusions prove $S_1 = S_2$.

It follows from this Theorem that *there is only one empty set*. So we are justified in speaking of "the" empty set, which we write as $\varnothing$ or $\{\}$. It is also called the *null set*.

Consider the following five sets:

$\varnothing \qquad \{\varnothing\} \qquad \{\{\}\} \qquad \{\varnothing, \{\}\} \qquad \{\{\{\}\}\}$

Which are equal? Which are elements of which? Which are subsets of which? How many elements does each have?

Cardinality / Power Set

The *cardinality* of a set is the number of elements it contains. We write the cardinality of a set S as $|S|$.

Examples:

$$|\{ 0, 1, 2, 3, 4 \}| = 5$$

$$|\{ \text{all primes between 2 and 20} \}| = 7$$

$$|\varnothing| = |\{ \}| = |\{ \text{unicorns} \}| = 0$$

A set whose cardinality can't be measured with any nonnegative integer is an *infinite* set. This is a useless and vague definition; we'll do better later.

The set of all subsets of any set S is called the *power set* of S and is denoted either $P(S)$ or 2^S. Examples:

$$P(\{ 1, 2 \}) = \{ \varnothing, \{1\}, \{2\}, \{1,2\} \}$$

$$P(\underline{\mathbf{Z}}) = \{\varnothing, \underline{\mathbf{Z}}, \{ \text{primes} \}, \{7\}, \underline{\boldsymbol{N}}, \ldots \}$$

$$P(\varnothing) = \{ \varnothing \}$$

Theorem: For any set S, both $\varnothing$ and S are members of $P(S)$.

Theorem: If S has cardinality k, then $P(S)$ has cardinality 2^k. (We've done this proof a zillion times.)

Now you know why it's called 2^S. Note that $|P(\varnothing)| = 1$.

By the way, all this works for infinite sets too.

Set Operations

Just like we have addition and multiplication on numbers, and $\wedge$ and $\vee$ on propositions, we have standard operations on sets.

Definition: Suppose A and B are sets. Then

$$A \cup B = \{ x \mid x \in A \;\; OR \;\; x \in B \}$$

$$A \cap B = \{ x \mid x \in A \;\; AND \;\; x \in B \}$$

We call $A \cup B$ the *union* of A and B; we call $A \cap B$ the *intersection* of A and B.

Example: Let

$$A = \{ \text{ all even integers } \}$$

$$B = \{ 1, 2, 3, 4, 5, 6 \}$$

$$C = \{ -1, 1, -3, 3, -5, 5 \}$$

Then $A \cap B = \{ 2, 4, 6 \}$, $B \cap C = \{ 1, 3, 5 \}$,
$B \cup C = \{ -5, -3, -1, 1, 2, 3, 4, 5, 6 \}$,
and $A \cap C = \{ \}$, the empty set.

Terminology: Two sets A and B are called *disjoint* if their intersection is empty, that is, if $A \cap B = \emptyset$.

Laws of $\cup$ and $\cap$

The following are true for all sets A, B, and C.
The set $\boldsymbol{U}$ is the *universe*, an agreed-upon set that contains everything under discussion. (E.g., the integers or the reals might be $\boldsymbol{U}$. There isn't always a universe!)

Commutativity: $A \cup B = B \cup A$

$A \cap B = B \cap A$

Associativity: $A \cup (B \cup C) = (A \cup B) \cup C$

$A \cap (B \cap C) = (A \cap B) \cap C$

Distributivity: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Idempotency: $A \cup A = A$

$A \cap A = A$

Identity: $A \cup \varnothing = A$

$A \cap \boldsymbol{U} = A$

Domination: $A \cup \boldsymbol{U} = \boldsymbol{U}$

$A \cap \varnothing = \varnothing$

Absorption: $A \cup (A \cap B) = A$

$A \cap (A \cup B) = A$

Containment: $A \cap B \subseteq A \subseteq A \cup B$

Complements

Let A and B be sets. The *relative complement of B in A*, written $A - B$, is the set of things in A that aren't in B:

$$A - B = \{ x \in A \mid x \notin B \}$$

Example: Suppose that $A = \{ 1, 2, 3 \}$, $B = \{2\}$, and $C = \{ 3, 4, 5 \}$.

Then $A - B$ is $\{ 1, 3 \}$, $C - B$ is equal to C,
$A - C$ is $\{ 1, 2 \}$, $C - A$ is $\{ 4, 5 \}$,
$B - C$ is equal to B, and $B - A$ is the empty set.

When a universe $\boldsymbol{U}$ is understood, we can define the *complement of A* as the set of all things that are *not* in A. We write $\underline{A}$ for the complement of A:

$$\underline{A} = \{ x \in \boldsymbol{U} \mid x \notin A \}$$

The complement of A is actually just $\boldsymbol{U} - A$.

As an example, if the universe is all integers and E is the set of even integers, then $\underline{E}$ is the set of odd integers.

NOTE: Normally the complement of A is written with a bar *over* the A. Until I figure out how to do this in PowerPoint, I have to use a bar *under* the A. This notation is not to be used anywhere else!

More Relationships

Double Complement: The complement of $\overline{A}$ (A with two bars) equals A

DeMorgan's Laws:

$$\overline{(A \cup B)} = \overline{A} \cap \overline{B}$$

$$\overline{(A \cap B)} = \overline{A} \cup \overline{B}$$

Inverse Laws:

$$A \cup \overline{A} = \boldsymbol{U}$$

$$A \cap \overline{A} = \varnothing$$

The following statements are equivalent, that is, for any sets A and B they are either all four true or all four false:

$$A \subseteq B$$

$$A \cup B = B$$

$$A \cap B = A$$

$$\overline{B} \subseteq \overline{A}$$

(How do we prove this? There's a trick: We prove that the first statement implies the second, then that the second implies the third, the third implies the fourth, and the fourth implies the first! It follows by transitivity (the Law of the Syllogism) that each implies each.)

One Last Operator

Let A and B be two sets. The *symmetric difference* of A and B, written $A \square B$, is the set

$$A \square B \;=\; A-B \;\square\; B-A$$

That is, $A \square B$ is the set of things that are *either* in A but not in B, *or* in B but not in A. Said yet another way, the set $A \square B$ is the set of things that are *either in A or in B but not both*. [picture needed here]

Example: Let $A = \{ 1, 2, 3 \}$ and $B = \{ 3, 4, 5 \}$. Then $A \square B$ is $\{ 1, 2, 4, 5 \}$.

Note that $A \square B = B \square A$, which explains the name.

Theorem: Two sets S and T are disjoint if and only if $S \square T = S \square T$.

Proof: First assume S and T are disjoint. Then clearly $S-T = S$ and $T-S = T$. So the union of $S-T$ and $T-S$, which by definition is $S \square T$, is equal to $S \square T$.

Now assume $S \square T = S \square T$ and assume that S and T are not disjoint, i.e., there is some element $x \square S \square T$. Clearly x is not in $S-T$ (since it's in T) nor in T–S (since it's in S), hence x is not in $S \square T$ by the definition of $\square$. Since $S \square T = S \square T$ it must be that x is not in $S \square T$ either, which is false. QED [real proof by picture]

Duality Again

Definition: Suppose F is any formula or expression involving only variables that stand for sets, the operators □, □, and complement (overbar), and values $\boldsymbol{U}$ (standing for some understood universe) and $\varnothing$ (the null set). Then the *dual* of F, written F^{d}, is the expression obtained from F by replacing every $\boldsymbol{U}$ with $\varnothing$, every $\varnothing$ with $\boldsymbol{U}$, every □ with □ , and every □ with □.

Example: Let F be the expression $(A$ □ $B)$ □ $\underline{C} = 0$. Then F^{d} is $(A$ □ $B)$ □ $\underline{C} = \boldsymbol{U}$. Note that $(F^{\mathrm{d}})^{\mathrm{d}} = F$.

Theorem: If T is a theorem about sets containing only the symbols described above, then T^{d} is also a theorem.

The expression A □ B cannot be "dualized" as written. But we know that A □ B is equivalent to the expression A □ $B = B$. Taking the dual of this, we get A □ $B = B$, which is equivalent to B □ A. This shows that the dual of A □ B is B □ A.

Note how many of the equalities are duals of each other.

Venn Diagrams

In previous slides we've seen concepts presented by use of fairly intuitive pictures. These pictures are called *Venn Diagrams*. They lead to good intuitive understanding (but don't constitute rigorous proof).

Traditionally, sets are represented by circles, and the understood universe ***U*** by an all-enclosing box.

[At this point we'll draw some pictures on the board and show some theorems by means of Venn Diagrams. No chance that I'm going to try to do it in PowerPoint.]

[We'll also discuss, for fun, the use of Venn Diagrams to prove the classical syllogisms in A, E, I, and O, including the necessary extensions.]

Index Sets

(This is a slide about notation.) We know how to write

$$\sum_{i=1}^{n} x_i$$

It should come as no surprise that we can write

$$\bigcup_{i=1}^{n} S_i \; = \; S_1 \cup S_2 \cup S_3 \cup \ldots \cup S_n$$

where each S_i is a set, and the same for intersection.

There is a more general way of using this notation. Suppose we have any set I, and for each $i \in I$ we have a set S_i. Then we can "union up" all the sets S_i with

$$\bigcup_{i \in I} = \{ x \mid x \in S_i \text{ for } \textit{at least one } i \in I \}$$

A set I used in this way, where each element of I labels some set S_i, is called an *index set*. An index set need not hold only integers; it can hold all kinds of objects.

We also have

$$\bigcap_{i \in I} S_i = \{ x \mid x \in S_i \text{ for } \textit{every } i \in I \}$$

Example: Suppose we use $\boldsymbol{Q}$, the rationals, as an index set, and for each rational number $q \in \boldsymbol{Q}$ define S_q to be the real numbers between $-q$ and q inclusive. Then

$$\bigcap_{q \in \boldsymbol{Q}} S_i = \{ 0 \}$$

[Russell’s Two MDs]

Is every “collection of objects” a set?
The answer, surprisingly, is no!

Consider the following “set”:

P = { those sets that are elements of themselves }

or, said another way,

$$P = \{ X \mid X \text{ is a set and } X \in X \}$$

For example, let S be the set of all sets. Since S is itself a set, it is a member of itself, that is, $S \in S$! Since P is, by definition, the sets that have this weird property, we have $S \in P$. Another example of a set in P is the set I of all infinite sets. Since I is itself an infinite set, we must have $I \in I$, so $I \in P$.

Now we don’t really care about P. We just care about:

N = {those sets that are *not* elements of themselves}

or

$$N = \{ X \mid X \text{ is a set and } X \notin X \}$$

For example, $\underline{\mathbf{Z}}$ is not a member of itself, since $\underline{\mathbf{Z}}$ is not an integer. That is, $\underline{\mathbf{Z}} \notin \underline{\mathbf{Z}}$, thus $\underline{\mathbf{Z}} \in N$. Similarly for the set of all dogs and the set of all finite sets. Any set that is *not a member of itself* is, by definition, in N.

[Russell, contd.]

We now ask the following question: Is the set N an element of itself, or is it not? That is, is it the case that $N \in N$, or is it the case that $N \notin N$? (Clearly it's one or the other!)

Suppose $N \in N$. Well, if $N \in N$ then N is *not* a member of itself (since that's the definition of N!). That is, if $N \in N$ then $N \notin N$, a contradiction.

So it must be that $N \notin N$. But if $N \notin N$, then, again by the definition of N, it must be that $N \in N$, which we just proved impossible!

Look what we did: We assumed only that the set N exists, and we proved a contradiction. It follows by every rule of logic that *the set N, as specified, does not exist*. It turns out that there are lots of sets that you can specify but that do not exist.

This phenomenon is known as *Russell's Paradox*. It forced a reformulation of set theory to take care of the question of what could and couldn't be considered a set. In modern set theory, no set can be an element of itself.