MATH 25 CLASS 2 NOTES, SEP 23 2011

Contents

Quick links to definitions/theorems

- Set definition
- The method of induction
- Definition of divisibility

1. Set notation

Before delving into number theory proper, we will spend a few moments discussing some preliminary ideas. One of the most fundamental concepts in mathematics is that of a **set**. Instead of giving a precise definition (which turns out to be quite hard), we will content ourselves by informally defining a set as follows:

Definition 1 (Informal)**.** *A **set** is an unordered collection of distinct objects.*

A set can have either finitely many or infinitely many objects. We often use various letters or other symbols to denote a set. If we want to actually list the elements, in a set, we use curly braces, { and }, to delimit the objects in a set. For instance, if S consists of the numbers $1, 2, 3$, we may write $S = \{1, 2, 3\}$. If an object x is in the set S, we say that x is an **element** of S, and sometimes write this using the notation $x \in S$. That symbol looks like an epsilon, but isn't the same. An object can only belong to a set once or not at all – an object cannot be an element of a set more than once. (If you want to allow multiple copies of the same element in a set-like object, you should look at *multisets*.) The elements of a set do not have to be numbers; they can be whatever you want them to be. For example, the set of past and current US Presidents consists of forty-three men. (Notice that although Grover Cleveland was President on two non-consecutive occasions, he is only counted once in the above set.) Elements of sets can be functions, geometric objects, and even other sets, and we may freely mix and match any of these types of objects in a given set.

If a set has infinitely many elements, and we want to list the elements of that set, what do we do? Obviously we can't write them all down. In most situations, we will be able to describe the elements of an infinite set by describing some common property that 1) objects in the set satisfy, and 2) objects not in the set do not satisfy. For instance, perhaps S is the set of all positive integers which end in the digit 5. Then we may write $S = \{x | x \text{ is a positive integer ending in } 5\}$. In general, if $P(x)$ is some statement about the number x, we write $\{x | P(x)\}$ for the set of elements which

make $P(x)$ true. If we want to initially restrict our attention to elements in a set X, we write $\{x \in X | P(x)\}$. For example, $\{x \in \mathbb{Z} | x > 0\}$ is the set of positive integers, while $\{x \in \mathbb{R} | x > 0\}$ is the set of positive real numbers.

We may want to want to assemble new sets from old sets. Let A, B be two sets. Then we write $A \cup B$ for the set consisting of all elements either in A or in B and call this the **union** of A and B. Similarly, we write $A \cap B$ for the set consisting of all elements in both A and B, and call this the **intersection** of A and B. For example, if $A = \{0, 1, 2\}$ and $B = \{1, 3\}$, then $A \cup B = \{0, 1, 2, 3\}$ while $A \cap B = \{1\}$. (Again, notice that although 1 is in A and B, it still only appears once in the set $A \cup B$.)

2. Logical statements

Math is primarily about determining the truth value of various statements. For example, a statement like "The number 3 is even" is obviously false, while the statement "The area of a circle of radius r is πr^2" is true, but non-trivial to prove. In what follows, P and Q will be generic statements which are either true or false.

The language of mathematics is packed with statements of the form 'If P, then Q', where P, Q might be statements which can be either true or false. For example, the statement 'If S is a square, then S is a rectangle' is a true statement, while the statement 'If $f : \mathbb{R} \to \mathbb{R}$ is integrable, then f is continuous' is a false statement. Notice that to disprove this statement, we need only exhibit one counterexample; for instance, any piecewise continuous function (which itself is not continuous) will do. We write $\sim P$ for the *negation* of P. This is the statement which is false exactly when P is true, and can be obtained from P by adding the word 'not'. For example, if P is the statement 'S is a square', then $\sim P$ is the statement 'S is not a square'.

We bring all this up because the statement 'If P, then Q', can be expressed in several other ways. The mathematical shorthand for this statement is $P \implies Q$, which we sometimes read 'P implies Q'. Two other forms this statement might take are 'P is a sufficient condition for Q', or 'Q is a necessary condition for P'. The first statement says that as long as P is true, then Q is true, which is exactly what the original statement says, and the latter statement says that Q must be true if P is true: that is, if P is true, then Q is also true. Another way of saying 'If P, then Q' is by saying 'P is true only if Q is true', or more succinctly, 'P only if Q'. (The word 'only' is of critical importance, since omitting it completely changes the logical content of the statement.)

An important logical point is that the statement $P \implies Q$ **IS NOT ALWAYS EQUIVALENT** to the statement $Q \implies P$. We say two statements are equivalent if one is true exactly when the other is true. For example, consider the statement 'If S is a square, then S is a rectangle'. In this statement, P is 'S is a square', while Q is 'S is a rectangle'. Then it is obvious that $Q \implies P$ is false, since the statement 'If S is a rectangle, then S is a square' is clearly not true. The statement $Q \implies P$ is sometimes called the *converse* of $P \implies Q$.

On the other hand, $P \implies Q$ is logically equivalent to the statement $\sim Q \implies \sim P$, which is sometimes called the *contrapositive* of $P \implies Q$. This might not be obvious, but a careful consideration of what it means for $P \implies Q$ to be true, or consideration of a few examples, will explain why this statement is true.

Finally, the *inverse* of $P \implies Q$ is the statement $\sim P \implies \sim Q$. This is the contrapositive of the converse, so while the inverse and converse are logically equivalent to each other, whether the inverse and converse are true is independent of whether the original statement $P \implies Q$ is true.

Example. Let n be an integer, and let P be the statement "n ends in the digit 0", and Q the statement "n is even". Then $P \implies Q$ is evidently true, since any number which ends in 0 must be even. The converse is the statement "If n is even, then n ends in the digit 0", which is clearly false (n ending in $2, 4, 6, 8$ are all counterexamples), while the contrapositive is the statement "If n is not even, then n does not end in the digit 0". Finally, the inverse is the statement "If n does not end in the digit 0, then n is not even", which obviously is false, for the same reasons the converse is false.

To study these issues from logic closely is actually very subtle and deep, and goes far beyond the content of this class. We will only need the informal observations made above.

3. Proof by induction

Often, a mathematical statement will make an assertion which can be parameterized by positive integers. For example, there is a story about the young C. F. Gauss. One day, when he was ten years old, his teacher, who apparently was not very creative, told his students to sum all the numbers from 1 to 100 before they could go to recess (or something like that). While his classmates were furiously adding $1+2+3+\ldots$, Gauss reflected for a few seconds, wrote a number down on his board, and then turned it in. Of course, he was right, and the number he wrote down was 5050.

Gauss realized that $1 + 2 + \ldots + n = n(n+1)/2$. Before describing how he did it, let's talk about how one uses induction to prove this formula. First, notice that this formula is a statement about all positive integers n. Let $P(n)$ be this statement for the particular value of n; for instance, $P(2)$ is the claim that $1 + 2 = 3$, while $P(4)$ is the claim $1 + 2 + 3 + 4 = 10$. Notice that simple calculation shows that both $P(2)$ and $P(4)$ are true.

If we want to prove $P(n)$ is true for all positive n, we probably can't use brute force. Induction is a general strategy for proving that a statement is true for all positive integers n. It consists of two steps:

- Prove $P(1)$ is true (this is usually easy), and
- Prove that, for any positive n, if $P(n)$ is true, then $P(n+1)$ is also true.

Why does this work? Suppose we've proven both statements true. In particular, we know $P(1)$ is true. But then the second statement tells us that $P(2)$ is true, which in turn tells us that $P(3)$ is true, ad infinitum. So we've proven that $P(n)$ is true for every positive integer n. A way to visualize the induction strategy is to think about setting up an infinite chain of dominos. If $P(n)$ corresponds to toppling the nth domino over, then the first step corresponds to knocking the first domino in the chain over, and the second step corresponds to setting up the dominos in such a way so that if the nth domino falls, then the $n+1$th domino does as well.

Let's use this strategy to prove the formula for the sum of the first n positive integers. First, verifying $P(1)$ is trivial; it's just the statement $1 = 1$. Next, suppose $P(n)$ is true. We write out what this means:

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}.$$

We want to show that $P(n+1)$ is true. This is a statement about $1+2+\ldots+n+(n+1)$, so it makes sense to add $n+1$ to both sides of the equation above. This gives

$$1 + 2 + \ldots + n + (n+1) = \frac{n(n+1)}{2} + (n+1).$$

Remember, we're trying to prove the statement $P(n+1)$, which is the equation

$$1 + 2 + \ldots + n + (n+1) = \frac{(n+1)(n+2)}{2}.$$

The LHS (left hand side) of these two equations are equal. One easily checks that the RHS are equal as well. So we've proven that if $P(n)$ is true, then $P(n+1)$ is true as well. Then induction tells us that $P(n)$ must be true for all n, as desired.

Of course, one could cosmetically modify induction by not starting with $P(1)$; for instance, one might only want to prove $P(n)$ is true for all $n \geq 3$, in which case one starts by proving $P(3)$ instead of $P(1)$. But the general idea is the same.

Incidentally, this isn't the way Gauss discovered the formula $P(n)$. He realized that if you sum the first and last terms in $1 + 2 + \ldots + n$, you get $n + 1$. If you sum the second and second to last terms, you also get $n + 1$. One continually pairs the integers in this way to get some number of pairs summing to $n + 1$. If n is even, there are exactly $n/2$ such pairs, while if n is odd, there are $(n-1)/2$ pairs, with the middle number of $(n+1)/2$ by itself. In both cases, adding up these terms gives $n(n+1)/2$.

Exercise 1. Use induction to prove the following equation for the sum of the first n squares:

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

4. Divisibility

Let's start with some number theory proper. Let a and b be two integers (not necessarily positive, although most cases we consider will be positive integers).

Definition 2. *We say that b **divides** a if there exists an integer q such that $a = qb$. We sometimes write this as $b|a$. If b does not divide a, then we sometimes write $b \nmid a$. If b divides a, we sometimes say that b is a **divisor** of a.*

Let's look at some basic examples and prove some basic facts about divisibility.

Examples.

- One has $3|12$, say, while $2 \nmid 5$, because $12 = 3 \cdot 4$, while $5 = 2 \cdot (2.5)$, and 2.5 is not an integer. Notice that $b|a$ is the same thing as saying that a is a multiple of b.

- Let's prove a few facts from Exercise 1.3 of the book. First, we'll prove that if $a|b$ and $b|c$, then $a|c$.

  Proof. Since $a|b$ and $b|c$, we can find integers q_1, q_2 such that $b = q_1 a, c = q_2 b$. Substitute the first equation for b into the second; we get $c = q_2 q_1 a$. Since $q_2 q_1$ is an integer, $a|c$, as desired. □

  (What's that box for at the end? It signifies that we've finished our proof, and is meant as a way to organize our writing.)
- Another fact is that if $a|b$ and $b|a$, then $a = \pm b$.

  Proof. Write $b = q_1 a, a = q_2 b$. Again, substituting the first into the second equation, we get $a = q_1 q_2 a$. At this point, we want to cancel a from both sides. However, we can only do this if $a \neq 0$. So let's first analyze what happens if $a = 0$. If $a = 0$, then the equation $b = q_1 a = 0$ tells us $b = 0$ as well, so $a = \pm b$ is definitely true in this case. So now that we've handled what happens if $a = 0$, we can go back to $a \neq 0$ case. We can cancel a from both sides of $a = q_1 q_2 a$, which gives $q_1 q_2 = 1$. However, the only way two integers multiply to 1 is if they are both equal to 1 or ± 1. This implies that $b = \pm a$, as desired. □

- Here is a useful fact (Theorem 1.3a of the text). If $c|a_1, a_2, \ldots, a_k$, then $c|(a_1 u_1 + \ldots + a_k u_k)$ for any integers $u_1, \ldots, u_k$.

  Proof. Since $c|a_i$ for all i, we have $a_i = c q_i$ for some integer q_i. Then $a_1 u_1 + \ldots + a_k u_k = c(q_1 u_1 + \ldots + q_k u_k)$. Since $q_1 u_1 + \ldots + q_k u_k$ is an integer, this implies that $c|(a_1 u_1 + \ldots + a_k u_k)$, as desired. □

- As an illustration of this fact, we know that $3|6, 15$, say. Then this fact tells us that $3|(6x + 15y)$, for any integers x, y.

In one of the proofs above we see that there are occasions where we might need to do a *case-by-case* analysis. Always be wary when you divide an equation by a number, for example, because it is illegal to divide by 0 and you may need to separately analyze what happens if that number is equal to 0.

Exercise 2. You should consult Exercise 1.3 of the text for more basic properties. Let's look at a few of them now. Suppose $d|a$. Is it necessarily true that $|d| \leq |a|$? Why or why not? If not, how might you slightly modify this statement to make it true?