Midterm Review
Math 2000A

Sean Fitzpatrick

The midterm for Math 2000A takes place in class on Thursday, October 16th. You're responsible for the material covered in class up to (and including) the lecture on Thursday October 9th. This includes Chapters 1-7 and section 8.1 in the textbook, as well as any handouts posted on Moodle.

Chapter 1: Assertions

The material in Chapter 1 consists mainly of basic terminology. The two main questions answered in Chapter 1 are:

- What makes a sentence an assertion? (Assertions are sometimes also referred to as statements.)
- What is a deduction, and when is it valid?

You'll recall that an **assertion** must have a definite truth value; that is, it must be either true or false (but not both). A **deduction** consists of a series of assertions, called hypotheses, followed by another assertion, known as the conclusion. A deduction is **valid** if the conclusion is true whenever all of the hypotheses are true.

Note that our definition of a valid deduction is a conditional statement: **if** the hypotheses are true, **then** the conclusion is true. To better understand conditional statements, we will introduce the formalism of propositional logic in Chapter 2.

Exercises:

1. Which of the following sentences are assertions?
   (a) The integer 24 is even.
   (b) Is the integer $3^{15} - 1$ even?
   (c) The product of 2 and 3 is 7.
   (d) The sum of x and y is 3.
   (e) If the integer x is odd, is x^2 odd?
   (f) It is not possible for $3^{15} - 1$ to be both even and odd.
   (g) The product of x^2 and x^3 is x^6.

(h) The integer $2^{524287} - 1$ is prime.

Note: A sentence such as "If x is even, then x^2 is even" occupies a bit of grey area: it involves a variable x, but the sentence is true, regardless of the value of x. In Chapter 7 we learn that we can eliminate the ambiguity by writing this as an assertion with a universal quantifier: "For all $x \in \mathbb{Z}$, if x is even, then x^2 is even." In class we discussed the fact that conditional statements sometimes have a hidden/assumed universal quantifier, so that something which appears to be an assertion may in fact be a predicate. In any case, I'll avoid trying to trick you with something like this on the midterm.

Chapter 2: Propositional logic

In Chapter 2, we begin to formalize the ideas in Chapter 1. A general discussion of deductions and their validity is too cumbersome to handle without some introduction of notation and guidelines. In propositional logic, we use letters to represent assertions. For example, we might have a deduction such as the following:

$$\begin{aligned} &Hypotheses: \\ &\qquad n \text{ is an integer} \\ &\qquad n \text{ is even} \\ &\qquad n \text{ is not a multiple of } 4 \\ &Conclusion: n = 2k, \text{ where } k \text{ is odd} \end{aligned}$$

We try to simplify discussion of this deduction by introducing a **symbolization key**: we let H_1, H_2, H_3 represent our three hypotheses, and let C represent our conclusion, as follows:

$$\begin{aligned} H_1 &: n \text{ is an integer} \\ H_2 &: n \text{ is even} \\ H_3 &: n \text{ is not a multiple of } 4 \\ C &: n = 2k, \text{ where } k \text{ is odd} \end{aligned}$$

Our deduction can then by put in the form $H_1, H_2, H_3; \therefore C$. Typically, we start with basic assertions such as the above, often known as primitive or simple assertions. From these we can build more complicated "compound" assertions using logical operators called **connectives**. The basic logical connectives are as follows, where P and Q represent any assertions:

Operation	Also known as	Symbol	Meaning
Negation	"not"	$\neg P$	It is not the case that P
Conjunction	"and"	$P \wedge Q$	Both P and Q
Disjunction	"or"	$P \vee Q$	Either P or Q
Conditional	"implies"	$P \rightarrow Q$	If P, then Q
Biconditional	"iff"	$P \leftrightarrow Q$	P if and only if Q

You are expected to be familiar with the truth values of each of these compound statements, given the truth value of P and Q. For example, $\neg P$ is true if P is false, and vice-versa.

The conjunction $P \wedge Q$ is true only when both P and Q are true, and is false in all other cases. The disjunction $P \vee Q$ is true if P is true, or Q is true, *or both*.[1] We say that two assertions are **logically equivalent** if they have the same truth values. Usually this applies to compound statements. For example, the equivalence

$$A \vee B \equiv B \vee A$$

is the statement that the assertion $A \vee B$ will be true whenever $B \vee A$ is true, and vice-versa. In fact, logical equivalence is can be expressed as a biconditional statement: $P \equiv Q$ means the same thing as $P \leftrightarrow Q$. Note that a biconditional statement is a pair of conditional statements: $P \leftrightarrow Q$ is equivalent to $(P \to Q) \wedge (Q \to P)$.

For the purposes of mathematics (proving theorems and so forth), the conditional statements are perhaps the most important, and the ones you should be most sure that you understand. We noted above that a deduction can be put into the form of a conditional statement: the deduction $H_1, H_2, \ldots, H_n; \therefore C$, where the H_i are our hypotheses, and C is the conclusion, can be put in the form

$$H_1 \wedge H_2 \wedge \cdots \wedge H_n \to C,$$

since a deduction is valid if C is true whenever *all* of the hypotheses are true. The most common example of a valid deduction is *Modus Ponens*, which has the general form

$$P \to Q, P; \therefore Q.$$

In Chapter 3 on two-column proofs, Modus Ponens is known as "$\to$-elimination". This is the observation that if our conclusion C follows from our hypotheses, and the hypotheses are true, then C must also be true. (This is just a restatement of what it means for a deduction to be valid.) It is very important to make sure that you understand the logical structure of the Modus Ponens deduction, since it's the logical backbone of many, many results. It's also one that people mix up far too often. Note that it is **never** possible to conclude P from a conditional statement $P \to Q$, **even if we know Q is true**. P must be *assumed*, or *given*. The fallacy of concluding P from $P \to Q$ is sometimes known as "begging the question". (Which is itself a phrase that is misused far too often!) The truth table for $P \to Q$ is

P	Q	$P \to Q$
T	T	T
T	F	F
F	T	T
F	F	T

Note in particular that it's possible for P to be false when both $P \to Q$ and Q are true. It is only when P is true and Q is false that $P \to Q$ fails to be true. This leads to the

[1] It is also possible to consider the "Exclusive Or" which allows for P or Q to be true, but not both. We don't make use of the exclusive or in this course. If it is ever needed, it will be made explicitly clear that we are using the exclusive or. (Some people appeared to have the impression that in an assertion given in English, the placement of a comma – a *comma!* – would make the difference between the usual inclusive or and the exclusive or. This sort of cruel and unusual trickery will never be employed in this course.)

logical equivalence $\neg(P \to Q) \equiv P \wedge \neg Q$; another equivalence established in class was $P \to Q \equiv \neg P \vee Q$.

Recall that a **tautology** is an assertion (denoted by T) that is always true, and that a **contradiction** is an assertion (denoted by F) that is always false. The two most important examples are given by the **Law of the Excluded Middle**: for any assertion P,

$$P \vee \neg P \equiv T \quad \text{and } P \wedge \neg P \equiv F.$$

With this terminology in place, we can codify the rules of propositional logic in terms of logical equivalences and basic valid deductions. Since you already have a **handout** on Moodle with a list of the most common logical equivalences (de Morgan's laws, distributive rules, contrapositive, etc), I won't repeat them here; instead, you should access this file for details. The basic valid deductions are given as Exercise 2.50 in the textbook. You should make sure that you've studied these. I'll assume that you're familiar with them.

Exercises: The following textbook exercises are highly recommended: 2.5, 2.9, 2.14, 2.21, 2.25, 2.31, 2.36, 2.40, 2.46, 2.53. Presumably you've already completed these exercises, but it won't hurt to review your solutions. Other problems:

1. Suppose that P and Q are statements for which $P \to Q$ is *false*. What conclusion (if any) can be made about the truth value of the following statements?

   $$\text{(a) } \neg P \to Q \quad \text{(b) } Q \to P \quad \text{(c) } P \vee Q$$

2. Use known logical equivalences to prove the following equivalences involving conditional statements with disjunctions:

   (a) $P \to (Q \vee R) \equiv (P \wedge \neg Q) \to R$

   (b) $(P \vee Q) \to R \equiv (P \to R) \wedge (Q \to R)$ (note that this is the logical basis for proof by cases)

3. Use known logical equivalences to prove the following equivalences involving conditional statements with conjunctions:

   (a) $(P \wedge Q) \to R \equiv (P \to R) \vee (Q \to R)$

   (b) $P \to (Q \wedge R) \equiv (P \to Q) \wedge (P \to R)$

4. For the following problem, $a \in \mathbb{R}$ is a real number, and f is a real-valued function defined on an interval containing a. Consider the following statement:

   If f is differentiable at $x = a$, then f is continuous at $x = a$.

   Note: For the problem that follows, it is not necessary to know the meaning of the terms "differentiable" and "continuous" (or, for that matter, "function" and "interval").

   Which of the following statements have the same meaning as the above conditional statment, and which ones are negations of this statement? Which ones are neither?

(a) If f is continuous at $x = a$, then f is differentiable at $x = a$.

(b) If f is not differentiable at $x = a$, then f is not continuous at $x = a$.

(c) If f is not continuous at $x = a$, then f is not differentiable at $x = a$.

(d) f is not differentiable at $x = a$, or f is continuous at $x = a$.

(e) f is not continuous at $x = a$, or f is not differentiable at $x = a$.

(f) f is differentiable at $x = a$ and f is not continuous at $x = a$.

5. The conditional statement $(\neg P \wedge (P \vee Q)) \rightarrow Q$ is known as the *disjunctive syllogism*.

   (a) Express the statement in words; then, give an example by assigning P and Q to specific assertions. (Perhaps P represents "Spot is a dog.")

   (b) Show that the disjunctive syllogism is a tautology.

Two column proofs

Two column proofs are one method for determining the validity of a deduction. Recall that the format of a two column proof consists of rows (i.e. lines) divided into two columns. The left-hand column contains assertions, and the right-hand column contains a justification for each assertion. The first lines should consist of the hypotheses of the deduction, and the final line (assuming the deduction is valid) will be the conclusion. The intermediate lines are all obtained from the lines above using logical arguments.

The most common justifications used in the right-hand columns will be the rules of propositional logic listed in Exercise 2.50, along with definitions and the logical equivalences given on the earlier handout.

Example: (Exercise 3.6 (1) in the textbook) Give a two column proof of the deduction

$$P \vee Q, Q \vee R, \neg Q; \therefore P \wedge R.$$

Solution:

1	$P \vee Q$	Hypothesis
2	$Q \vee R$	Hypothesis
3	$\neg Q$	Hypothesis
4	P	$\vee$-elim (lines 1 and 3)
5	R	$\vee$-elim (lines 2 and 3)
6	$P \wedge R$	$\wedge$-intro (lines 4 and 5)

Two situations/techniques that arise in two column proofs are **subproofs** (also known as "$\rightarrow$-introduction") and proof by contradiction (which is itself usually used in a subproof). A subproof is used when we want to show that one assertion implies another (i.e. we want to show $P \rightarrow Q$ for some assertions P and Q) and this is not given as an hypothesis. To do

this, we assume that P is true (this is the first line of the subproof), and then attempt to obtain Q. Once we obtain Q we can close off the subproof, and add $P \to Q$ as a line in our proof.

A proof by contradiction relies on the tautology $(P \to (Q \wedge \neg Q)) \to \neg P$: if assuming P leads to a contradiction $Q \wedge \neg Q$, then it must be that P is false and $\neg P$ is true. A proof by contradiction also appears as a subproof. If we want to obtain $\neg P$, then we should assume P as the first line of the subproof, and attempt to obtain $Q \wedge \neg Q$.

Remark: To see that the above is a tautology, note that since $Q \wedge \neg Q \equiv F$, we have $P \to (Q \wedge \neg Q) \equiv \neg P \vee F \equiv \neg P$, so

$$(P \to (Q \wedge \neg Q)) \to \neg P \equiv \neg(P \to (Q \wedge \neg Q)) \vee (\neg P) \equiv \neg(\neg P) \vee \neg P \equiv P \vee \neg P \equiv T.$$

I will ask you to do one two-column proof on the midterm, and it will probably have a subproof, which may or may not involve a proof by contradiction, so exercises **3.13** and **3.17** in the textbook are good practice. If you need to use proof by contradiction, this will be specified in the problem.

Note: By getting them out of the way on the midterm, we can avoid doing two-column proofs again on the final exam (which will otherwise be cumulative). We'll end with two more examples.

Chapters 4 and 5: Sets and Predicates

We've noted that certain sentences are not quite assertions, since they contain variables whose values affect whether or not the sentence is true or false; for example, the sentence $2x + 3y = 42$. Such sentences are called **predicates**. We'll come back to predicates in our review of Chapters 6 and 7. Typically it is necessary to specify what possible values the variables in a predicate are allowed to assume. We do so by requiring that our variables belong to a **set**. This provides the context in which our predicate(s) should be considered.

We define a set to be a "well-defined collection of objects". This definition is far from ideal, since we've replaced one English term (set) with a synonymous one (collection). We won't feel too bad about this though, because nobody has ever really come up with a satisfactory definition of a set that avoids this problem, even at more advanced levels. (One can at least partly get around the problem by defining sets in terms of various axioms that they must satisfy; these axioms are chosen to make sure we avoid uncomfortable situations like Russell's Paradox (Google it).) Our solution to the problem is to just consider plenty of examples of things that we consider to be sets, and hope that we get sufficiently used to the idea that we can stop worrying about the definition.

In any case, these objects are usually referred to as the **elements** or **members** of the set. If A denotes a given set and x is one of the objects in A, we denote the membership relation between x and A by $x \in A$. This denotes the assertion that the object x is an element of the set A.[2] If an object x does not belong to a set A we write $x \notin A$.

[2]We're distinguishing here between "sets" and "objects", but there's nothing to stop us from considering a set whose elements are other sets, so the distinction can get a bit fuzzy. The main thing to keep in mind is that the relation $x \in A$ tells us which thing should be considered the set, and which should be the object.

One way of specifying a set is by explicitly listing its elements; this is often referred to as the "roster method"[3]. For example, we could define

$$A = \{0, 1, 4, \pi, \text{Lethbridge}\}.$$

The objects of the set A would then be the numbers 0 ,1, 4, and π, and for some reason we've also decided to throw in the city of Lethbridge. Or perhaps "Lethbridge" just refers to the *word* Lethbridge and not the city it represents. If we're worried that we might run into some sort of confusion or ambiguity like this, we might want to insist that our sets are contained within some larger, **universal** set that provides us with some context. (We might, for example, have specified that we were only considering sets whose elements are either numbers or cities.)

Another way to specify a set is using the "set builder" notation. In this case we specify a set A as the set of all elements of some universal set U that satisfy a given property, which we express using a predicate. The notation

$$A = \{x \in U : P(x)\}$$

means that A is the set of all elements x for which a given predicate $P(x)$ is true. For example, the interval $(0, 1)$ of real numbers can be defined by $(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$.

It frequently happens (as it did above) that we are interested in a set A whose elements are all chosen from some larger set B. We express this relationship by saying that A is **contained** in B, or that A is a **subset** of B, and write $A \subseteq B$. The precise definition is:

$$A \subseteq B \leftrightarrow x \in A \rightarrow x \in B$$

Remark: As we noted in class, this definition contains a hidden quantifier. We didn't mention it at the time due to the fact that we've been covering the textbook in order, and in the text, quantifiers don't make an appearance until Chapters 6 and 7. To define the subset relation more carefully, we should say that $A \subseteq B$ if and only if for every $x \in A$, it's true that $x \in B$ as well. Alternatively, viewing A and B as subsets of some universal set U, we can say that $A \subseteq B$ if and only if for all $x \in U$, if $x \in A$, then $x \in B$. (If we allow ourselves to think of x as a *specific* element of A, then the requirement that A be "well-defined" means that relation $x \in A$ is an assertion, but as we discussed in class, this can sometimes get us into trouble.)

Once we define the subset relation we can say that two sets A and B are **equal** if and only if both $A \subseteq B$ and $B \subseteq A$ hold. This means that any element of A must be an element of B and vice-versa, or in other words, that A and B contain precisely the same elements.

We briefly discussed the **cardinality** of a finite set A; this is simply the number of elements in A, and is usually denoted by $|A|$. (Our textbook uses the notation $\#A$.) For example, $|\{-1, 0, 3, 102\}| = 4$. We'll discuss cardinality in more detail later on; you can assume there will be no problems about cardinality on the midterm.

Another type of set we can obtain from a given set A is the **power set** of A, usually denoted by $\mathcal{P}(A)$. The power set of A is defined to be the set of all subsets of A. One

[3]The roster method can also be used to specify a set with infinitely many elements by giving a pattern that they follow. For example, the natural numbers can be given using the roster method as $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$.

such subset (the one you should make sure not to forget) is the **empty set**. This is the set containing no elements whatsoever, and it is denoted by $\emptyset$ or $\{\}$. The empty set is a subset of every set, including itself. It's possible to show that if $|A| = n$, then the cardinality of $\mathcal{P}(A)$ is 2^n. Thus, writing out the elements of a power set becomes a tedious task very quickly. For example, if $A = \{0, 1, 2, 3\}$, then

$$\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{3\}, \{0,1\}, \{0,2\}, \{0,3\}, \{1,2\}, \{1,3\}, \{2,3\}, \\ \{0,1,2\}, \{0,1,3\}, \{0,2,3\}, \{1,2,3\}, \{0,1,2,3\}\}.$$

Remark: Expressions such as $x \in A$, $A \subseteq B$, and $A = B$ involve *relationships*; in the first case, between an object and a set, and in the latter two cases, between two sets. We also considered *operations* on sets, which take one or more sets, and produce a new set. These are the operations of complement, union, intersection, and set difference, which are about to discuss. If you find yourself confused between relationships between sets and operations on sets, it might be helpful to think of basic arithmetic as an analogy. Given numbers x and y, expressions such as $x \leq y$, $x \geq y$, and $x = y$ denote relationships between the numbers x and y: they tell us how to compare them. On the other hand, expressions such as $x + y$, $-x$, $x - y$, $x \cdot y$, x/y are operations on the numbers x and y: each one takes one or more numbers and gives us a new number, without necessarily telling us anything about how those numbers compare.

Set operations

The basic set operations are as follows: Let A and B be subsets of some universal set U. We define:

- The **complement** of A, denoted A^c (this is denoted by $\overline{A}$ in the textbook, but in many 3000-level math courses you'll find that this notation refers to a completely different set operation) is defined by

  $$A^c = \{x \in U : x \notin A\}.$$

  Thus, $x \in A^c$ if and only $x \notin A$.

- The **union** of A and B is denoted by $A \cup B$ and defined by

  $$A \cup B = \{x \in U : x \in A \text{ or } x \in B\}.$$

- The **intersection** of A and B is denoted by $A \cap B$ and defined by

  $$A \cap B = \{x \in U : x \in A \text{ and } x \in B\}.$$

- The **set difference** $A \setminus B$ is defined by

  $$A \setminus B = \{x \in U : x \in A \text{ and } x \notin B\} = \{x \in A : x \notin B\}$$

There are various relationships among the set operations that we encountered at some point. For example, it follows immediately from the definition that $A \setminus B = A \cap B^c$. The rule $\neg(\neg P) \equiv P$ from propositional logic tells us that $(A^c)^c = A$ for any set A. The complement can also be defined using set difference as $A^c = U \setminus A$. (In cases where ambiguity with regard to notation for the complement is anticipated, the notation $U \setminus A$ for the complement may be preferred, even though it is more cumbersome.)

Other relationships we encountered include de Morgan's laws, which state that

$$(A \cup B)^c = A^c \cap B^c \quad \text{and} \quad (A \cap B)^c = A^c \cup B^c,$$

and the distributive laws, which state that for any sets A, B, C we have

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad \text{and} \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

We noted that each basic set equality has a corresponding logical equivalence (although the proofs sometimes require the full power of first-order logic, which we discuss in the next section).

Exercises: From the textbook, 4.29, 5.5, 5.6, 5.14, 5.23, 5.26.

Other practice:

Given $U = \mathbb{Z}$, $A = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$, $B = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$, and $C = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$,

1. Express the sets A, B, C using set builder notation.
2. Compute $A \cap B$, $B \setminus A$, and $A \cup C$.
3. Compute $A \setminus C$, $A \cap C^c$, and $C \setminus A$.
4. Compute $(A \cup B) \cap C$ and $(A \cup B) \setminus C$.

Chapter 6: First order logic

In Chapters 4 and 5 we discussed sets, and found that in some cases we did not have the tools needed to rigorously establish relationships among sets and set operations. In particular, the subset relation $A \subseteq B$ is defined in terms of a predicate: $A \subseteq B$ if and only if $x \in A \to x \in B$. To solidify this as a definition we need to convert this predicate into an assertion. Chapter 6 is where we finally introduce the last ingredient needed to properly discuss sets; namely, quantifiers.

There are two quantifiers. The **universal quantifier**, denoted $\forall$, allows us to assert that a given predicate $P(x)$ is true *for all* values of the variable x. For example, if $P(x)$ is the predicate $x^2 \geq 0$, we obtain the assertion $\forall x, P(x)$, which translates to "For all x, $x^2 \geq 0$", or "$x^2 \geq 0$ for any x", and so on. (There are many equivalent ways of rephrasing this statement in English. We noted that this is not quite enough to obtain an assertion: we need to provide some context for the variable x. (For real numbers, this statement is true; if we allow complex numbers, then it is false.) The solution is to always specify some universal set U and require that the variable x take values in this set. Thus, we can write the assertion $\forall x \in \mathbb{R}, x^2 \geq 0$, which we know to be true.

The **existential quantifier**, denoted $\exists$, allows us to assert that a given predicate $P(x)$ is true *for some* x. Again, we assume that x takes values in some universal set U. If $P(x)$ represents the predicate $x^2 - 1 = 0$, then the assertion $\exists x \in \mathbb{R} : P(x)$ can be read as "$x^2 - 1 = 0$ for some real number x", or "There exists some real number x such that $x^2 - 1 = 0$", or "For at least one real number x, we have $x^2 - 1 = 0$", and so on.

With quantifiers at hand, we can finally solidify our definition of the subset relation. We say that $A \subseteq B$ if and only if $\forall x \in A, x \in B$. Or, if we view A and B as subsets of some universal set U, then $A \subseteq B$ if and only if $\forall x \in U, x \in A \to x \in B$. If A is not a subset of B, then $\exists a \in A : a \notin B$. If this is not clear, see the discussion of negations below. (If it is clear, keep this example in mind when thinking of negations in general.)

If our predicate involves more than one variable, then we need one quantifier for each variable before we can obtain an assertion. One important thing to keep in mind is that *order matters* when we're dealing with quantifiers. For example, consider the predicate $P(x, y)$ given by $x + y = 2$. There are various ways of forming an assertion from this predicate, depending on which quantifier is applied to each variable, and the order in which they are applied. For example, consider the assertions

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : x + y = 2, \quad \text{and} \quad \exists y \in \mathbb{R} : \forall x \in \mathbb{R}, x + y = 2.$$

In the first case, we're asserting that, given any x, we can find a y such that $x + y = 2$. This statement is true. Given x, we simply take $y = 2 - x$ and we're done. In the second assertion, we've changed the order in which the variables (and their quantifiers) appear. We are now claiming that we can find some y such that, no matter what value x has, $x + y = 2$. This statement is false. Once we fix y, the equation $x + y = 2$ is valid only for $x = 2 - y$, and not for any other value of x.

The negation of quantified statements with one variable are given by

$$\neg(\forall x \in U, P(x)) \equiv \exists x \in U : \neg P(x)$$
$$\neg(\exists x \in U, Q(x)) \equiv \forall x \in U, \neg Q(x).$$

Note that to negate a quantified statement, we switch the quantifier and negate the predicate. Remember that the universal set U is there to tell us the context in which we're considering the variable x. The universal set will remain the same for both the original statement and its negation. For example, the negation of $\forall x \in \mathbb{R}, x^2 > 0$ is, $\exists x \in \mathbb{R} : x^2 \not> 0$ (or equivalently – and more informatively – $\exists x \in \mathbb{R} : x^2 \leq 0$). While it may or may not be true that $\exists x \notin \mathbb{R} : x^2 > 0$, (or $\exists x \notin \mathbb{R} : x^2 \leq 0$) this has no bearing on the truth of the original statement: we are saying that something is true *for every real number*. Thus, to show this claim is false, we need to show that there exists some x that does not have this property, where x is *also* a real number.

If there is more than one variable/quantifier in our statement, then to form the negation we start on the outside, and work our way in. Each time we pass a quantifier, we switch it, and once we reach the predicate, we form its negation. For example, let $\mathbb{P}$ denote the set of *positive* real numbers (that is, $\mathbb{P} = (0, \infty)$), let f be a function, let $a \in \mathbb{R}$ be a fixed real number in the domain of f, and consider the statement

$$\forall r \in \mathbb{P}, \exists s \in \mathbb{P} : \forall x \in \mathbb{R}, |x - a| < s \to |f(x) - f(a)| < r.$$

Here, there are three variables, r, s, and x. The first two belong to the set $\mathbb{P}$, and the last to $\mathbb{R}$. (It's possible to have different universal sets for different variables. For example, we may want to consider a statement involving powers x^n where x is a real number and n is an integer.) The predicate $P(r, s, x)$ in this case is $|x - a| < s \to |f(x) - f(a)| < r$. (We indicated that a and f were fixed choices, so we don't consider them as variables.) Since the predicate is in the form of a conditional statement, we use the fact that $\neg(A \to B) \equiv A \wedge \neg B$ to form the negation. The overall negation is as follows:

$$\begin{aligned}
\neg(\forall r \in \mathbb{P}, \exists s \in \mathbb{P} : &\forall x \in \mathbb{R}, |x - a| < s \to |f(x) - f(a)| < r) \\
&\equiv \exists r \in \mathbb{P} : \neg(\exists s \in \mathbb{P} : \forall x \in \mathbb{R}, |x - a| < s \to |f(x) - f(a)| < r)) \\
&\equiv \exists r \in \mathbb{P} : \forall s \in \mathbb{P}, \neg(\forall x \in \mathbb{R}, |x - a| < s \to |f(x) - f(a)| < r) \\
&\equiv \exists r \in \mathbb{P} : \forall s \in \mathbb{P}, \exists x \in \mathbb{R} : \neg(|x - a| < s \to |f(x) - f(a)| < r) \\
&\equiv \exists r \in \mathbb{P} : \forall s \in \mathbb{P}, \exists x \in \mathbb{R} : |x - a| < s \text{ and } |f(x) - f(a)| \geq r.
\end{aligned}$$

(Note: in case you're worried, this one is more complicated than what you'll see on the exam, but you might find that understanding this negation comes in handy later in life, if your later life includes other math courses.)

Exercises: From the textbook, 6.2, 6.16, 6.17.

Other problems:

1. Assume that the universal set is $\mathbb{Z}$. Consider the following sentence:

$$\exists t \in \mathbb{Z} : t \cdot x = 20.$$

   (a) Explain why this sentence is not a assertion.

   (b) If 5 is substituted for x, is the resulting sentence a assertion? If it is a assertion, is it true or false?

   (c) If 8 is substituted for x, is the resulting sentence a assertion? If it is a assertion, is it true or false?

   (d) If -2 is substituted for x, is the resulting sentence a assertion? If it is a assertion, is it true or false?

   (e) For which integers x is the predicate $\exists t \in \mathbb{Z} : t \cdot x = 20$ true?

   (f) Add a second quantifier so that the above predicate becomes an assertion that is (i) true (ii) false.

2. Explain why each of the statements is false:

   (a) $\forall x \in \mathbb{R}, x^2 > 0$.

   (b) $\forall a \in \mathbb{Z}, \sqrt{a^2} = a$.

   (c) $\exists x \in \mathbb{Q} : x^2 - 3x - 7 = 0$. (Hint: quadratic formula)

   (d) $\forall m \in \mathbb{Z}, m^2$ is even.

   (e) $\exists x \in \mathbb{R} : x^2 + 1 = 0$.

3. Write the negations of the following assertions (assume that $\mathbb{Z}$ is the universal set):

   (a) $\exists m : \exists n : m > n$

   (b) $\forall m, \forall n, m > n$

   (c) $\exists m : \forall n, m > n$

   (d) $\exists n : \forall m, m > n$

   (e) $\forall m, \exists n : m > n$

   (f) $\forall n, \exists m : m > n$

4. Which of the assertions in the previous question are true? Which are false?

Chapter 7: Proofs with quantifiers

There are various proofs involving quantifiers that we encountered. Consider the existential statement "$\exists x \in U : P(x)$". This may be an assertion that we wish to prove is true, or something that we know is true and wish to use in another proof. We considered two ways of proving an existential statement: constructive proofs and non-constructive proofs. You won't be asked for any non-constructive proofs on the exam, since they tend to be more difficult and to require knowledge from other courses. For example, suppose we wanted to prove the statement

$$\exists x \in \mathbb{R} : \cos x = x.$$

A constructive proof would simply exhibit a value of x that works; however, in this case solving for x can only be done approximately, and we rely on a non-constructive proof. (Students from Math 1560 might know how it goes: Let $f(x) = \cos x - x$, which is a continuous function. We check that $f(0) = 1 > 0$, and $f(\pi/2) = -\pi/2 < 0$. Thus, by the Intermediate Value Theorem, there exists some $c \in (0, \pi/2)$ such that $f(c) = 0$. You would not be expected to produce such a proof in Math 2000.)

For an example of a statement for which we can give a constructive proof, consider $\exists x \in \mathbb{R} : x^2 - 2x + 1 = 0$. We can prove this as follows: Suppose that $x = 1$. Then $x^2 - 2x + 1 = 1^2 - 2(1) + 1 = 0$. (Since we showed that $x = 1$ has the desired property, we can be sure such an x exists.)

We can also use existential statements in proofs. For example, consider the following assertion:

If $n^2 - 1$ is even, then $n^2 - 1$ is divisible by 4.

To prove this assertion, we need to show that there exists some integer $m \in \mathbb{Z}$ such that $n^2 - 1 = 4m$. Suppose that n^-1 is even. Then there exists some $k \in \mathbb{Z}$ such that $n^2 - 1 = 2k$. (We can introduce this existential statement since this is the definition of an even number.) Rearranging, we see that $n^2 = 2k + 1$, which tells us that n^2 is odd. As we proved in class, n^2 is odd if and only if n is odd. (The square of an odd number is odd and the square of an even number is even.) Since n is odd, there exists some integer $l \in \mathbb{Z}$ such that $n = 2l + 1$. (A second existential statement we know to be true.) But if $n = 2l+1$, then $n^2 = 4l^2+4l+1$, so $n^2 - 1 = 4l^2 + 4l = 4(l^2 + l)$, which shows that $n^2 - 1$ is a multiple of 4, and that is what we needed to show.

Similarly, an assertion "$\forall x \in U, P(x)$" can be either something we need to prove, if its truth has not yet been established, or something that we can use in another proof, if we already know that it is true. For example, one fact about real numbers is that $\forall x \in \mathbb{R}, x^2 \geq 0$. One way to apply a true assertion with a universal quantifier is to note that if it holds for all $x \in U$, then it must hold for any particular choice of x. Thus, we can make a deduction such as, "For all $x \in \mathbb{R}$, $x^2 \geq 0$. 2 is a real number. Therefore, $2^2 \geq 0$."

To prove an assertion with a universal quantifier, we usually begin with a sentence such as "Let $x \in U$ be arbitrary", or "Let $x \in U$ be given," or something similar that indicates that the argument to follow will be valid independently of the value of x. For example, we can use one assertion with a universal quantifier to prove another, as in the following deduction: "For all $x \in \mathbb{R}$, $x^2 \geq 0$. Therefore, for all $x \in \mathbb{R}$, $x^2 + 1 > 0$." The proof is as follows: Let $x \in \mathbb{R}$ be any real number. We know that $y^2 \geq 0 \forall y \in \mathbb{R}$. (We've used y rather than x here since we already chose x to represent our arbitrary choice of real number.) Thus, in particular, $x^2 \geq 0$. Since $1 > 0$, it follows that $x^2 + 1 \geq 0 + 1 > 0$, and since x was arbitrary, the result follows.

Note that since the negation of the assertion $\forall x \in U, P(x)$ is $\exists x \in U : \neg P(x)$, if we wish to *disprove* this assertion, then we just need to find one x for which the predicate $P(x)$ is false. Such an x is known as a **counterexample**.

We can use quantifiers to prove various results involving relationships among sets. For example, suppose we wanted to prove the following:

$$\text{If } A \nsubseteq B, \text{ then there exists some } a \in A \text{ such that } a \notin B.$$

We first note that $A \subseteq B$ if and only if $\forall a \in A, a \in B$, and then take the negation of this statement to obtain $\exists a \in A : a \notin B$, which is what we wanted. If we want to prove the distributive property $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, we need to prove both inclusions $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ and $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. Let's prove the first inclusion (the second will be left as an exercise):

Let $x \in A \cup (B \cap C)$ be arbitrary. (We need to show *any* x in this set belongs to the other. Note: it could be that this set is empty, and then no such x exists. But since we're proving both inclusions, if one set is empty, the other one must be, too.)

Since $x \in A \cup (B \cap C)$, either $x \in A$ or $x \in B \cap C$. If $x \in A$, then $x \in A \cup B$ and $x \in A \cup C$, so $x \in (A \cup B) \cap (A \cup C)$ and we're done. If $x \notin A$, then $x \in B \cap C$. (Note: in the two-column proof version we've just applied the Law of the Excluded Middle and "$\vee$-elimination", and are in the middle of a proof by cases.) If $x \in B \cap C$, then $x \in B$ and $x \in C$, so $x \in A \cup B$ and $x \in A \cup C$. Thus, $x \in (A \cup B) \cap (A \cup C)$.

Other proofs of set equalities can be performed using known results. Basic results you should be familiar with include de Morgan's laws, the distributive properties, and basic results like the definition $A \setminus B = A \cap B^c$ for the set difference. For example, suppose wish to prove the following equality:

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

We proceed as follows:

$$\begin{aligned}(A \cup B) \setminus (A \cap B) &= (A \cup B) \cap (A \cap B)^c \text{ (definition of set difference)} \\ &= (A \cup B) \cap (A^c \cup B^c) \text{ (de Morgan's laws)} \\ &= [A \cap (A^c \cup B^c)] \cup [B \cap (A^c \cup B^c)] \text{ (distributive law)} \\ &= (A \cap A^c) \cup (A \cap B^c) \cup (B \cap A^c) \cup (B \cap B^c) \text{ (distributive law)} \\ &= \emptyset \cup (A \setminus B) \cup (B \setminus A) \cup \emptyset \\ &= (A \setminus B) \cup (B \setminus A).\end{aligned}$$

As we noted above, one can disprove an assertion with a universal quantifier by providing a counterexample. For example, consider the following proposition: Let A, B, and C be subsets of some universal set U. If $A \cap C \subseteq B \cap C$, then $A \subseteq B$.

There is no universal quantifier explicitly mentioned, but we are suggesting that this statement will be true for any choice of sets A, B, C. Thus, to show that it is false, we need only give one example of such sets where the proposition is false. Here is such an example: Let $A = \{1\}$, $B = \{2\}$, and $C = \{3\}$. Then $A \cap C = \emptyset$ and $B \cap C = \emptyset$, and we know that $\emptyset \subseteq \emptyset$, but it is not true that $\{1\} \subseteq \{2\}$. Thus, the proposition is false.

Finally, the introduction of quantifiers allows us to consider unions and intersections more generally. To do so, we introduce the notion of an **index set** I. Common examples of index sets include $I = \{1, 2, \ldots, n\}$, $I = \mathbb{N} = \{1, 2, 3, \ldots, \}$, and $I = \mathbb{R}$. An **indexed family** of sets is a set of sets of the form $\mathcal{A} = \{A_\alpha : \alpha \in I\}$. For example, we could consider collections of sets such as $\mathcal{A} = \{\{0, n, -n : n \in \mathbb{N}\}$, or $\mathcal{B} = \{(-a, a) : a \in \mathbb{R}\}$. Given an indexed family of sets (which we assume as usual are all subsets of a universal set U), we define

$$\bigcup_{\alpha \in I} A_\alpha = \{x \in U : \exists \alpha \in I : x \in A_\alpha\}$$
$$\bigcap_{\alpha \in I} A_\alpha = \{x \in U : \forall \alpha \in I, x \in A_\alpha\}.$$

One warning: we need to assume that the index set I is *nonempty* or strange things happen: if you want something to puzzle about, try to convince yourself that if $I = \emptyset$, then the union above is empty, while the intersection is all of U! For more details on indexed families of sets, see the handout posted earlier on Moodle.

Exercises: From the text, 7.5, 7.7, 7.10, 7.15, 7.16, 7.21, 7.22, 7.25, 7.26, 7.27.

1. Let A, B, and C be subsets of a universal set U. Are the following propositions true or false? Justify your conclusions:
   (a) If $A \cup C \subseteq B \cup C$, then $A \subseteq B$.
   (b) If $A \cup C = B \cup C$, then $A = B$.
   (c) If $A \cup C = B \cap C$, then $A = B$.
   (d) if $A \cup C = B \cup C$ and $A \cap C = B \cap C$, then $A = B$.
2. Let A, B, and C be subsets of some universal set U. Prove or disprove each of the following:

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

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

(c) $(A \cup B) \setminus A = B \setminus A$

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

3. Let I be a nonempty indexing set, let $\mathcal{A} = \{A_\alpha : \alpha \in I\}$ be an indexed family of sets, and let B be a set. Using the results proved on the handout on indexed families of sets (generalized de Morgan's laws, distributive laws, etc) prove the following:

(a) $\left(\bigcup_{\alpha \in I} A_\alpha\right) \setminus B = \bigcup_{\alpha \in I}(A_\alpha \setminus B)$

(b) $\left(\bigcap_{\alpha \in I} A_\alpha\right) \setminus B = \bigcap_{\alpha \in I}(A_\alpha \setminus B)$

(c) $B \setminus \left(\bigcup_{\alpha \in I} A_\alpha\right) = \bigcap_{\alpha \in I}(B \setminus A_\alpha)$

(d) $B \setminus \left(\bigcap_{\alpha \in I} A_\alpha\right) = \bigcup_{\alpha \in I}(B \setminus A_\alpha)$

Chapter 8: Divisibility and Congruence

Divisibility and congruence are two common relations on the integers. (We'll discuss relations in general at the end of this review.) For integers $m, n \in \mathbb{Z}$, we say that m **divides** n, and write $m|n$, if there exists an integer $k \in \mathbb{Z}$ such that

$$n = mk.$$

Other synonymous phrases are that n is a **multiple of** m, or n is **divisible** by m, or m is a **factor of** n. A basic property of divisibility is that if $a|b$ and $a|c$, then $a|(b+c)$. To see this, note that if $a|b$ and $a|c$, then there exist integers k and l such that $b = ak$ and $c = al$, and thus $b + c = ak + al = a(k + l)$. On the other hand, if $a|b$ and $a \not| c$, then we can conclude that $a \not| (b + c)$. One thing to be careful about is that it is **not** true that if $a|(bc)$ then $a|b$ or $a|c$. For example, we could take $a = 6$, $b = 3$, and $c = 4$. However, if a and b have no common factors and $a|(bc)$, then we can conclude that $a|c$. (To prove this we would need to discuss greatest common factors and the Euclidean algorithm, but this is beyond what we had time to cover in class.)

The divisibility relation involves one integer dividing evenly into another. However in general we expect there to be a remainder upon division. This is formalized in the **Division algorithm**:

Theorem: For any integers k and n with $k > 0$, there exist *unique* integers q and r with $r \in \{0, 1, \ldots, k - 1\}$ such that

$$n = kq + r.$$

Here r is the **remainder** upon dividing n by k. Note that we always take $0 \leq r < k$ since if $r \geq k$ we can simply increase the value of q. For example, if $k = 5$ and $n = 32$, we would write $32 = 5(6) + 2$, rather than, say, $32 = 5(4) + 12$ - we don't write the remainder until we've removed the largest multiple of k from n that is less than or equal to n.

If $r = 0$, then $n = kq$ and $k|n$. Otherwise, it is not n that is a multiple of k, but $n - r$; $n - r = kq$, so $k|(n - r)$. This situation comes up frequently, so it is given a name. Given two

integers m and n, we say that m is **congruent to** n **modulo** k, and write $m \equiv n \pmod{k}$, if $m - n$ is divisible by k. That is, we have

$$\begin{aligned} m \equiv n \pmod{k} &\leftrightarrow k|(m-n) \\ &\leftrightarrow m - n = kq \text{ for some } q \in \mathbb{Z} \\ &\leftrightarrow m = n + kq \text{ for some } q \in \mathbb{Z} \end{aligned}$$

Thus, if $n = kq + r$, with q and r given by the division algorithm, we have $n \equiv r \pmod{k}$. In fact, we can say that $m \equiv n \pmod{k}$ if and only if m and n have the same remainder upon division by k. This follows from some basic properties of congruence:
Theorem: For any $a, b, c \in \mathbb{Z}$ and $k \in \mathbb{N}$ we have:

1. $a \equiv a \pmod{k}$.
2. If $a \equiv b \pmod{k}$, then $b \equiv a \pmod{k}$.
3. If $a \equiv b \pmod{k}$ and $b \equiv c \pmod{k}$, then $a \equiv c \pmod{k}$.

Items 1 and 2 are straightforward to check. For item 3, note that if $a \equiv b \pmod{k}$ and $b \equiv c \pmod{k}$, then we have integers $p, q \in \mathbb{Z}$ such that $b = a + kp$ and $c = b + kq$. But then

$$c = b + kq = (a + kp) + kq = a + k(p + q),$$

so $a \equiv c \pmod{k}$. Applying this to the claim about remainders above, if m and n both have remainder r upon division by k, then from the division algorithm we get $m \equiv r \pmod{k}$ and $n \equiv r \pmod{k}$. This tells us that $r \equiv n \pmod{k}$ (using 2), and thus that $m] \equiv n \pmod{k}$ (using 3). A similar argument shows that if $m \equiv n \pmod{k}$ and $n \equiv r \pmod{k}$, then $m \equiv r \pmod{k}$.

For example, let $k = 7$, $m = 36$ and $n = 64$. Then $m - n = 36 - 64 = -28 = 7(-4)$, so $36 \equiv 64 \pmod{7}$. We also note that

$$\begin{aligned} 36 &= 7(5) + 1 \text{ and} \\ 64 &= 7(9) + 1, \end{aligned}$$

so both 36 and 64 have the same remainder upon division by 7.
Exercises: From the text, 8.9, 8.11, 8.13, 8.14, 8.19, 8.25, 8.27.

1. Prove that for each integer $n \in \mathbb{Z}$, $n^3 \equiv n \pmod{3}$. (Hint: consider cases based on the remainder when n is divided by 3.)
2. (a) Prove that if $a \not\equiv 0 \pmod{5}$, then $a^2 \equiv 1 \pmod{5}$ or $a^2 \equiv 4 \pmod{5}$.
   (b) Conclude that if a^2 is divisible by 5, then a is divisible by 5.
   (c) Prove that $\sqrt{5}$ is irrational.
   Hint for (c): if not, then $\sqrt{5} = a/b$ with a/b in lowest terms. Thus $a = \sqrt{5}b$, so $a^2 = 5b^2$. Argue that both a and b must be divisible by 5, contradicting the assumption that a/b was in lowest terms.
3. Prove that if $3|(a^2 + b^2)$, then $3|a$ and $3|b$.
   Hint: use proof by contrapositive, and consider cases. Explain why it's sufficient to suppose that $3 \not| a$.

Chapter 9: Functions

This is probably the longest chapter in the course, partly because there's a lot we can say about functions, and partly because understanding functions is important for most other mathematics courses you're going to encounter. We began with one more set operation: given two sets A and B, their **Cartesian product** is denoted $A \times B$ and defined by

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}.$$

Here, the element $(a, b) \in A \times B$ is called an **ordered pair**. We define equality of ordered pairs by

$$(a, b) = (c, d) \text{ if and only if } a = c \text{ and } b = d.$$

Note in particular that $(a, b) \neq (b, a)$ unless $a = b$. The Cartesian product is compatible with both unions and intersections, in the sense that for any sets A, B, and C,

$$A \times (B \cup C) = (A \times B) \cup (A \times C) \text{ and } (A \cup B) \times C = (A \times C) \cup (B \times C)$$
$$A \times (B \cap C) = (A \times B) \cap (A \times C) \text{ and } (A \cap B) \times C = (A \times C) \cap (B \times C)$$

Given two sets A and B, we say that a set $f \subseteq A \times B$ defines a **function** from A to B, and write $f : A \to B$ if

1. For each $a \in A$, there exists some $b \in B$ such that $(a, b) \in f$. (Each $a \in A$ appears as the first coordinate of an ordered pair.)

2. The element $b \in B$ from item 1 is *unique*: if $(a, b_1) \in f$ and $(a, b_2) \in f$, then $b_1 = b_2$.

We call the set A the **domain** of f, and the set B is called the **codomain** of f. The **range** of f is the set

$$\text{ran}(f) = \{b \in B \mid \exists a \in A : (a, b) \in f\}.$$

In practice we don't usually think of functions in terms of the formal definition above. Instead, we note that since for each $a \in A$, the element $b \in B$ such that $(a, b) \in f$ is unique, we can think of f as a rule that assigns each $a \in A$ to a unique element $b \in B$. To emphasise that a and b are related by the function f, we write $b = f(a)$. That is,

$$b = f(a) \leftrightarrow (a, b) \in f.$$

With this notation we can also re-write the range of f as $\text{ran}(f) = \{f(a) \mid a \in A\}$, and we can think of the function f as the set $f = \{(a, f(a)) \mid a \in A\} \subseteq A \times B$. However, when we are viewing a function as a map from A to B that assigns elements of A to elements of B, then this set is usually referred to as the **graph** of f.

Many functions that you're familiar with are defined in the case that A and B are both subsets of $\mathbb{R}$. For example, we can define

$$f : \mathbb{R} \to \mathbb{R} \text{ given by } f(x) = x^2$$
$$g : \mathbb{R} \to \mathbb{R} \text{ given by } g(x) = 4x - 3$$
$$h : [0, \infty) \to \mathbb{R} \text{ given by } h(x) = \sqrt{x}.$$

In all the above examples we had to specify a formula to define the rule by which the function assigns an element of $\mathbb{R}$ to another real number. This is basically the best we can do here, since it's impossible to list all of the elements in the domain of the function. In other cases the sets A and B might be finite, in which case we can completely define the function by specifying its value on every element of the domain. For example, let $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c\}$. Then we can define a function $f : A \to B$ by

$$f(1) = b,\ f(2) = a,\ f(3) = a,\ f(4) = c.$$

Note that there are many possible functions from A to B; I just happened to pick one. The only rules you need to follow are those given in the definition of a function: every element of A needs to be assigned, and it can only be assigned once. There is no restriction on how the elements of B appear in the range: a particular element of B may appear more than once, or it may appear not at all.

In many cases we need to apply two or more functions in sequence. If $f : A \to B$ and $g : B \to C$ are functions, we define the **composition** $g \circ f : A \to C$ by $(g \circ f)(a) = g(f(a))$ for all $a \in A$. Note that for the composition $g \circ f$ to make sense, we need to have $\text{ran}(f) \subseteq \text{dom}(g)$. For example, if $f : \mathbb{R} \to \mathbb{R}$ is given by $f(x) = x^2 + 4$ and $g : \mathbb{R} \to \mathbb{R}$ is given by $g(x) = 3x + 1$, we have

$$g \circ f(x) = g(f(x)) = g(x^2 + 4) = 3(x^2 + 4) + 1 = 3x^2 + 13.$$

Note that in this case, since $A = B = C = \mathbb{R}$, we can also define the composition $f \circ g$, which is given by

$$f \circ g(x) = f(g(x)) = f(3x + 1) = (3x + 1)^2 + 4 = 9x^2 + 6x + 5.$$

It's important to note that $f \circ g \neq g \circ f$. This is almost always the case; in fact, if $f : A \to B$ and $g : B \to C$, we can define $g \circ f$, but unless $C = A$, $f \circ g$ is not even defined.

Note that the definition of a function involves restrictions with respect to the domain A: every element of A needs to be assigned to an element of B, and it can only be assigned once. When we want to place restrictions on the codomain as well, we introduce special types of functions. A function $f : A \to B$ is **one-to-one** if every element of B is assigned to *at most one* element of A. Formally, we define f to be one-to-one by requiring that for every $a_1, a_2 \in A$, if $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$. (In practice it is usually more convenient to work with the contrapositive: for all $a_1, a_2 \in A$, if $f(a_1) = f(a_2)$, then $a_1 = a_2$.) A function $f : A \to B$ is **onto** if $\text{ran}(f) = B$; that is, if for every $b \in B$, there exists some $a \in A$ such that $f(a) = b$. In the example above with $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c\}$, the given function f is onto, since a, b, and c all appear in the range of f, but it is not one-to-one, since both 2 and 3 are sent to a.

If a function $f : A \to B$ is both one-to-one and onto, we say that f is a **bijection**. Since f is onto, we know that every $b \in B$ comes from some $a \in A$; that is, for all $b \in B$ we have $b = f(a)$ for some $a \in A$. Since f is one-to-one, we know that this element $a \in A$ is *unique*. This means that we can define a new function $f^{-1} : B \to A$, called the **inverse** of f, by

$$f^{-1}(b) = a \text{ if and only if } b = f(a).$$

We know that f^{-1} is a function by the argument above: it is defined on the entire domain B, since f is onto, and it sends each $b \in B$ to a unique $a \in A$, since f is one-to-one. If we let $I_A : A \to A$ and $I_B : B \to B$ denote the **identity functions**, given by $I_A(a) = a$ for all $a \in A$ and $I_B(b) = b$ for all $b \in B$, then we have the **cancellation properties**

$$f^{-1} \circ f = I_A \text{ and } f \circ f^{-1} = I_B.$$

Thus, the inverse of a function f undoes the effect of applying f. For example, if $f(x) = x+4$ is the function on $\mathbb{R}$ defined by adding 4, then $f^{-1}(x) = x - 4$ – the inverse of addition is subtraction. Similarly if $g(x) = 3x$ with $x \in \mathbb{R}$, then $g^{-1}(x) = x/3$ – if we want to undo a multiplication, we divide by the same number we multiplied by.

The last topic on functions is that of images and preimages of sets. We can begin with the preimage of a point: given $f : A \to B$, we can define the **preimage** of an element $b \in B$ to be the *set*

$$f^{-1}(b) = \{a \in A \,|\, f(a) = b\}.$$

There is an unfortunate overlap of notation between preimages and inverse functions: when you encounter the expression $f^{-1}(b)$, it's important to decide from the context whether this is referring to the value of an inverse function (the single element $a \in A$ such that $a = f^{-1}(b)$, which is the same as saying $f(a) = b$) or the set of values $a \in A$ that f sends to b. To avoid confusion, some people will write $f^{-1}(\{b\})$ for the preimage so that it's clear we're talking about a set, but most people find this notation to be too clumsy. For example, suppose we define $f : \{1, 2, 3, 4, 5\} \to \{u, v\}$ by

$$f(1) = v,\ f(2) = v,\ f(3) = u,\ f(4) = v,\ f(5) = u.$$

Then $f^{-1}(u) = \{3, 5\}$ and $f^{-1}(v) = \{1, 2, 4\}$. For another example, define $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = x^2$. Then we have $g^{-1}(0) = \{0\}$, $g^{-1}(a) = \{\sqrt{a}, -\sqrt{a}\}$, if $a > 0$, and $g^{-1}(b) = \emptyset$ if $b < 0$.

Remark: If the function f is not a bijection, then it's safe to assume that $f^{-1}(b)$ refers to a preimage, since the inverse function would not be defined. Note that if f is not onto, then $f^{-1}(b)$ could be empty, and if f is not one-to-one, then $f^{-1}(b)$ could contain more than one element of A. Requiring f to be a bijection means that $f^{-1}(b)$ contains *exactly one* element $a \in A$, which is why the inverse makes sense as a function when f is a bijection.

Now, let $f : A \to B$ be a function, and let $C \subseteq A$ and $D \subseteq B$ be subsets of A and B, respectively. Then we can define the **image** of C by

$$f(C) = \{f(c) \,|\, c \in C\} = \{b \in B \,|\, \exists c \in C \text{ such that } f(c) = b\},$$

and the **preimage** of D by

$$f^{-1}(D) = \{a \in A \,|\, f(a) \in D\}.$$

Thus, the image of a set $C \subseteq A$ is the set of all values that f takes when we input elements of C, and the preimage of $D \subseteq B$ is the set of all elements of A that f sends to D. Note that the definition of the image of a set is very similar to that of the range of a function; in

fact, we have that $f(A) = \text{ran}(f)$, and $f(C)$ can be viewed as the range of f if we restrict the function to the smaller domain C.

As for preimages of points, we note that if f is onto, then $f^{-1}(D)$ will have at least as many elements as D (since for each $d \in D$ there will be some $a \in A$ with $f(a) = d$, and the same element a can't be sent to more than one element of D, or f would not be a function). If f is not onto, this need not be the case. In particular if $D \cap \text{ran}(f) = \emptyset$, then $f^{-1}(D) = \emptyset$. Similarly, if f is one-to-one, then the set $f^{-1}(D)$ cannot be any larger than D.

For example, let $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{a, b, c, d\}$ and define $f : A \to B$ by

$$f(1) = b,\ f(2) = d,\ f(3) = b,\ f(4) = a,\ f(5) = a,\ f(6) = b.$$

Note that f is neither one-to-one or onto. If $C = \{1, 3, 5\} \subseteq A$, we have

$$f(C) = \{f(1), f(3), f(5)\} = \{b, b, a\} = \{a, b\}.$$

If $D_1 = \{a, b\}$ and $D_2 = \{c, d\}$, we have

$$\begin{aligned} f^{-1}(D_1) &= \{x \in A \,|\, f(x) = a \text{ or } f(x) = b\} = \{1, 3, 4, 5, 6\} \\ f^{-1}(D_2) &= \{x \in A \,|\, f(x) = c \text{ or } f(x) = d\} = \{2\}. \end{aligned}$$

Note that since $c \notin \text{ran}(f)$, the set $f^{-1}(D_2)$ only contains the elements $x \in A$ such that $f(x) = d$.

We considered a number of properties of images and preimages that show up in almost any situation where we have to deal with functions acting on sets. The first two have to deal with how the two types of sets interact: let $f : A \to B$ be a function, and let $C \subseteq A$ and $D \subseteq B$. Then we have

$$\begin{aligned} f(f^{-1})(D) &\subseteq D, \text{ with equality if } f \text{ is onto} \\ C &\subseteq f^{-1}(f(C)), \text{ with equality if } f \text{ is one-to-one.} \end{aligned}$$

A good example to illustrate this is the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$. Let's take $C = [0, 2]$ and $D = [-1, 1]$. Then

$$\begin{aligned} f(C) &= \{x^2 \,|\, 0 \leq x \leq 2\} = [0, 4] \\ f^{-1}(D) &= \{x \in \mathbb{R} : -1 \leq x^2 \leq 1\} = [-1, 1]. \end{aligned}$$

To calculate $f(C)$ we used the fact that if $0 \leq x \leq 2$, then $0^2 =\leq x^2 \leq 4 = 2^2$. For $f^{-1}(D)$, note that negative numbers are not in the range of f, so requiring $-1 \leq x^2 \leq 1$ is the same as requiring $0 \leq x^2 \leq 1$: we never have $x^2 < 0$, so the restriction $-1 \leq x < 0$ is redundant, and if $-1 \leq x \leq 1$, then $0 \leq x^2 \leq 1$. Now we can compute

$$\begin{aligned} f^{-1}(f(C)) &= f^{-1}([0, 4]) = \{x \in \mathbb{R} \,|\, 0 \leq x^2 \leq 4\} = [-2, 2] \\ f(f^{-1}(D)) &= f([-1, 1]) = [0, 1]. \end{aligned}$$

Thus we see that $f(f^{-1}(D)) = [0, 1] \subseteq [-1, 1] = D$ and $C = [0, 2] \subseteq [-2, 2] = f^{-1}(f(C))$.

We also considered the behaviour of images and preimages with respect to unions and intersections. Given $f : X \to Y$ and sets $A, B \subseteq X$ and $C, D \subseteq Y$, we have

$$\begin{aligned} f(A \cup B) &= f(A) \cup f(B) \\ f(A \cap B) &\subseteq f(A) \cap f(B) \\ f^{-1}(C \cup D) &= f^{-1}(C) \cup f^{-1}(D) \\ f^{-1}(C \cap D) &= f^{-1}(C) \cap f^{-1}(D). \end{aligned}$$

Note that in the second line we have an inclusion and not equality. In this case we have equality provided f is one-to-one. Otherwise, the two sets need not be equal. For example, take $f(x) = x^2$ again, with $A = [-1, 0]$ and $B = [0, 1]$. Then $A \cap B = \{0\}$, so $f(A \cap B) = \{f(0)\} = \{0\}$, but $f(A) = f(B) = [0, 1]$, so $f(A) \cap f(B) = [0, 1]$.

Exercises: From the text, 9.12, 9.22, 9.28, 9.35, 9.38, 9.48, 9.50, 9.75, 9.83, 9.93, 9.100, 9.101, 9.102, 9.106, 9.111, 9.112.

1. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2 - 2x$.
   (a) Evaluate $f(-3), f(-1), f(1), f(3)$.
   (b) Determine the preimages $f^{-1}(0)$ and $f^{-1}(4)$.
   (c) What is the range of f? (Hint: either sketch the graph or complete the square to obtain $f(x) = (x - 1)^2 - 1$.)

2. Let $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Define a function $f : \mathbb{Z}_6 \to \mathbb{Z}_6$ by $f(x) \equiv x^2 + 4 \pmod 6$. (If $x^2 + 4 \geq 6$, take the remainder after dividing by 6 to get an element of $\mathbb{Z}_6$. For example, $3^2 + 4 = 13 = 2(6) + 1$, so $f(3) = 1$.) Similarly define $g : \mathbb{Z}_6 \to \mathbb{Z}_6$ by $g(x) \cong (x + 1)(x + 4) \pmod 6$.
   (a) Compute $f(x)$ for $x = 0, 1, 2, 3, 4, 5$.
   (b) Compute $g(x)$ for $x = 0, 1, 2, 3, 4, 5$.
   (c) Is the function f equal to the function g? Explain.

3. Determine whether each of the following functions is one-to-one and/or onto:
   (a) $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = 3x + 1$.
   (b) $F : \mathbb{Q} \to \mathbb{Q}$ defined by $F(x) = 3x + 1$.
   (c) $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^3$.
   (d) $G : \mathbb{Q} \to \mathbb{Q}$ defined by $G(x) = x^3$.
   (e) $h : \mathbb{R} \to \mathbb{R}$ defined by $h(x) = \dfrac{2x}{x^2 + 4}$.
   (f) $H : A \to B$ defined by $H(x) = \dfrac{2x}{x^2 + 4}$, where $A = [0, \infty)$ and $B = [0, 1/2]$.

4. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = 3x - 2$. Let
$$A = [2, 5] \quad B = [-1, 3] \quad C = [-2, 3] \quad D = [1, 4].$$
   Find each of the following:

(a) $f(A)$
(b) $f^{-1}(f(A))$
(c) $f^{-1}(C)$
(d) $f(f^{-1}(C))$
(e) $f(A \cap B)$
(f) $f(A) \cap f(A)$
(g) $f^{-1}(C \cap D)$
(h) $f^{-1}(C) \cap f^{-1}(D)$

5. Repeat the previous problem if $f : \mathbb{R} \to \mathbb{R}$ is defined by $f(x) = x^2 - 1$.

Chapter 10: Cardinality

Informally, the cardinality of a set A is the number of elements that it contains. When only sets with a finite number of elements are considered, this informal definition suffices, but once infinite sets are introduced it's necessary to be more careful. Our approach to cardinality relies heavily on the fact that we can compare sets by defining functions between them. We say that two sets A and B are **equivalent** if there exists a bijection $f : A \to B$, and write $A \approx B$. (Note that $A \approx B \leftrightarrow B \approx A$ since any bijection $f : A \to B$ defines the bijection $f^{-1} : B \to A$.)

To simplify notation, let $k \in \mathbb{N}$ be a positive integer, and let $\mathbb{N}_k = \{1, 2, \ldots, k\}$ denote the set of natural numbers less than or equal to k. We say that a set A is **finite** if there exists a bijection $f : A \to \mathbb{N}_k$ for some $k \in \mathbb{N}$, and define the **cardinality** of A, denoted $|A|$, by $|A| = k$. We also consider the empty set to be a finite set, with $|\emptyset| = 0$. Any set which is not finite is said to be **infinite**.

Since the composition of bijections is a bijection, we see that if $A \approx B$ and $B \approx C$, then $A \approx C$. It follows that $A \approx B$ if and only if $|A| = |B|$. (Try to work out the details of this proof yourself. If you get stuck, see Proposition 10.9 in the text.)

Given a finite set A and some element $x \notin A$, we can prove that $|A \cup \{x\}| = |A| + 1$. By induction (see the next chapter) it follows that if $A \cap B = \emptyset$, then $|A \cup B| = |A| + |B|$. This is called the **addition principle**. When $A \cap B \neq \emptyset$, we have the **principle of inclusion-exclusion**:

$$|A \cup B = |A| + |B| - |A \cap B|.$$

We also have the **multplication principle**: if A and B are finite sets, then so is $A \times B$, and $|A \times B| = |A| \cdot |B|$. The addition and multiplication principles can both be extended inductively to unions or products of finitely many sets, and together provide the foundational results in *combinatorics* – the theory of counting.

From the addition principle, it follows that if $A \subseteq B$, then $|A| \leq |B|$, since we can write $B = A \cup (B \setminus A)$ (a disjoint union), so $|B| = |A| + |B \setminus A| \geq |A|$. A consequence of this is that if A is finite, then A is not equivalent to any of its proper subsets. As noted above, we can compare sets using functions. The most important results are the following: for finite sets A and B,

1. $|A| \leq |B|$ if and only if there exists a one-to-one function $f : A \to B$.
2. $|A| \geq |B|$ if and only if there exists an onto function $f : A \to B$.

A consequence of item 1 above is the **Pigeonhole principle**: if $|A| > |B|$, then any function $f : A \to B$ cannot be one-to-one. The pigeonhole principle can be used to give simple proofs

to certain problems; for example, it guarantees that at any given time, there are two people in the city of Calgary with the exact same number of hairs on their head (since there are more people in Calgary than there are hairs on a human head).

For finite sets, a lot of the work that we do using functions seems unnecessary, since we can, after all, just count the elements of a finite set. However, by doing so we laid the groundwork for discussing infinite sets: we are able to verify that all of the ideas above agree with our intuitive notion of cardinality, and that they're consistent. From this, we're able to generalize to infinite sets, using the same ideas. In particular, we take it as a *definition* that two sets have the same cardinality if and only if they are equivalent. This allows us to discuss cardinality of infinite sets.

We say that a set A is **countable** if there exists a one-to-one function $f : A \to \mathbb{N}$. Note that this definition includes finite sets: if $|A| = k$, we have a bijection $f : A \to \mathbb{N}_k$, and we have the inclusion function $i : \mathbb{N}_k \to \mathbb{N}$ given by $f(n) = n$ for $n = 1, 2, \ldots, k$, which is clearly one-to-one. Composing these functions gives a one-to-one function $i \circ f : A \to \mathbb{N}$.

A set which is infinite but countable is called a **countably infinite** set. Any set which is infinite but not countable is called **uncountable**. If A is a countably infinite set, we can find a function $f : A \to \mathbb{N}$ which is in fact a bijection. Examples of countably infinite sets include $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$. Note that unlike for finite sets, an infinite set can be equivalent to a proper subset. (In fact, this can be taken as a *definition* of what it means for a set to be infinite.) We saw that a countable union of countable sets is countable, and that the product of two countable sets is uncountable.

If a set A is infinite and it is impossible to construct a bijection $f : A \to \mathbb{N}$, then A is an uncountable set. We didn't spend much time discussing uncountable sets, but the main result to remember is that the set $\mathbb{R}$ of real numbers is uncountable.

Exercises: from the text, 10.11, 10.15, 10.20, 10.28, 10.32, 10.47, 10.54.

1. Prove that for any $r \in \{0, 1, \ldots, n-1\}$, the set of all $m \in \mathbb{Z}$ such that $m \equiv r \pmod{n}$ is countably infinite.

Chapter 11: Proof by induction

The **principle of induction** states that if $A \subseteq \mathbb{N}$ is a subset of the natural numbers such that $1 \in A$, and for any $k \geq 1$, $k \in A \to k + 1 \in A$, then $A = \mathbb{N}$. We apply the principle of mathematical induction to the proof of statements of the form "for all $n \in \mathbb{N}, P(n)$", where $P(n)$ is some predicate. To do so, we let $A = \{n \in \mathbb{N} : P(n) \text{ is true}\}$. If we can show that $P(1)$ is true and that $P(k) \to P(k + 1)$ for $k \geq 1$, then it follows that $A = \mathbb{N}$, so that $P(n)$ is true for all $n \in \mathbb{N}$.

For example, suppose we want to prove that for all $n \in \mathbb{N}$, the predicate $P(n)$ given by

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

is true. Our proof consists of three parts: a **base case**, where we check that $P(1)$ is true; an **induction hypothesis**, where we assume that $P(k)$ is true, for some $k \geq 1$, and the **inductive step**, where we show that $P(k+1)$ follows from $P(k)$. Here is what a proof looks like for the above assertion:

We wish to show that for all $n \in \mathbb{N}$, $\sum_{i=1}^{n} i^2 = \dfrac{n(n+1)(2n+1)}{6}$. When $n = 1$, we have $\sum_{i=1}^{1} i^2 = 1^2 = 1$, while $\dfrac{1(1+1)(2(1)+1)}{6} = 1$, so the base case holds. Let us therefore assume that for some $k \geq 1$, we have $\sum_{i=1}^{k} i^2 = \dfrac{k(k+1)(2k+1)}{6}$. It follows that for $n = k+1$ we have

$$\begin{aligned}
\sum_{i=1}^{k+1} i^2 &= \sum_{i=1}^{k} i^2 + (k+1)^2 \\
&= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \text{ (by our induction hypothesis)} \\
&= (k+1)\left(\frac{k(2k+1)}{6} + (k+1)\right) \\
&= (k+1)\left(\frac{2k^2+k+6k+6}{6}\right) \\
&= (k+1)\left(\frac{2k^2+7k+6}{6}\right) \\
&= \frac{(k+1)(k+2)(2k+3)}{6},
\end{aligned}$$

and since $2k + 3 = 2(k + 1) + 1$, we see that the result holds for $n = k + 1$. It follows by induction that the formula is valid for all $n \in \mathbb{N}$.

Caution: note that in the inductive step above, we began with one side of the equation and worked towards the other. We did **not** begin by writing $\sum_{i=1}^{k+1} i^2 = \frac{(k+1)(k+2)(2k+3)}{6}$ and hoping that both sides of the equality reduce to the same thing. This might be okay for rough work, but as a presented solution, it makes it look like you're assuming that the statement is true before you even begin to try to prove it! (It's the same problem as beginning an answer to the request "Prove that P implies Q" with "Suppose Q is true...")

We also looked briefly at other methods of induction. We saw that in some cases it's necessary to begin the induction at some integer other than 1, and in other cases it's necessary to use **strong induction**. In strong induction we may require a base step involving more than one case (for example, we might need to check $P(1), P(2)$, and $P(3)$), and we show that $P(k+1)$ follows from assuming that $P(m)$ is true for all $1 \leq m \leq k$. It's unlikely that you'll encounter strong induction on the final exam, but you might run into it in another course.

Exercises: from the text, 11.8, 11.14, 11.18.

Also, go back and prove any of the induction problems from the Quiz 11 practice problems that you haven't already solved. (If you have already solved them, do them again.)

Equivalence relations

Our last chapter was on relations, and in particular, equivalence relations. Given two sets A and B, a **relation** from A to B is simply a subset $R \subseteq A \times B$. If $(a, b) \in R$ we say that a is **related to** b and write $a\,R\,b$. The **domain** of a relation R is the set

$$\mathrm{dom}(R) = \{a \in A \mid \exists b \in B : (a, b) \in R\},$$

and the **range** of R is the set

$$\text{ran}(R) = \{b \in B \mid \exists a \in A : (a, b) \in R\}.$$

Note that the definitions of domain and range are much more symmetric than they are for a function. However, a function is just a special type of relation: a relation $f \subseteq A \times B$ defines a function $f : A \to B$ if $\text{dom}(f) = A$, and for each $a \in A$, there is a *unique* $b \in B$ such that $(a, b) \in f$.

Examples of relations include the "less than" relation $x < y$ on an ordered set (such as $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, or $\mathbb{R}$), the "element" relation $a \in B$ from a universal set U to its power set $\mathcal{P}(U)$, the "subset" relation $A \subseteq B$ defined on the power set of some universal set U, and the "divides" relation $a|b$ on $\mathbb{Z}$.

We defined several properties that are satisfied by certain relations on a set A. We say that a relation $R \subseteq A \times A$ is

- **Reflexive**, if $(a, a) \in R$ for all $a \in A$
- **Symmetric**, if $(a, b) \in R \to (b, a) \in R$ for all $a, b \in A$
- **Antisymmetric**, if $(a, b) \in R \wedge (b, a) \in R \to a = b$ for all $a, b \in A$
- **Transitive**, if $(a, b) \in R \wedge (b, c) \in R \to (a, c) \in R$ for all $a, b, c \in A$

A relation that is reflexive, antisymmetric, and transitive is called a **partial order relation**. Examples include the relation $x < y$ on $\mathbb{R}$ and the relation $A \subseteq B$ on $\mathcal{P}(U)$ for some universal set U. I won't ask about partial order relations on the exam, but you might encounter them in later courses.

An **equivalence relation** is a relation that is reflexive, symmetric, and transitive. Equivalence relations appear in almost every area of math, so they're an important topic of study. The three properties of an equivalence relation are all satisified by the equality relation $a = b$ (which makes sense on any nonempty set A); in fact, equivalence relations should be viewed as providing a way to say that certain objects are in some way "the same" without requiring them to be equal. Two extreme examples of equivalence relations are the sets $R = \{(a, a) \mid a \in A\}$ and $S = A \times A$. The relation R is just the equality relation: we have $a \, R \, b$ if and only if $a = b$. With the relation S, *every* element of S is equivalent.

Our main example of an equivalence relation is congruence modulo n: we define a relation $\sim$ on $\mathbb{Z}$ by

$$a \sim b \leftrightarrow a \equiv b \pmod{n},$$

where n is a positive integer. For example, with $n = 5$, we have $-3 \sim 2$ and $3 \sim 2048$. In this case, we view two integers as being "the same" if they have the same remainder upon division by n.

Given an equivalence relation $\sim$ on a set A, we define the **equivalence class** of an element $a \in A$ by

$$[a] = \{b \in A : a \sim b\}$$

It follows from the properties of equivalence relations that $a \in [a]$ for all $a \in A$, that $a \sim b \leftrightarrow [a] = [b]$, and that if $a \not\sim b$, then $[a] \cap [b] = \emptyset$. In many cases, we consider the set of

all equivalence classes as a new set, which often inherits properties from the set A. This set is often denoted by $A/\sim = \{[a] : a \in A\}$. (The notation suggests that we are "dividing" the set into its equivalence classes.)

When our equivalence relation is congruence modulo n on the integers, this leads us to **modular arithmetic**. We define the set

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\},$$

where $[a] = \{b \in \mathbb{Z} \,|\, a \equiv b \pmod{n}\}$. Note that any element of an equivalence class can be chosen to be the "representative" of the class; with congruence we usually take the integers $0, 1, \ldots, n-1$ since these are the remainders defined by the division algorithm – they provide us with a set of "standard" representatives. It's possible to define addition and multiplication on the set $\mathbb{Z}_n$ in terms of the addition and multiplication of $\mathbb{Z}$. We define

$$[a] \oplus [b] = [a + b]$$
$$[a] \odot [b] = [a \cdot b],$$

where on the right-hand side of these equations a and b represent any representatives of the equivalence classes $[a]$ and $[b]$. It's important to check that these operations are **well-defined**; that is, that the answer does not depend on which integers a and b we choose. This follows from the fact that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$. However, other operations are not well-defined. For example, you can check that it is not necessarily true that $a^c \equiv b^d \pmod{n}$, so there's no way to define the value of an equivalence class raised to the power of another equivalence class. (It is possible to define $[a]^k = [a^k]$ when k is a fixed integer however, since this is just $[a] \odot [a] \odot \cdots \odot [a]$ (k times).)

A good exercise is to compute the addition and multiplication tables for $\mathbb{Z}_5$ and $\mathbb{Z}_6$.