MATH 3325: NOTES TO ACCOMPANY LECTURES

VERN I. PAULSEN

Abstract. This notes are intended to supplement the in class lectures.

Lecture 1

Inductive vs Deductive Reasoning

Inductive reasoning is the means by which we discover many patterns and relationships. Many principles of science are discovered by inductive reasoning. For example, by observing the relationship between the moon and tides, we learned how to predict when high and low tides would occur.

A limitation of inductive reasoning is that you never know how far patterns extend. Some bad examples of inductive reasoning would be:

I flip a coin ten times and it always comes up heads. I conclude that it will always come up heads and bet a lot of money that the next time I flip the coin it will come up heads.

I give everyone in my class a peanut butter sandwich, no one gets sick and I conclude everyone can eat peanut butter without getting sick.

I smoke a pack-a-day of cigarettes for a month with no ill effects and deduce that it will be ok to smoke for the rest of my life.

These examples are meant to illustrate the real problem with inductive reasoning. Namely, there is no certainty. A conclusion that is drawn might have many exceptions and needs to be subject to constant review and debate about whether or not it really is a "pattern" or just a fluke, like when the coin came up heads ten times in a row.

Deductive reasoning is the process by which we use logic and the given rules or axioms to deduce further facts. The nice thing about deductive reasoning and what sets it apart from inductive reasoning, is that as long as the axioms are correct or the rules are obeyed, then the conclusions of a deductive reasoning process are certain.

Although many areas of science work primarily by inductive reasoning, what sets the science of mathematics apart is that it is primarily based on deductive reasoning.

While most mathematicians often start with inductive reasoning to uncover a pattern that might be true, we then use deductive reasoning and proofs to determine what is true.

Here are some examples of deductive reasoning.

Date: October 28, 2013.

In chess when someone says, "checkmate", they are using the rules that govern how pieces move and deductive reasoning to decide that there is no escape for their opponent.

In the game of Clue, one gathers facts and then uses deductive reasoning to decide who was the murderer in which room and with which weapon.

In the American jury system, when it works like it should, the jury is supposed to first agree on what are the facts and then based on those facts and the rules of law given to them deduce the outcome.

Of course, in many of the above cases one often arrives at the "right" conclusion without really formally knowing why and sometimes arrives at the "wrong" conclusion through faults in their deductive reasoning.

The main purpose of this course is to help us all sharpen our deductive reasoning skills. Along the way we will learn a lot about formal mathematical proofs, how to produce them and why they are important.

Assignment: Read "Preface to the Students".

Some Basic Background

It is impossible to start a course without assuming that the student knows something. In this section we organize the things that we believe that you should know for this course.

0.1. **Sets and Set Notation.** A **set** is a collection of things called the **elements** or **members** of the set. Often we will denote the elements of a set by brackets. For example, when I write $K = \{3, 4, 5, 7, a\}$, it means that K is a set and the elements of K are the numbers $3, 4, 5, 7$ and the letter a. When A is a set and we want to indicate that x is an element of A we write $x \in A$. If we want to indicate that x is not an element of A we write $x \notin A$.

So for the above set K we have that $7 \in K$ and $6 \notin K$.

Often it is hard to list all the elements of a set, like I did with the set K, and instead we use **set builder notation.**

An example of this would be:

$$B = \{x : 1 \leq x \leq 100 \text{ and } x \text{ is an integer}\},$$

which tells me that B is the set of all integers from 1 to 100. When we use set builder notation the colon should always be read as, "such that". The set B has 100 elements, which is why set builder notation is a much better way to write it than listing all the elements.

Given two sets A and B we say that the sets are **equal** and write $A = B$ to mean that they have exactly the same elements. For example if $A = \{3, 4\}$ and $B = \{x : x^2 - 7x + 12 = 0\}$, then, by factoring the polynomial, we see that $A = B$.

One thing to be careful of. We have that $5 \in \{5\}$, but $5 \neq \{5\}$, because the left hand side is just the number 5 while the right hand side means the set with exactly one element, the number 5. So they are not equal, because they are "different things".

Given two sets A and B we say that A **is a subset of** B provided that every element of A is also an element of B. In this case we write, $A \subseteq B$. For example, if $B = \{x : 1 \leq x \leq 10 \text{ and } x \text{ is an integer}\}$ and $A = \{3, 4, 5\}$ then $A \subseteq B$.

Here is an example of deductive reasoning:

If $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Can you see why? Explaining why has a lot to do with what proofs are about.

We will often talk about the **empty set** which means the set with no elements. This is denoted by $\emptyset$ or $\emptyset$.

Here are some sets that we will encounter, along with the special notations that we use for them.

$\mathbb{N} = \{1, 2, 3, ...\}$ the set of **natural numbers.**

$\mathbb{Z} = \{...., -3, -2, -1, 0, 1, 2, 3, ...\}$ the set of **integers.**

$\mathbb{Z}^+ = \{0, 1, 2, 3, ...\}$ the set of **non-negative integers.**

$\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\}$ the set of **rational numbers.**

$\mathbb{R}$ the set of **real numbers.**

$\mathbb{C}$ the set of **complex numbers.**

Writing down a careful definition of what exactly is the set $\mathbb{R}$ is not so easy. In fact, this is done in Math 3333.

A set is **finite** if it has n elements for some natural number n, and is called **infinite** if it is not finite.

One of the interesting things that we'll see in Chapter 5, is that infinite sets can come in different "sizes". We'll expalain exactly what this means when we get to Chapter 5.

0.2. **The Natural Numbers.** Here are the basic arithmetic and order properties of $\mathbb{N}$.

1. *The Successor Property.*
   - 1 is a natural number.
   - Every natural number n has a unique successor, $n+1$, i.e., the "next" natural number.
   - 1 is NOT the successor of any natural number, i.e., the natural numbers "start" at 1.
2. *Closure Properties*
   - The sum of two natural numbers is a natural number.
   - The product of two natural numbers is a natural number.
3. *Associativity*
   - For all $x, y, z \in \mathbb{N}$, $x + (y + z) = (x + y) + z$.
   - For all $x, y, z \in \mathbb{N}$, $x(yz) = (xy)z$.
4. *Commutativity*
   - For all $x, y \in \mathbb{N}$, $x + y = y + x$.
   - For all $x, y \in \mathbb{N}$, $xy = yx$.
5. *Distributivity*

- For all $x, y, z \in \mathbb{N}$, $x(y+z) = xy + xz$,
- For all $x, y, z \in \mathbb{N}$, $(y+z)x = yx + zx$.

NOTE: We didn't really need the last one! Why?

6. *Cancellation*
   - For all $x, y, z \in \mathbb{N}$, if $x + z = y + z$, then $x = y$.
   - For all $x, y, z \in \mathbb{N}$, if $xz = yz$, then $x = y$.

0.3. **Primes and Divisors.** Given $a, b \in \mathbb{N}$ we say that a **divides** b or that a is a **divisor** of b or that b is a **multiple** of a if and only if there is a $k \in \mathbb{N}$ such that $b = ak$.

For example, 3 divides 12 since $12 = 3 \cdot 4$.

If you are bothered by what "if and only if" means, don't worry, that is something we'll talk more about later. For now, you could replace it by "exactly when". So a divides b exactly when there is $k \in \mathbb{N}$ with $b = ak$.

Note a always divides a.

A natural number p is *prime* if and only if $p > 1$ and the only natural numbers that divide p are p and 1.

Note: In this book, 1 is NOT prime. Sometimes books call 1 prime. Our book's definition agrees with the definition found on Wikipedia! Good job Wiki!

A natural number n is called *composite* if and only if $n \neq 1$ and n is not a prime.

So n is composite if and only if some natural number $a \neq 1$ and $a \neq n$ divides n.

For example, $2, 3, 5, 7, 11$ are primes, while $4 = 2 \cdot 2$, $6 = 3 \cdot 2$ and $8, 9, 10$ are composite.

0.4. **The Fundamental Theorem of Arithmetic.** Every natural number $n \neq 1$ can be expressed uniquely as a product of primes. For example, $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$ and $90 = 2 \cdot 3^2 \cdot 5$.

Remember the way that we do this: If the number is composite, then we can write it as a product of two things, $90 = 9 \cdot 10$ and then each of those factors is either prime or composite, $9 = 3 \cdot 3$ and $10 = 2 \cdot 5$ and eventually, we arrive at primes.

The book has more things in the preface but this is plenty for now! You should read these, but we will also return to these other facts as we need them.

Lecture 2

Logic and Proofs

In mathematics we use proofs, based on deductive reasonig and logic, to demonstrate that our conclusions are true. In the Chapter 1, we will be looking carefully at the basics of logic and the key concepts and their definitions.

0.5. **Propositions.** The first important concept in logic is a **Proposition.**

Definition. A **proposition** is a sentence that has exactly one truth value: it is either true, which we denote by T or false which we denote by F.

These concept needs lots of examples. Some propositions:

- The square of 3 is 9.
- The square of 2 is 5.
- 3 is a divisor of 6.
- 19 is a composite number.
- Vern is the tallest boy in our class.
- x is an integer, $1 < x < 3$ and $x^2 = 4$.
- The next time I flip a coin it will come up heads.
- By the year 2052, humans will be extinct.

Note that the last two are propositions, even though at the moment I cannot give them a truth value.

Some things that aren't propositions:

- $x^2 = 4$. (Reason: nobody said what x was.)
- She lives in Houston. (Reason: nobody said who "she" is.)
- What time is it?

Some things that could be propositions:

- Steve is tall.
- The US national debt is too big.

These would be propositions if we had precise definitions of "tall" and "too big".

A statement like *this sentence is false* is not a proposition. It is called a **paradox.** If it was true, it would be false and if it was false, it would be true!

We will often use letters to denote propositions, so I might write let P be a proposition.

0.6. **Negations.**

Definition. The **negation** of a proposition P, is denoted by $\sim P$ and $\sim P$ is the proposition "not P". The proposition $\sim P$ is true exactly when P is false and $\sim P$ is false exactly when P is true.

So the truth value of $\sim P$ is the opposite of the truth value of P.

Notice that there is often more than one way to express the negation of a proposition. For example the negation of the proposition that "Vern is the tallest boy in our class" could be expressed as:

- Vern is not the tallest boy in our class.
- There is a boy in our class taller than Vern.

Is "Vern is the shortest boy in our class" also a negation of "Vern is the tallest boy in our class" ?

0.7. **Conjunctions and Disjunctions.**

Definition. Given propositions P and Q the **conjunction** of P and Q is the propositons "P and Q". It is denoted by $P \wedge Q$ and it is the proposition that is true exactly when both P and Q are true.

The **disjunction** of P and Q, is the proposition "P or Q". It is denoted $P \vee Q$ and it is the proposition that is true exactly when at least one of P or Q is true.

Let's let P be the statement $3^2 = 10$ and Q be the statement "2 divides 6".

Then $P \wedge Q$ is the statement $3^2 = 10$ and 2 divides 6. T or F?

$P \vee Q$ could be written as the statement: Either $3^2 = 10$ or 2 divides 6. T or F?

Translate $(\sim P) \wedge Q$, $(\sim P) \vee Q$, $P \wedge (\sim Q)$ and $P \vee (\sim Q)$ into English sentences. Is each one T or F?

Sometimes, especially in computer science, people are interested in the **exclusive or** this means that exactly one of two statements is true. Express this in terms of conjunctions and disjunctions.

Answer: $(P \vee Q) \wedge [\sim (P \wedge Q)]$.

Sometimes when people write sentences in English it is hard to tell exactly what they meant. How about: At the grocery store I can buy apples, peaches and pears.

This time "and" really meant "or"!

Another example: Natural numbers greater than one can be composite and prime.

Again "and" meant "or".

The words "but", "while" and "although" usually mean conjunction. Here are some examples:

- Sally is a girl, but Steve is the tallest boy in our class.
- 39 is prime, although 6 is composite.
- Austin is the capitol of Texas, while Lansing is the capitol of Michigan.

The word "or" almost always means disjunction.

Can you think of any English sentences where "and" means disjunction? Any where "or" means conjunction?

0.8. **Propositional Forms and Truth Tables.** When we write $P \wedge Q$ we don't know if it is true or false until we know whether P is true or false and whether Q is true or false. Formulas like $P \wedge Q$, $P \wedge (\ Q)$, $(P \wedge Q) \vee R$ are called **propositional forms.** Once you know whether or not eaach of the terms in a propositional form are true or false, you can work out if the form is true or false. **Truth tables** are a good way to display all the possibilities. The way that you should read a T or F in the table, is to mean that "if we knew this proposition was T". Below are the truth tables for P and $\ P$, and for for $P, Q, P \wedge Q, P \vee Q, (\ P) \wedge Q$, etc.

P	$\sim P$
T	F
F	T

P	Q	$P \wedge Q$	$P \vee Q$	$(\sim P) \wedge Q$
T	T	T	T	F
T	F	F	T	F
F	T	F	T	T
F	F	F	F	F

We also do some propositional forms with 3 propositions, P, Q, R, e.g., $(P \wedge Q) \vee R, (P \vee Q) \wedge R$.

P	Q	R	$(P \wedge Q) \vee R$	$(P \vee Q) \wedge R$
T	T	T	T	T
T	T	F	T	F
T	F	T	T	T
F	T	T	T	T
T	F	F	F	F
F	T	F	F	F
F	F	T	T	F
F	F	F	F	F

0.9. **Tautologies and Contradictions.** A propositional form is called a **tautology** if it is true for every assignment of truth values to its components.

For example, $P \vee (\sim P)$ is a tautology. In plain English it says that either P is true or not P is true, but this is the same as saying that either P is true or P is false, which is always the case. If P is true this is true and if P is false this is true. This tautology is called the *Law of the Excluded Middle.*

A more complicated tautology is: $(P \vee Q) \vee (\sim P \wedge \sim Q)$.

In plain English this says that: either P or Q is true or both are false. Seeing that this is always true can be unraveled with a truth table, see page 4 of the book.

A **contradiction** is a propositional form that is always false. For example, $P \wedge (\sim P)$ is a contradiction since it is impossible for both P to be true and not P to be true.

0.10. **Equivalent Statements.** Two statements are equivalent if they say the same thing. For example, "Vern is not the tallest boy in the class" and "there is a boy in the class taller than Vern" are equivalent.

Two propositional forms are **equivalent** if they have the same truth tables.

For example, P and $\sim(\sim P)$ are equivalent. Because if P is true, then $\sim P$ is false and so $\sim(\sim P)$ is true. While if P is false, then $\sim P$ is true and so $\sim(\sim P)$ is false.

This is just the principle that if you negate something twice then you are back to the original statement.

An example of using this in plain English, "there is not a boy in the class taller than Vern" is the same as saying that "Vern is the tallest boy in the class". Note what we have done is that the first phrase is the negation of "there is a boy in the class taller than Vern" and since we have negated twice, we are just making the original statement.

Another example of equivalent propositional forms is $\sim P$ and $\sim\sim\sim P$.

The form P and $P \wedge P$ are equivalent propositional forms.

Here is a more complicated example. The propositional forms $\sim(P \wedge Q)$ and $(\sim P) \vee (\sim Q)$ are equivalent. First try seeing why in plain English, then form the truth table. See page 5 of the book for the truth table.

In plain English: $\sim(P \wedge Q)$ is saying that "P and Q are not both true" which means that "either P is not true or Q is not true". So the "either" is a disjunction and we have $(\sim P) \vee (\sim Q)$.

HW1, Due 9/4:

Write plain English negations(besides just putting a "not" in the sentence) of the following propositions:

- 17 is a composite number.
- Humans will be extinct by January 1, 2052.
- The next time I roll a die it will come up a 3.

Make truth tables for each of the following propositional forms:

- $\sim(P \wedge Q)$
- $(P \wedge Q) \vee (P \wedge R)$

Lecture 3: 9/4

Quick Review: Suppose that A, B, C, D and E are propositions with A, B, C all true and D, E both false. State whether the following are true or false: $A \wedge (C \wedge D)$, $(A \vee E) \wedge (C \vee D)$.

Is $P \wedge Q$ equivalent to $Q \wedge P$? Find a form equivalent to $\sim(P \wedge Q)$.

A **denial** of a proposition is any statement equivalent to its negation.

A denial of a propositional form P is any propositional form equivalent to $\sim P$. So $\sim\sim\sim P$, $\sim\sim\sim\sim\sim P$ are both denials of P.

A denial of $P \wedge Q$ would be any propositional form equivalent to $\sim(P \wedge Q)$. Can you think of one? If not, see the theorem below to find one.

Here is a summary of some important equivalences.

Theorem 1.1.1. For propositions P, Q, and R the following are equivalent:

- (a) P and $\sim(\sim P)$ Double Negation Law
- (b) $P \vee Q$ and $Q \vee P$ Commutative Law
- (c) $P \wedge Q$ and $Q \wedge P$ Commutative Law

- (d) $P \vee (Q \vee R)$ and $(P \vee Q) \vee R$ Associative Law
- (e) $P \wedge (Q \wedge R)$ and $(P \wedge Q) \wedge R$ Associative Law
- (f) $P \wedge (Q \vee R)$ and $(P \wedge Q) \vee (P \wedge R)$ Distributive Law
- (g) $P \vee (Q \wedge R)$ and $(P \vee Q) \wedge (P \vee R)$ Distributive Law
- (h) $\sim (P \wedge Q)$ and $(\sim P) \vee (\sim Q)$ DeMorgan's Law
- (i) $\sim (P \vee Q)$ and $(\sim P) \wedge (\sim Q)$ DeMorgan's Law

These are proved in the book. I'll discuss a couple.

More importantly, let's see how to use these in sentences.

Let P be the statement "Prof. Plum is the murderer", Q the statement "the murder was in the library", and R the statement "the murderer used a knife".

Then $P \wedge (Q \vee R)$ is true provided that "Prof. Plum is the murderer and either the murder was in the library or a knife was used. By (f) this sentence means the same thing as $(P \wedge Q) \vee (P \wedge R)$ which is "either Prof. Plum commited the murder in the library or Prof. Plum used a knife to commit the murder".

Using (h), we see that the negation of the statement, "Prof. Plum commited the murder in the library" is "either Prof. Plum is not the murderer or the murder did not take place in the library".

Conditionals and Biconditionals

New kinds of propositional forms.

Definition. Let P and Q be propositions the **conditional sentence** $P \implies Q$ is the statement that "if P is true then Q is true" or "when P is true, Q is true". P is called the **antecedent** and Q is called the **consequent.**

Note that if P is a false proposition, then Q can be any proposition and $P \implies Q$ will still be true!

Here's some "if-then" statements, we'll decide if they are true or false.

(1) If $2 + 2 = 5$ then 14 is odd.
(2) If $2 + 2 = 5$ then 14 is even.
(3) If a line in the plane is vertical, then its slope is undefined.
(4) If two lines in the plane are parallel and not vertical, then they have the same slope. This sentence gave me trouble in class, the problem is that it is not stated very clearly. Let's restate as: "If two lines in the plane are parallel and at least one is not vertical, then both slopes exist and are equal."
(5) If Vern is the tallest boy in the class then Richard is a girl.
(6) If f is differentiable at x_0 and $f'(x_0) = 0$ then $f(x_0)$ is a relative maximum.
(7) If f is differentiable at x_0 and $f(x_0)$ is a relative maximum, then $f'(x_0) = 0$.
(8) If you score above 90 on the test, then you will get an A.

Note that deciding if (8) is true or false depends on my grading scale. Let's suppose that I use a straight scale, then (8) is true.

It turns out that $P \implies Q$ can be expressed in terms of $\sim$'s and $\vee$'s. More precisely, it is equivalent to $(\sim P) \vee Q$. To see this we build the truth table.

P	Q	$P \implies Q$	$(\sim P) \vee Q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Definition. The **converse** of $P \implies Q$ is the statement $Q \implies P$.

The **contrapositive** of $P \implies Q$ is the statement $(\sim Q) \implies (\sim P)$.

State converses of all of the previous sentences. Which are true which are false? Here are a few:

(1) If 14 is odd, then 2+2=5. (true)

(2) If 14 is even, then 2+2 =5. (false)

(3) If the slope of a line in the plane is undefined, then the line is vertical. (true)

(4) If two lines in the plane have slopes that exist and are equal, then they are parallel and at least one is not vertical. (true)

(6) If $f(x_0)$ is a relative maximum, then f is differentiable and $f'(x_0) = 0$.(false)

(8) If you get an A then you scored above 90 on the test. (true, for straight scale)

State contrapositives of all of the previous sentences. Which are true which are false?

(1) If 14 is not odd, then $2+2 \neq 5$. OR If 14 is even, then $2+2 \neq 5$.(true)

(2) If 14 is odd, then $2+2 \neq 5$.(true)

(3) If the slope of a line in the plane is defined, then the line is not vertical.(true)

(4)

The contrapositive is still very complicated. Note that both the antecedent and consequent have an "and". Remember that when we negate "A and B" it becomes "either not A or not B". The clause that "one is not vertical" means "either A is not vertical or B is not vertical" which negates to "A is vertical and B is vertical"

If at least one slope does not exist or both slopes exist but are not equal, then either the lines are not parallel or both lines are vertical.(true)

Whew! Much harder than I thought when I wrote it down!

(5) If Richard is a boy, then Vern is not the tallest boy in the class.(true)

(6) If $f(x_0)$ is not a relative maximum, then either f is not differentiable at x_0 or $f'(x_0) \neq 0$. (false, $f(x_0)$ could be a relative minimum with f differentiable at x_0 and $f'(x_0) = 0$.) (7) If $f'(x_0)$ is not the number 0, then either f is not differentiable at x_0 or $f(x_0)$ is not a relative maximum.(true) (8) If

you did not get an A, then you did not score above 90 on the test.(true, for straight scale.)

So we see that there is no general relationship between a statement being true and its converse being true. But in every example, the contrapositive is true when the original statement is true, so by inductive reasoning we might guess that this is always the case! Now we will show this with a cold, hard proof!

Theorem 1.2.1. For propositions P and Q.

- (a) $P \implies Q$ is equivalent to its contrapositive $(\sim Q) \implies (\sim P)$.
- (b) $P \implies Q$ is NOT equivalent to its converse $Q \implies P$.

Proof: We'll do (b) first. To prove that something is not true, it is enough to give an example and in the sentences that we had above we have lots of examples. One could also do this with a truth table.

The easiest way to prove (a) is to do a truth table.

I want to do it another way. We saw above that $P \implies Q$ is equivalent to $(\sim P) \vee Q$. This says you negate the first and $\vee$ with the second.

Hence, $(\sim Q) \implies (\sim P)$ is equivalent to $\sim (\sim Q) \vee (\sim P)$, which by the double negation property is equivalent to $Q \vee (\sim P)$ which is $(\sim P) \vee Q$, by commutativity. But this last statement is equivalent to $P \implies Q$.

Lecture 4: 9/9

Quick Review: $P \implies Q$ read "P implies Q" means that whenever P is true, then Q is true. So $P \implies Q$ is true when this happens. For example, if P is the proposition that "6 divides the number n" and Q is the proposition that "3 divides the number n" then "P implies Q" is the statement: "If 6 divides the number n, then 3 divides the number n", which is a true statement.

The converse of the statement $P \implies Q$ is the statement $Q \implies P$. In this case the converse is the statement that "if 3 divides the number n, then 6 divdes the number n" which is not true.

The contrapositive of the statement $P \implies Q$ is the statement $\sim Q \implies \sim P$. In this case the contrapositive is the statement: "If 3 does not divide the number n, then 6 does not divide the number n". In this case the contrapositive is true.

In fact, last time we saw that the statement $P \implies Q$ and its contrapositive $\sim Q \implies \sim P$ are equivalent statements. In other words either both statements are true or both statements are false.

This is an example of a biconditional.

Definition. Let P and Q be propositions. The **biconditional** denoted, $P \iff Q$, is the statement that P and Q have the same truth values. In other words, either P and Q are both true or P and Q are both false. In words, the biconditional is stated as "P if and only if Q".

Stated differently: whenever P is true it must be the case that Q is true AND whenever P is false it must be the case that Q is false.

The statement that whenever P is true, Q is true is the statement that $P \implies Q$.

The second statement that whenever P is false Q is false is the statement that $(\sim P) \implies (\sim Q)$ which is the contrapositive of $Q \implies P$.

So the statement $P \iff Q$ is the same as saying that $P \implies Q$ AND $Q \implies P$.

This at least explains the notation. Put more formally, we are saying that $P \iff Q$ and $[P \implies Q] \wedge [Q \implies P]$ are equivalent propositional forms.

Some good examples of the biconditional are:

- 2 divides the natural number b if and only if b=2k for some natural number k
- 2 divides the natural number b and 3 divides the natural number b $\iff$ 6 divides the natural number b,
- $[P \implies Q] \iff [(\sim Q) \implies (\sim P)]$.
- $[P \wedge Q]$ is true $\iff$ $[Q \wedge P]$ is true.
- A line in the plane is horizontal $\iff$ it has slope 0.
- A line in the plane is vertical $\iff$ its slope is undefined.
- Two lines in the plane are parallel $\iff$ either they both have a slope that is defined and is the same number or they both have slope that is undefined.

Notice that when we are talking about propositional forms, then saying that they are equivalent is the same as saying that we have an "if and only if", so for example we could write:

$[P \wedge Q] \iff [Q \wedge P]$,

$[P \implies Q] \iff [\sim Q \implies \sim P]$,

and one of deMorgan's laws, $[\sim (P \wedge Q)] \iff [(\sim P) \vee (\sim Q)]$.

The truth table for the biconditional is:

P	Q	$P \iff Q$
T	T	T
T	F	F
F	T	F
F	F	T

A good way to deal with the biconditional is given by (b) below:

Theorem 1.2.2. For propositions P,Q and R.

- (a) $P \implies Q$ is equivalent to $(\sim P) \vee Q$.
- (b) $P \iff Q$ is equivalent to $(P \implies Q) \wedge (Q \implies P)$.
- (c) $\sim (P \implies Q)$ is equivalent to $P \wedge (\sim Q)$.
- (d) $\sim (P \wedge Q)$ is equivalent to $P \implies (\sim Q)$.
- (d') $\sim (P \wedge Q)$ is equivalent to $Q \implies (\sim P)$.
- (e) $P \implies (Q \implies R)$ is equivalent to $(P \wedge Q) \implies R$.
- (f) $P \implies (Q \wedge R)$ is equivalent to $(P \implies Q) \wedge (P \implies R)$.

- (g) $(P \vee Q) \implies R$ is equivalent to $(P \implies R) \wedge (Q \implies R)$.

These can all be done with truth tables. We did (a) earlier.

For an example, let's reason out (c) in words.

Recall that $P \implies Q$ means that "when P is true, then Q is true". So for this to not be the case, then there must be the case that P is true and Q is false. So we have $P \wedge (\sim Q)$.

Here is (c) done in symbols:

We know by (a), that $P \implies Q$ is equivalent to $(\sim P) \vee Q$. So by deMorgan's Law, the negation of one OR the other being true is that they are both false. So $\sim [(\sim P \vee Q]$ is equivalent to $[\sim\sim P] \wedge [\sim Q]$ which by double negation is $P \wedge [\sim Q]$.

Here is an example typical of problem 1.2.7

Make a truth table for $(P \wedge Q) \implies (P \vee Q)$. First common sense: $P \wedge Q$ is the statement that P AND Q are true, while $P \vee Q$ is the statement that P OR Q is true. So this statement should be universally true–a tautology!

P	Q	$P \wedge Q$	$P \vee Q$	$(P \wedge Q) \implies (P \vee Q)$
T	T	T	T	T
T	F	F	T	T
F	T	F	T	T
F	F	F	F	T

HW2, Due 9/11: Section 1.1: 4 b,d,e; 6b,d,f; 9a,b; 11b Section 1.2: 3 a,b,c,d,e; 5b,d; 6d,f,j; 7a,d; 12a,c

Many authors and often in ordinary English instead of the words "if" and "then" people will say "necessary" or "sufficient".

So, when someone says: "In order for Q to be true it is sufficient that P be true" they mean that "to check that Q is true it is enough to know that P is true".

In other words, "if P is true then Q is true".

The word "necessary" is hard to understand until you think about contrapositive:

"In order for P to be true it is necessary for Q to be true".

This means that whenever Q is false, it must be the case that P is false, i.e., that $(\sim Q) \implies (\sim P)$, which we know is the same as $P \implies Q$.

Finally, when someone says that: "in order for P to be true it is necessary and sufficient for Q to be true", then the "P necessary Q" part says $P \implies Q$ and the "P sufficient Q" part says $QimpliesP$.

Therefore, the statement, "in order for P to be true it is necessary and sufficient for Q to be true" is another way to express the biconditional $P \iff Q$.

Quantifiers and Truth Sets

A statement like "$x \geq 2$" is not a proposition, because we don't know what x is, so we can not assign a true or false to this statement. A sentence

like this with a variable is called an **open sentence** or a **predicate.** It can only be true or false AFTER x is assigned a particular value.

When we have an open sentence with a variable x, it is generally written as P(x). Thus, P(3) is true while P(1) is false.

Simlarly, when we have more variables, like the open sentence " x+y=z" we might write as P(x,y,z). So here, P(1,2,3) is true and P(2,1,3) is true, but P(3,1,2) is false.

When we have an open sentence, the collection of objects that can be substituted in for the variable is called the **universe,** or **universe of discourse.** Often I will write U for the universe.

The elements of the universe that can be substituted in to make the sentence true is called the **truth set.**

So for example, if my universe is $\mathbb{N}$ and my open sentence is $P(x) : x \geq 2$, then my truth set would be

$$\{2, 3, 4, ...\} = \{x \in \mathbb{N} : x \neq 1\}.$$

This is an important example. It shows that when my universe is $\mathbb{N}$ then the open sentences $P(x) : x \geq 2$ and $Q(x) : x \neq 1$ have the same truth sets.

Definition. With a universe specified, two open sentences P(x) and Q(x) are **equivalent** if and only if they have the same truth sets.

So another way to think about this is that P(x) and Q(x) are equivalent if and only if

$$\{x \in U : P(x) \text{ is true } \} = \{x \in U : Q(x) \text{ is true } \}.$$

So when my universe is $\mathbb{N}$ the open sentence $P(x) : x^2 = 4$ and the open sentence $Q(x) : x = 2$ are equivalent.

Example: Let $U = \mathbb{Z}$, let $P(x) : x^2 \leq 4$, let $Q(x) : x^2 - 4x + 3 = 0$. Give the truth sets for P and for Q.

But when my universe is $\mathbb{Z}$ then these open sentences are no longer equivalent.

Definition. Given an open sentence P(x) the sentence

$$(\exists x)P(x)$$

is read as "there exists an x such that P(x)". When my universe U is given, then this sentence is true iff and only if there exists an $x \in U$ such that $P(x)$ is true. In other words this sentence is true if and only if the truth set of $P(x)$ is non-empty.

The symbol "$\exists$" is called the **existential quantifier.**

So the sentence $P(x)$ doesn't have a truth value, but $(\exists x)P(x)$ does as soon as the universe is given.

For these examples, take $U = \mathbb{N}$. Let $P(x) : x \geq 2$, and $Q(x) : x < 1$. Then $(\exists x)P(x)$ is true, but $(\exists x)Q(x)$ is false.

If I change my universe to $U = \mathbb{Z}$ then both are true.

If $U = \mathbb{N}$ with $R(x) : 30 \leq x \leq 40$ and x is prime, then is $(\exists x)R(x)$ true?

Definition. Given an open sentence P(x) the sentence

$$(\forall x)P(x)$$

is read as "for all x, P(x)". When my universe U is given then this statement is true if and only if the truth set of P(x) is the entire universe.

The symbol $\forall$ is called the **universal quantifier.**
Here are some true statements for $U = \mathbb{R}$.
$(\forall x)(x < x + 2)$
$(\forall x)(x \leq x + 2)$
$(\forall x)(x^2 \geq 0)$
$(\forall x)(x = 0 \vee x^2 > 0)$
When $U = \mathbb{N}$ then
$(\forall x)(2x$ is even)
$(\forall x)(6x$ is divisible by 3)
are true.
Note that the sentence $(\forall x)(x^2 + 1 \geq 2)$ is true in the universe $\mathbb{N}$ but not in $\mathbb{R}$.

Lecture 5: 9/11

Quick Review: Last time introduced universes, open sentences, truth sets, the concept of open sentences being equivalent in a universe, and the quantifiers, $\exists$ and $\forall$.

Example: Give a universe and use quantifiers to translate the following sentences.

"Every natural number is strictly less than its predecessor."

"Every real number is either 0 or has an inverse."

It is possible to have multiple variables and quantifiers. Here the universe is $\mathbb{N}$. Translate the following into plain English and decide if it is true or false:

$$(\forall x)(\exists y)(x < y).$$

$$(\exists x)(\forall y)(x \leq y).$$

$$(\forall x)(\exists y)(y < x).$$

Definition. Two sentences with quantifiers are said to be **equivalent in a given universe** if they have the same truth value in that universe. Two quantified sentences are **equivalent** if they are equivalent in every universe.

For example, $(\exists x)(P(x) \wedge Q(x))$ and $(\exists x)(Q(x) \wedge P(x))$ are equivalent in every universe.

For example, if my universe is $\mathbb{R}$ then $(\forall x)(x^2 > 0)$ and $(\exists x)(x^2 + 1 = 0)$ are equivalent because they are both false. But they don't make sense in every universe. For example, if my universe is "all cows".

Here are some useful equivalences.

Theorem 1.3.1. If A(x) is an open sentence with variable x, then
(a) $\sim [(\forall x)A(x)]$ is equivalent to $(\exists x)(\sim A(x))$.
(b) $\sim [(\exists x)A(x)]$ is equivalent to $(\forall x)[\sim A(x)]$.

First, let's discuss why these are true, then we will see some common sense uses.

(a) We have that $\sim [(\forall x)A(x)]$ is true iff $[(\forall x)A(x)]$ is false iff the truth set of $A(x)$ is not the entire universe iff there is an $x \in U$ with $A(x)$ false iff there exists $x \in U$ with $\sim A(x)$ true iff $(\exists x)[\sim A(x)]$ is true.

(b) We have that $\sim [(\exists x)A(x)]$ is true iff $[(\exists x)A(x)]$ is false iff the truth set of $A(x)$ is empty iff $A(x)$ is false for all $x \in U$ iff $\sim A(x)$ is true for every $x \in U$ iff $(\forall x)[\sim A(x)]$.

Here are some examples of using this theorem.

Supose that I want to decide whether the statement S:"it is not the case that for every prime p, $p^2 + 1$ is prime" is true or false. In this case my universe is the set of primes U and my open sentence is "$A(p) : p^2 + 1$ is prime". So S is " $\sim [\forall p]A(p)$ which has the same truth value as "$(\exists p)[\sim A(p)]$" which is the statement R: "there exists a prime p such that $p^2 + 1$ is not prime".

So S is true iff R is true and S is false iff R is false.

Here's what's been gained: To show S is true I would need to check *every* prime. To show R is true I just need an example.

Look at $p = 7$, since $7^2 + 1 = 50 = 5 \cdot 10$ is not prime, so R is true, so S is true.

The above rules are also useful for unraveling the denials of complicated sentences.

Suppose that my sentence is:

"Every odd natural number is prime."

and I would like to form a denial of this sentence.

First, take my universe to be $\mathbb{N}$, let P(x) be the proposition: "x is odd" and take Q(x) to be: "x is prime".

Then this sentence becomes:

$$(\forall x)(P(x) \implies Q(x)).$$

So the denial is:

$$(\exists x)[\sim (P(x) \implies Q(x))].$$

But we saw that the negation of $P \implies Q$ is $P \wedge (\sim Q)$.

So the denial is:

$$(\exists x)[P(x) \wedge (\sim Q(x))],$$

which is in words is:

"there exists a natural number x such that x is odd and x is not prime".

This is a true statement, we could take x=1 or x=15, many examples only need one!

Since the denial of the original statement is true, the original statement is false.

Here's a complicated statement to find a denial of, where this stuff helps:

$$(\forall x)(\exists y)(\exists z)(x+y>z).$$

The denial is:

$$(\exists x) \sim \big((\exists y)(\exists z)(x+y>z)\big),$$
$$(\exists x)(\forall y) \sim \big((\exists z)(x+y>z)\big),$$
$$(\exists x)(\forall y)(\forall z)[\sim (x+y>z)],$$
$$(\exists x)(\forall y)(\forall z)(x+y\leq z).$$

Another quantifier:

Definition. For an open sentence P(x) the proposition $(\exists! x)P(x)$ is read as "there exists a unique x such that P(x)". this statement is true if the truth set of P(x) has *exactly one element.*

For example if $P(x): x^2 = 9$ then $(\exists! x)P(x)$ is true when my universe is $\mathbb{N}$ but is false when my universe is $\mathbb{Z}$.

Some typical examples of HW3:

Use $U = \mathbb{N}$ to translate: "there is a natural number that is strictly larger than every other natural number" into symbols.

Answer: $(\exists x)(\forall y)(y < x)$.

Form a denial in symbols, then in words.

Answer:

$$(\forall x) \sim \big((\forall y)(y<x)\big)$$
$$(\forall x)(\exists y) \sim (y<x)$$
$$(\forall x)(\exists y)(x\leq y)$$

For every natural number there is another natural number that is greater than it.

Basic Proof Methods

We will cover the ideas in sections 1.4 and 1.5 of the book here.

Mathematics always has to start somewhere. The truths that we hold to be self-evident are called either **axioms** or **postulates.** Sometimes I'll just refer to these as "facts". For example, when we are dealing with the integers, then one of the axioms is that $x+y=y+x$, this is not something that we try to prove. Similarly, $2+2=4$ is a fact, not something that I will try to prove.

Sometimes the list of axioms is pretty short. Euclidean geometry has only 5 postulates and everything else that we prove about triangles, etc., come from those 5 axioms.

A **theorem** is always a true statement whose truth follows from the given facts. A **proof** is the way that we give a justification for why a theorem is true.

First to get an idea of how we make proofs. In a proof you can always do the following things:

- State an assumption, axiom, or previously proved result.
  So I might say "since 2+2=4..." or "since addition is commutative..."
- Replacement Rule: Restate a sentence in a logiclly equivalent way.
  So if the sentence says "since x is not even" I might replace that with "since x is odd".
- Tautology: Replace a sentence by using a tautology.
  For example, if dealing with real numbers I might say: "Either $x > 0$ or $x \leq 0$...". Then I am really using the tautology $P \vee (\sim P)$.
- Modus Ponens: If I know that P is true and I know that $P \implies Q$ is true, then I can deduce that Q is true.
  A fancy Latin name for something pretty obvious. In logical symbols this is expressed as $[P \wedge (P \implies Q)] \implies Q$. Perhaps better is an example. Suppose that P is the statement that "x is even" and Q is the statement that "x=2k". We know that $P \implies Q$. So if at some point in a proof, I have discovered that x is an even integer, then I can say that, "hence x =2k for some integer k".

Enough talk, action! Here is an example of a theorem and proof.

Theorem: Let a, b, c be natural numbers. If a divides b and b divides c then a divides c.

Proof: By the definition of what "divides" means, the statement "a divides b" means that there is an integer k so that $b = ak$. Also, by this definition, there is an integer$j$ so that $c = bj$.

Hence, by the associative axiom, $c = bj = (ak)j = a(kj)$. Since the product of two integers is again an integer kj is an integer.

Thus, a divides c. □

I'll often use the symbol □ so you can easily tell where the proof ends.

In this proof we really only basically used the definition and axioms.

0.11. **Replacing a sentence by a logically equivalent statement.** **Theorem:** Let $x \in \mathbb{N}$. If $x \neq 1$, then $4 \leq 2x$ and $2x \leq x^2$.

Discussion: This sentence has the form $P \implies [Q \wedge R]$ This is logically equivalent to: $[P \implies Q] \wedge [P \implies R]$, so what we will do is show that both $P \implies Q$ and $P \implies R$ are true.

Note sometimes: $4 \leq 2x$ and $2x \leq x^2$ is written as $4 \leq 2x \leq x^2$ in which case the "and" is harder to see!

Proof: Since $x \in \mathbb{N}$ and $x \neq 1$, we know that $2 \leq x$ or $(x-2) \geq 0$. Since $2 \geq 0$, we have that $2(x-2) \geq 0$ or $2x - 4 \geq 0$, which is the same as $4 \leq 2x$. (This is $P \implies Q$)

Also, since $x \geq 0$, we have that $x(x-2) \geq 0$ or $x^2 - 2x \geq 0$. Thus, $2x \leq x^2$. (This is $P \implies R$)

Hence, $x \in \mathbb{N}$ and $x \neq 1$ implies that $4 \leq 2x \leq x^2$. □

Theorem: Let $x \in \mathbb{N}$. If $x \neq 2$, then either $x = 1$ or $2x < x^2$.

Discussion: This is of the form $P \implies [Q \vee R]$. This is harder to see but it is equivalent to $[P \wedge (\sim Q)] \implies R$ and also to $[P \wedge (\sim R)] \implies Q$. If you can't see this in your head–do a truth table.

Using the first we could instead prove: If $x \neq 2$ and $x \neq 1$ then $2x < x^2$.

Using the 2nd we could instead prove: If $x \neq 2$ and $2x \geq x^2$ then $x = 1$.

Which looks easier? I go for 1.

Proof: equivalently, we will prove that for $x \in \mathbb{N}$, if $x \neq 2$ and $x \neq 1$ then $2x < x^2$.

Since $x \neq 1$ and $x \neq 2$, we have $2 < x$, or $x - 2 > 0$. Since we also have that $x > 0$, we have that $x(x-2) > 0$, which is $x^2 - 2x > 0$. Or, $2x < x^2$. □

0.12. **Proof by contrapositive.** This is a special case of replacing a statement by a logically equivalent statement. Recall that $P \implies Q$ is equivalent to its contrapositive statement $(\sim Q) \implies (\sim P)$. So if we need to prove $P \implies Q$ we could prove $(\sim Q) \implies (\sim P)$ instead.

Often it is easier to see why the contrapositive of a statement is true. Here is an example of **proof by contrapositive.**

Theorem: Let $n \in \mathbb{Z}$. If n^2 is odd, then n is odd. **Proof:** The contrapositive of this statement is that if n is even, then n^2 is even.

If n is even, then there is $k \in \mathbb{Z}$ so that $n = 2k$. Hence, $n^2 = 4k^2 = 2(2k^2)$, which shows that n^2 is an even number. □

0.13. **Distinguish between your proof and your scrap work.** When we want to prove that $P \implies Q$, then we really need to start at P and work our way forward until we arrive at Q. But sometimes, to understand what is going on, we will start at Q and work backwards towards P. This is not really part of our proof and should **NOT** be included when we turn in a proof. Still it can be helpful. Here is an example.

Theorem: Let $a, b \in \mathbb{R}$. If $b > a > 0$, then $b^2 - a^2 > 0$.

Scrap Work: Here Q, i.e., the consequent, is the statement that $b^2 - a^2 > 0$. Note that $b^2 - a^2 = (b-a)(b+a)$. Now I see what is happening, both $(b-a) > 0$ and $(b+a) > 0$ and we know that the product of two strictly positive numbers is strictly positive.

This is not a proof–but does tell me how to get one.

Proof: Since $b > a$ we have that $b - a > 0$. Since $a > 0$ and $b > a$ we have that $b > 0$. Now since $b > 0$ and $a > 0$ we get that $b + a > 0$. Because $(b-a) > 0$ and $(b+a) > 0$ we have that the product, $(b-a)(b+a) > 0$. Finally, $(b-a)(b+a) = b^2 - a^2$. □

0.14. **Proof by Exhaustion.**

This involves dividing truth sets up into cases. To make it more concrete, we will start with an example.

Recall that

$$|x| = \begin{cases} x & \text{when } x \geq 0 \\ -x & \text{when } x < 0 \end{cases}.$$

Theorem: Let $x \in \mathbb{R}$. If $x \neq 0$, then $|x| > 0$.

Discussion: Here $P(x)$ is the statement $x \neq 0$ and $Q(x)$ is the statement that $|x| > 0$. So the truth set for $P(x)$ is

$$\{x : x > 0\} \cup \{x : x < 0\}.$$

These two subsets will define what we mean by "cases". The principle of proof by exhaustion says that if for each $x > 0$ I prove that $Q(x)$ is true AND for each $x < 0$ I prove that $Q(x)$ is true, then $P \implies Q$ is true.

It gets its name from the fact that by considering each case I have "used up" all the x's for which $P(x)$ is true. Another phrase for "used up" is "exhausted".

Proof: We will consider two cases.

Case $x > 0$**:** In this case $|x| = x > 0$.

Case $x < 0$**:** Recall that multiplying by (-1) reverses inequalities. Hence, $x < 0$ implies that $-x > (-1)0 = 0$. Finally, $|x| = -x > 0$.

Since these two cases exhaust all the times that $P(x)$ is true the proof is complete. □

Theorem: If $x \in \mathbb{R}$, then $-|x| \leq x \leq +|x|$.

Proof: We will consider two cases.

Case $x \geq 0$**:** In this case $|x| = x$ and so $x \leq |x|$. Also $-|x| \leq 0$, while $0 \leq x$ so by transitivity, $-|x| \leq x$. Thus, $-|x| \leq x \leq +|x|$.

Case $x < 0$**:** In this case $|x| = -x$ and so $-|x| = x$ and $-|x| \leq x$. Since $x < 0$ and $0 \leq |x|$ by transitivity, $x \leq |x|$. Thus, $-|x| \leq x \leq +|x|$.

Since these cases exhaust all possible x's we are done. □

0.15. **Proof by contradiction.**

These are really an apllication of the law of the excluded middle. Recall that this says that either P is true or $\sim P$ is true. So if $\sim P$ is false, then it must be that P is true.

So one way to prove that P is true is to prove that $\sim P$ is false. To prove that $\sim P$ is false, we will start by *assuming* or, as we will often say *supposing,* that $\sim P$ is true and after some steps arrive at a contradiction. This contradiction says that $\sim P$ true is impossible and so $\sim P$ is false and P is true.

This technique is called **proof by contradiction.** Below are some examples, comments in parentheses.

Theorem: The graphs of $y = 2x + 1$ and $y = 2x + 7$ do not intersect. (This is the statement P.)

Proof: Suppose that the graphs did intersect. (This is $\sim P$ the denial of P.) Then there would be a point (a, b) that is on both graphs. This implies that $b = 2a + 1$ and that $b = 2a + 7$.

This implies that $2a+1 = 2a+7$. Cancelling the $2a$ from both sides yields, $1 = 7$, which is not true, a contradiction. (Since $\sim P$ is false, P is true.)

This contradiction completes the proof. □

Here are some "deeper" things that can be seen by this method.

Before we do this next example, recall that when we write a rational number r as a ratio of two integers,

$$r = \frac{b}{c}$$

then we can assume that b and c have no factors in common. This is because if a divides both b and c then we could write $b = ak$ and $c = aj$ and we would have that

$$r = \frac{b}{c} = \frac{ak}{aj} = \frac{k}{j}.$$

Continuing in this manner one can eliminate all common factors.

We will also use the fundamental theorem of arithmetic from the preface.

This is also an example of a two part proof–we will first prove something useful that we will use later.

Theorem: Let m be an integer and let p be a prime. If p divides m^2, then p divides m.

Proof: We will prove the contrapositive of this statement, namely, that if p does not divide m then p does not divide m^2.

By the fundamental theorem of arithmetic, we can write m uniquely as a product of primes and since p does not divide m it is not one of these primes. But then m^2 is written as the product of the squares of these primes.

This expresses m^2 as a product of primes and none of them are p. The fundamental theorem says that the way to write a number as a product of primes is unique. So since we have one way to write m^2 as a product of primes that does not use p, it must be that p does not divide m^2. □

Theorem: $\sqrt{2}$ is an irrational number.

Proof: Suppose that $\sqrt{2}$ was rational. Then we could write

$$\sqrt{2} = \frac{m}{n}$$

where m and n integers with no common factors.

Squaring both sides of this equation yields,

$$2 = \frac{m^2}{n^2} \text{ and so } 2n^2 = m^2.$$

This implies that 2 divides m^2. By the result that we just did, this means that 2 divides m. So we can write $m = 2k$ for some integer k.

Now we have that $2n^2 = m^2 = (2k)^2 = 4k^2$. Cancelling a 2 from both sides of this equation, yields, $n^2 = 2k^2$.

This implies that 2 divides n^2 and so again, using the above result, 2 divides n.

Thus, m and n both have a common factor of 2. This contradicts that they had no factors in common.

This contradiction shows that the statement "$\sqrt{2}$ is rational" is false, and so $\sqrt{2}$ must be irrational. □

Theorem: There are infinitely many primes.

Proof: Suppose that there were only finitely many primes. List them, $\{p_1, , , , , p_n\}$. Set $m = p_1 \cdot p_2 \cdots p_n + 1$. If we try to divide m by any of these primes then we get a remainder of 1.

Thus, m can not be written as a product of primes. This contradicts the fundamental theorem of arithmetic. Hence, our assumption that there are only finitely many primes must be false. □

0.16. **The Biconditional.**

To prove a statement of the form $P \iff Q$ we will almost alwyas use the fact that this is equivalent to the statement $(P \implies Q) \wedge (Q \implies P)$. This breaks the proof that $P \iff Q$ into two parts. One part where we show $P \implies Q$ and another part where we show $Q \implies P$.

Since $Q \implies P$ is the converse of $P \implies Q$, in the proof we will often first prove $P \implies Q$ and say "now we will prove the converse".

Theorem: Let $a, b \in \mathbb{N}$. The numbers a and b are both odd if and only if ab is odd.

Proof: First assume that both are odd. Then there are integers k and j so that $a = 2k + 1$ and $b = 2j + 1$. Hence,

$$ab = (2k + 1)(2j + 1) = 4kj + 2k + 2j + 1 = 2(2kj + k + j) + 1,$$

which is an odd integer.

To prove that if ab is odd, then both a and b are odd. We will use the contrapositive:

If a and b are not both odd then ab is not odd. (That is ab is even.) We will prove this by exhaustion. This has two cases.

Case a not odd: So $a = 2k$ which implies that $ab = 2(kb)$ which is even.

Case b not odd: So $b = 2j$ and $ab = a(2j) = 2(aj)$ which is even.

Done. □

Theorem: Let $a, b \in \mathbb{N}$. The numbers a and b are both even if and only if $a + b$ is even and ab is even.

Proof: If a and b are both even then there are integers k, j so that $a = 2k$ and $b = 2j$. Hence, $a + b = 2(k + j)$ which is even and $ab = 2(2kj)$ which is even.

To prove that if $a + b$ and ab are both even, then a and b are both even, we will prove the contrapositive statement: If a and b are not both even, then $a + b$ and ab are not both even.

Again we will do a proof by exhaustion. This time we need 3 cases. If a and b are not both even then one or the other is odd.

Case a is odd and b is even: Then $a+b$ is odd, so $a+b$ and ab are not both even.

Case a is odd and b is odd: Then ab is odd, so $a+b$ and ab are not both even.

Case b is odd and a is even: Then $a+b$ is odd, so $a+b$ and ab are not both even.

(Note the 4th case would be b odd and a odd, which is already done.) □

Proofs with Quantifiers

Given an open sentence $P(x)$ where x belongs to some universe U. The statement $\forall x, P(x)$ is true exactly when $P(x)$ is true for every $x \in U$. Said differently, $\forall x, P(x)$ is true exactly when the truth set of $P(x)$ is the entire universe U.

When the universe has not already been established, we will often write statements like $\forall n \in \mathbb{N}, P(n)$ to indicate that for this statement, $\mathbb{N}$ is the universe. Here are some examples.

Theorem: $\forall n \in \mathbb{N}$, $n^2 - 2n + 2 \geq 1$.

Proof: $n^2 - 2n + 2 = n^2 - 2n + 1 + 1 = (n-1)^2 + 1$. Since $(n-1)^2 \geq 0$ for every $n \in \mathbb{N}$, we have that $(n-1)^2 + 1 \geq 0 + 1 = 1$. □

Theorem: For every prime p, $p + 7$ is composite.

Proof: We will do a proof by exhaustion, where we divide the primes into two cases: even primes and odd primes.

Case p is an even prime: In this case $p = 2$ and so $p + 7 = 2 + 7 = 9 = 3 \cdot 3$ which is composite.

Case p is an odd prime: In this case $p + 7$ is the sum of two odd numbers and so $p + 7$ is even, which makes it composite.

□

For a statement of the form $\forall x, P(x)$ to be false, we need that the truth set of $P(x)$ is NOT the whole universe. In other words we just need one x such that $P(x)$ is false.

An x such that $P(x)$ is false is called a **counterexample** to the statemtent $P(x)$.

For example, if our universe is the set $\mathbb{P}$ of all primes, then 2 is a counterexample to the statement

$$\forall x \in \mathbb{P}, x \text{ is odd.}$$

(In fact, it is the only counterexample.)

For each of the statements give a proof when the statement is true or provide a counterexample.

Example: $\forall n \in \mathbb{N}$, $3 + 2n^2$ is prime.

Solution: No idea if this is true or false. So I'll start by looking for a counterexample:

$n = 1$, $3 + 2n^2 = 3 + 2 = 5$, prime, not a counterexample.

$n = 2$, $3 + 2n^2 = 3 + 2(4) = 11$ prime, not a counterexample.
$n = 3$, $3 + 2n^2 = 3 + 2(9) = 21 = 3 \cdot 7$, a counterexample.
Hence, the statement is false.

Example: $\forall n \in \mathbb{N}$, $n^2 + n$ is even.
Solution: Break this into cases.
Case n is even: Then n^2 and n are both even and so $n^2 + n$ is even.
Case n is odd: Then n^2 and n are both odd and so $n^2 + n$ is even(since we have seen that the sum of two odd numbers is even.)

In the first example, if we hadn't searched a little longer for a counterexample, then we might have thought that it was true. This would have been another bad example of using inductive reasoning instead of deductive reasoning.

A very famous example of this dates from 1536. **Mersenne** noticed that for $p = 2, 3, 5, 7$ the number $2^p - 1$ is prime. This lead him to believe that:

$$\forall p \in \mathbb{P},\ 2^p - 1 \text{ is prime.}$$

If he had jut had the patience to check $p = 11$, he would have discovered that this is false! That is $p = 11$ is a counterexample to the above statement. However, now Mersenne is famous and many people have worked on trying to figure out eactly which numbers n have the property that $2^n - 1$ is prime. The primes that are of the form $2^n - 1$ for some $n \in \mathbb{N}$ are now called **Mersenne primes.**

0.17. **Proof by contradiction with a "for all".**

Suppose that we have a statement of the form $\forall x, P(x)$ and we want to use a proof by contradiction to show that it is true. Then we need to show that the negation is false. The denial is: $\sim [\forall x, P(x)]$ which is equivalent to $(\exists x)(\sim P(x))$.

Theorem: $\forall n \in \mathbb{N}$, $3n + 2 \geq 5$.
Proof: We will do a proof by contradiction. Suppose that the negation of this statement is true. Then

$$\exists n \in \mathbb{N}, 3n + 2 < 5.$$

But for such an n we have that $3n < 3$ which implies $n < 1$. This contradicts $n \in \mathbb{N}$. $\square$

0.18. **Proofs with $\exists$.**

In some ways these are very easy. To prove that a statement of the form $\exists x, P(x)$ we just need to show that there is at least one x in the universe so that for that particular x the statement $P(x)$ is true. That is, we only need to give an example x where $P(x)$ is true.

Theorem: $\exists x \in \mathbb{N}$ such that $x^2 + 3$ is prime.

Proof: Let $x = 2$, then $2^2 + 3 = 7$ which is prime. □

Sometimes producing an actual x can be a tricky business and we need to rely on other facts. Here is an example from calculus, where I have no idea at all what the actual value of x is.

Theorem: $\exists x \in \mathbb{R}$, such that $x^4 - 3x + 1 = 0$.
Proof: Let $f(x) = x^4 - 3x + 1$. Then f is a continuous function. We have that $f(0) = 1 > 0$ and $f(1) = -1 < 0$. Since $f(1) \leq 0 \leq f(0)$, by the Intermediate Value Theorem, there is $x, 0 < x < 1$ with $f(x) = 0$. □

The Division Algorithm

We will use this now, but we will actually prove later in this book.
The Division Algorithm: Given integers a and b with $a \neq 0$, then there exists a unique pair of integers, (q, r) such that

$$b = aq + r \text{ and } 0 \leq r < |a|.$$

The integer a is called the **divisor,** the integer q is called the **quotient,** and the integer r is called the **remainder.**
Example: $b = 13, a = 3$ then $13 = 3 \cdot 4 + 1$, so $q = 4, r = 1$.

Definition: Let a, b, c, d be non-zero integers.

- c is called a **common divisor** of a and b if and only if c divides a and c divides b.
- d is called the **greatest common divisor** of a and b which is denoted $d = gcd(a, b)$ if and only if
  (i) d is a common divisor of a and b
  (ii) if c is any common divisor of a and b, then $c \leq d$.

Example: $a = 12, b = 18$ then $2, 3$ are both common divisors and $6 = gcd(12, 18)$. One way to see the last is to notice that any common divisor must be less than or equal to 12 and check that no number e with $6 < e \leq 12$ is a common divisor. A way we learned in elementary school was to write as products of primes, $a = 2 \cdot 2 \cdot 3$, and $b = 2 \cdot 3 \cdot 3$ and then look for primes in common. Both have one 2 and one 3. But(obviously) we didn't prove this!

In this section we want to learn some things about the gcd that do not use things that we learned without proof.

Definition If a and b are integers, then any integer of the form $ax + by$ where x and y are integers is called a **linear combination of a and b.**

Theorem 1.7.1: Let a, b be non-zero integers. If c is a common divisor of a and b, then c is a divisor of every linear combination of a and b.

Proof: Let k and j be integers so that $a = ck$ and $b = cj$. If x and y are integers, then

$$ax + by = (ck)x + (cj)y = c(kx + jy),$$

which shows that c divides $ax + by$. Since this was an arbitrary linear combination, we have that c divides every linear combination. □

A **lemma** is just a name for a "baby" theorem. So lemmas are theorems. When we call a theorem a lemma, then we are trying to tell the reader that this one is not as important as a "grown-up" theorem. Often lemmas are proven to break the proof of a theorem up into smaller bite-size pieces.

However, some of our most important theorems are called "lemma" because at the time, the mathematician that proved it thought that the lemma wasn't important but that the "theorem" that came after was the really important fact. Often history proves them wrong: others find that the lemma was what was important and the theorem, not so much!

Lemma: Let a and b be non-zero integers. The smallest positive linear combination of a and b is a common divisor.

Proof: Let s and t be integers so that $d = as + bt$ is the smallest positive linear combination of a and b. We must prove that d is a common divisor.

Using the division algorithm, we may write $a = qd + r$ with $0 \leq r < d$.

Then $r = a - qd = a - q(as + bt) = a(1 - qs) + b(-qt) < d$. This shows that r is a linear combination smaller than d. So r can not be positive and we have that $r = 0$. Because $r = 0$, $a = qd$ and d divides a.

Similarly, d divides b. $\square$

Here's theorem 1.7.3, in better words.

Theorem 1.7.3: Let a and b be non-zero integers. The gcd of a and b is the smallest positive linear combination of a and b.

Proof: By the lemma we know that if $d = as + bt$ is the smallest positive linear combination, then d is one of the common divisors of a and b.

All that we need to show that $d = gcd(a, b)$ is to show that there cannot be a common divisor larger than d.

So suppose that is a positive integer and that c divides a and b. Then there are integers $a = ck$ and $b = cj$. Then

$$d = as + bt = cks + cjt = c(ks + jt).$$

This shows that c is a positive integer that divides the positive integer d. By 1.4, exercise 7g, $c \leq d$. thus, d is larger than every other common divisor. $\square$

Two non-zero integers a and b are called **relatively prime** or **coprime** if and only if $gcd(a, b) = 1$.

Note that if p is prime and a is any number then since the only non-negative divisors of p are 1 and p then $gcd(p, a)$ can only be 1 or p. When p divides a we get $gcd(a, p) = p$ and when p does not divide a we get $gcd(p, a) = 1$.

Euclid's Lemma: Let a, b, p be non-zero integers with p prime. If p divides ab then either p divides a or p divides b.

Remark: This statement is of the form $P \implies (Q \vee R)$ which we know is equivalent to $P \wedge (\sim Q) \implies R$. This is the form we'll prove.

Proof: Assume that p divides ab and that p does not divide a. Write $ab = pk$ for some integer k.

Since p does not divide a, then as we saw above, $gcd(p, a) = 1$. This means that we can find integers s and t so that $1 = as+pt$. Hence, $b = b(as+pt) = (ba)s + p(bt) = (pk)s + p(bt) = p(ks + bt)$.

This shows that p divides b. □

Here is the contrapositive statement of Euclid's Lemma:

Let a, b, p be non-zero integers with p prime. If p does not divide a and p does not divide b then p does not divide ab.

This statement fails when p is not prime. For example, 4 does not divide 6 and 4 does not divide 10 but 4 does divide $6 \cdot 10 = 60$.

Problem 1.7.2a: $(\forall n)(5n^2 + 3n + 4$ is even)

Proof: We will do cases.

Case n even: Then n=2k for some k and so $5n^2+3n+4 = 20k^2+6k+4 = 2(10k^2 + 3k + 2)$ which is even.

Case n odd: Then $n = 2k + 1$ for some k and so $5n^2 + 3n + 4 = 5(2k+1)^2 + 3(2k+1) + 4 = 20k^2 + 20k + 5 + 6k + 3 + 4 = 2(10k^2 + 13k + 6)$ which is even.

Problem 1.7.13a: $1 = gcd(13, 15)$ this problem asks us to find s and t so that $1 = 13s + 15t$. First, divide 13 into 15, to get 15= 13(1) +2 or 2= 15 -13. Now divide 2 into 13 to get 13= 6(2) + 1. This tells us that

$$1 = 13 - 6(2) = 13 - 6(15 - 13) = 15(-6) + 13(7).$$

Chapter 2: Set Theory

In this chapter we will develop the basics of set theory. We will not try to give a precise definition of what a set is in these notes. Defining sets in a mathematically precise manner is more difficult than it might seem. Read the book for some of the history and especially **Russell's paradox.**

We recall a few of the things discussed in the first lecture.

For our purposes sets will either be indicated as lists $A = \{1, 3, 5, 7, 9, 11\}$ or in **set builder notation**, $\{x : P(x)\}$ which should be read as the set of all x's in some universal set such that $P(x)$ is true. So $A = \{x : x \in \mathbb{N}, x \text{ odd }, x \leq 11\}$.

We use the symbols $\emptyset$ or $\emptyset$ to indicate the set with no elements, called the **empty set** or **null set.**

0.19. **Subset.** We use the notation $A \subseteq B$ to indicate that A is a subset of B. Using our logic notation this can be written as

$$(A \subseteq B) \iff (\forall x)(x \in A \implies x \in B).$$

Equality can be written as:

$$(A = B) \iff (\forall x)(x \in A \iff x \in B)$$

or as

$$(A = B) \iff (A \subseteq B) \wedge (B \subseteq A).$$

Here are a few basic facts.

Theorem 2.1.1.

(a) For every set A, $\emptyset \subseteq A$.
(b) For every set A, $A \subseteq A$.
(c) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Definition: Let A be a set. The **power set of** A denoted $\mathcal{P}(A)$ is the set of all subsets of A.

Example: Let $A = \{1, 2, 3\}$. Then

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

Note that when $x \in A$, then it is $\{x\} \in \mathcal{P}(A)$, NOT $x \in \mathcal{P}(A)$.

Here is a helpful way to check if you have included everything in the list for $\mathcal{P}(A)$:

Theorem 2.1.4. Let A be a set with n elements then $\mathcal{P}(A)$ has 2^n elements.

We will prove this later.

Theorem 2.1.5. Let A and B be sets with $A \subseteq B$. Then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
Proof: Let $X \in \mathcal{P}(A)$. Then $X \subseteq A$, so by 2.1.1c, $X \subseteq B$, which implies that $X \in \mathcal{P}(B)$. □

2.2 Set Operations

Given sets A and B. The **union of** A **and** B denoted $A \cup B$ is the set

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

The **intersection of** A **and** B denoted $A \cap B$ is the set

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

The **difference of** A **and** B(I don't like the books language!) I prefer **the difference of** B **from** A or A **take away** B denoted $A - B$ is the set

$$A - B = \{x : x \in A \text{ and } x \notin B\}.$$

Note that if $A = \{1, 2, 3, 4\}$ and $B = \{3, 4, 5, 6\}$. Then,

$$A \cup B = \{1, 2, 3, 4, 5, 6\} \text{ and } A \cap B = \{3, 4\}.$$

Using the books language, the difference of A and B is the set

$$A - B = \{1, 2\},$$

while the difference of B and A is the set

$$B - A = \{5, 6\}.$$

So the main thing is that "the difference of A and B" is NOT the same as "the difference of B and A". Usually, in the English language, "and" doesn't care which order you write things in! Which is why I don't like the books language.

There is a good reason that we use $\cup$ and $\cap$. If A and B are given in set builder notation as $A = \{x : P(x)\}$ and $B = \{x : Q(x)\}$, then

$$A \cup B = \{x : P(x) \vee Q(x)\} \text{ and } A \cap B = \{x : P(x) \wedge Q(x)\}.$$

Sets A and B are called **disjoint** iff $A \cap B = \emptyset$.

0.20. **Venn Diagrams.** These are pictures that help us to "see" various relationships. They are NOT proofs, but often help us to understand what is going on. I will draw these in class.

Here is a result that lists many basic facts about the relationships between the concepts above. I wil only prove a couple.

Theorem 2.2.1. Let A, B and C be sets.

(a) $A \subseteq (A \cup B)$,
(b) $A \cap B \subseteq A$,
(c) $A \cap \emptyset = \emptyset$,
(d) $A \cup \emptyset = A$,
(e) $A \cap A = A$,
(f) $A \cup A = A$,
(g) $A \cup B = B \cup A$(commutativity)
(h) $A \cap B = B \cap A$(commutativity)
(i) $A - \emptyset = A$
(j) $\emptyset - A = \emptyset$,
(k) $A \cup (B \cup C) = (A \cup B) \cup C$ (associativity)
(l) $A \cap (B \cap C) = (A \cap B) \cap C$ (associativity)
(m) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (distributivity)
(n) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (distributivity)
(o) $(A \subseteq B) \iff (A \cup B = B)$
(p) $(A \subseteq B) \iff (A \cap B = A)$
(q) If $A \subseteq B$ then $(A \cup C) \subseteq (B \cup C)$
(r) If $A \subseteq B$ then $(A \cap C) \subseteq (B \cap C)$.

We will prove (m) and (q) to see, not because they are hard, but to see how to do proofs.

To prove (m) we will use our observation that $X = Y \iff (X \subseteq Y) \wedge (Y \subseteq X)$ and do a proof by exhaustion.

$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ Let $x \in A \cap (B \cup C)$, then $x \in A$ and $x \in (B \cup C)$. Hence, $xinA$ and ($x \in B$ or $x \in C$). **Case** $x \in A$ **and** $x \in B$ Then $x \in (A \cap B)$ and so $x \in (A \cap B) \cup (A \cap C)$.

Case $x \in A$ **and** $x \in C$ Then $x \in (A \cap C)$ and so $x \in (A \cap B) \cup (A \cap C)$.

$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ We will do a proof by exhaustion.

Case $x \in (A \cap B)$ Then $x \in A$ and $x \in (B \cup C)$ so $x \in A \cap (B \cup C)$.
Case $x \in (A \cap C)$ Then $x \in A$ and $x \in (B \cup C)$ so $x \in A \cap (B \cup C)$.
This completes the proof of (m).

To prove (q). We have to show that $(A \cup C) \subseteq (B \cup C)$. Again, cases. If $x \in A$, then since $A \subseteq B$, we have $x \in B$ and hence, $x \in (B \cup C)$. If $x \in C$, then $x \in (B \cup C)$. So, $(A \cup C) \subseteq (B \cup C)$.

Equation (m) can also be related to logic. Suppose that $A = \{x : P(x)\}, B = \{x : Q(x)\}$ and $C = \{x : R(x)\}$. Then $A \cap (B \cup C) = \{x : P(x) \wedge (Q(x) \vee R(x))\}$. From logic we know that $P(x) \wedge (Q(x) \vee R(x))$ is equivalent to $(P(x) \wedge Q(x)) \vee (P(x) \wedge R(x))$. We have, $\{x : (P(x) \wedge Q(x)) \vee (P(x) \wedge R(x))\} = (A \cap B) \cup (A \cap C)$.

Example: Give an example of sets A, B, C such that $(A \cap B) \cup C \neq (A \cap C) \cup (B \cap C)$. We drew a Venn diagram to see why these sets are not equal and then by assigning one number to each region in the Venn diagram, we got actual sets for the example.

Complements of Sets

Given a universe U and a subseteq $A \subseteq U$, the **complement of A** denoted A^c is the set

$$A^c = U - A.$$

Thus, $x \notin A \iff x \in A^c$.

When A is given as the truth set of some statement $P(x)$, so that $A = \{x : P(x)\}$ then $A^c = \{x :\sim P(x)\}$.

If $U = \mathbb{Z}$ and A is the set of even integers then A^c is the set of odd integers.

If $U = \mathbb{R}$ and $A = \{x : x \geq 0\}$, then $A^c = \{x : x < 0\}$.

Theorem 2.2.2. Let U be the universe, A, B subsets of U. Then:

(a) $(A^c)^c = A$,
(b) $A \cup A^c = U$.
(c) $A \cap A^c = \emptyset$
(d) $A - B = A \cap B^c$
(e) $(A \subseteq B) \iff (B^c \subseteq A^c)$ (contrapositive)
(f) $(A \cup B)^c = A^c \cap B^c$ (De Morgan Law)
(g) $(A \cap B)^c = A^c \cup B^c$ (De Morgan Law)
(h) $(A \cap B = \emptyset) \iff (A \subseteq B^c)$

Proof of (d): $x \in (A - B) \iff (x \in A \text{ and } x \notin B) \iff (x \in A \text{ and } x \in B^c) \iff (x \in A \cap B^c)$

Proof of (e): First assume that $A \subseteq B$. Let $x \in B^c$, then $x \notin B$. Since A is a smaller set, $x \notin A$. Hence, $x \in A^c$.

Now assume that $B^c \subseteq A^c$. If $x \in A$ then $x \notin A^c$. Since B^c is a smaller set, $x \notin B^c$. Hence, $x \in B$.

Proof (f): $[x \in (A \cup B)^c] \iff [x \notin (A \cup B)] \iff [x \notin A \text{ and } x \notin B] \iff [x \in A^c \text{ and } x \in B^c] \iff [x \in (A^c \cap B^c)]$

We now show how to derive some of these in the case that A and B are defined by statements.

So suppose that $A = \{x : P(x)\}$ and $B = \{x : Q(x)\}$.

The first thing to see is that (e) becomes:

$$A \subseteq B \iff [P(x) \text{ true} \implies Q(x) \text{ true}] \iff [\sim Q(x) \text{ true} \implies \sim P(x) \text{ true}]$$
$$\iff \{x :\sim Q(x)\} \subseteq \{x :\sim P(x)\} \iff B^c \subseteq A^c.$$

Thus, (e) is just a set theory version of the contrapositive.

Similarly, (f) is:

$$(A \cup B)^c = \{x : P(x) \vee Q(x)\}^c = \{x :\sim (P(x) \vee Q(x))\}$$
$$= \{x : (\sim P(x)) \wedge (\sim Q(x))\} = \{x :\sim P(x)\} \cap \{x :\sim Q(x)\}$$
$$= \{x : P(x)\}^c \cap \{x : Q(x)\}^c = A^c \cap B^c.$$

Cartesian Products

Given sets A and B their **product** or **Cartesian product** is the set

$$A \times B = \{(a, b) : \forall a \in A, \forall b \in B\}.$$

Example: Let $A = \{1, 2\}$ and $B = \{e, f, g\}$ then

$$A \times B = \{(1, e), (1, f), (1, g), (2, e), (2, f), (2, g)\}$$

while

$$B \times A = \{(e, 1), (f, 1), (g, 1), (e, 2), (f, 2), (g, 2)\}.$$

Some key properties:

Theorem 2.2.3. Let A, B, C, D be sets.

(a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$
(b) $A \times (B \cap C) = (A \times B) \cap (A \times C)$
(c) $A \times \emptyset = \emptyset$
(d) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$
(e) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$
(f) $(A \times B) \cap (B \times A) = (A \cap B) \times (A \cap B)$

Proof (a): We have that

$$(a, y) \in A \times (B \cup C) \iff [a \in A] \wedge [y \in (B \cup C)] \iff$$
$$[a \in A] \wedge [(y \in B) \vee (y \in C)] \iff [a \in A \wedge y \in B] \vee [a \in A \wedge y \in C]$$
$$\iff [(a, y) \in A \times B] \vee [(a, y) \in A \times C] \iff (a, y) \in (A \times B) \cup (A \times C).$$

Exercise 2.2.9b: We are given that $A \subseteq (B \cup C)$ and $A \cap B = \emptyset$ and we need to prove that $A \subseteq C$.

Let $x \in A$, then $x \in (B \cup C)$. So $x \in A$ and either $x \in B$ or $x \in C$. Since $x \in A$ and $A \cap B = \emptyset$, we have that $x \notin B$. So since x is in either B or C, it must be in C. Hence, $x \in C$.

Hence, $x \in A$ implies $x \in C$, that is, $A \subseteq C$.

Exercise 2.2.9e: We will do a proof without words!

$$(A - C) - (B - C) = (A \cap C^c) - (B \cap C^c) = (A \cap C^c) \cap (B \cap C^c)^c =$$
$$(A \cap C^c) \cap (B^c \cup (C^c)^c) = (A \cap C^c) \cap (B^c \cup C) =$$
$$(A \cap C^c \cap B^c) \cup (A \cap C^c \cap C) = A \cap C^c \cap B^c = (A \cap B^c) \cap C^c = (A - B) - C.$$

Mathematical Induction

We will cover proofs using the principle of mathematical induction. First we look at what this principle says.

Principle of Mathematical Induction(PMI): Let $S \subseteq \mathbb{N}$ have the following two properties:

(i) $1 \in S$,(Basis for induction)
(ii) whenever $n \in S$ then $(n + 1) \in S$.(Inductive step)
Then $S = \mathbb{N}$.

We look at a first example of how to use this.

Consider the statement

$$P(n): \text{ The sum of the first } n \text{ integers is equal to } \frac{n(n+1)}{2}.$$

So

$$P(1): 1 = \frac{1(1+1)}{2},$$
$$P(2): 1 + 2 = \frac{2(2+1)}{2},$$

etc.

We will write this as:

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

but this last expression is a little sloppy, since for P(1) it is not clear what is meant.

Now let

$$S = \{n \in \mathbb{N} : P(n) \text{ is a true formula}\} = \{n \in \mathbb{N} : 1 + \cdots + n = \frac{n(n+1)}{2}\}.$$

Proving that P(n) is true for every $n \in \mathbb{N}$ is the same as proving that $S = \mathbb{N}$. By the PMI, we can do this by showing two things:

(i) That P(1) is true(Basis for induction)

(ii) that P(n) true implies that P(n+1) is true(inductive step).

Proof: Since $\frac{1(1+1)}{2} = \frac{2}{2} = 1$ we see that P(1) is true.

Now assume that P(n) is true,

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

and we want to show that the next formula, P(n+1) is true,

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

So to show that P(n+1) is true

$$\begin{aligned} 1 + \cdots + n + (n+1) &= [1 + \cdots + n] + (n+1) = \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} = \frac{(n+1)n + (n+1)2}{2} = \frac{(n+1)(n+2)}{2}. \end{aligned}$$

Comments: Many students are bothered and/or confused by the fact that we want to prove P(n) is true and in the middle of the proof, we are assuming P(n) is true! Sometimes to make clearer what is going on, I will use different letters, like P(k) instead of P(n). The real point is that we want to prove that $(\forall n)(P(n)$ is true) In the middle of the proof when we assume that P(n) is true, we mean that it is true for a particular integer n. Then we go on to show that when it is true for a particular n, then it is true for the next value integer, (n+1).

This proof that we just did is often the way that we will use PMI:

Suppose we are given statements, P(n) for each natural number n and we would like to prove that they are all true. The PMI says that:

(i) if P(1) is true(Basis for induction)

(ii) if P(n) true implies P(n+1) is true(Inductive step)

then P(n) is true for every natural number n.

Here are some examples.

Prove that $(\forall n \in \mathbb{N})(n + 4 < 7n^2)$.

Proof: Let P(n) be the statement that $n + 4 < 7n^2$. Since $1 + 4 = 5$ and $7(1)^2 = 7$ and $5 < 7$, we have that P(1) is true.

Now assume that $n + 4 < 7n^2$ and we must prove that $(n + 1) + 4 < 7(n + 1)^2$. We have

$$(n + 1) + 4 = n + 4 + 1 < 7n^2 + 1 < 7n^2 + 14n + 7 = 7(n + 1)^2.$$

□

Prove that $1 + 3 + \cdots + (2n - 1) = n^2$.

Again this is a little sloppy, what we are really being asked is to prove that the sum of the first n odd integers is n^2. So that is our statement P(n).

Proof: The sum of the fisrt odd integer is 1 and $1 = 1^2$. So P(1) is true.

Now assume P(n) that $1 + \cdots + (2n - 1) = n^2$ and we must prove P(n+1) that $1 + \cdots + (2(n + 1) - 1) = (n + 1)^2$.

So P(n+1) has added on one more odd integer. Thus,

$$[1+\cdots+(2n-1)]+(2(n+1)-1) = n^2+(2n+2-1) = n^2+2n+1 = (n+1)^2.$$

Prove that $(x - y)$ **divides** $(x^n - y^n)$ **for all** $n \in \mathbb{N}$.

When n=1 this is true, so we have the basis for induction. Now assume that $(x-y)$ divides $x^n - y^n$, we must show that $(x-y)$ divides $x^{n+1} - y^{n+1}$. We'll use a trick I call getting "something for nothing". In this case we'll add and subtract $x^n y$, which adds nothing.

Write

$$x^{n+1} - y^{n+1} = x^{n+1} - x^n y + x^n y - y^{n+1} = x^n(x - y) + y(x^n - y^n)$$

since (x-y) divides both terms it divides the sum.

Problem 6g: Prove that $\frac{1}{1\cdot 2} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$.

When $n = 1$ we have that $\frac{1}{1\cdot 2} = \frac{1}{2} = \frac{1}{1(1+1)}$, so the bbasis for induction is true.

Now assume that the n-th statement is true, namely

$$\frac{1}{1 \cdot 2} + \cdots + \frac{1}{n(n + 1)} = \frac{n}{n + 1},$$

and we show that the (n+1)-st statement is true, namely, that

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

We have

$$[\frac{1}{1 \cdot 2} + \cdots + \frac{1}{n(n + 1)}] + \frac{1}{(n + 1)(n + 1 + 1)} = \frac{n}{n + 1} + \frac{1}{(n + 1)(n + 2)}$$

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

Problem 6h: Prove that $\frac{1}{2!}+\frac{2}{3!}+\cdots+\frac{n}{(n+1)!}=1-\frac{1}{(n+1)!}$

When $n=1$ we have that $\frac{1}{2!}=\frac{1}{2}=1-\frac{1}{(1+1)!}$. So the basis for induction is true. Now assume that $\frac{1}{2!}+\frac{2}{3!}+\cdots+\frac{n}{(n+1)!}=1-\frac{1}{(n+1)!}$. Then

$$[\frac{1}{2!}+\frac{2}{3!}+\cdots+\frac{n}{(n+1)!}]+\frac{(n+1)}{(n+2)!}=1-\frac{1}{(n+1)!}+\frac{(n+1)}{(n+2)!}=$$
$$1-\frac{(n+2)}{(n+2)!}+\frac{(n+1)}{(n+2)!}=1-[\frac{(n+2)-(n+1)}{(n+2)!}=1-\frac{1}{(n+2)!}$$

The next result uses complex numbers and the multiple angle formulas:

$$cos(A+B)=cos(A)cos(B)-sin(A)sin(B)$$
$$sin(A+B)=sin(A)cos(B)+cos(A)sin(B)$$

Theorem 2.4.1. DeMoivre's Formula. Let $\theta\in\mathbb{R}$. For all $n\in\mathbb{N}$, $(cos(\theta)+isin(\theta))^n=cos(n\theta)+isin(n\theta)$. **Proof:** We will use induction. The equation is clearly true for $n=1$. Now assume that it is true for n and we must prove that $(cos(\theta)+isin(\theta))^{n+1}=cos((n+1)\theta)+isin((n+1)\theta)$. We have

$$(cos(\theta)+isin(\theta))^{n+1}=(cos(\theta)+isin(\theta))(cos(\theta)+isin(\theta))^n=$$
$$(cos(\theta)+isin(\theta))(cos(n\theta)+isin(n\theta))=$$
$$cos(\theta)cos(n\theta)+icos(\theta)sin(ntheta)+isin(\theta)cos(n\theta)+(i)^2sin(\theta)sin(n\theta)=$$
$$[cos(\theta)cos(n\theta)-sin(\theta)sin(n\theta)]+i[sin(n\theta)cos(\theta)+cos(n\theta)sin(\theta)]$$
$$=cos((n+1)\theta)+isin((n+1)\theta)$$

Not every formula holds starting at $n=1$. Sometimes we want to prove that a formula holds for every $n\geq k$. We use the following:

Generalized Principle of Mathematical Induction(GPMI): Let $S\subseteq\mathbb{N}$. If

(i) $k\in S$(Basis)

and

(ii) for $n\geq k$ whenever $n\in S$ we have $(n+1)\in S$(Inductive Step)

Then $S=\{n\in\mathbb{N}:n\geq k\}$.

Example: Prove that $n^3<n!$ for all $n\geq 6$. [Note $5^3=125$ while $5!=120$ so $5^3<5!$ is false.]

We have that $6^3=216$ while $6!=720$ so the basis for induction holds. Now assume that $n^3<n!$ and we must prove that $(n+1)^3<(n+1)!$. We have that

$$(n+1)^3=(n+1)(n+1)^2=(n+1)(n^2+2n+1)$$
$$<(n+1)(n^2+n^2+n^2)=(n+1)[3n^2]<(n+1)[n^3]<(n+1)[n!]=(n+1)!$$

Example: Prove that $n^2 + 6 > 5n$ for all $n \geq 4$.

We have $4^2 + 6 = 22 > 5 \cdot 4$, so the basis for induction holds. Now assume that $n^2 + 6 > 5n$.

Then we have that

$$(n+1)^2+6 = n^2+2n+1+6 > n^2+2n+7 = n(n+2) \geq n(6)+7 > 5n+5 = 5(n+1).$$

Other Forms of Induction

Sometimes when we do a proof by induction we need to use more than just that P(n) is true. Sometimes we need to use that P(k) is true for all $1 \leq k \leq n$. This is called the *Principle of Complete Induction.* I will state it differently than the book. I think that this version is less confusing.

Theorem (Principle of Complete Induction(PCI))**.** *Let $S \subseteq \mathbb{N}$. If*

- $1 \in S$*(Basis)*
- $\{1, ..., n\} \subseteq S$ *implies that* $(n+1) \in S$*(inductive step),*

then $S = \mathbb{N}$.

Example. Every natural number greater than 1 has a prime divisor.

For this example if we try to use PMI, then it turns out that knowing that say 20 has a prime divisor does not help in deciding if 21 does. But we will see that knowing that every number before 20 has a prime divisor does!

Proof. Let $S = \{k : k = 1$ or k has a prime divisor $\}$.(remember that 1 is not prime so it doesn't have a prime divisor.) We have that $1 \in S$. Assume that $\{1, ..., n\} \subseteq S$. This means that every number, $2, ..., n$ has a prime divisor. Now we need to see if $n + 1 \in S$, which is the same as proving that $n + 1$ has a prime divisor. There are 2 cases.

Case n+1 is prime. Since a number divides itself, $n + 1$ has a prime divisor, itself.

Case n+1 is not prime. Since n+1 is not prime, there are numbers k, j so that $n + 1 = kj$ with $k \neq 1$ and $j \neq 1$. This implies that $2 \leq k \leq n$. So $k \in S$ and $k \neq 1$, which means that k has a prime divisor. Let p be a prime that divides k, so $k = pb$ and $n + 1 = p(bj)$ so p divides $n + 1$. Therefore, $n + 1 \in S$. □

Theorem (2.5.3 The Fundamental Theorem of Arithmetic)**.** *Every natural number $n > 1$ can be written uniquely as a product of primes.*

We will do part of the proof. We will skip the "uniquely" part.

Proof. Let $S = \{k : k = 1$ or k can be written uniquely as a product of primes $\}$. Again $1 \in S$. Let $\{1, ..., n\} \subseteq S$. We must prove that $(n+1) \in S$. Two cases.

Case n+1 is prime: Then it is written as a product of primes.

Case n+1 is not prime: Then $n + 1 = kj$ with $k \neq 1$ and $j \neq 1$. This implies that $2 \leq k \leq n$ and $2 \leq j \leq n$. Hence, both k and j can be written uniquely as a product of primes. Combining these products, writes $n + 1$ as a product of primes. □

0.21. **The Well Ordering Principle.** This case is also called the **Least Element Property.** It states that given any non-empty set $S \subseteq \mathbb{N}$, then there is $k \in S$ such that $k \leq j$ for every $j \in S$. Thus, k is the "first" element in S, which is where the phrase "well-ordering" comes from. But also k is the "least" element in S.

Proof. We do cases.

Case $1 \in S$ Then clearly, $k = 1$.

Case $1 \notin S$ Let $J = \{j \in \mathbb{N} : j \notin S\}$, i.e., $J = S^c$. Since $1 \in J$, $J \neq \emptyset$. Since S is not empty, $J \neq \mathbb{N}$. Hence, the PCI must fail to be true. So there is a set $\{1, ..., n\} \subseteq J$ for which $(n+1) \notin J$. Hence, we see that $1 \notin S, ..., n \notin S$ but $(n+1) \in S$. Set $k = n + 1$. Thus, if $j \in S$, then $j \geq k$. □

Theorem (The Division Algorithm 2.5.1)**.** *For all $a, b \in \mathbb{Z}$ with $a \neq 0$ there exists a unique pair of integers (q, r) such that $b = aq + r$ and $0 \leq r < |a|$.*

Proof. We will do the case that $b > 0$ and $a > 0$. Other cases are similar. Let $T = \{m \in \mathbb{N} : am > b\}$ Now since $a \geq 1$, we have $(b+1)a \geq (b+1)1 = b + 1 > b$. Thus, $(b + 1) \in T$ and so $T \neq \emptyset$. By the well-ordering principle, there is $k \in T$ such that $ak > b$ but $k - 1 \notin T$ which implies $a(k - 1) \leq b$.

Let $q = k-1$ and set $r = b-aq$. Then $aq \leq b < a(q+1) \implies 0 \leq b-aq < a$ so $0 \leq r < a$. Done □

0.22. **Inductive Definition.** The inductive principle can also be used to define sequences of numbers.

For example, if we set $a_1 = 1$ and $a_{n+1} = (n + 1)a_n$, Then we get that $a_2 = 2a_1 = 2 \cdot 1, a_3 = 3a_2 = 3 \cdot 2 \cdot 1$, this is the definition of $n!$.

Another famous sequence of numbers defined inductively are the Fibonacci numbers. These are defined by setting $f_1 = f_2 = 1$ and for $n \geq 1, f_{n+2} = f_{n+1} + f_n$. Thus, $f_3 = f_2 + f_1 = 1 + 1 = 2, f_4 = f_3 + f_2 = 2 + 1 = 3, f_5 = f_4 + f_3 = 3 + 2 = 5, f_6 = f_5 + f_4 = 5 + 3 = 8$.

Principles of Counting

In this section we will look at some famous formulas for counting the numbers of elements of sets. Given a finite set A we will let $|A|$ = the number of elements in A. (The book uses $\overline{\overline{A}}$–too hard to make!) Some special cases, $|\{a\}| = 1, |\{a, b\}| = 2, |\emptyset| = 0$.

Theorem (Sum Rule)**.** *Let A and B be finite sets. If $A \cap B = \emptyset$, then $|A \cup B| = |A| + |B|$.*

This extends:

Theorem. *Let $\mathcal{A} = \{A_1, ..., A_n\}$ be a finite collection of finite sets. If $A_i \cap A_j = \emptyset$ for all $i \neq j$(i.e., if they are pairwise disjoint), then*

$$|\bigcup_{i=1}^{n} A_i| = |A_1| + \cdots + |A_n|.$$

Proof. The proof is by induction on the number of sets. We have that it is true for $n = 1$ and $n = 2$, using the last theorem.

Now assume that it is true for a collection of n sets and assume that we are given a collection of $n + 1$ sets, $A_1, ..., A_n, A_{n+1}$. Set $B = \cup_{i=1}^{n} A_i$. Then $B \cap A_{n+1} = \emptyset$ and so

$$|\bigcup_{i=1}^{n+1} A_i| = |B \cup A_{n+1}| = |B| + |A_{n+1}| = |A_1| + \cdots + |A_n| + |A_{n+1}|.$$

□

Next we consider the case when the sets have non-empty intersection.

Theorem (2.6.3)**.** *Let A and B be finite sets. Then*

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

Proof. Write $A = (A - B) \cup (A \cap B)$ these sets are disjoint. Hence, $|A| = |A - B| + |A \cap B|$. Similarly, $B = (B - A) \cup (A \cap B)$ expresses B as a disjoint union, so $|B| = |B - A| + |A \cap B|$.

Finally, $A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$ is a disjoint union. Hence,

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

□

Principle of Inclusion and Exclusion. Once you have the case of two sets, one can do more sets using the case of 2 and the distributivity rules for union and intersection. For example,

$$\begin{aligned} |A \cup B \cup C| = |(A \cup B) \cup C| = |A \cup B| + |C| - |(A \cup B) \cap C| = \\ |A| + |B| - |A \cap B| + |C| - \big(|(A \cap C) \cup (B \cap C)|\big) = \\ |A| + |B| + |C| - |A \cap B| - \big(|A \cap C| + |B \cap C| - |(A \cap C) \cap (B \cap C)|\big) = \\ |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \end{aligned}$$

Notice that we obtain that $|A \cup B \cup C|$ is the sum of all single sets, minus the sum of intersections of all pairs, plus the intersection of all three.

This generalizes to $|A_1 \cup \cdots \cup A_n|$: It is the sum of $|A_i|$, minus the sum of the intersection of all pairs, plus the intersection of all triples, etc. In Exercise 5, you will work out this formula for a union of 4 sets.

Product Rules.

Theorem (Product Rule)**.** *Let A and B be finite sets then $|A \times B| = |A| \cdot |B|$.*

Proof. Say $|A| = n$ and write $A = \{a_1, ..., a_n\}$ and let $|B| = m$ and write $B = \{b_1, ..., b_m\}$. For each $1 \leq i \leq n$, let

$$C_i = \{(a_i, b) : b \in B\} = \{(a_i, b_1), ..., (a_i, b_m)\},$$

so that $|C_i| = m$. Note $C_i \subseteq A \times B$, for $i \neq j$ C_i and C_j are disjoint and $\bigcup_{i=1}^{n} C_i = A \times B$.

Hence,

$$|A \times B| = |C_1| + \cdots + |C_n| = m + \cdots + m = mn.$$

□

This extends to the product of more sets:

Theorem (2.6.5. Generalized Product Rule)**.** *Let $A_1, ..., A_n$ be finite sets. Then*

$$|A_1 \times \cdots \times A_n| = |A_1| \cdots |A_n|.$$

Proof. This is proved by induction. We have already done the case of $n = 1$ and $n = 2$. Now assume that $|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|$ and suppose that we have a collection of $(n + 1)$ sets.

Notice that $A_1 \times \cdots \times A_n \times A_{n+1} = (A_1 \times \cdots \times A_n) \times A_{n+1}$. Hence, by the case for 2,

$$|A_1 \times \cdots \times A_n \times A_{n+1}| = |A_1 \times \cdots \times A_n| \cdot |A_{n+1}| = (|A_1| \cdots |A_n|) \cdot |A_{n+1}|.$$

□

Example. We can order pizzas that come in small S, medium M, or large L; and either Thin crust(T) or Chicago style thick crust(C); and with 5 different toppings, cheese, olive, pepperoni, ham and green peppers. How many one toppings can we order?

Think of ordering a pizza as filling in a form with 3 blanks. In the first blank you put the size, in the second the crust thickness and in the 3rd blank the topping. This identifies 1 topping pizzas with an ordered triple. These ordered triples are elements of the product of three sets, where the sets are $Size = \{S, M, L\}$, $Thickness = \{T, C\}$ and $Topping = \{Ch, O, P, H, G\}$. So the number of pizzas is

$$|Size| \cdot |Thickness| \cdot |Topping| = 3 \cdot 2 \cdot 5 = 30.$$

Note the general principle here: choices multiply!

Permutations. Given a set of say three letters, $A = \{a, b, c\}$, the set of all **permutations** is the set of all ordered triples that you could make using each letter once. So the permutations are

$$abc, acb, bac, bca, cab, cba$$

so 6 permutations. Sometimes I'll call these "words" in the three letters.

So in general given a set A with n elements the set of all permutations of A is the set of all possible ordered n-tuples that can be filled in using each element exactly once.

Theorem (2.6.6)**.** *Given a set A with n elements, the set of all permutations of A has $n!$ elements.*

Proof. We give the idea of the proof, then do a formal inductive proof.

To write down all of the permutations in A we think of filling in n blanks. In the 1st blank, we can use any element of A so we have n choices. Since we cannot use the same element twice, for the 2nd blank we only have $(n-1)$ choices. For the third lank, there are 2 elements that we cannot use, so we have only $(n-2)$ choices. This continues until we get to the last blank and there is only one element left, so only 1 choice.

Thus, the number of choices is

$$n \cdot (n-1) \cdots 2 \cdot 1 = n!$$

To prove formally, let B_n be the number of permutations of an n element set. We have that $B_1 = 1$. Now assume that $B_n = n!$ and suppose that we have a set of $(n+1)$ elements.

Now to form a permutation of this $(n+1)$-element set, we first pick an element for the first blank, for which we have $(n+1)$ choices. We are now left with a set of n elements to fill in the remaining blanks. By the inductive assumption, we have B_n ways to fill in these remaining blanks. Thus,

$$B_{n+1} = (n+1)B_n = (n+1)[n!] = (n+1)!$$

□

Example. I have 10 CD's in my player, my shuffle play plays them in any order. How many different "listening experiences" can I have? Answer: $10! = 3,628,800$.

Example. We have 26 letters. How many 6 letter passwords can we make if

(1) We allow letters to repeat?
(2) We can only use each letter once?

Answers: (1) $(26)^6$
(2) $26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 \cdot 21 = \frac{(26)!}{(20)!}$.
The answer in (2) is a special case of the following:

Theorem (2.6.7. Permutation Rule)**.** *Let A be a set with n elements and let $0 \leq r \leq n$. Then the number of permutations of any set of r of these n elements is*

$$n \cdot (n-1) \cdots (n-r+1) = \frac{n!}{(n-r)!}.$$

Definition. Let $0 \leq r \leq n$ given a set A of n elements the number of subsets of A with exactly r elements is denoted by

$$\binom{n}{r}$$

which is called the **binomial coefficient** or **n choose r.**

Some of these are easy to see:

There is exactly one subset with 0 elements(the null set) so $\binom{n}{0} = 1$.

There are n one element subsets so $\binom{n}{1} = n$.

The only n element subset is the set itself, so $\binom{n}{n} = 1$.

The following gives the answer in general.

Theorem (2.6.8. The Combination Rule)**.** *Given a set with n elements, the number of r element subsets is*

$$\binom{n}{r} = \frac{n \cdot (n-1) \cdots (n-r+1)}{r(r-1) \cdots 1} = \frac{n!}{(n-r)!r!}$$

Note that when $r = 0$ we know that $1 = \binom{n}{0}$ while the formula gives us, $\binom{n}{0} = \frac{n!}{(n-0)!0!}$, so to make these formulas apply to the case $r = 0$(and $r = n$) we define

$$0! = 1.$$

Example. Before we do the proof first an example. Let $n = 5$ and $r = 2$. So we want all 2 element subsets of a set of 5 elements, say $\{a, b, c, d, e\}$. First we count the permutations this gives $5 \cdot 4$. But each permutation would have say (a, b) and (b, a) which would count twice but that is really just one set, $\{a, b\}$. So each permutation counts the sets twice, Wo the number of sets is

$$\frac{5 \cdot 4}{2} = 10.$$

Proof. First the number of permutations of any r by the Permutation Rule is $\frac{n!}{(n-r)!}$. Each permutation gives a set of r elements, but each set appears the same number of times as there are permutations of a set of r elements. Since there are $r!$ permutations of each set. The number of subsets is the number given by the Permutation Rule divided by $r!$, which is

$$\frac{n!}{(n-r)!}/r! = \frac{n!}{(n-r)! \cdot r!}.$$

□

Example. Pizza's Again. Use the same set-up as before. Now the question is how many different 2 topping pizzas, provided that you have to order two different toppings?

Solution: Since there are 5 toppings and we want to choose 2, the number of different toppings that we can choose is

$$\binom{5}{2} = \frac{5!}{(5-2)!2!} = \frac{5 \cdot 4}{2} = 10$$

So we have 3 choices for size, 2 choices for crust, and 10 choices for topping, so altogether

$$3 \cdot 2 \cdot 10 = 60$$

different pizzas.

Example. Pizza's a third time. Same set-up but allow double toppings, so ordering Cheese twice means you get twice as much cheese. How many different pizzas?

Solution: If you order two different toppings, then we already saw that it is 10 choices. In addition to these 10 we can order each topping doubled. There are 5 toppings so we can order each one doubled for 5 more choices. Hence we have $10 + 5 = 15$ choices for toppings. So altogether

$$3 \cdot 2 \cdot 15 = 90$$

different pizzas.

Example. From a deck of 52 cards, how many 5 card hands?

$$\frac{52!}{(52-5)!5!} = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 5,197,920.$$

How many with 4 Aces? Answer need all 4 A's plus one other card, there are 52- 4 = 48 cards left. So 48.

Probability of getting 4 A's:

$$\frac{48}{5,197,920}$$

Example. Megacorp has 50 workers and 200 Vice Presidents.

a) It wants to pick 5 workers to give bonuses of \$1, \$2, \$3, \$4, \$5 each. How many ways?

b) It wants to pick 5 VP's to give a bonus of \$1,000,000 each. How many ways?

Answer a): The Permutation Rule, because you can tell the workers apart (since the bonuses are different): $50 \cdot 49 \cdot 48 \cdot 47 \cdot 46$.

Answer b): The Combination Rule, you cannot tell the VP's apart(because the bonuses are all the same):

$$\binom{200}{5} = \frac{200 \cdot 199 \cdot 198 \cdot 197 \cdot 196}{5!}$$

Theorem (2.6.9)**.** *Let* $0 \leq r \leq n$. *Let* $a, b \in \mathbb{R}$.

a) $(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{(n-r)}$.

b) $\binom{n}{r} = \binom{n}{n-r}$

c) $\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}, \ \forall 1 \leq r \leq n.$

Proof. **a):** First consider what happens when you want to do the product of $(a+b)(c+d)(e+f)$. The product has 8 terms

$$ace + acf + ade + adf + bce + bcf + bde + bdf$$

and each term is a product of three things.

One way to see how we got these was that for each of the eight terms we first chose one element of $\{a, b\}$ followed by one element of $\{c, d\}$ and finally one element of $\{e, f\}$. There are two choices from each set for a total of $2 \cdot 2 \cdot 2 = 8$ terms.

So when we want to multiply $(a+b)(a+b)(a+b)$ again it is a sum of 8 terms where for each term we choose one element from the set $\{a, b\}$ followed by one element of the set $\{a, b\}$, followed by one element of the set $\{a, b\}$. But now if we choose a then a then b we get aab. If we choose a then b then a we get aba.

But since $aab = aba = a^2b$, all that matters was that we chose 2 a's and 1 b. Also, one we choose 2 a's we are forced to choose 1 b. So all that really mattered is that we chose 2 a's. So we get a^2b for each of the terms,

$$aab, aba, baa.$$

We got aab, when we chose a from the 1st and 2nd sets, we got aba when we chose a from the 1st and 3rd set and we got baa when we chose a from the 2nd and 3rd set.

So the number of times that we can get a^2b is the number of times that we can choose 2 a's from our 3 sets.

Now to do the general case. Suppose that we want to find

$$(a+b)^n = (a+b)(a+b)\cdots(a+b).$$

To get a term with a in it r times, we must choose an a from the set $\{a, b\}$ exactly r times. But the set $\{a, b\}$ appears n times.

So we get a exactly r times, $\binom{n}{r}$ times. If we pick a exactly r times, then we must pick b the remaining $(n-r)$ times. So our term will have r a's and $(n-r)$ b's and so be equal to $a^r b^{(n-r)}$.

Thus, we see that in the product, the quantity $a^r b^{(n-r)}$ appears exactly $\binom{n}{r}$ times.

Since the product is equal to the sum of all these possible terms, we get that

$$\begin{aligned}(a+b)^n = b^n + \binom{n}{1} a^1 b^{(n-1)} + \binom{n}{2} a^2 b^{(n-2)} + \cdots + \binom{n}{n-1} a^{(n-1)} b^1 + a^n \\ = \sum_{r=0}^{n} \binom{n}{r} a^r b^{(n-r)}.\end{aligned}$$

b): There are two ways to see this. First by the formula:

$$\binom{n}{n-r} = \frac{n!}{[n-(n-r)]!(n-r)!} = \frac{n!}{r!(n-r)!} = \binom{n}{r}.$$

The second is that $\binom{n}{r}$ counts the number of ways that we can pick r elements from an n element set. But each time we form a set of r elements there is a set of $(n-r)$ elements left over. So the number of ways to pick r elements is the same as the number of ways to pick $(n-r)$ elements, which is what $\binom{n}{n-r}$ represents.

c): Use the formulas:

$$\binom{n-1}{r} + \binom{n-1}{r-1} = \frac{(n-1)!}{[(n-1)-r]!r!} + \frac{(n-1)!}{[(n-1)-(r-1)]!(r-1)!} =$$
$$\frac{(n-1)!}{(n-1-r)!r!} + \frac{(n-1)!}{(n-r)!(r-1)!} = \frac{n-r}{n-r}\frac{(n-1)!}{(n-r-1)!r!} + \frac{r}{r}\frac{(n-1)!}{(n-r)!(r-1)!}$$
$$= \frac{(n-1)![n-r]}{(n-r)!r!} + \frac{(n-1)![r]}{(n-r)!r!} = \frac{(n-1)![n-r+r]}{(n-r)!r!} = \binom{n}{r}$$

□

A special case is when $a = b = 1$.

Theorem. $2^n = \sum_{r=0}^{n} \binom{n}{r}$

Proof. Set $a = b = 1$ in 2.6.9a, then

$$2^n = (1+1)^n = \sum_{r=0}^{n} \binom{n}{r} 1^r 1^{(n-r)} = \sum_{r=0}^{n} \binom{n}{r}.$$

□

We now have enough math to prove a result that the book stated much earlier.

Theorem (2.1.4)**.** *Let A be a set with n elements, then the power set of A, $\mathcal{P}(A)$ has 2^n elements. That is, the total number of subsets of A is 2^n.*

Proof. The number of subsets of A with r elements is $\binom{n}{r}$. Hence the total number of subsets of A is the sum of the number of subsets with 0 elements, 1 elements,....., n elements, which is

$$\sum_{r=0}^{n} \binom{n}{r} = 2^n.$$

□

Chapter 3: Relations and Partitions

Definition. Given sets A and B a **relation R from A to B** is just a subset $R \subseteq A \times B$. We say that an element a is **R-related** to b and write **aRb** iff $(a, b) \in R$. When $A = B$ we call R a **relation on A.**

Example. Let $A = \{1, 2, 3\}$ and $B = \{4, 5, 6\}$ and set $R = \{(1, 4), (2, 5), (3, 6)\}$. Then 1R4, 2R5, 3R6. A simpler way to write the relation R is that

$$R = \{(a, b) : b - a = 3\}.$$

Example. Let $A = \mathbb{N}$ and define a relation on $\mathbb{N}$ by setting

$$R = \{(a, b) : a - b \text{ is even } \}.$$

Then aRb iff either a and b are both even or a and b are both odd.

Example. $A = \mathbb{R}$ and define a relation on $\mathbb{R}$ by

$$R = \{(x, y) : y - x > 0\}.$$

Then xRy iff the point (x,y) is "above" the line x=y.

Definition. Given a relation R from A to B. The **domain of R** is the set

$$Dom(R) = \{a \in A : \exists b \in B, aRb\}.$$

The **range of R** is the set

$$Ran(R) = \{b \in B : \exists a \in A, aRb\}.$$

Example. Let $A = \{0, 1, 2, 3\}$ and $B = \{4, 5, 6, 7\}$ and let $R = \{(a, b) : b-a = 3\}$. Then $Dom(R) = \{1, 2, 3\}$ since no b is related to 0, and $Ran(R) = \{4, 5, 6\}$ since no a is related to 7.

Example. Let $A = \mathbb{R}$ and define a relation R on $\mathbb{R}$ by setting

$$R = \{(x, y) : x^2 + y^2 \leq 1\}.$$

Then $Dom(R) = Ran(R) = [-1, +1]$.

Definition. Given a relation R from A to B, for each $a \in A$ the set

$$R_a = \{b \in B : (a, b) \in R\}$$

is called the **vertical section through a.** The set

$${}_bR = \{a \in A : (a, b) \in R\}$$

is called the **horizontal section through b.**

In class we drew some pictures of these.

Relations and Directed Graphs

Directed graphs also called **digraphs** are pictures that can help us to "see" relations, much as Venn diagrams were a visual aid. Given a relation from A to B we draw dots for each of the elements of A and dots for each of the elements of B and then draw an arrow from the dot for a to the dot for b iff aRb.

When A=B, we just draw points for the set A once and connect points with arrows iff they are related. When we have a point $a \in A$ such that aRa, then we draw a loop at that point.

In class we drew pictures of some digraphs.

Operations on Relations

Definition. Given a set A the **identity relation on A** denoted I_A is

$$I_A = \{(a, a) : a \in A\}.$$

Definition. Given a relation R from A to B, the **inverse of R** is the relation from B to A,

$$R^{-1} = \{(b, a) \in B \times A : (a, b) \in R\}.$$

Note that when we draw a digraph for R then the digraph for R^{-1} is obtained by reversing all of the arrows.

When the relation R is given by a formula, then the relation R^{-1} is given by the inverting the formula.

Example. When $A = \mathbb{R}$ and $R = \{(x, y) : x < y\}$ then $R^{-1} = \{(y, x) : x < y\} = \{(y, x) : y > x\}$. But when we draw things we like to regard the first component as the x variable and the second variable as the y variable. So, making this substtution,

$$R^{-1} = \{(x, y) : x > y\}$$

is the region "below" the line y=x.

Example (3.1.4g)**.** Let $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y > 3x - 4\}$, the region above the line $y = 3x - 4$.. Then $R^{-1} = \{(x, y) : x > 3y - 4\}$. Solving for y we get $\frac{x+4}{3} > y$, so that R^{-1} is the region below the line $y = \frac{x+4}{3}$.

Theorem (3.1.2)**.** *Let $R \subseteq A \times B$ be a relation. Then*
a) $Dom(R^{-1}) = Ran(R)$,
b) $Ran(R^{-1}) = Dom(R)$.

Definition. Given relations $R \subseteq A \times B$ and $S \subseteq B \times C$, the **composite of R and S** is the relation from A to C given by

$$S \circ R = \{(a, c) : \exists b, (a, b) \in R, (b, c) \in S\}.$$

If we think of R as a digraph from A to B and S as a digraph from B to C, then $S \circ R$ is the set of arrows from A to C that you get by going through a point in B. We drew pictures in class.

Example. $A = \{1, 2, 3\}$, $B = \{e, f, g\}$, $C = \{x, y, z, w\}$ and let $R = \{(1, e), (1, f), (2, f), (3, g)\}$, and $S = \{(e, x), (e, y), (f, z), (g, w)\}$ Then

$$S \circ R = \{(1, x), (1, y), (1, z), (2, z), (3w)\}.$$

Example (3.1.6d)**.** $A = B = C = \mathbb{R}$ and $R_3 = \{(x, y) : y = 7x - 10\}$, $R_2 = \{(x, y) : y = -5x + 2\}$. Find $R_2 \circ R_3$ and $R_3 \circ R_2$.

First we do $R_2 \circ R_3$. To make it look more like the definition, we set $R_3 = \{(a, b) : b = 7a - 10\}$, and $R_2 = \{(b, c) : c = -5b + 2\}$. Then to have $(a, b) in R_3$ and $(b, c) \in R_2$ means that $c = -5b + 2 = -5(7a - 10) + 2 = -35a + 52$ function composition! Re-labelling,

$$R_2 \circ R_3 = \{(x, y) : y = -35x + 52\}.$$

So for $R_3 \circ R_2$ we will get the composition, $y = 7(-5x+2)-10 = -35x+4$.

Theorem (3.1.3)**.** *Let A, B, C, D be sets,with $R \subseteq A \times B$, $S \subseteq B \times C$ and $T \subseteq C \times D$. Then:*
a) $(R^{-1})^{-1} = R$
b) $T \circ (S \circ R) = (T \circ S) \circ R$,
c) $I_B \circ R = R$ *and* $R \circ I_A = R$,
d) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

We'll prove d). We have that $(c, a) \in (S \circ R)^{-1}$ iff $(a, c) \in (S \circ R)$ iff $\exists b \in B$ such that $(a, b) \in R$ and $(b, c) \in S$ iff $\exists b \in B$ such that $(c, b) \in S^{-1}$ and $(b, a) \in R^{-1}$ iff $(c, a) \in S^{-1} \circ R^{-1}$.

Equivalence Relations

Definition. Given a relation R on A, we say that:

- R is **reflexive** iff $\forall x \in A$, xRx, i.e., $(x, x) \in R$.
- R is **symmetric** iff $\forall x, y \in A$, $(x, y) \in R$ implies that $(y, x) \in R$.
- R is **transitive** iff $\forall x, y, z \in A$, $(x, y) \in R$ and $(y, z) \in R$ implies $(x, z) \in R$.
- R is an **equivalence relation** iff R is reflexive, symmetric and transitive.

We drew pictures of digraphs to see what these meant pictorially.

Example. Let A be the set of students in class and define xRy iff x and y got the same score on the test. Check that this is an equivallence relation. If we let the relation be that x and y have the same birthday, then that is also an equivalence relation.

Example. Let $A = \mathbb{Z}$ and define aRb iff $a - b$ is even. Check that this is an equivalence relation.

Example. Let $A = \mathbb{Z}$ and define aRb iff $a - b$ is odd. Not reflexive($a - a$ is even), is symmetric($a - b$ odd implies that $b - a$ is odd), not transitive(if $a - b$ is odd and $b - c$ is odd, then $a - c = (a - b) = (b - c)$ is even).

Example. Let $A = \mathbb{Z}$ and let aRb iff $a - b$ is divisible by 3. Check that this is an equivalence realation.

Example. Let $A = \mathbb{R}$ and set xRy iff $x \leq y$. This is reflexive, and transitive but not symmetric.

Example. Let $A = \mathbb{R}$ and set xRy iff $x^2 + y^2 \leq 1$. Not reflexive, is symmetric, not transitive.

Definition. Let R be an equivalence relation on A. The **equivalence class of x determined by R** is the set

$$x/R = \{y \in A : xRy\}.$$

This set is also denoted by $[x]$ and $\overline{x}$ in other texts and is also called **x modulo R** or **x mod R**.

The set of all equivalence classes is called **A modulo R** and is denoted A/R.

Example. Let $A = \mathbb{Z}$ and let xRy iff $x - y$ is even. When x is even then x/R is the set of all even integers. In particular, $0/R = 2/R$. When x is odd then x/R is the set of all odd integers, so $1/R = 3/R$. Thus, A/R has two elements $0/R = [0]$ and $1/R = [1]$. We also have that $[0] = [2] = 2\mathbb{Z}$, while $[1] = [3] = 2\mathbb{Z} + 1$.

Example. Let $A = \mathbb{R}$ and set xRy iff $x^2 = y^2$. This is an equivalence relation and $[a] = a/R = \{+a, -a\}$. So each equivalence class has two elements except for 0 and $[0] = \{0\}$.

Example. Let A be the set of students in the class and let aRb iff a and b have the same birthday. Then $[Jim] = Jim/R$ is the set of all people that have the same birthday as Jim. Thus, A/R has one element for each birthday of a student in the class. In a sense it can be thought of as the collection of birthdays. Given a birthday, we get a set, namely, all the students with that day for their birthday.

Theorem (3.2.1)**.** *Let A be a set and R an equivalence relation on A. Then:*

a) *For each $x \in A$, $x/R \subseteq A$ and $x \in x/R$ so x/R is non-empty.*
b) *xRy iff $x/R = y/R$.*
c) *x and y are not related iff $(x/R) \cap (y/R) = \emptyset$.*

Proof. **a)** By definition x/R is a subset of A. Since R is symmetric, xRx and so $x \in x/R$, which guarantees that x/R is non-empty.

b) b) is a biconditional, we prove both implications. First assume that xRy.

Let $z \in x/R$. Then xRz and by symmetryzRx. Since xRy and R is transitive, we get zRy so $z \in y/R$. Thus, $x/R \subseteq y/R$.

Assume that $z \in y/R$, then yRz and by symmetry, zRy. Since also yRx, again by transitivity, zRx and so $z \in x/R$. Thus, $y/R \subseteq x/R$. These two containments show that $x/R = y/R$. Hence, $xRy \implies x/R = y/R$.

Conversely, assume that $x/R = y/R$. By a), $x \in x/R = y/R$ so $x \in y/R$ which by the definition means that yRx and so xRy.

c) Again a biconditional. First assume that x and y are not related, we must prove this implies $(x/R) \cap (y/R) = \emptyset$. We prove the contrapositive: $(x/R) \cap (y/R) \neq \emptyset \implies xRy$. Since the intersection is non-empty, there exists $z \in (x/R) \cap (y/R)$. This implies that xRz and yRz. Hence, xRz and zRy, which by transitivity implies that xRy.

Now we must prove the converse: $(x/R) \cap (y/R) = \emptyset \implies$ x and y are not related. Again we prove the contrapositive: $xRy \implies (x/R) \cap (y/R) \neq \emptyset$. But if xRy then by b), $x/R = y/R$. Hence, $(x/R) \cap (y/R) = x/R$ which is non-empty by a). □

It is good to remember this contrapositive statement of c):

$$(x/R) \cap (y/R) \neq \emptyset \text{ iff } xRy.$$

Combined with b) we get:

$$(x/R) \cap (y/R) \neq \emptyset \text{ iff } x/R = y/R.$$

Thus, we have:
Either $(x/R) \cap (y/R) = \emptyset$ or $x/R = y/R$.

The Congruence Relation

Definition. Fix $m \in \mathbb{N}$. Given $x, y \in \mathbb{Z}$, we say that **x is congruent to y modulo m** iff m divides $x - y$. We write $x \equiv_m y$ or $x = y (\text{mod m})$. We let

$$R_m = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : m \text{ divides } x - y\}$$

denote this relation.

Note that we have been a little redundant since $x \equiv_m y$ and xR_my both are used to denote this relation.

Theorem (3.2.2)**.** *For each fixed $m \in \mathbb{N}$, the relation $\equiv_m$ is an equivalence relation.*

Proof. Since $x - x = 0$ we have that $m \cdot 0 = x - x$ and so m divides $(x - x)$ and thus $x \equiv_m x$. Hence, $\equiv_m$ is reflexive.

If $x \equiv_m y$, then $\exists k \in \mathbb{Z}$ so that$mk = x - y$. Hence, $m(-k) = (y - x)$ and so $y \equiv_m x$. Thus, $\equiv_m$ is reflexive.

Finally, if $x \equiv_m y$ and $y \equiv_m z$ then this means that $\exists k, j \in \mathbb{Z}$ so that $x - y = mk$ and $y - z = mj$. Hence, $x - z = (x - y) + (y - z) = m(k + j)$, so that m divides $x - z$ and $x \equiv_m z$. Thus, $\equiv_m$ is transitive. □

Definition. Let $m \in \mathbb{N}$. We set

$$[x]_m = x/R_m = \{y \in \mathbb{Z} : x \equiv_m y\}.$$

We let $\mathbb{Z}_m = \mathbb{Z}/R_m$ denote the set of equivalence classes.

Example. Let $m = 3$ then

$$[0]_3 = \{y \in \mathbb{Z} : \exists k \in \mathbb{Z}, y = 3k\} = \{3k : k \in \mathbb{Z}\},$$

$$[1]_3 = \{y \in \mathbb{Z} : \exists k \in \mathbb{Z}, y - 1 = 3k\} = \{3k + 1 : k \in \mathbb{Z}\},$$

$$[2]_3 = \{y \in \mathbb{Z} : \exists k \in \mathbb{Z}, y - 2 = 3k\} = \{3k + 2 : k \in \mathbb{Z}\}.$$

Since, $0 \equiv_3 3$ we have that $[3]_3 = [0]_3$. Similarly, $[4]_3 = [1]_3$, $[5]_3 = [2]_3$, etc.

Thus, $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$.

The following theorem explains this phenomena exactly.

Theorem (3.2.3)**.** *Let $m \in \mathbb{N}$ be fixed. Then*

(a) *Given $x, y \in \mathbb{Z}$, $x \equiv_m y$ iff the remainder when x is divided by m is equal to the remainder when y is divided by m*
(b) *The set $\mathbb{Z}_m$ has exactly m equivalence classes and these are given by $\mathbb{Z}_m = \{[0]_m, [1]_m, ..., [m-1]_m\}$*

Proof. **(a):** By the divison algorithm, there are unique (q_1, r_1) so that $x = mq_1 + r_1$ with $0 \leq r_1 < m$ and (q_2, r_2) so that $y = mq_2 + r_2$ with $0 \leq r_2 < m$. Note that $x - y = m(q_1 - q_2) + (r_2 - r_1)$. Thus, m divides $x - y$ iff m divides $r_2 - r_1$.

But since $r_1 \geq 0$, $r_2 - r_1 < r_1 < m$. While, since $r_1 \geq 0$, $r_1 - r_2 \geq 0 - r_2 > -m$. Thus, $-m < r_2 - r_1 < +m$. This shows that m divides $r_2 - r_1$ iff $r_2 - r_1 = 0$.

Thus, we have: $x \equiv_m y$ iff m divides $x - y$ iff m divides $(r_2 - r_1)$ iff $r_2 = r_1$.

(b): The above calculation also shows that for $0 \leq r_1 < m$ and $0 \leq r_2 < m$, that $r_1 \equiv_m r_2$ iff $r_1 = r_2$. Thus, for $0 \leq r_1 < m$ and $0 \leq r_2 < m$, we have that $r_1/R \neq r_2/R$ and so $(r_1/R) \cap (r_2/R) = \emptyset$.

Thus, each of the equivalence classes $[r]_m, 0 \leq r < m$ are distinct. That is, $[0]_m, [1]_m, ..., [m-1]_m$ are all distinct equivalence classes.

Now given any $x \in \mathbb{Z}$ by the division algorithm, we may write it as $x = mq + r$, with $0 \leq r < m$. Since $x - r = mq$ we have that $x \equiv_m r$, and so $x/R = r/R = [r]_m$. Thus, every equivalence class is one of these classes and

$$\mathbb{Z}_m = \{[0]_m, ..., [m-1]_m\}.$$

□

Partitions

A **partition** of a set is a way to divide the set up into disjoint non-empty subsets, so that every element of the set belongs to exactly one subset. For example, the US is divided up into states. The State of Texas is divided up into counties. The US is also divided up into zip codes or into time zones. Each of these is a partition, since no two states intersect, no two time zones intersect, etc.

Definition. Let A be a non-empty set. A collection $\mathcal{P}$ of subsets of A is called a **partition of A** iff
(i) if $X \in \mathcal{P}$ then $X \neq \emptyset$,
(ii) if $X \in \mathcal{P}$ and $Y \in \mathcal{P}$ then either $X = Y$ or $X \cap Y = \emptyset$,
(iii) $\cup_{X \in \mathcal{P}} X = A$.

Example. Let $A = \mathbb{Z}$ let $E = \{x \in \mathbb{Z} : x \text{ is even } \}$, and let $O = \{x \in \mathbb{Z} : x \text{ is odd } \}$. Then $\mathcal{P} = \{E, O\}$ is a partition of $\mathbb{Z}$.

Example. Let $A = \mathbb{R}$ and let $G_n = [n, n+1)$. Then $\mathcal{P} = \{G_n : n \in \mathbb{Z}\}$ is a partition of $\mathbb{R}$.

Example. Let $A = \mathbb{R}$ and let $C_n = [n, n+1]$, and let $\mathcal{P} = \{C_n : n \in \mathbb{Z}\}$ is NOT a partition of $\mathbb{R}$.

Example. Let $A = \mathbb{N}$. Let $P = \{n \in \mathbb{N} : n \text{ is prime } \}$, let $D = \{n \in \mathbb{N} : n \text{ is not prime but is divisible by a prime } \}$, then $\mathcal{P} = \{P, D, \{1\}\}$, is a partition of $\mathbb{N}$.

Theorem (3.3.1)**.** *If R is an equivalence relation on a non-empty set A. Then the set of equivalence classes is a partition of A.*

Proof. We showed that each equivalence class is non-empty, every element of $x \in A$ belongs to an equivalence class(so the union is all of A), namely $x \in x/R$ and that given two equivalence classes, either $(x/R) \cap (y/R) = \emptyset$. □

Next we show that every partition yields an equivalence relation.

Theorem (3.3.2)**.** *Let $\mathcal{P}$ be a partition of the non-empty set A. For $x, y \in A$ define a relation Q by xQy iff $\exists C \in \mathcal{P}$ such that $x \in C$ and $y \in C$. Then*
(a) Q is an equivalence relation on A,
(b) $A/Q = \mathcal{P}$, that is, the sets in $\mathcal{P}$ are precisely the equivalence classes modulo Q.

Proof. **(a):** To see that Q is reflexive, note that since $\cup_{C \in \mathcal{P}} C = A$, given any $x \in A$ there exists $C \in \mathcal{P}$ with $x \in C$. Since $x \in C$ and $x \in C$ we have xQx.

To see that Q is symmetric, note that if xQy then there is $C \in \mathcal{P}$ with $x \in C$ and $y \in C$ But this also implies that yQx.

To see that Q is transitive. Assume that xQy and that yQz. Since xQy $\exists C_1 \in \mathcal{P}$ such that $x \in C_1$ and $y \in C_1$. Since yQz there exists $C_2 \in \mathcal{P}$ such that $y \in C_2$ and $z \in C_2$. We have that $y \in C_1 \cap C_2$. So by the property of a partition, $C_1 = C_2$. Thus, $x \in C_1$ and $z \in C_1$ and so xQz.

(b): Let $x \in A$, we want to prove that $x/Q \in \mathcal{P}$. Let $y \in x/Q$ then $\exists C_1 \in \mathcal{P}$ such that $x \in C_1$ and $y \in C_1$. We claim that $x/Q = C_1$. To see this, if $z \in C_1$, then since $x \in C_1$ and $z \in C_1$ we have xQz and so $z \in x/Q$. This proves that $C_1 \subseteq x/Q$. Suppose that $w \in x/Q$ then there is a set $C_2 \in \mathcal{P}$, with $x \in C_2$ and $w \in C_2$. But $x \in C_1 \cap C_2$ and so $C_1 = C_2$. Since $C_1 = C_2 \implies w \in C_1$ so $x/Q \subseteq C_1$.

Thus, $x/Q = C_1$ and we have shown that every set in A/Q is one of the sets in $\mathcal{P}$.

Let $C \in \mathcal{P}$. Then $C \neq \emptyset$, so there is $x \in C$. Now repeat the argument above to show that $x/Q = C$.

Thus, every every set in $\mathcal{P}$ is in A/Q. □

Ordering Relations

Given $x, y \in \mathbb{R}$ and setting xRy iff $x \leq y$ defines an order relation on $\mathbb{R}$. What are the special properties of this relation? We also wish to generalize the concept of "less than or equals" to more general setttings.

Definition. A relation R on a set A is called **antisymmetric** iff xRy and yRx implies that $x = y$.

Example. Let $A = \mathbb{R}$ and set xRy iff $x \leq y$. Then xRy and yRx means that $x \leq y$ and $y \leq x$, so $x = y$ Thus, $\leq$ is antisymmetric.

Example. Let $A = \mathbb{R}$ and set xRy iff $x < y$. Then xRy and yRx means that $x < y$ AND $y < x$. This is never true. (Remember if P is never true, then $P \implies Q$ is always true!) Hence, xRy and yRx implies that $x = y$ and so this is also antisymmetric!! Note that R is not reflexive.

Definition. A relation R on a set A is called a **partial order** or **partial ordering** iff R is reflexive, antisymmetric and transitive. A set A together with a partial order R is called a **partially ordered set** or a **poset.**

Example. Each of the sets $\mathbb{N}, \mathbb{Z}$ and $\mathbb{R}$ together with xRy iff $x \leq y$ are posets.

Example. Let $A = \mathbb{N}$ and define aRb iff a divides b. Check that this is a partial order on $\mathbb{N}$.

Example. The 26 letter alphabet with the usual alphabet ordering is a poset.

Example (The Dictionary Order)**.** Consider all strings of length two that can be made with two letters of the alphabet, so "words" of length two. So altogether we have $(26)^2$ words. Define $w_1 R w_2$ if either the first letter in w_1 comes before the first letter of w_2 or when the first letters of both words are the same then the second letter of w_1 comes before or is the same as the second letter of w_2. So $abRcd$ and $aaRab$. This is a partial order.

This can of course be applied to words of greater length and even to words of different length-which is how our dictionary works.

Example (The Dictionary Order on $\mathbb{R}^2$)**.** Let $A = \mathbb{R} \times \mathbb{R}$ and define a relation by $(a, b)R(c, d)$ iff either $a < c$ or $a = c$ and $b \leq d$. This is a partial order.

Definition. Let R be a partial order on A and let $a, b \in A$ with $a \neq b$. We say that **a is the immediate predecessor of b** or that **a is the immediate succesor of a** iff aRb and there does not exist $c \in A$ with $a \neq c$, $b \neq c$ and aRc and cRb.

Another way to say this last awkward statement is that: if aRc and cRb then either $a = c$ or $c = b$.

Example. In $\mathbb{N}$ 2 is the immediate predecessor of 3.

Example. In $\mathbb{R}$ no number has an immediate predecessor.

Example. In the dictionary order on words of length two, bc is the immediate predecessor of bd. The immediate predecessor of ca is bz.

Department of Mathematics, University of Houston, Houston, Texas 77204-3476, U.S.A.
E-mail address: vern@math.uh.edu