Contents

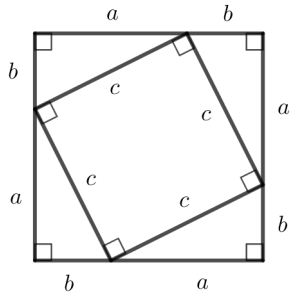
1 Proofs, Logic, and Sets

In this chapter, we introduce a number of foundational concepts for rigorous mathematics, including an overview of mathematical proof, elements of Boolean and propositional logic, and basic elements of set theory.

1.1 Overview of Mathematical Proof

- In colloquial usage, to provide "proof" of something means to provide strong evidence for a particular claim.
- In mathematics, we formalize this intuitive idea of proof by making explicit the types of logical inferences that are allowed.
    - To provide a mathematical proof of a claim is to give a sequence of statements showing that a particular collection of assumptions (typically called hypotheses) imply the stated result (typically called the conclusion).
    - Each statement in a proof follows logically from the previous statements in the proof or facts known to be true from elsewhere. This type of reasoning is usually called deductive reasoning.
    - Although proofs often employ mathematical notation (including symbols and equations), they are ultimately written in sentences, in natural language.
- Here is an example of a proof of a famous result from geometry:

- Theorem (Pythagoras): If a and b are the lengths of the legs of a right triangle, and c is the length of the hypotenuse of the right triangle, then $a^2 + b^2 = c^2$.
  - Proof: Consider the dissection, given below, of a square with side length $a + b$ into four right triangles with side lengths a and b, along with a quadrilateral in the center:



  - The four triangles are all congruent to the original right triangle since they are all right triangles with leg lengths a and c. Thus, their hypotenuses all have length c.
  - Furthermore, each of the angles of the interior quadrilateral are right angles: the two non-right angles in the triangle sum to $\pi/2$ radians and a full segment has angle measure π radians, so the remaining angle at each vertex of the quadrilateral measures $\pi - \pi/2 = \pi/2$ radians (a right angle).
  - Since the interior quadrilateral has all angles measuring $\pi/2$ radians and its sides all have length c, it is a square.
  - Now observe that the area of the large square is equal to the sum of the areas of the four triangles and the smaller square.
  - Since the area of the large square is $(a+b)^2$, the area of each triangle is $\frac{1}{2}ab$, and the area of the interior square is c^2, we must have $(a+b)^2 = 4 \cdot \frac{1}{2}ab + c^2$.
  - Expanding yields $a^2+2ab+b^2 = 2ab+c^2$, and finally, subtracting $2ab$ from both sides yields $a^2+b^2 = c^2$, as claimed.

- In the proof of the Pythagorean theorem above, we started with the assumptions that a and b were the lengths of the legs and c was the length of the hypotenuse of a right triangle.
  - We then gave a deductive argument whose conclusion was the desired outcome, namely, that $a^2+b^2 = c^2$.
  - Each step in the argument was justified logically from results previously established to be true, either earlier in the argument or from elsewhere.

- Notice that we invoked various known facts from geometry and algebra in the course of our proof.
  - For example, we accepted as true all of the following statements or operations: (i) the sum of the two non-right angles in a right triangle is $\pi/2$ radians, (ii) the area of a square is the square of the length of its side, (iii) we may subtract equal quantities from both sides of an equality to obtain a new equality, and (iv) the algebraic identity $(a+b)^2 = a^2 + 2ab + b^2$.
  - In order for our proof to be completely valid, we would need to justify all of those additional facts that we invoked.
  - Of course, to justify each of those facts, we will probably need to invoke further others, and so on. It is not hard to see that this demand for justification would never end, unless at some point we simply declare some fundamental assumptions, and then justify everything in terms of those assumptions.

- In mathematics, we refer to a set of fundamental assumptions of this nature as axioms.
  - An example of an axiom of arithmetic is the commutative property of addition: "For any numbers a and b, $a + b = b + a$".
  - When proving theorems, we allow ourselves only to use statements derived from the axioms, or from statements we have previously proven.

- We also construct various special terms for new objects using definitions.
    - An example of a definition in arithmetic is: "A prime number is a positive integer $n > 1$ that is only divisible by 1 and itself".
    - Of course, this definition in turn relies on other information (such as what a positive integer is, what the statement $n > 1$ means, and what it means for an integer to be divisible by another integer), so in order for this definition to make sense, we would need to have previously defined all of these things.
- Here is another example of a famous proof regarding prime numbers[1]:
- Theorem (Euclid): There are infinitely many prime numbers.
    - Proof: Suppose, by way of contradiction, that the claimed result were not true, meaning that there are only finitely many prime numbers p_1, p_2, ... , p_k.
    - Consider the number $N = p_1 p_2 \cdots p_k + 1$.
    - Since $N > p_1$, $N > p_2$, ... , and $N > p_k$, we see that N cannot equal any of the primes on the list, and therefore N cannot be prime, since it would necessarily have to be on the list.
    - Therefore N is composite. Consider the prime factorization of N: at least one prime on the list must appear in it, say p_i.
    - Then p_i divides N, and since p_i also divides the product $p_1 p_2 \cdots p_k$, we see that p_i therefore divides $N - p_1 p_2 \cdots p_k = 1$.
    - But this is impossible, because p_i is prime and therefore $p_i > 1$.
    - We have reached a contradiction, and therefore the original assumption (that there were only finitely many primes) must have been incorrect. We conclude that there must be infinitely many primes, as claimed.
- As in our proof of the Pythagorean theorem, we have appealed to several other facts which we have not explicitly established, such as the fact that every composite integer has a prime factorization, and the fact that every prime number is strictly larger than 1.
- Notice also that the structure of the proof given above is different from our proof of the Pythagorean theorem.
    - When we proved the Pythagorean theorem, we started with the given hypotheses and established the conclusion directly from them: this is often referred to as a direct proof.
    - When we proved that there are infinitely many primes, we instead gave a proof by contradiction, which starts from the given hypotheses along with the assumption that the desired conclusion is false, and shows that these assumptions lead to a logical contradiction. This proof method is also called indirect proof.
- Once we have given a formal proof of a result, we have established that the result to be true. We emphasize that in mathematics, a result is only considered "true" if it is true in *every possible case*; even a single exception will make a result false.
    - For example, the statement "Every prime is odd" is false, because the even number 2 is prime. (We say that the number 2 is a counterexample to the given statement, since it is an example for which the statement is false.)
    - However, the statement "Every prime greater than 2 is odd" is true, because 2 is the only even prime number.
    - There are, of course, statements that are not true, such as "$3 + 5 = 7$", and there are also statements whose truth or falsity is not currently known, such as "It will rain tomorrow" but which must nevertheless be either true or false.
- In mathematics, a result that is believed to be true, typically based on some evidence that is not definitive, is often called a conjecture. Here is an example:

[1] We will discuss prime numbers in detail in a later chapter, but for now recall that a prime number is a positive integer $p > 1$ that is divisible only by 1 and itself.

- Conjecture (Goldbach): If n is an even integer greater than 2, then n can be expressed as the sum of two prime numbers.
  - Goldbach made this conjecture in 1742, and it is among the oldest major unsolved problems in number theory.
  - It is easy to find numerical evidence suggesting that Goldbach's conjecture is true: we can write $4 = 2+2$, $6 = 3+3$, $8 = 3+5$, $10 = 3+7$, $12 = 5+7$, $14 = 3+11$, $16 = 5+11$, $18 = 7+11$, and so forth.
  - However, it would require only a single counterexample to Goldbach's conjecture (namely, an even number greater than 2 that cannot be expressed as the sum of two prime numbers) to disprove the result.
  - Thus, even if we check many more examples, this sort of evidence cannot prove Goldbach's conjecture: even if we checked the first thousand, or million, or billion, or trillion, even numbers, there are always more even integers for which we have *not* verified the conjecture[2] that could potentially be counterexamples.
- Avoiding an outcome where a result is assumed to be true but is actually false is the fundamental reason for providing rigorous proofs in mathematics.
  - There are results that appear to be true for a long time but for which there do, in fact, exist counterexamples, and there are numerous other results that seem intuitively true but which are (in fact) false.
  - By using rigorous deductive arguments to justify calculations and arguments, we can avoid such pitfalls.
- Example (Pólya's Conjecture): As is likely familiar, every positive integer has a unique factorization as a product (possibly involving only one term) of prime numbers. Call a number "P-lucky" if the total number of prime factors, including duplicates, is odd, and call a number "P-unlucky" if the total number of prime factors is even.
  - For example, since $4 = 2 \cdot 2$, we see 2 is P-unlucky, while $5 = 5$, $12 = 2 \cdot 2 \cdot 3$, and $32 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$ are all P-lucky.
  - Now we ask: for each positive integer $n > 1$, are there more P-lucky integers from 1 to n inclusive, or are there more P-unlucky integers?
  - It is not hard to see that 2, 3, 5, 7, 8, 11, 12, 13, 17, 18, 19, 20, 23 are P-lucky, while 1, 4, 6, 9, 10, 14, 15, 16, 21, 22, 24, 25 are P-unlucky. For each n with $2 \leq n \leq 25$, one can see that there are always at least as many P-lucky integers up to n as there are P-unlucky integers.
  - If one continues these calculations, this pattern of having at least as many P-lucky integers as P-unlucky integers persists for quite a long time (it is not hard to show by hand that it persists up through $n = 100$).
  - It was conjectured in 1919 by Pólya that, in fact, there are always at least as many P-lucky integers as P-unlucky integers up to n for every positive integer n.
  - Perhaps surprisingly, in contrast to the numerical evidence above, this conjecture turns out to be false! But the first counterexample does not occur until $n = 906,150,257$, as was shown computationally in the 1980s by M. Tanaka.
  - The point of this example is that, despite what numerical calculations and examples might suggest, it is possible for a statement to appear true for many, many examples yet still eventually be false.
- Example (Riemann Rearrangement): Historically, infinite sums and infinite series were treated fairly cavalierly, and most manipulations of infinite sums (e.g., rearranging the terms) were assumed to be valid, since rearranging a finite sum arbitrarily will never change the value.
  - But in fact, there exist infinite sums that, upon rearranging the terms appropriately, will yield a different sum.
  - For an explicit example, consider the infinite series

$$S = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \frac{1}{7} - \frac{1}{8} + \frac{1}{9} - \frac{1}{10} + \cdots$$

    which is called the alternating harmonic series. (Using calculus one may show that its sum is $\ln(2)$.)

[2] In fact, as of 2019, Goldbach's conjecture has been numerically verified for all even numbers less than $4 \cdot 10^{18}$.

- If we divide each of the terms by 2 and "pad" the series by including zeroes, we get the series

$$\frac{1}{2}S = 0 + \frac{1}{2} + 0 - \frac{1}{4} + 0 + \frac{1}{6} + 0 - \frac{1}{8} + 0 + \frac{1}{10} + \cdots .$$

- Now add this series to the original one term-by-term. The summed series is

$$\frac{3}{2}S = 1 + 0 + \frac{1}{3} - \frac{1}{2} + \frac{1}{5} + 0 + \frac{1}{7} - \frac{1}{4} + \frac{1}{9} + 0 + \cdots$$

  which, after removing the zero terms, yields

$$\frac{3}{2}S = 1 + \frac{1}{3} - \frac{1}{2} + \frac{1}{5} + \frac{1}{7} - \frac{1}{4} + \frac{1}{9} + \cdots .$$

- It is not hard to verify that this new series has all the same terms (with the same signs) as the original series, but the sum has been changed!
- The point of this example is to illustrate that a seemingly obvious and intuitive statement, namely, "rearranging the terms in a sum will never change the value", is actually false in certain situations.
- In fact, as first proven by Riemann in the 1800s, for any convergent series of real numbers, rearrangement either will never change the sum, or there exists a rearrangement having any desired value at all.

1.2 Elements of Logic

- In order to examine proof techniques and methods of argument more formally, we will first study basic logic.

1.2.1 Propositions and Conditional Statements

- The basic statements in logic are called propositions:
- Definition: A logical proposition (often simply a proposition) is a well-defined statement that is either true or false.
  - Example: "$2 + 4 = 6$" is a proposition that is true.
  - Example: "$2 \cdot 4 = 7$" is a proposition that is false.
  - Example: "112950129410147 is a prime number" is a proposition, because this number is either prime or not prime. (In fact, the proposition is true, although this is not so easy to show.)
  - Non-example: "How many perfect squares are less than 20?" is not a proposition, because it is not a statement that is either true or false (it is, in fact, a question).
  - Non-example: "If n is a prime number, dinosaur potatoes" is not a proposition, because it does not make sense.
  - Example: "$(x + 6a)^2 - 57 = y^3$" is a proposition, because it is an algebraic statement (whether it is true or false depends on the values of the variables x, a, and y).
  - Non-example: "$(x + 6a)^2 - 57$" is not a proposition, because it is an algebraic expression and not a statement.
- We often negate propositions using the word "not". In general, if A is a proposition, then we can form a new proposition, called "not A", whose truth value is the opposite of A.
  - Example: If A is the proposition "$2 + 4$ is equal to 6", then "not A" is the proposition "$2 + 4$ is not equal to 6". Observe that A is true while "not A" is false.
- Several of the examples of theorems and conjectures we discussed in the previous section were phrased as conditional statements having the general form "If A, then B" where A and B were both propositional statements.

- For example, in the Pythagorean theorem the proposition A would be "a and b are the lengths of the legs of a right triangle, and c is the length of the hypotenuse of the right triangle" and the proposition B would be "$a^2 + b^2 = c^2$".
- In Goldbach's conjecture, the proposition A would be "n is an even integer greater than 2" and the proposition B would be "n can be expressed as the sum of two prime numbers".

- We would like to formalize the idea of a conditional statement, and analyze when such a statement is true or false.
  - Consider the conditional statement "If Kat goes to work, she will receive a paycheck".
  - We would generally agree that this statement agrees with reality (i.e., is true) if Kat does go to work and does receive a paycheck.
  - On the other hand, if Kat goes to work and does not receive a paycheck, we would consider the conditional statement to be false.
  - However, if Kat does *not* go to work, but still receives a paycheck, the conditional statement is still consistent with what occurred (since it never claimed anything about what would happen if Kat did not go to work).
  - Likewise, if Kat does *not* go to work and does not receive a paycheck, the conditional statement is also consistent with what occurred (again, since it never claimed anything about what would happen if Kat did not go to work).

- We can summarize the behavior of conditional statements using a truth table, in which we write out all possible truth values for all of the propositions involved.
  - Here is the truth table for the conditional statement "If A, then B":

A	B	If A, then B
True	True	True
True	False	False
False	True	True
False	False	True

  - The key observation is that the behavior of a conditional statement depends only on the truth values of the propositions involved, and not on any other information.

- There are other variations on the standard conditional statement "If A, then B" that are frequently important as well.

- Definition: The converse of the conditional statement "If A, then B" is the conditional statement "If B, then A".
  - Example: The converse if the statement "If Kat goes to work, then she will receive a paycheck" is "If Kat receives a paycheck, then Kat went to work" (at least, up to modifying the verb tenses to make the sentence grammatical).

- It is extremely important to observe that the converse of a conditional statement is *not* logically equivalent to the original statement.
  - Even in the example above, it is clear that "If Kat goes to work, then she will receive a paycheck" is not the same as "If Kat receives a paycheck, then Kat went to work". In the specific event where Kat does not go to work but does receive a paycheck, the first statement is false but the second one is true.
  - We can also see that a conditional and its converse are not logically equivalent using a truth table:

A	B	If A, then B	If B, then A
True	True	True	True
True	False	False	True
False	True	True	False
False	False	True	True

- There are many examples of theorems whose converse is true. For example, the converse of the Pythagorean Theorem is true:
- Theorem (Pythagorean Converse): If $a^2 + b^2 = c^2$, then a and b are the lengths of the legs of a right triangle, and c is the length of the hypotenuse of the right triangle.
    - For simplicity we are assuming that a, b, and c are positive numbers (meaning that they are eligible to be lengths). As written, the statement is not true if we allow a, b, c to be negative.
    - Proof: Construct a right triangle with leg lengths a and b, and let the length of the hypotenuse be x.
    - Then by the Pythagorean theorem (which we have proven), we know that $a^2 + b^2 = x^2$.
    - Because $a^2 + b^2 = c^2$ by hypothesis, we obtain $c^2 = a^2 + b^2 = x^2$ and therefore since c, x are nonnegative, we have $c = x$.
    - Then a and b are indeed the lengths of the legs of a right triangle, and c is the length of the hypotenuse, as claimed.
- Notice that the proof of the converse of the Pythagorean Theorem was different from the proof of the Pythagorean Theorem itself.
    - This should not be surprising, because as we emphasized above, a conditional statement and its converse are different!
- There are many other results whose converse is false.
    - For example, consider the converse of Goldbach's conjecture: "If n can be expressed as the sum of two prime numbers, then n is an even integer greater than 2".
    - This statement above is clearly false, because we can give a counterexample, namely, $n = 5$: notice that $5 = 2 + 3$ is the sum of two prime numbers, but 5 is not an even integer greater than 2.
    - For another example, consider the fact "if $n = 3$, then $n^2 = 9$". The converse of this statement is "If $n^2 = 9$, then $n = 3$", which is false because if $n^2 = 9$ then n could also equal -3.
- In addition to the converse, there are two other variations on a conditional statement that are frequently useful:
- Definition: The inverse of the conditional statement "If A, then B" is the conditional statement "If not A, then not B". The contrapositive of the conditional statement "If A, then B" is the conditional statement "If not B, then not A".
    - Notice that the contrapositive is the converse of the inverse (and also the inverse of the converse).
    - Example: The inverse if the statement "If Kat goes to work, then she will receive a paycheck" is "If Kat does not go to work, then she will not receive a paycheck", while the contrapositive is "if Kat does not receive a paycheck, then she did not go to work".
    - We can examine the converse, inverse, and contrapositive together with a truth table:

A	B	Original If A, then B	Converse If B, then A	Inverse If not A, then not B	Contrapositive If not B, then not A
True	True	True	True	True	True
True	False	False	True	True	False
False	True	True	False	False	True
False	False	True	True	True	True

- From the truth table, we can see that the converse and inverse always have the same truth values, meaning that they are logically equivalent. Likewise, the original statement is logically equivalent to its contrapositive.
    - Once these equivalences are noticed, it is often not very hard to convince oneself that they are true even for informal uses of conditional statements.

- In our example with "If Kat goes to work, then she will receive a paycheck", suppose Kat does not receive a paycheck, then (presuming the conditional statement was correct) she could not have gone to work since otherwise she would have received a paycheck.
- Therefore, the statement "If Kat does not receive a paycheck, then she did not go to work" is true.
- Running the logic the other way around, the statement "If Kat does not receive a paycheck, then she did not go to work" also implies the statement "If Kat goes to work, then she will receive a paycheck".
- This means the original statement conveys exactly the same information as its contrapositive.

- Remark: Our observation that a conditional statement is equivalent to its contrapositive motivates one possible strategy for establishing a conditional statement, namely, that we could instead try to establish its contrapositive. In certain situations, the contrapositive may be more natural to prove.
  - We will give examples of these so-called contrapositive proofs later.

- Notice that a conditional statement "if A, then B" and its converse "if B, then A" are both true precisely when A and B have the same truth value (i.e., both true or both false).
  - We often abbreviate this situation by saying "A if and only if B": such a statement is sometimes called a biconditional, since it is shorthand for the two separate conditional statements "if A, then B" and "if B, then A".
  - Here is a truth table for the biconditional:

A	B	A if and only if B
True	True	True
True	False	False
False	True	False
False	False	True

- As a final remark, we will point out that there are many different ways to phrase conditional statements in English. Here are some equivalent ways of phrasing "if A, then B":
  - A implies B.
  - A is sufficient for B.
  - B if A.
  - $A \Rightarrow B$.
  - B is implied by A.
  - B is necessary for A.
  - A only if B.
  - $B \Leftarrow A$.

- Here are some equivalent ways of phrasing "A if and only if B":
  - A is equivalent to B.
  - $A \Leftrightarrow B$.
  - A iff B.
  - A is necessary and sufficient for B.

1.2.2 Boolean Operators and Boolean Logic

- In addition to conditionals, we often also join propositions together using operators like "and" and "or". We can formalize these operations from their usage in standard language:

- Definition: If A is a proposition, then the proposition $\neg A$ (read as "not A") has the opposite truth value to A: it is true whenever A is false, and is false whenever A is true.
  - When writing statements in words, we often simply use the word "not", as we did earlier.
  - Notation: Since the symbol $\neg$ is not typically found on keyboards, in computer science the "not" operator is often written with a tilde ($\sim$) or an exclamation point (!).
  - Here is the truth table (such as it is) for the "not" operator:

A	$\neg A$
True	False
False	True

- Definition: If A and B are propositions, then the proposition $A \wedge B$ (read as "A and B") is true precisely when both A and B are true, and the proposition $A \vee B$ (read as "A or B") is true precisely when at least one of A and B is true.
    - When writing statements in words, we often simply use the words "and" and "or". Do note that there are many ways in English to phrase these ideas, and they do not always use the exact words "and" and "or" (see, for example, the definition of "or" above, which used the word "and").
    - Remark: We emphasize that in mathematics, the word "or" is always taken to mean "inclusive or" unless otherwise specified. Thus, the statement "A or B" always includes the possibility that both A and B are true. In occasions where we need to make use of "exclusive or", which is true when A is true or B is true but not both, we will explicitly say that both statements cannot be true.
    - Notation: In computer science, the "and" operator is also often written with an ampersand (&), while the "or" operator is often written as a single or double pipe (| or ||).
    - Here are the truth tables for the "and" and "or" operators:

A	B	$A \wedge B$	$A \vee B$
True	True	True	True
True	False	False	True
False	True	False	True
False	False	False	False

- By combining propositions with these various operators, we can construct more complicated statements, such as $(A \vee B) \wedge (\neg A \wedge \neg C)$.
- Analysis of statements constructed with these logical operators is often called Boolean algebra (named after the logician Georges Boole).
    - We use the word "algebra" because the Boolean operators $\neg$, $\wedge$, and $\vee$ obey many properties of elementary algebra.
    - For simplicity, we often write $F = G$ when two logical formulas are logically equivalent.
- Proposition (Boolean Algebra): For any propositions A, B, and C, the following are true:
    1. (Commutative Laws) We have $A \wedge B = B \wedge A$ and $A \vee B = B \vee A$.
    2. (Associative Laws) We have $(A \wedge B) \wedge C = A \wedge (B \wedge C)$ and $(A \vee B) \vee C = A \vee (B \vee C)$.
    3. (Identity) We have $A \wedge \text{True} = A$ and $B \vee \text{False} = B$.
    4. (Double Negative) We have $\neg(\neg A) = A$.
    5. (Absorption) We have $A \wedge A = A = A \vee A$, $A \wedge \text{False} = \text{False}$, and $B \vee \text{True} = \text{True}$.
    6. (Distributive Laws) We have $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$ and $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$.
    7. (Inverse) We have $A \wedge (\neg A) = \text{False}$ and $A \vee (\neg A) = \text{True}$.
    8. (De Morgan's Laws) We have $\neg(A \wedge B) = (\neg A) \vee (\neg B)$ and $\neg(A \vee B) = (\neg A) \wedge (\neg B)$.
        - We emphasize here that many of these properties are analogous to properties of arithmetic and algebra. For example, the commutative law for addition says that $a + b = b + a$ for any numbers a and b; the commutative law quoted above in (1) tells us that the analogous statement is true for the operators $\wedge$ and $\vee$.
        - Proof: Each of these equivalences is easy to verify using a truth table.
        - When analyzing compound expressions, it is often helpful to add additional columns for the individual components of the expression.
        - We illustrate the ideas with a truth table establishing the first equivalence in (6):

A	B	C	$B \vee C$	$A \wedge (B \vee C)$	$A \wedge B$	$A \wedge C$	$(A \wedge B) \vee (A \wedge C)$
True	True	True	True	True	True	True	True
True	True	False	True	True	True	False	True
True	False	True	True	True	False	True	True
True	False	False	False	False	False	False	False
False	True	True	True	False	False	False	False
False	True	False	True	False	False	False	False
False	False	True	True	False	False	False	False
False	False	False	False	False	False	False	False

- Example: Show that the formula $\neg(A \vee \neg B) \vee (A \wedge B)$ is equivalent to B.
  - The easiest method for showing such an equivalence is simply to write down a truth table:

A	B	$A \vee \neg B$	$\neg(A \vee \neg B)$	$A \wedge B$	$\neg(A \vee \neg B) \vee (A \wedge B)$
True	True	True	False	True	True
True	False	True	False	False	False
False	True	False	True	False	True
False	False	True	False	False	False

  - Alternatively, we could apply some of the basic equivalences above, as follows:

$$\begin{aligned}
\neg(A \vee \neg B) \vee (A \wedge B) &= [\neg A \wedge \neg(\neg B)] \vee (A \wedge B) && \text{(de Morgan's law)} \\
&= (\neg A \wedge B) \vee (A \wedge B) && \text{(double negative)} \\
&= (B \wedge \neg A) \vee (B \wedge A) && \text{(commutative law)} \\
&= B \wedge (\neg A \vee A) && \text{(distributive law)} \\
&= B \wedge \text{True} && \text{(inverses)} \\
&= B && \text{(identity)}
\end{aligned}$$

- We can also describe explicitly the conditional statements "if A, then B" and "A if and only if B":
- Definition: The conditional statement $A \Rightarrow B$ (read as "A implies B") is defined to be the proposition $\neg A \vee B$. The conditional statement $A \Leftarrow B$ (read as "A is implied by B") is defined to be the proposition $A \vee \neg B$. The biconditional statement $A \Leftrightarrow B$ (read as "A if and only if B") is defined to be the proposition $(A \wedge B) \vee (\neg A \wedge \neg B)$.
  - Equivalently, we may view these conditional statements as being defined by their truth tables:

A	B	$A \Rightarrow B$	$A \Leftarrow B$	$A \Leftrightarrow B$
True	True	True	True	True
True	False	False	True	False
False	True	True	False	False
False	False	True	True	True

  - It is easy to see that the conditional $A \Rightarrow B$ is the same as the conditional statement "if A, then B" that we discussed earlier, while $A \Leftarrow B$ is the converse "if B, then A", while $A \Leftrightarrow B$ is the biconditional "A if and only if B".
  - From the truth table we can also immediately see, for example, that $(A \Rightarrow B) \wedge (B \Rightarrow A)$ is logically equivalent to $A \Leftrightarrow B$.
- By applying the definitions, we can unwind logical formulas involving conditionals:
- Example: Show that $A \Rightarrow (B \Rightarrow A)$ is always true.
  - In words, this conditional says "If A is true, then B implies A". Since "B implies True" is a true statement, we should expect the given statement to be true always.
  - Here is a truth table:

A	B	$B \Rightarrow A$	$A \Rightarrow (B \Rightarrow A)$
True	True	True	True
True	False	True	True
False	True	False	True
False	False	True	True

- Alternatively, we could apply some of the basic equivalences and the definition of $\Rightarrow$:

$$\begin{aligned} A \Rightarrow (B \Rightarrow A) &= \neg A \vee (B \Rightarrow A) && \text{(definition of conditional)} \\ &= \neg A \vee (\neg B \vee A) && \text{(definition of conditional)} \\ &= \neg A \vee (A \vee \neg B) && \text{(commutative law)} \\ &= (\neg A \vee A) \vee \neg B && \text{(associative law)} \\ &= \text{True} \vee B && \text{(inverses)} \\ &= \text{True} && \text{(absorption)} \end{aligned}$$

1.3 Sets and Set Operations

- The informal idea of a set is quite simple: it is a well-defined collection of distinct elements. Sets are one of the foundational objects of mathematics, and in this section we discuss a number of basic properties of sets.

1.3.1 Sets

- "Definition"[3]: A set is a well-defined collection of distinct elements.
  - The elements of a set can be essentially anything: integers, real numbers, other sets, people.
  - Sets are generally denoted by capital or script letters, and when listing the elements of a set, curly brackets $\{\cdot\}$ are used.
  - Sets do not have to contain any elements: the empty set $\emptyset = \{\ \}$ is the set with no elements at all.
  - Two sets are the same precisely if all of their elements are the same. The elements in a set are not ordered, and no element can appear in a set more than once: thus the sets $\{1, 4\}$ and $\{4, 1\}$ are the same.
- There are two primary ways to describe a set.
  - One way is to list all the elements: for example, $A = \{1, 2, 4, 5\}$ is the set containing the four numbers 1, 2, 4, and 5, while $B = \{\star, \text{potato}, 17, \{1, 2\}\}$ is the set containing the four elements $\star$, potato, the number 17, and the set $\{1, 2\}$.
  - The other way to define a set is to describe properties of its elements[4]: for example, the set S of one-letter words in English has two elements: $S = \{\text{a, I}\}$.
- Definition: If S is a set, $x \in S$ means "x is an element of S", and $x \notin S$ means "x is not an element of S".
  - Example: For $S = \{1, 2, 5\}$ we have $1 \in S$ and $5 \in S$ but $3 \notin S$ and $\pi \notin S$.
  - Example: For S equal to the set of English words starting with the letter A, we have apple $\in S$ and antlers $\in S$, while potatoes $\notin S$.
- We often employ "set-builder" notation for sets, which has the form {dummy variable : conditions}, and consists of all elements satisfying the given conditions phrased in terms of the dummy variable.
  - For example, the set S of real numbers between 0 and 5 is denoted $S = \{x : x \text{ is a real number and } 0 < x < 5\}$.
  - Example: $S = \{n : n \text{ is a positive integer less than } 6\} = \{1, 2, 3, 4, 5\}$.

[3] We will remark here that this statement is not really a well-formed definition, which is why we have written the word "Definition" in quotes. As we will discuss later, it is necessary to be more specific about what kinds of sets and definitions of sets are allowed, or else it is possible to construct logical paradoxes using sets (e.g., by "defining" a set in such a way that it cannot actually exist).

[4] As we noted above, it is possible to run into trouble by trying to define sets in this "naive" way of specifying qualities of their elements.

- In practice, to save time we will often not give a totally explicit description of a set when we are describing a pattern that is clear from the context.
  - For example, if we write $A = \{1, 2, 3, 4, \dots, 10\}$, we mean that A is the set of positive integers from 1 to 10: explicitly, $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.
  - Instead of writing all 10 elements of A, we could also describe A as $A = \{n : n \text{ is a positive integer and } 1 \leq n \leq 10\}$, or more simply, "$A$ is the set of positive integers from 1 to 10 inclusive".
  - In general, it is best to write an explicit description of the pattern, unless there is no chance of confusion. (If we were to write $B = \{3, 5, 7, \dots\}$, is the intended set the odd integers starting with 3, or the prime numbers starting with 3?)
- Certain sets of numbers arise frequently and are given special symbols:
  - The set $\{\dots, -2, -1, 0, 1, 2, \dots\}$ of integers is denoted $\mathbb{Z}$. (The use of the letter "Z" comes from the fact that the German word for "numbers" is "Zahlen".)
  - The set of rational numbers is denoted $\mathbb{Q}$ ("quotients"). Typical examples of rational numbers include $\frac{1}{2}$, $-\frac{4}{17}$, 12, and 0.
  - The set of real numbers is denoted $\mathbb{R}$ ("reals"). Typical examples of real numbers include π, e, $\sqrt{2}$, 1, $\frac{4}{3}$, and -12.
  - The set of complex numbers is denoted $\mathbb{C}$ ("complex"). Typical examples of complex numbers include i, $2 - 3i$, $\pi + ei$, and 17. (Recall that $i = \sqrt{-1}$ is the imaginary unit.)
  - Remark: The set $\{1, 2, 3, \dots\}$ of positive integers is often denoted $\mathbb{N}$ ("natural numbers"). However, some authors also consider 0 a natural number, and therefore instead define $\mathbb{N} = \{0, 1, 2, 3, \dots\}$. To avoid this ambiguity, we will write $\mathbb{Z}_+$ for the positive integers and $\mathbb{Z}_{\geq 0}$ for the nonnegative integers.
- By using the notation above, we can give more compressed descriptions of other sets of numbers.
  - Example: The set $S = \{n \in \mathbb{Z} : n^2 < 10\}$ consists of the integers n having the property that $n^2 < 10$. Explicitly, $S = \{-3, -2, -1, 0, 1, 2, 3\}$.
  - Example: The set $T = \{x \in \mathbb{R} : 0 < x < 5\}$ consists of all real numbers x having the property that $0 < x < 5$.
- Another fundamental property of sets is the number of elements they contain:
- Definition: If A is any set, the cardinality of A, denoted $\#A$ or $|A|$, is the number of distinct elements of A.
  - Example: For $A = \{1, 2, 3\}$ and $B = \{2, 4, 6, 8, 10, \dots, 100\}$, then $\#A = 3$ and $\#B = 50$.
  - Example: The cardinality of the empty set $\emptyset$ is 0. In fact, the empty set is the only set of cardinality 0.
  - Example: The cardinalities of the sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all infinite.
  - Warning: We will discuss cardinality in the context of infinite sets more carefully later. As a preview, we will say now that, although $\mathbb{Z}$ and $\mathbb{R}$ are both infinite sets, the cardinality of $\mathbb{R}$ is strictly greater than the cardinality of $\mathbb{Z}$. This is the case because, as we will prove, there is no way to label all of the real numbers with the elements of $\mathbb{Z}$: thus, in a very concrete sense, there are "strictly more" real numbers than integers.

1.3.2 Subsets

- Associated to a set is the natural idea of a subset, consisting of another set containing some of the elements of the original set. We can describe this relation formally as follows:
- Definition: If A and B are two sets with the property that every element of A is also an element of B, we say A is a subset of B (or that A is contained in B) and write $A \subseteq B$.

- More explicitly, we say $A \subseteq B$ if $x \in A$ implies $x \in B$ for any element x.
- Example: If $A = \{1, 2, 3\}$, $B = \{1, 4, 5\}$, and $C = \{1, 2, 3, 4, 5\}$, then $A \subseteq C$ and $B \subseteq C$ but neither A nor B is a subset of the other.
- Example: If S is the set of all English words and T is the set of all English words starting with the letter P, then $T \subseteq S$.
- Example: If A is any set, then the empty set $\emptyset$ is contained in A.
- Example: We have a chain of containments $\mathbb{Z}_{>0} \subseteq \mathbb{Z}_{\geq 0} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

- Warning: Subset notation is not universally agreed upon: the notation $A \subset B$ is also commonly used to say that A is a subset of B.
  - There is no distinction except for when A can be equal to B: some authors allow $A \subset B$ to include the possibility that A could be equal to B, while others insist that $A \subset B$ means that A is a subset of B which cannot be all of B.
  - We will always use the notation $A \subseteq B$, thereby including the possibility that $A = B$, and if we wish to say specifically that A is a subset of B that is not equal to B, we will write $A \subsetneq B$.
  - On occasion we also write $B \supseteq A$ ("B is a superset of A") when we want to emphasize the set B. Its meaning is identical to $A \subseteq B$, namely, that A is a subset of B.

- Here are a few very basic properties of subsets:
- Proposition (Properties of Subsets): For any sets A, B, C, we have the following:

1. (Identity) We have $A \subseteq A$.
   - Proof: This is trivial, since if $x \in A$ then clearly $x \in A$.
2. (Transitivity) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.
   - Proof: If $x \in A$, then since $A \subseteq B$ by definition we also have $x \in B$. But then since $B \subseteq C$, by definition we have $x \in C$. Therefore, every element of A is an element of C, so $A \subseteq C$.
3. (Cardinality) If $A \subseteq B$, then $\#A \leq \#B$.
   - Proof: If $A \subseteq B$, then every element of A is also an element of B. Thus, trivially, the total number of elements in B is at least as large as the number of elements of A.

- We say that two sets are equal if their elements are the same:
- Definition: If A and B are sets, then we say $A = B$ when every element of A is an element of B and vice versa.
- A straightforward, but surprisingly useful, way to show that two sets are equal is to show that each set is a subset of the other one:
- Proposition (Set Equality and Containment): For any two sets A and B, we have $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.
  - We will remark that this result is essentially just a rephrasing of the definition of set equality. Nonetheless, we will go carefully through the argument as a way of illustrating how to give a formal argument for a statement of this sort.
  - Proof: First suppose $A = B$. Then by definition of set equality, for any element $x \in A$ we have $x \in B$.
  - Thus by the definition of subset, we see $A \subseteq B$.
  - In the same way, for any $y \in B$ we have $y \in A$, and therefore $B \subseteq A$. Therefore $A \subseteq B$ and $B \subseteq A$, as required.
  - For the other direction, suppose $A \subseteq B$ and $B \subseteq A$.
  - For any element $x \in A$, then because $A \subseteq B$, we have $x \in B$.
  - Conversely, for any element $x \in B$, then because $B \subseteq A$, we have $x \in A$.

- Therefore, by the definition of set equality, we have $A = B$, as claimed.

- From the proposition above, if we are asked to show that two sets A and B are equal, a natural approach is to show the two containments $A \subseteq B$ and $B \subseteq A$. Here is a simple example of an argument of this form:

- Example: Show that the sets $S = \{2\}$ and $S = \{n \in \mathbb{Z} : n \text{ is both a prime number and even}\}$ are equal.

  - We show separately the two containments $S \subseteq T$ and $T \subseteq S$.
  - To show $S \subseteq T$, we simply observe that 2 is both a prime number and even: this tells us that every element of S is contained in T.
  - To show $T \subseteq S$, suppose n is both a prime number and even. If $n \geq 4$, then since n is even we can write $n = 2k$ where k is a positive integer greater than 1. But this would contradict the assumption that n is a prime number, so we cannot have $n \geq 4$. This leaves only the possibility that $n = 2$, and so we see $T \subseteq S$.
  - Since we have shown $S \subseteq T$ and $T \subseteq S$, we conclude $S = T$.

- As a final remark, we emphasize that it is very important not to mix up the statements $A \subseteq B$ (A is a subset of B) and $A \in B$ (A is an element of B), especially because we often use the same word "contains" to refer to both of them.

  - In many cases the sense of the word "contains" is clear from context because there will be only one meaningful way to interpret a statement.
  - For example, if B is a set of numbers, then if we say "B contains 5", then clearly this means $5 \in B$ because the statement $5 \subseteq B$ does not make sense (because 5 is not a set). If we say "B contains $\{1, 2\}$" then clearly this means $\{1, 2\} \subseteq B$ because we could not have $\{1, 2\} \in B$ (because $\{1, 2\}$ is not a number).
  - On the other hand, if B is a set some of whose elements are also sets, confusion can arise.
  - For example, if $B = \{1, 2, \{2\}, 3, \{2, 3\}\}$, then we have $2 \in B$, $\{2\} \subseteq B$, $\{2\} \in B$, $3 \in B$, $\{3\} \subseteq B$, $\{3\} \notin B$, $\{2, 3\} \in B$, $\{2, 3\} \subseteq B$, and $\{\{2, 3\}\} \subseteq B$.
  - Because of the possibility of confusion, it is best always to identify the type of containment (i.e., as an element or as a subset) when working with sets containing other sets.

1.3.3 Intersections and Unions

- Given two sets A and B, we can construct new sets from them in various ways. Two fundamental constructions are the union and intersection:

- Definition: For any two sets A and B, the intersection $A \cap B$ is defined to be the set whose elements are elements in both A and B, and the union $A \cup B$ is defined to be the set whose elements are in either A or B (or both).

  - More formally, we have $x \in A \cap B$ if and only if $x \in A$ and $x \in B$, while $x \in A \cup B$ if and only if $x \in A$ or $x \in B$.
  - In symbols, $(x \in A \cap B) \Leftrightarrow (x \in A) \wedge (x \in B)$ and $(x \in A \cup B) \Leftrightarrow (x \in A) \vee (x \in B)$.

- Here are a few examples of intersections and unions:

  - Example: If $A = \{1, 2, 3\}$ and $B = \{1, 4, 5\}$, then $A \cap B = \{1\}$ and $A \cup B = \{1, 2, 3, 4, 5\}$.
  - Example: If $A = \{1, 2, 3\}$ and $D = \{1, 2, 3, 4, 5\}$, then $A \cap D = \{1, 2, 3\} = A$ and $A \cup D = \{1, 2, 3, 4, 5\} = D$. Notice here that A is a subset of D, and $A \cap D = A$ with $A \cup D = D$.
  - Example: If $E = \{2, 4, 6, 8, \dots\}$ is the set of all positive even integers and $O = \{1, 3, 5, 7, \dots\}$ is the set of all positive odd integers, then $O \cap E = \emptyset$ is the empty set (no integer is both even and odd), while $O \cup E = \{1, 2, 3, 4, \dots\} = \mathbb{Z}_+$ is the set of all positive integers.
  - Example: If $E = \{2, 4, 6, 8, \dots\}$ is the set of all positive even integers and $S = \{0, 1, 4, 9, 16, \dots\}$ is the set of all perfect squares, then $E \cap S = \{4, 16, 36, 64, \dots\}$ is the set of all positive even perfect squares.

- There are various relationships between subsets, intersections, and unions, including the observations made in the second example above:
- Proposition (Subsets, Intersection, Union): For any sets A and B, the following hold:

  1. $A \cap B$ is a subset of both A and B.
     - Proof: If $x \in A \cap B$, then by definition $x \in A$ and $x \in B$. Therefore, every element of $A \cap B$ is an element of A (meaning $A \cap B \subseteq A$) and every element of $A \cap B$ is an element of B (meaning $A \cap B \subseteq B$).
  2. A and B are both subsets of $A \cup B$.
     - Proof: If $x \in A$ then by definition $x \in A$ or $x \in B$. Thus every element of A is an element of $A \cup B$, meaning $A \subseteq A \cup B$. The same applies if $x \in B$ so we also see $B \subseteq A \cup B$.
  3. $A \subseteq B$ if and only if $A \cap B = A$.
     - Proof: Since the statement is an "if and only if" we must show that $A \subseteq B$ implies $A \cap B = A$, and also that $A \cap B = A$ implies $A \subseteq B$.
     - So first suppose $A \subseteq B$. If $x \in A$, then by the definition of $A \subseteq B$, we know that $x \in B$. Therefore, $x \in A$ and $x \in B$ so by definition, $x \in A \cap B$. This shows $A \subseteq A \cap B$. Since $A \cap B \subseteq A$ by (1), we conclude $A \cap B = A$ as required.
     - Now suppose $A \cap B = A$. Then in particular, $A \subseteq A \cap B$: therefore, for any $x \in A$, we have $x \in A \cap B$. This means that if $x \in A$, we have $x \in A$ and $x \in B$. Therefore $x \in A$ implies $x \in B$, and so $A \subseteq B$ as claimed. This establishes both implications of (3).
  4. $A \subseteq B$ if and only if $A \cup B = B$.
     - Proof: This statement follows using arguments very similar to those we just gave for (3).

  - Remark: Statements (3) and (4) can be thought of intuitively as follows: if every element of A is contained in B, then the elements common to both are simply the elements of A, while the elements in at least one of the two are simply the elements of B. The proofs above are simply formalizations of these ideas.

- Because the intersection and union are defined in terms of simple statements using the logical operators $\wedge$ and $\vee$, many of the properties of $\wedge$ and $\vee$ carry over to intersection and union. Explicitly, we have:
- Proposition (Unions and Intersections): For any sets A, B, and C, the following hold:

  1. (Commutative Laws) We have $A \cap B = B \cap A$ and $A \cup B = B \cup A$.
     - One option to establish these equalities is to show each pair of containments (namely, $A \cap B \subseteq B \cap A$ and $B \cap A \subseteq A \cap B$ along with the analogous statements with unions). We will instead establish the equality directly using a chain of equivalences.
     - Proof: Observe that $x \in A \cap B$ is equivalent to $(x \in A) \wedge (x \in B)$ by the definition of intersection, and this statement is equivalent to $(x \in B) \wedge (x \in A)$ by the commutative property of $\wedge$, and this statement is equivalent to $x \in B \cap A$ by the definition of intersection.
     - Therefore, we see that $x \in A \cap B$ is equivalent to $x \in B \cap A$, and so the sets $A \cap B$ and $B \cap A$ are the same.
     - The argument for showing $A \cup B = B \cup A$ is the same, upon replacing $\cap$ and $\wedge$ with $\cup$ and $\vee$ respectively.
  2. (Associative Laws) We have $(A \cap B) \cap C = A \cap (B \cap C)$ and $(A \cup B) \cup C = A \cup (B \cup C)$.
     - Proof: We have a chain of equivalences, as follows:

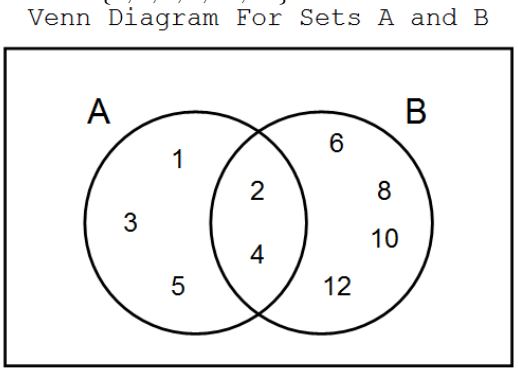
$$\begin{array}{lrl} x \in (A \cap B) \cap C & \text{if and only if} & (x \in A \cap B) \wedge (x \in C) \quad \text{(def. of } (A \cap B) \cap C\text{)} \\ & \text{if and only if} & [(x \in A) \wedge (x \in B)] \wedge (x \in C) \quad \text{(def. of } A \cap B\text{)} \\ & \text{if and only if} & (x \in A) \wedge [(x \in B) \wedge (x \in C)] \quad \text{(associative law for } \wedge\text{)} \\ & \text{if and only if} & (x \in A) \wedge (x \in B \cap C) \quad \text{(def. of } B \cap C\text{)} \\ & \text{if and only if} & x \in A \cap (B \cap C) \quad \text{(def. of } A \cap (B \cap C)\text{)} \end{array}$$

- From this chain of equivalences we conclude that $x \in (A \cap B) \cap C$ is equivalent to $x \in A \cap (B \cap C)$, and so the sets $(A \cap B) \cap C$ and $A \cap (B \cap C)$ are the same.
- The argument for showing $(A \cup B) \cup C = A \cup (B \cup C)$ is the same, upon replacing $\cap$ and $\wedge$ with $\cup$ and $\vee$ respectively.

3. (Absorption + Empty Set) We have $A \cap A = A = A \cup A$, $A \cap \emptyset = \emptyset$, and $A \cup \emptyset = A$.
   - Proof: Observe that $x \in A$ is equivalent to $(x \in A) \wedge (x \in A)$ and $(x \in A) \vee (x \in A)$ by the absorption properties of $\wedge$ and $\vee$ respectively. Thus, $A \cap A = A$ and $A \cup A = A$ as required.
   - The other properties follow immediately from parts (3) and (4) of the previous proposition and the fact that $\emptyset \subseteq A$.
4. (Distributive Laws) We have $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
   - Proof: Like in (1) and (2) above, it is straightforward to construct a chain of equivalences for each of these statements, invoking the distributive laws for $\wedge$ and $\vee$ in the middle, to obtain these results.
5. (Minimality) If C is any set with $C \subseteq A$ and $C \subseteq B$, then $C \subseteq A \cap B$. Likewise, if D is any set with $A \subseteq D$ and $B \subseteq D$, then $A \cup B \subseteq D$.
   - Proof: Suppose that $C \subseteq A$ and $C \subseteq B$. Then for any $x \in C$, we have $x \in A$ and also $x \in B$, and therefore by the definition of intersection, we have $x \in A \cap B$. Thus, $C \subseteq A \cap B$.
   - The other property follows in essentially the same way.

- Because the associative and commutative laws tell us that the order in which multiple intersections or multiple unions are evaluated does not matter, we can meaningfully say what it means to take the intersection or union of more than 2 sets.
  - Explicitly, the intersection of any collection of sets is the set of elements contained in all of them, while the union of any collection of sets is the set of elements contained in at least one of them.
  - Example: If $A = \{1, 2, 3\}$, $B = \{1, 3, 4\}$, and $C = \{1, 3, 9\}$, then $A \cap B \cap C = \{1, 3\}$ while $A \cup B \cup C = \{1, 2, 3, 4, 9\}$.
  - On the other hand, per the distributive laws, we cannot mix unions and intersections without specifying the order of operations.
  - Example: If $A = \{1, 2, 3\}$, $B = \{1, 3, 4\}$, and $C = \{1, 3, 9\}$, then $(A \cap B) \cup C = \{1, 3\} \cup \{1, 3, 9\} = \{1, 3, 9\}$ while $A \cap (B \cup C) = \{1, 2, 3\} \cap \{1, 3, 4, 9\} = \{1, 3\}$.
  - We can see that the expression "$A \cap B \cup C$" therefore does not make sense[5], because it is not immediately clear which of the two expressions $(A \cap B) \cup C$ and $A \cap (B \cup C)$ it is supposed to mean.

- A very useful tool for visualizing unions and intersections of sets is a Venn diagram, in which we represent each set as a region, with overlaps of regions corresponding to intersections of the sets in such a way that any possible combination of intersections corresponds to an area in the diagram.
  - An example makes the idea clearer than a description in words; here is a Venn diagram corresponding to the sets $A = \{1, 2, 3, 4, 5\}$ and $B = \{2, 4, 6, 8, 10, 12\}$:



[5] It is a moderately common convention that intersections are always performed before unions (much like in the order of operations for arithmetic, in which multiplications are performed before additions), in which case we would always interpret $A \cap B \cup C$ to mean $(A \cap B) \cup C$.

- In the Venn diagram above, we place all of the elements of A into the region (in this case, a circle) labeled A, and likewise we place all the elements of B into the region labeled B, with elements in both sets (i.e., in $A \cap B$) in the overlap between the two regions.

- Using a Venn diagram, we can see that there is a relationship between the cardinalities of A, B, $A \cup B$, and $A \cap B$:

- Theorem (Sizes of Unions and Intersections): If A and B are any sets, then $\#(A \cup B) + \#(A \cap B) = \#A + \#B$.

  - Proof: Observe that if we count the total number of elements in A and add it to the total number of elements in B, then we have counted every element in the union $A \cup B$ (since every element in $A \cup B$ is either in A or in B) but we have double-counted the elements in the intersection $A \cap B$.
  - Therefore, both expressions $\#(A \cup B) + \#(A \cap B)$ and $\#A + \#B$ count every element in $A \cap B$ twice and every other element once, so they are equal.

- Example: A survey of 100 pet owners shows that 55 own a cat and 61 own a dog, and none have any other pets. How many owners have both a cat and a dog?

  - If we let A denote the set of cat owners in the survey and B denote the set of dog owners in the survey, then the given information says that $\#A = 55$, $\#B = 61$, and $\#(A \cup B) = 100$.
  - Therefore, we see that $\#(A \cap B) = \#A + \#B - \#(A \cup B) = 55 + 61 - 100 = 16$, meaning that $\boxed{16}$ owners have both a cat and a dog.

- As a corollary of the theorem above, we obtain a useful formula about the sizes of nonintersecting sets.

- Definition: If A and B are sets with $A \cap B = \emptyset$, we say A and B are disjoint sets.

  - From the definition, two sets are disjoint precisely when they have no elements in common. Thus, for example, the sets $\{1, 2, 3\}$ and $\{4, 5, 6\}$ are disjoint.

- Corollary (Unions of Disjoint Sets): If A and B are disjoint sets, then $\#(A \cup B) = \#A + \#B$.

  - Proof: If A and B are disjoint then $A \cap B = \emptyset$ so $\#(A \cap B) = 0$. Then the desired statement follows immediately from the cardinality formula for unions and intersections above.

1.3.4 Complements and Universal Sets

- So far we have given constructions for new sets (namely, the intersection and union) using the logical operators $\wedge$ and $\vee$.

  - It is natural to wonder: why have we not explained how to use the operator $\neg$ to construct new sets?
  - Here is a sensible-seeming definition: define the complement of A, denoted A^c, to be the set of all elements not in A. In symbols, we would say that $(x \in A^c) \Leftrightarrow \neg(x \in A)$ for any x.
  - One reason this definition is a poor choice is that it not generally useful. To illustrate, suppose $A = \{1, 2, 3, 4, 5\}$: then, according to the definition given, the elements of A^c include 6, 7, 8, 9, 10, but also -2, $4/3$, π, $\sqrt{3}$, potato, clock, and the set containing every dog on the planet named Fido.
  - Perhaps it might be useful to consider the set containing this wide and varied selection of elements, but it is more likely that we are only interested in the elements not in A that are integers (or perhaps real numbers).

- A better approach is, instead, to decide ahead of time what sorts of elements we are interested in discussing, and only take the elements not in A inside this specific "universe".

  - It might seem convenient if we could use same universal set in all contexts.
  - However, it turns out that assuming that there exists a general "universal set" of all possible elements leads to a logical contradiction, as first observed by Bertrand Russell.

- Theorem (Nonexistence of a Set of All Sets): There cannot exist a set of all sets (i.e., a set U such that every other set is an element of U).
  - Proof: We show the result by contradiction, so assume to the contrary that there does exist a set of all sets U.
  - Since U is itself a set, by definition it is an element of itself.
  - Define the set T to be the subset of U consisting of all sets (such as U) that do contain themselves as an element, and take T^c to be its complement, consisting of all sets (such as the set $\{1, 2, 3\}$) that do not contain themselves as an element.
  - Now we ask: is T^c an element of T^c?
  - If $T^c \in T^c$, then by definition, T^c would be a set that contains itself. But then, because T^c is the set of all sets that do *not* contain themselves, we would have $T^c \notin T^c$. This is a contradiction, because we assumed $T^c \in T^c$.
  - If $T^c \notin T^c$, then by definition, T^c is a set that does not contain itself. But then, by the definition of T^c, this would mean $T^c \in T^c$. This is also a contradiction, because we assumed $T^c \notin T^c$.
  - Either case leads to a logical contradiction, so there cannot exist a universal "set of all sets" U.
- With this particular issue about universal sets noted, we can give the proper definition of the complement of a set:
- Definition: If U is a universal set and $A \subseteq U$, then the complement of A (as a subset of U), denoted as A^c, is the set of elements of U not in A. In symbols, $(x \in A^c) \Leftrightarrow \neg(x \in A)$ for any $x \in U$.
  - Notation: Other notations used for the complement of A as a subset of U include A', $\overline{A}$, $U \backslash A$, and $U - A$.
  - Remark: We must always specify what the universal set U is. In some cases, there might be a natural choice based on context: if we are discussing sets of integers, a sensible assumption often is that $U = \mathbb{Z}$. However, even if we are only discussing integers, there is no reason that we couldn't instead take $U = \mathbb{Q}$ or $U = \mathbb{R}$, and for this reason it is best always to specify precisely what U is.
  - Example: With universal set $U = \{1, 2, 3, 4, 5, 6\}$, if $A = \{1, 3, 4\}$ and $B = \{1, 2, 3, 4, 5, 6\}$, then $A^c = \{2, 5, 6\}$ and $B^c = \emptyset$.
- We collect a number of basic properties of sets and their complements:
- Proposition (Properties of Complements): For any sets A and B inside a universal set U, the following hold:
  1. (Identity/Absorption) We have $A \cap U = A$ and $A \cup U = U$.
     - Proof: These properties follow immediately from the fact that $A \subseteq U$ and parts (3) and (4) of the proposition about subsets, intersection, and union.
  2. (Double Negative) We have $(A^c)^c = A$.
     - Proof: Observe that $x \in (A^c)^c$ if and only if $\neg(x \in A^c)$ if and only if $\neg(\neg(x \in A^c))$, and the latter is equivalent to $x \in A$ by the double-negative property of $\neg$.
  3. (Inverse) We have $A \cap A^c = \emptyset$ (i.e., A and A^c are disjoint sets) and $A \cup A^c = U$.
     - Proof: Observe that $x \in A \cap A^c$ if and only if $(x \in A) \wedge (x \in A^c)$ if and only if $(x \in A) \wedge \neg(x \in A)$, and this last statement is always false because $P \wedge \neg P$ is always false for any proposition P.
     - Therefore, the statement $x \in A \cap A^c$ is always false, meaning that $A \cap A^c = \emptyset$.
     - In a similar way, we can see that $x \in A \cup A^c$ is always true for any $x \in U$, meaning that $A \cup A^c = U$.
  4. (De Morgan's Laws) We have $(A \cap B)^c = A^c \cup B^c$ and $(A \cup B)^c = A^c \cap B^c$.
     - Proof: Like the above, we have a chain of equivalences as follows: for any $x \in U$,

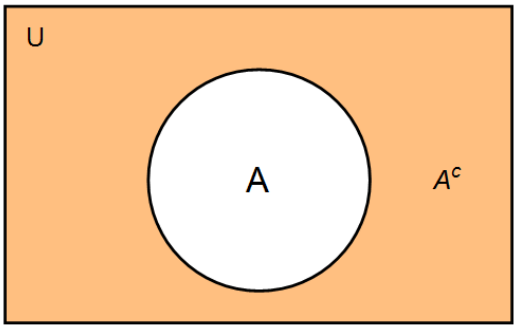
$$\begin{array}{rlrl} x \in (A \cap B)^c & \text{if and only if} & \neg(x \in A \cap B) & \text{(def. of } (A \cap B)^c\text{)} \\ & \text{if and only if} & \neg[(x \in A) \wedge (x \in B)] & \text{(def. of } A \cap B\text{)} \\ & \text{if and only if} & \neg(x \in A) \vee \neg(x \in B) & \text{(de Morgan's law).} \\ & \text{if and only if} & (x \in A^c) \vee (x \in B^c) & \text{(def. of } A^c \text{and } B^c\text{)} \\ & \text{if and only if} & x \in A^c \cup B^c & \text{(def. of } A^c \cup B^c\text{)} \end{array}$$

- Therefore, $x \in (A \cap B)^c$ is equivalent to $x \in A^c \cup B^c$, and so $(A \cap B)^c = A^c \cup B^c$ as claimed.
- The statement $(A \cup B)^c = A^c \cap B^c$ follows in the same way.

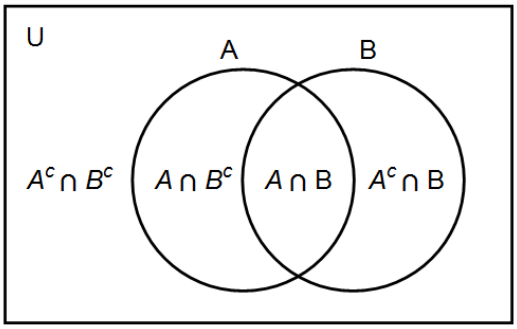
5. We have $\#A + \#A^c = \#U$. In particular, if A is finite, then $\#A^c = \#U - \#A^c$.
   - Proof: Since A and A^c are disjoint by (3) above, the cardinality formula for disjoint sets immediately yields $\#A + \#A^c = \#(A \cup A^c) + \#(A \cap A^c) = \#U + 0 = \#U$ as required.
   - If A is a finite set, then we may subtract $\#A$ from both sides, yielding $\#A^c = \#U - \#A$.

- We can easily visualize many of these properties using Venn diagrams.
  - In a Venn diagram, we typically identify the universal set U in the corner of the diagram, and (from our interpretation of A^c as all the elements of U not in A) we represent A^c as the area outside the region marked as A.
  - It is then clear from the diagram, for example, that $\#U = \#A + \#A^c$, since both sides count the total number of elements in the entire Venn diagram:

Venn Diagram For A and A^c



Venn: Unions and Intersections



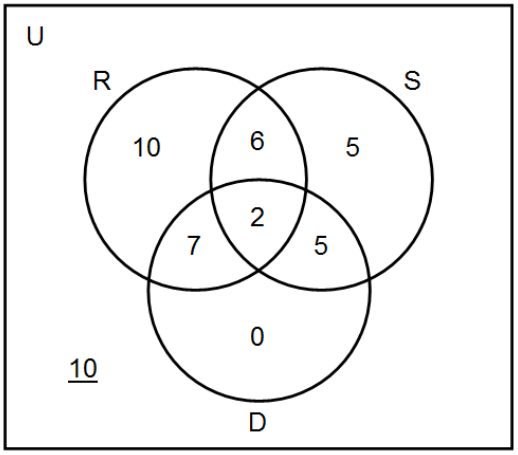
  - If we draw the Venn diagram for two sets A and B, we can also label each region using intersections as shown above.
  - Notice that $A \cap B^c$ is the region inside A and outside B (consistent with the definition of $A \cap B^c$ as the set of all elements in A and in B^c), while $A^c \cap B$ is the region outside A and inside B and $A^c \cap B^c$ is the region outside both A and B.
  - We can then immediately verify many of the results above using the Venn diagram.
  - For example, observe that $(A \cup B)^c$ by definition consists of the region outside $A \cup B$: since $A \cup B$ consists of the three regions $A \cap B^c$, $A \cap B$, and $A^c \cap B$, this means $(A \cup B)^c$ consists of the single remaining region $A^c \cap B^c$. This means $(A \cup B)^c = A^c \cap B^c$, which is one of de Morgan's laws.
  - We will note that properties of intersections, unions, and complements are easy to visualize using Venn diagrams; however, to prove such properties, we must work with the actual definitions. It is worth observing, though, that we can often gain intuition about what is going on by consulting a Venn diagram.

- Venn diagrams also provide us with an easy method for solving problems that involve overlapping categories (with the idea being that instead of listing all of the elements, we can simply identify each region's cardinality):

- Example: In a literature class, a total of 45 short stories are read. Of these, 25 are romantic, 18 are science fiction, and 14 are dystopian. Furthermore, 8 of the science fiction stories are romantic, 2 of which are also dystopian; also, every dystopian story is either romantic or science fiction, and there are 7 dystopian science fiction stories. Determine the number of short stories that are (i) romantic or dystopian, (ii) non-dystopian science fiction, (iii) either romantic or dystopian but not science-fiction, and (iv) none of the three categories.
  - If we let U be the set of the 45 short stories, R be the romantic stories, S be the science-fiction stories, and D be the dystopian stories, we can make a Venn diagram and label various regions with the corresponding number of stories.
  - From the given information, we know that $\#U = 45$, $\#R = 25$, $\#S = 18$, $\#D = 14$, $\#(R \cap S) = 8$, $\#(R \cap S \cap D) = 2$, $\#(S \cap D) = 7$, and that $\#(D \cap R^c \cap S^c) = 0$ (because there are no stories that are dystopian, but not romantic and not science fiction).

- We can use this information to label the cardinalities of some regions in the Venn diagram. For example, since $\#(R \cap S \cap D) = 2$ and $\#(R \cap S) = 8$, this means that the number of elements in $R \cap S$ not in D must be $8 - 2 = 6$. Similarly, since $\#(S \cap D) = 7$, this means that the number of elements in $S \cap D$ not in R must be $7 - 2 = 5$.
- Then since the total number of elements in S is equal to 18, we see that the number of elements in S not in R or D must be $18 - 6 - 2 - 5 = 5$. Continuing in this way, we can fill in all of the remaining entries inside the R, S, and D regions:

Venn Diagram For Short Stories



- Then we see that the number of short stories that are romantic or dystopian is $10+6+7+2+5+0 = \boxed{30}$, the number of non-dystopian science fiction is $6 + 5 = \boxed{11}$, the number of stories that are romantic or dystopian but not science-fiction is $10+7+0 = \boxed{17}$, and the number of stories outside the three categories is $\boxed{10}$.

1.3.5 Cartesian Products

- There are a few additional concepts related to sets that we will use later. First is the idea of an ordered pair:
- "Definition": If A is a set with a and b elements of A, the ordered pair with first coordinate a and second coordinate b is (a, b). Two ordered pairs (a, b) and (c, d) are equal precisely when their corresponding elements are equal (i.e., when $a = c$ and $b = d$).
  - In particular, (a, b) and (b, a) are different ordered pairs unless $a = b$; this difference is the reason for the term "ordered pair".
  - We remark that (much like our "definition" of a set) this definition is not really rigorous. The key statement is that $(a, b) = (c, d)$ is equivalent to $a = c$ and $b = d$.
  - In fact, it is possible to define ordered pairs in terms of sets[6], but there are various tedious details to be checked (which are irrelevant for our purposes), so we will simply take the definition as given above.
- The collection of all ordered pairs with coordinates from two given sets is known as the Cartesian product:
- Definition: If A and B are any sets, the Cartesian product is the set $A \times B$ consisting of all ordered pairs (a, b) where $a \in A$ and $b \in B$. In set-builder notation, $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$.
  - Example: If $A = \{1, 2\}$ and $B = \{1, 3, 5\}$, then $A \times B = \{(1, 1), (1, 3), (1, 5), (2, 1), (2, 3), (2, 5)\}$.
  - Example: If $A = \{\text{Heads}, \text{Tails}\}$ then $A \times A = \{(\text{Heads}, \text{Heads}), (\text{Heads}, \text{Tails}), (\text{Tails}, \text{Heads}), (\text{Tails}, \text{Tails})\}$.

[6] Here is a construction of ordered pairs due to Kuratowski: define $(a, b)_K = \{\{a\}, \{a, b\}\}$. Then we may extract the "first coordinate" a from the ordered pair by observing that for all elements E in $(a, b)_K$, we have $a \in E$, and we may extract the "second coordinate" b in a similar (but more complicated) manner. One may then show that $(a, b)_K = (c, d)_K$ is logically equivalent to $a = c$ and $b = d$, and so this construction has the desired property of ordered pairs. Some care is required with this argument, because if $a = b$ then $(a, b)_K = \{\{a\}\}$ only has a single element, and also, a and b could themselves be arbitrary sets (e.g., it could be that $a = \{b, \{b\}, \{b, \{b\}\}\}$ where $b = \{\emptyset, \{\emptyset\}\}$) and so the elements in the set $(a, b)_K$ could potentially interact with one another in peculiar ways.

- A common use of the Cartesian product is to list all possible outcomes when one event is followed by another. The second example above indicates the possible outcomes of flipping one coin followed by flipping another coin.
- Example: The set $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ is the set of all ordered pairs of positive integers. Explicitly, we have $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} = \{(1,1), (1,2), (1,3), \ldots, (2,1), (2,2), (2,3), \ldots, (3,1), \ldots\}$.
- Example: The set $\mathbb{R} \times \mathbb{R}$ is the set of all ordered pairs (x, y) of real numbers. This collection of ordered pairs is the coordinates of the points in the xy-plane (also called the Cartesian plane), and is frequently written as $\mathbb{R}^2$.

- Cartesian products possess a number of basic properties:
- Proposition (Properties of Cartesian Products): For any sets A, B, C, and D, the following hold:

1. (Distributive Laws, I) We have $A \times (B \cap C) = (A \times B) \cap (A \times C)$ and $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
   - Proof: First suppose $(x, y) \in A \times (B \cap C)$. Then by definition of the Cartesian product, $x \in A$ and $y \in B \cap C$, meaning that $y \in B$ and $y \in C$ by the definition of intersection.
   - Hence, again by definition of the Cartesian product, we have $(x, y) \in A \times B$ and also $(x, y) \in A \times C$, and therefore $(x, y) \in (A \times B) \cap (A \times C)$ by the definition of intersection. Thus, $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$.
   - For the other containment, suppose $(x, y) \in (A \times B) \cap (A \times C)$. Then by definition, $(x, y) \in A \times B$ and $(x, y) \in A \times C$, so by the definition of Cartesian product, $x \in A$, $y \in B$, and $y \in C$.
   - Thus, $x \in A$ and $y \in B \cap C$, so $(x, y) \in A \times (B \cap C)$. We conclude $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$, and therefore we have equality.
   - The other statement follows by essentially the same argument.
2. (Distributive Laws, II) We have $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$ and $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.
   - Proof: First suppose $(x, y) \in (A \times B) \cap (C \times D)$. Then $(x, y) \in A \times B$ and $(x, y) \in C \times D$, so by definition of the Cartesian product, $x \in A$ and $y \in B$, and also $x \in C$ and $y \in D$.
   - Thus, $x \in A \cap C$ and $y \in B \cap D$, and so again by definition of the Cartesian product, we have $(x, y) \in (A \cap C) \times (B \cap D)$ as required.
   - For the other containment, suppose $(x, y) \in (A \cap C) \times (B \cap D)$. Then $x \in A \cap C$ and $y \in B \cap D$, so $x \in A$ and $x \in C$, and also $y \in B$ and $y \in D$. Then $(x, y) \in A \times B$ and also $(x, y) \in C \times D$, and therefore $(x, y) \in (A \times B) \cap (C \times D)$ as claimed.
   - For the second statement, if $(x, y) \in A \times B$ then $x \in A$ and $y \in B$. Hence $x \in A \cup C$ and $y \in B \cup D$, and so $(x, y) \in (A \cup C) \times (B \cup D)$. This means $A \times B \subseteq (A \cup C) \times (B \cup D)$.
   - Likewise, we also have $C \times D \subseteq (A \cup C) \times (B \cup D)$. Hence $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$ by the minimality property of union, as required.
   - Remark: We remark that the sets $(A \times B) \cup (C \times D)$ and $(A \cup C) \times (B \cup D)$ are not necessarily equal. For a specific example, if $A = \{1\}$, $B = \{2\}$, $C = \{3\}$, and $D = \{4\}$ then $(A \times B) \cup (C \times D) = \{(1,2), (3,4)\}$ while $(A \cup C) \times (B \cup D) = \{(1,2), (3,2), (1,4), (3,4)\}$. In fact, the correct general statement is $(A \cup C) \times (B \cup D) = (A \times B) \cup (A \times D) \cup (C \times B) \cup (C \times D)$.
3. (Empty Set) We have $A \times \emptyset = \emptyset \times A = \emptyset$.
   - Proof: By definition, the set $A \times \emptyset$ consists of all ordered pairs (x, y) where $x \in A$ and $y \in \emptyset$.
   - Since the second statement (namely, $y \in \emptyset$) cannot be true, there are no ordered pairs (x, y) in $A \times \emptyset$, and thus $A \times \emptyset = \emptyset$.
   - In the same way, we see that $\emptyset \times A = \emptyset$.
4. (Cardinality) The cardinality of $A \times B$ is given by $\#(A \times B) = \#A \cdot \#B$, if we adopt the convention that $0 \cdot \infty = 0$.
   - Proof: From (3) above, we know that $\#(A \times B) = 0$ if $A = \emptyset$ or $B = \emptyset$, regardless of the cardinality of the other set.
   - Now assume A and B are nonempty. If both sets are finite, then we may arrange the elements of $A \times B$ in a rectangular array with rows labeled by the elements of A and columns labeled by the elements of B.

- Every element of $A \times B$ appears in the array precisely once, and so the cardinality of $A \times B$ is the total number of elements in the array, which is $\#A \cdot \#B$. Thus, $\#(A \times B) = \#A \cdot \#B$ in this case.
- Now suppose both sets are nonempty and at least one set is infinite. If A is infinite, then $A \times B$ contains the infinitely many elements of the form (a, b_1) for arbitrary $a \in A$ and a fixed $b_1 \in B$, while if B is infinite, then $A \times B$ contains the infinitely many elements of the form (a_1, b) for arbitrary $b \in B$ and a fixed $a_1 \in A$. In both cases, we see $\#(A \times B)$ is infinite, as required.
- We conclude that in all cases (subject to the convention $0 \cdot \infty = 0$) we have $\#(A \times B) = \#A \cdot \#B$.
- Remark: This result about the cardinality of $A \times B$ is one reason we refer to this set using the word "product".

1.4 Quantifiers

- In this section we will discuss quantifiers, which are logical operators that allow us to describe propositional statements about "all possible" values of a variable at once.

1.4.1 Quantifiers and Variables

- We have already encountered numerous examples of propositional statements that involve variables.
  - For example, the proposition P that says "n is a prime number" involves the variable n.
  - The truth value of P clearly depends on the specific value of the variable. If $n = 3$, then P is true, while if $n = 4$, then P is false.
  - In cases where propositions depend on variables, we usually want to identify this dependence explicitly: thus, rather than saying P is the proposition "n is a prime number", we could instead define $P(n)$ to be the proposition "n is a prime number".
  - Then, rather than writing out "if $n = 3$, then P is true" and "if $n = 4$, then P is false" we can simply say "$P(3)$ is true" and "$P(4)$ is false".
- Many of our theorems' statements use statements involving variables, and they frequently make assertions about how many values of the input variables make the statements true.
  - For example, take $T(a, b, c)$ to be the statement "a and b are the lengths of the legs of a right triangle and c is the length of the hypotenuse", and $E(a, b, c)$ be the statement "$a^2 + b^2 = c^2$".
  - Then the Pythagorean theorem reads as follows: "For any a, b, and c, $T(a, b, c)$ implies $E(a, b, c)$".
  - As another example, if $I(n)$ is the statement "n is an even integer greater than 2", and $S(n)$ is the statement "n is the sum of two prime numbers", then Goldbach's conjecture states "For every n, $I(n)$ implies $S(n)$".
  - As a third example, if $P(k)$ is the statement "k is a prime number", then Euclid's theorem on the infinitude of prime numbers can be phrased as "There exist infinitely many integers k for which $P(k)$ is true".
- The phrases "for any", "for every", and "there exist" are examples of quantifiers: they give a numeral statement about (i.e., they quantify) the number of values of the variable for which the proposition is true.
  - The quantifiers "for any" and "for every" both signify that the proposition is universally true for any value of the input variable. We refer to this quantifier (often also called "for all") as the universal quantifier, and denote it as $\forall$ (an upside-down letter A, standing for the word "all").
  - The quantifier "there exists" signifies that the proposition is true for at least one possible value of the input variable. We refer to this quantifier as the existential quantifier, and denote it as $\exists$ (a backwards letter E, standing for the word "exists").
- Here are more formal descriptions of how we use and refer to these quantifiers:

- Notation: Suppose U is a universal set and $P(x)$ is a proposition. The statement $\forall x\, P(x)$, read as "for all x, $P(x)$", means that for any $x \in U$ the statement $P(x)$ is true. The statement $\exists x\, P(x)$, read as "there exists an x where $P(x)$", means that there is some element $x \in U$ for which the statement $P(x)$ is true.
  - In some cases, to make the logical statements easier to parse, we will add commas or parentheses to quantified statements; commas do not change the statement's meaning, while parentheses give a clearer indication about how quantifiers are applying to statements.
  - Thus, $\forall n$, $P(n)$ means the same thing as $\forall n\, P(n)$: namely, "for all n, $P(n)$ is true", while $\forall n\, (P(n) \Rightarrow Q(n))$ means "for all n, the statement $P(n)$ implies the statement $Q(n)$".
  - By convention, we view the statements $\forall x$ and $\exists x$ as "binding" the variable x in the statements that follow, and thus we may replace all instances of the variable name with a different one without changing the meaning of the statement.
  - Thus, for example $\forall n\, P(n)$, $\forall x\, P(x)$, and $\forall (\star)\, P(\star)$ are all logically equivalent, regardless of what the proposition P says.
- Example: Suppose U is the set of positive integers and $P(n)$ is the statement "n is a prime number". Determine the meanings and truth values of (i) $\forall n\, P(n)$, (ii) $\exists n\, P(n)$, and (iii) $\exists m\, P(m)$.
  - The statement $\forall n\, P(n)$ means "for every positive integer n, n is a prime number", which is $\boxed{\text{false}}$.
  - The statement $\exists n\, P(n)$ means "there exists a positive integer n for which n is a prime number", which is $\boxed{\text{true}}$.
  - The statement $\exists m\, P(m)$ means "there exists a positive integer m for which m is a prime number", which is $\boxed{\text{true}}$, and is logically equivalent to the previous statement.
- Example: Suppose U is the set of real numbers, $Q(x)$ is the statement "$1 < x < 2$", and $R(x)$ is the statement "$x^2 < 3$". Determine the meanings and truth values of (i) $\forall x\, Q(x) \Rightarrow R(x)$, (ii) $\exists x\, Q(x) \Rightarrow R(x)$, (iii) $\forall x\, R(x) \vee Q(x)$, and (iv) $\exists x\, R(x) \wedge \neg Q(x)$.
  - The statement $\forall x\, Q(x) \Rightarrow R(x)$ means "for all real numbers x, the statement $1 < x < 2$ implies that $x^2 < 3$", which is $\boxed{\text{false}}$ because it is not the case that every real number x with $1 < x < 2$ has $x^2 < 3$ (for example, $x = 1.8$ has $1 < x < 2$ but $x^2 = 3.24$ is not less than 3).
  - The statement $\exists x\, Q(x) \Rightarrow R(x)$ means "there exists a real number x such that the statement $1 < x < 2$ implies that $x^2 < 3$", which is $\boxed{\text{true}}$ because there is a real number x, namely, $x = 1.5$, such that $1 < x < 2$ and $x^2 < 3$. (In fact there are many such real numbers x.)
  - The statement $\forall x\, R(x) \vee Q(x)$ means "for all real numbers x, we have $1 < x < 2$ or $x^2 < 3$", which is $\boxed{\text{false}}$ because there exist many real numbers, such as $x = 3$, where $1 < x < 2$ and $x^2 < 3$ are both false.
  - The statement $\exists x\, R(x) \wedge \neg Q(x)$ means "there exists a real number x such that $1 < x < 2$ and where $x^2 < 3$ is false", which is $\boxed{\text{true}}$ (for example, $x = 1.8$ has $1 < x < 2$ while $x^2 < 3$ is false).
- As shorthand, if we wish to restrict further the allowed values of a variable bound by a quantifier, we often label the set S of allowed values with the variable: thus, $\exists x \in S$, $P(x)$ means "there exists an $x \in S$ such that $P(x)$ is true".
  - Example: If U is the universe of real numbers, $\exists x \in \mathbb{Q}$, $x^2 = 2$ means "there exists a rational number x such that $x^2 = 2$".
  - For convenience we will also occasionally write these restrictions in other slightly different ways: for example, $\exists x > 0$, $x^2 = 2$ means "there exists an $x > 0$ such that $x^2 = 2$". (Note that the truth value of this statement will depend on the allowed universe for x, which is no longer clear from the context.)
- We will also remark that the universal quantifier $\forall$ behaves similarly to the operator $\wedge$, while the existential quantifier $\exists$ behaves similarly to the operator $\vee$.
  - The reason for this behavior can be seen in the situation when $U = \{a, b\}$ has two elements: then $\forall x \in U$, $P(x)$ is the same as $P(a) \wedge P(b)$, while $\exists x \in U$, $P(x)$ is the same as saying $P(a) \vee P(b)$.

- When U has more elements (but is still finite), the corresponding statements instead become longer chains connected by $\wedge$ and $\vee$ respectively.
- The real utility of the quantifiers is that they allow us to make statements about all the elements in an arbitrary set in a compact way, whether or not the set is finite, and without having to list a separate statement about every element individually.

1.4.2 Properties of Quantifiers

- Many of our definitions (particularly regarding sets), and consequently many of the corresponding propositions and their proofs, have implicitly used quantifiers.
  - Example: The definition of subset can be written as "$A \subseteq B$ precisely when $\forall x,\, x \in A \Rightarrow x \in B$".
  - Example: The definition of intersection can be written "$\forall x,\, x \in A \cap B \Leftrightarrow [(x \in A) \wedge (x \in B)]$".
- We will now briefly examine some important properties of quantifiers that will allow us to formalize certain useful statements. First, we describe how to negate quantified statements, the procedure for which is easiest to see from an example:
  - Example: What would it mean to say that "for every person P, P likes ice cream" is false? It would mean that there is at least one person P such that P does not like ice cream.
  - Example: What would it mean to say that "there exists a person P such that P likes pickles" is false? It would mean that no person likes pickles, or, equivalently, for any person P, P does not like pickles.
  - In both cases, we see that negating a quantified statement yields another quantified statement with the opposite quantifier. This is in fact true generally:
- Proposition (Negation of Quantifiers): For any universal set U and statement $P(x)$, the negation of $\forall x, P(x)$ is $\exists x, \neg P(x)$ and the negation of $\exists x,\, P(x)$ is $\forall x,\, \neg P(x)$.
  - Proof: First suppose the statement $\forall x\, P(x)$ is true: this means that for every $x \in U$, the statement $P(x)$ is true.
  - This means that there is no $x \in U$ for which $P(x)$ is false, which is to say, there is no $x \in U$ for which $\neg P(x)$ is true.
  - In turn, this means that the statement $\exists x,\, \neg P(x)$ is false. Thus, in this case $\forall x\, P(x)$ has the opposite truth value to $\exists x,\, \neg P(x)$.
  - Now suppose that $\forall x\, P(x)$ is false, meaning that is not the case that for every $x \in U$, the statement $P(x)$ is true.
  - This implies that there must exist at least one $x \in U$ for which the statement $P(x)$ is false, which is to say, there exists $x \in U$ for which $\neg P(x)$ is true.
  - In turn, this means that the statement $\exists x,\, \neg P(x)$ is true. As before, we see that $\forall x\, P(x)$ has the opposite truth value to $\exists x,\, \neg P(x)$.
  - Since $\forall x\, P(x)$ must be either true or false, and $\exists x,\, \neg P(x)$ has the opposite truth value in both cases, we conclude that the negation of $\forall x, P(x)$ is $\exists x, \neg P(x)$.
  - The other statement follows in the same way.
- Example: Write the negations of the statements (i) $\exists y \in \mathbb{R},\, y^2 < 0$ and (ii) $\forall x,\, (x \in A) \Rightarrow (x \in B)$ as equivalent positive statements.
  - For (i), we have $\neg\left[\exists y \in \mathbb{R},\, y^2 < 0\right] = \forall y \in \mathbb{R},\, \neg(\, y^2 < 0) = \forall y \in \mathbb{R},\, y^2 \geq 0$ in symbols.
  - If we translate the statement into English, the original reads "there exists a real number y such that $y^2 < 0$", while the negation is "for all real numbers y, $y^2 \geq 0$".
  - For (ii), we have $\neg[\forall x,\, (x \in A) \Rightarrow (x \in B)] = \exists x,\, \neg[(x \in A) \Rightarrow (x \in B)]$ in symbols.
  - By using the definition of "implies" in terms of "or", we can rewrite $\exists x,\, \neg[(x \in A) \Rightarrow (x \in B)]$ as $\exists x,\, \neg[\neg(x \in A) \vee (x \in B)]$, and then by applying de Morgan's laws and the double negative property, we see $\exists x,\, \neg[\neg(x \in A) \vee (x \in B)]$ is equivalent to $\exists x,\, (x \in A) \wedge (x \notin B)$.

- If we translate the statements into English, the original statement (which is the definition of $A \subseteq B$) says that every element $x \in A$ also has $x \in B$. The negated statement says that there exists an x such that $x \in A$ and $x \notin B$.

- We will often also want to make use of statements that contain multiple quantifiers. It is necessary to take substantial care when analyzing such statements, as we will illustrate with a few examples:

- Example: For $U = \mathbb{Z}$, determine the meanings and truth values of (i) $\forall a \exists b$, $a + b = 1$ and (ii) $\exists a \forall b$, $a + b = 1$.

  - Translating directly into English shows that $\forall a \exists b$, $a + b = 1$ means "for all integers a there exists an integer b such that $a + b = 1$". This statement is $\boxed{\text{true}}$ because no matter what integer a is, the integer $b = 1 - a$ satisfies the requirement that $a + b = 1$.
  - On the other hand, in English the statement $\exists a \forall b$, $a + b = 1$ means "there exists an integer a such that for all integers b, we have $a + b = 1$". This statement is $\boxed{\text{false}}$ because there is no possible integer a such that $a + b = 1$ for *every* integer b. (Certainly, for a single choice of b there is such an a, but that choice does not work for every possible b.)

- Notice that the only difference between the two statements in the example above was the order of the quantifiers. To emphasize, the order in which variables are quantified is *extremely* important and can have a great effect on the truth value of the resulting proposition!

- Example: Suppose U is the set of all people and $M(a, b)$ is the statement "a has given money to b". Identify the meanings of (i) $\exists a \exists b$, $M(a, b)$, (ii) $\exists b \exists a$, $M(a, b)$, (iii) $\forall a \forall b$, $H(a, b)$, and (iv) $\forall b \forall a$, $H(a, b)$.

  - The statement $\exists a \exists b$, $M(a, b)$ means "there exists a person a such that there exists a person b where a has given money to b". Observe that this is equivalent to saying that there exist two people, a and b, where a has given money to b.
  - The statement $\exists b \exists a$, $M(a, b)$ means "there exists a person b such that there exists a person a where a has given money to b". Observe that this is equivalent to saying that there exist two people, a and b, where a has given money to b, which is the same as the statement $\exists a \exists b$, $M(a, b)$ above.
  - The statement $\forall a \forall b$, $H(a, b)$ means "for any person a, it is true that for any person b, a has given money to b". Observe that this is equivalent to saying that for every (ordered) pair of people, a and b, a has given money to b.
  - The statement $\forall b \forall a$, $H(a, b)$ means "for any person b, it is true that for any person a, a has given money to b", which is likewise equivalent to saying that for every (ordered) pair of people, a and b, a has given money to b.
  - We see in both cases that reversing the order of the quantifiers does not change the meaning of the statement.

- The key difference between these two examples of interchanging quantifiers is that the first example (where the order mattered) had quantifiers of different types, while the second example (where the order did not matter) had quantifiers of the same type.

  - This fact is true in general: interchanging the order of quantifiers of different types will yield a statement not logically equivalent to the original, while interchanging the order of quantifiers of the same type will yield a logically equivalent statement.
  - We note that by "interchanging quantifiers" we specifically mean swapping the order of two consecutive quantifiers. In statements with more than two quantifiers, interchanging non-consecutive quantifiers of the same type can alter the meaning.

- By using multiple quantifiers, we can analyze the interaction between quantifiers and statements involving $\wedge$ and $\vee$, which we again motivate using some examples.

  - Example: What would it mean to say that "for every person P, P likes ice cream and P likes potatoes"? Clearly, this statement is the same as saying that everyone likes ice cream, and also everyone likes potatoes. In more explicit quantified language, we could phrase this as "for every person P it is true that P likes ice cream, and also for every person P it is true that P likes potatoes".

- Example: What would it mean to say that "for every person P, P likes ice cream or P likes potatoes"? Unlike the example above, this is certainly not equivalent to "for every person P it is true that P likes ice cream, or for every person P it is true that P likes potatoes": for example, if half of people like ice cream and the other half like potatoes, the first statement would be true but the second would be false.
- Here, we can see that the quantifier $\forall$ distributes over $\wedge$, but not over $\vee$.
- Example: What would it mean to say that "there exists a person P such that P likes ice cream or P likes potatoes"? Clearly, this statement is the same as saying "either there exists a person P who likes ice cream, or there exists a person P who likes potatoes".
- Example: What would it mean to say that "there exists a person P such that P likes ice cream and P likes potatoes"? Unlike before, this is not equivalent to "there exists a person P who likes ice cream, and there exists a person who likes potatoes", because there could be some people who like ice cream and others who like potatoes, but no one who likes both.
- Here, we can see that the quantifier $\exists$ distributes over $\vee$, but not over $\wedge$.

- We can formalize these observations as follows:
- Proposition (Distribution of Quantifiers): For any universal set U and statements $P(x)$ and $Q(x)$, the following hold:

1. The statements $\forall x,\, [P(x) \wedge Q(x)]$ and $[\forall x,\, P(x)] \wedge [\forall x,\, Q(x)]$ are equivalent.
   - Proof: The first statement means that for every $x \in U$, both $P(x)$ and $Q(x)$ are true. This is equivalent to saying that $P(x)$ is true for every $x \in U$, and also $Q(x)$ is true for every $x \in U$, which is the second statement.
2. The statement $[\forall x,\, P(x)] \vee [\forall x,\, Q(x)]$ implies $\forall x,\, [P(x) \vee Q(x)]$, but is not equivalent in general.
   - Proof: The first statement means that either $P(x)$ holds for every $x \in U$, or $Q(x)$ holds for every $x \in U$.
   - If $P(x)$ holds for every $x \in U$, then $P(x) \vee Q(x)$ holds for every $x \in U$, so the second statement is true.
   - Likewise, if $P(x)$ holds for every $x \in U$, then $P(x) \vee Q(x)$ again holds for every $x \in U$, so the second statement is true.
   - Thus, $[\forall x,\, P(x)] \vee [\forall x,\, Q(x)]$ implies $\forall x,\, [P(x) \vee Q(x)]$. Our example above shows that they are not equivalent in general.
3. The statements $\exists x,\, [P(x) \vee Q(x)]$ and $[\exists x,\, P(x)] \vee [\exists x,\, Q(x)]$ are equivalent.
   - Proof: The first statement means that there exists some $x \in U$ such that $P(x)$ is true or $Q(x)$ is true. This is equivalent to saying that $P(x)$ is true for some $x \in U$ or that $Q(x)$ is true for some $x \in U$, which is the second statement.
4. The statement $\exists x,\, [P(x) \wedge Q(x)]$ implies $[\exists x,\, P(x)] \wedge [\exists x,\, Q(x)]$, but is not equivalent in general.
   - Proof: The first statement means that there is some $x \in U$ for which $P(x)$ is true and $Q(x)$ is true.
   - Then $\exists x,\, P(x)$ is true (because there is an x for which $P(x)$ is true) and $\exists x,\, Q(x)$ is also true (because there is an x for which $Q(x)$ is true), so the second statement is true.
   - Thus, $\exists x,\, [P(x) \wedge Q(x)]$ implies $[\exists x,\, P(x)] \wedge [\exists x,\, Q(x)]$. Our example above shows that they are not equivalent in general.

1.4.3 Examples Involving Quantifiers

- With judicious use of quantifiers and logical operators, we can re-express essentially any mathematical statement using purely formal notation.
  - We will remark that many statements have implicit quantifiers, and it is not always obvious how quantifiers are being employed, or how many of them there will be.

- Example: Write the statement "The square of any real number is greater than or equal to zero" in formal notation.

- First, we add variable names and write the quantifiers more explicitly: "For all real numbers x, $x^2 \geq 0$".
- Now we simply translate the quantifiers, yielding the purely formal statement $\boxed{\forall x \in \mathbb{R},\, x^2 \geq 0}$.

- Example: Write "Every even integer greater than 2 can be written as the sum of two prime numbers" in formal notation, writing $E_{>2}$ for the set of even integers greater than 2 and P for the set of primes.
  - First, we add variable names and write the quantifiers more explicitly: "For all even integers n greater than 2, n can be written as the sum of two prime numbers".
  - More formally, this is $\forall n \in E_{>2}$, n can be written as the sum of two prime numbers.
  - We still need to translate the statement "n can be written as the sum of two prime numbers" into formal language.
  - If we label the prime numbers p_1 and p_2, then "n can be written as the sum of two prime numbers" is equivalent to "there exist prime numbers p_1 and p_2 such that $n = p_1 + p_2$". More formally, this reads $\exists p_1 \in P\, \exists p_2 \in P,\, n = p_1 + p_2$.
  - If we put everything together, we get the formal statement $\boxed{\forall n \in E_{>2}\, \exists p_1 \in P\, \exists p_2 \in P,\, n = p_1 + p_2}$.

- Example: Write "Every positive real number has exactly two square roots" in formal notation.
  - First, we add variable names and write the quantifiers more explicitly: "For all positive real numbers x, x has exactly two square roots y and z".
  - Now, saying that y and z are square roots of x is the same as saying $y^2 = x$ and $z^2 = x$.
  - The phrase "x has exactly two square roots y and z" is trickier to reformulate, but it can be expanded to the following: first, $y \neq z$, and also, if a is any other number such that $a^2 = x$, then $a = y$ or $a = z$.
  - Putting all of this together, we obtain the following formal statement: $\forall x \in \mathbb{R}_{>0}\, \exists y \exists z \forall a\,,\, (y^2 = x) \wedge (z^2 = x) \wedge (y \neq z) \wedge [(a^2 = x) \Rightarrow (a = y) \vee (a = z)]$.

- Example (for students who like limits): Analyze the quantifiers in the statement "For any $\epsilon > 0$ there exists $\delta > 0$ such that for any x with $0 < |x - x_0| < \delta$, it is true that $|f(x) - L| < \epsilon$", and then write it in purely formal language.
  - The first quantified variable is ϵ, and it is quantified as "for any", which is the quantifier $\forall$.
  - Next, δ is quantified, with the quantifier $\exists$.
  - After these, x is quantified as "for any", which is also the quantifier $\forall$ (note that its conditions involve the previously-quantified variable δ along with the unquantified variable x_0).
  - Finally, there is the statement involving the unbound variables f and L, which has no quantifiers.
  - Note that although the statements involving $0 < |x - x_0| < \delta$ and $|f(x) - L| < \epsilon$ are not phrased using "if-then" language, we can view the statement as a conditional; namely, as the statement "$0 < |x - x_0| < \delta$ implies $|f(x) - L| < \epsilon$".
  - Thus, a fully symbolic (albeit rather tricky to parse!) version of this statement reads as follows: $\forall \epsilon > 0$, $\exists \delta > 0$, $\forall x$, $[0 < |x - x_0| < \delta] \Rightarrow [|f(x) - L| < \epsilon]$.
  - Remark: The statement is the (in)famous formal ϵ-δ definition of limit (specifically, it is the definition for when the function $f(x)$ has limit L as x approaches x_0), as first stated by Cauchy and used to great effect in the early 1800s in placing calculus on a solid theoretical footing. Although this definition may seem complicated, it is extremely important because it gives a formal and usable definition of limit, on which (in turn) a vast number of other fundamental analytic concepts (such as continuity, convergence, the derivative, and the integral) are based.

- We will remark that in practice, we rarely actually seek to translate mathematical statements into purely formal language like we did above, because such formal statements are harder for humans to read and (much) harder for humans to understand.
  - In principle, such translation is helpful when trying to understand the precise structure of the statement. In practice, however, it is usually simpler to work in regular language most of the time, and sometimes resort to a mix of formal and informal statements when needed to manipulate a complicated statement.

- However, we will also note that there is a very active area of research (namely, automated reasoning and automated theorem proving) on how to design computational algorithms that can provide formal proofs of mathematical statements and the correctness of algorithms. These algorithms (ultimately) operate entirely with formalized statements.
- Many theorems from classical and modern mathematics (such as the fundamental theorem of algebra, the fundamental theorem of calculus, the four-color theorem, and the prime number theorem) have now been formally verified using automated systems, and several previously-unsolved problems (such as Kepler's sphere-packing conjecture) have been completed using formal proof assistants.

1.4.4 Families of Sets

- We now briefly mention a few miscellaneous topics related to families of sets.
  - Consider the set of prime numbers: $P = \{2, 3, 5, 7, 11, \dots\}$. It is natural to label the primes in increasing order as $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, and so forth.
  - Then, for example, the set of the first 5 prime numbers is $\{p_1, p_2, p_3, p_4, p_5\} = \{p_i : 1 \leq i \leq 5\}$.
  - Alternatively, we could identify the specific labels using an indexing set I: in this case, if we wrote $I = \{1, 2, 3, 4, 5\}$, then the set of the first five primes is $\{p_i : i \in I\}$.
  - As long as the identification between elements and indices is clear, we may index over an arbitrary set. (Often, we index over sets of numbers, although in principle we can index over any set.)
- Using indexing sets is especially useful when we consider sets of other sets. A fundamental example is the set of all subsets of a given set:
- Definition: Let A be a set. The power set of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A. Explicitly, $\mathcal{P}(A) = \{x : x \subseteq A\}$.
  - Example: For $A = \{1, 2\}$, the power set is $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.
  - Example: For $B = \{a, b, c\}$, the power set is $\mathcal{P}(B) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.
  - Example: The power set of the empty set is $P(\emptyset) = \{\emptyset\} = \{\{\}\}$, the set containing the empty set.
  - Example: The power set of $\mathbb{Z}_+$ is the set of all sets of positive integers. Some elements of $\mathcal{P}(\mathbb{Z}_+)$ include $\{2, 4, 6, 12\}$, $\{1\}$, the set $\{1, 4, 9, 16, \dots\}$ of squares, the set $\{2, 4, 6, 8, 10, \dots\}$ of even positive integers, the set $\{2, 3, 5, 7, \dots\}$ of prime numbers, and the empty set.
- By using indexing sets, we can extend the definition of intersection and union to arbitrary collections of sets. (We often call a collection of sets a family, to avoid the linguistic confusion of referencing sets of sets.)
- Definition: Suppose that $\mathcal{F}$ is a family of sets F_i indexed by the set I. We define the intersection of the elements of $\mathcal{F}$, denoted by $\bigcap_{i \in I} F_i$, to be the set of all elements common to all the sets F_i; explicitly, $x \in \bigcap_{i \in I} F_i$ if and only if $x \in F_i$ for all $i \in I$. We define the union of the elements of $\mathcal{F}$, denoted by $\bigcup_{i \in I} F_i$, to be the set of all elements in at least one of the F_i; explicitly, $x \in \bigcup_{i \in I} F_i$ if and only if there exists some $i \in I$ with $x \in F_i$.
  - In purely formal language, these definitions are $\forall x, [x \in \bigcap_{i \in I} F_i] \Leftrightarrow [\forall i \in I, x \in F_i]$ and $\forall x, [x \in \bigcup_{i \in I} F_i] \Leftrightarrow [\exists i \in I, x \in F_i]$.
  - Note that if $\mathcal{F} = \{A, B\}$, these definitions reduce to our original definitions of the intersection and union of two sets.
- Example: Let $I = \{1, 2, 3, \dots\}$ be the set of positive integers, and for each $i \geq 1$ let $F_i = \{1, 2, 3, \dots, i\}$ be the positive integers less than or equal to i. Find $\bigcup_{i \in I} F_i$ and $\bigcap_{i \in I} F_i$.
  - For each positive integer n, we have $n \in F_n$, and so the union $\bigcup_{i \in I} F_i = \{1, 2, 3, \dots\} = \mathbb{Z}_+$ is the set of all positive integers. On the other hand, since $F_1 = \{1\}$ and $1 \in F_i$ for all $i \in I$, we have $\bigcap_{i \in I} F_i = \{1\}$.

Well, you're at the end of my handout. Hope it was helpful.