MATH327 Lexicon

Fall 2016

Last Updated:
Thursday 15th September, 2016 at 8:54pm

0 Notation

Definition. The following summarizes the names and notations for standard collections of numbers.

- The **natural numbers** are $\mathbb{N} = \{1, 2, 3, \dots\}$.
- The **integers** are $\mathbb{Z} = \{\cdots - 2, -1, 0, 1, 2, \dots\}$.
- The **rationals**, $\mathbb{Q}$, are ratios of integers with nonzero denominators.
- The **real numbers**, $\mathbb{R}$, are the numbers with decimal representations.
- The **complex numbers**, $\mathbb{C}$, are numbers of the form $x+iy$ where x and y are real numbers and $i^2 = -1$.

1 Logic

1.1 Basic Logic

Definition 1.1. A **proposition** is a declarative sentence which is either true or false.

Class Example 1.1. Examples

1. The capitol of the U.S. is Washington, DC.
2. 14 is odd.
3. 3028009 is prime.
4. I will die on Dec 21, 2022.

Non-Examples:

1. Let $x = 8$
2. How old are you?
3. $3x + 1 = y$.

Definition 1.2. The **negation** of a proposition is a statement having the opposite truth value.

Class Example 1.2. Unuseful negations:

- It is not true that 14 is odd.
- 14 is not odd

Should be: 14 is even.
Example: Negate $x > 0$... $x \leq 0$

Definition 1.3. Logical **AND**, $\wedge$, has truth table given by:

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Logical **OR**, $\vee$, has truth table given by:

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Logical **NOT**, $\neg$, has truth table given by:

P	$\neg P$
T	F
F	T

Note: Order of operations is $\neg$, $\wedge$, $\vee$. So $\neg P \vee Q \wedge R$ is interpreted as $(\neg P) \vee (Q \wedge R)$.

Class Example 1.3. The truth table for $(P \vee Q) \wedge \neg Q$ is given by

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

Example 1.1. Determine which of the following propositions are true and which are false:

1. An apple is a fruit and $4 > \sqrt{10}$.
2. WSU is in Minnesota and $4 < \sqrt{10}$.
3. George Washington was the first president or 8 is even.
4. Germany is a country in Europe or $\pi = 3$.
5. 7 is an even number or $e < 2$.

Example 1.2. Give the negation of the following:

1. We will win the first or second game.
2. Roses are red and violets are blue.
3. The apple is red or it is not yellow.
4. The integer n is even and not a multiple of 5.

Example 1.3. Give an example of the truth table for a propositional form that is a combination of the logical operations $\wedge$, $\vee$, $\neg$, and at least three logical inputs P, Q, and R. (Make sure to indicate intermediate computation steps.)

Example 1.4. Give an example of two logical expressions in P and Q that only disagree on one set of inputs.

Example 1.5. Determine the truth table for $P \vee \neg P$.

Definition. A propositional form that is always true is called a **tautology**.

Definition 1.4. Two propositional forms are **logically equivalent** if and only if they have the same truth table outputs for the same truth table inputs.

Class Example 1.4. Notice $(P \vee Q) \wedge \neg Q$ is equivalent to $P \wedge \neg Q$ since the truth table calculation gives the same result.

P	Q	$\neg Q$	$P \wedge \neg Q$
T	T	F	F
T	F	T	T
F	T	F	F
F	F	T	F

Problem 1.1. *Prove or disprove:* $P \wedge (Q \vee R)$ *is equivalent to* $(P \wedge Q) \vee (P \wedge R)$.

Problem 1.2. *Prove or disprove:* $P \vee (Q \wedge R)$ *is equivalent to* $(P \vee Q) \wedge (P \vee R)$.

Problem 1.3. *Find a propositional form equivalent to* $\neg(P \wedge Q)$ *that does not use parenthesis. Justify your answer.*

Problem 1.4. *Find a propositional form equivalent to* $\neg(P \vee Q)$ *that does not use parenthesis. Justify your answer.*

Definition 1.5. Logical **IMPLIES**, $\Rightarrow$, has truth table given by:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Example 1.6. Give an example of the truth table for a propositional form that is a combination of $\Rightarrow$, at least two of the logical operations $\wedge$, $\vee$, $\neg$, and at least three logical inputs P, Q, and R. (Make sure to indicate intermediate computation steps.)

Problem 1.5. *Express* $P \Rightarrow Q$ *in terms of* $\neg$, $\wedge$, $\vee$ *in a simplified way. Justify your answer.*

Corollary 1.6. *Express* $\neg(P \Rightarrow Q)$ *in terms of* $\neg$, $\wedge$, $\vee$ *in a simplified way. Justify your answer.*

Definition 1.6. The **converse** of $P \Rightarrow Q$ is $Q \Rightarrow P$.

Definition 1.7. The **contrapositive** of $P \Rightarrow Q$ is $\neg Q \Rightarrow \neg P$.

Problem 1.7. *Prove or disprove that an implication is logically equivalent to its converse.*

Problem 1.8. *Prove or disprove that an implication is logically equivalent to its contrapositive.*

Definition 1.8. Logical **If and Only If**, $\Leftrightarrow$ or iff, has truth table given by:

P	Q	$P \Leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

Problem 1.9. *Express* $P \Leftrightarrow Q$ *in terms of* $\neg$, $\wedge$, $\vee$ *in a simplified way. Justify your answer.*

1.2 Predicates and Quantifiers

Definition 1.9. An **open sentence** or **predicate** is a proposition that contains one or more variables and which becomes a proposition only when the variables are replaced by the names of specific objects.

Class Example 1.5. Let $P(x)$ be the predicate $x > 3$. Then $P(4)$ is true, but $P(2)$ is false.

Definition 1.10. The **universe of discourse**, U, is the collection of objects available for consideration in a predicate. The **truth set** of a predicate is the collection of objects from U that make it a true proposition.

Class Example 1.6. Let $P(x)$ be the predicate $x > 3$ with universe of discourse $\mathbb{R}$. Then the truth set is the open interval $(3, \infty)$.

Example 1.7. Give an example of a predicate that has different truth sets in two different universes.

Definition 1.11. With a universe specified, two open sentences $P(x)$ and $Q(x)$ are **equivalent** if and only if they have the same truth set.

Class Example 1.7. The open sentences "$3x + 1 = 7$" and "$8 - x = 6$" are equivalent in the universe of $\mathbb{R}$ since the truth set for both is $\{2\}$.

Example 1.8. Give an example of two open sentences P and Q and two different universes U and V such that P is equivalent to Q in U, but not in V.

Definition 1.12. For a predicate $P(x)$, the proposition $(\exists x)P(x)$, read as "**there exists** x **such that** $P(x)$", is true if and only if the truth set is not empty, i.e. there is at least one element in the universe that makes $P(x)$ true.

Definition 1.13. For a predicate $P(x)$, the proposition $(\exists! x)P(x)$, read as "**there exists a unique** x **such that** $P(x)$", is true if and only if the truth set contains exactly one element of the universe, i.e. there is one and only one x in the universe that makes $P(x)$ true.

Definition 1.14. For a predicate $P(x)$, the proposition $(\forall x)P(x)$, read as "**for all** x**,** $P(x)$" or "**for every** x**,** $P(x)$", is true if and only if the truth set is the whole universe, i.e. all elements of the universe make $P(x)$ true.

Class Example 1.8. The following are true in the given universe:
$(\exists x)(x^2 = 1)$, the integers
$(\exists! x)(x^2 = 1)$, positive real number
$(\forall x)(x^2 \geq 0)$, real numbers

Example 1.9. Label the following as true or false in the universe of real numbers. Explain why.

1. $(\forall x)(x + x \geq x)$
2. $(\exists x)(3^x = x^2)$
3. $(\exists! x)(x \geq 0 \wedge x \leq 0)$
4. $(\forall x)(\exists y)(x + y = 0)$
5. $(\exists x)(\forall y)(x + y = 0)$
6. $(\exists x)(\exists y)(x^2 + y^2 = -1)$

Problem 1.10 (*)**.** *Give a logically equivalent expression to $(\exists! x)P(x)$ that does not use the !. You may use any of the other logical symbols $\exists, \forall, \vee, \wedge, \neg, \Rightarrow$. Justify your answer.*

Problem 1.11 (*)**.** *Give a logically equivalent expression to $\neg(\exists x)P(x)$ that does not use $\exists$. Justify your answer.*

Corollary 1.12. *Give a logically equivalent expression to $\neg(\forall x)P(x)$ that does not use $\forall$. Justify your answer.*

Example 1.10. Give the symbolic negations of the statements in Example 1.9.

1.3 Induction

Requires completion of Extended Set Theory and Basic Number Theory

Principle of Mathematical Induction: If $S \subseteq \mathbb{N}$ such that $1 \in S$ and for all $k \in \mathbb{N}$ $k \in S \Rightarrow k+1 \in S$, then $S = \mathbb{N}$.

Class Example 1.9 (Explicit Demonstration)**.** Consider the statement $P(n) : 1+2+3+\cdots+n = \frac{n(n+1)}{2}$. Let $S = \{n \in \mathbb{N} | P(n)\}$. Then $S = \mathbb{N}$.

Proof. Notice that $P(1)$ is true since $\frac{1(1+1)}{2} = \frac{2}{2} = 1$. Thus $1 \in S$. Now suppose $n \in \mathbb{N}$ such that $n \in S$. Then

$$\begin{aligned} 1+2+3+\cdots+n &= \frac{n(n+1)}{2} \\ 1+2+3+\cdots+n+n+1 &= \frac{n(n+1)}{2} + n + 1 \\ &= \frac{n(n+1)+2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

Hence, $P(n+1)$ is true and thus $n+1 \in S$. So by the Principle of Mathematical Induction, $S = \mathbb{N}$. □

Note: In practical usage rarely is there a reference to a set S or a statement P. In reality, these are implicit in the logic, but never directly stated. The above example should look like the following.

Class Example 1.10 (Practical Demonstration)**.** For all $n \in \mathbb{N}$,

$$1+2+3+\cdots+n = \frac{n(n+1)}{2}.$$

Proof. Notice for $n = 1$, $\frac{1(1+1)}{2} = \frac{2}{2} = 1$. Hence the equality is true for $n = 1$.

Now suppose it is true for some $n = k \in \mathbb{N}$. Then

$$\begin{aligned} 1+2+3+\cdots+k &= \frac{k(k+1)}{2} \\ 1+2+3+\cdots+k+k+1 &= \frac{k(k+1)}{2} + k + 1 \\ &= \frac{k(k+1)+2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2}. \end{aligned}$$

Hence the equality is true for $k+1$.

Thus, by induction $1+2+3+\cdots+n = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$. □

Note: There are two ways of using the assumption that the statement holds for $n = k$. In both of the above examples we used the statement $P(k)$ and then constructed out of it $P(k+1)$. The alternate method is to start with the statement of $P(k+1)$ and use the truth of $P(k)$ at some point to prove it. This alternate method is employed in the proof below.

Class Example 1.11 (Practical Demonstration)**.** For all $n \in \mathbb{N}$,

$$1+2+3+\cdots+n = \frac{n(n+1)}{2}.$$

Proof. Notice for $n = 1$, $\frac{1(1+1)}{2} = \frac{2}{2} = 1$. Hence the equality is true for $n = 1$.

Now suppose it is true for some $n = k \in \mathbb{N}$. Then

$$\begin{aligned}1 + 2 + 3 + \cdots + k + 1 &= (1 + 2 + 3 + \cdots k) + k + 1\\ &= \frac{k(k+1)}{2} + k + 1\\ &= \frac{k(k+1) + 2(k+1)}{2}\\ &= \frac{(k+1)(k+2)}{2}.\end{aligned}$$

Hence the equality is true for $k + 1$.

Thus, by induction $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$. □

Problem 1.13. *Prove that for all* $n \geq 1$,

$$\cos(x) \cdot \cos(2x) \cdot \cos(4x) \cdots \cos(2^{n-1}x) = \frac{\sin(2^n x)}{2^n \sin(x)}.$$

(Hint: From trigonometry, $\sin(2\theta) = 2\sin(\theta)\cos(\theta)$*.)*

Problem 1.14. *Prove that for all* $n \geq 1$,

$$\cos(x) + \cos(3x) + \cos(5x) + \cdots + \cos((2n-1)x) = \frac{\sin(2nx)}{2\sin(x)}.$$

(Hint: from trigonometry, $\cos(a + b) = \cos(a)\cos(b) - \sin(a)\sin(b)$ *and* $\sin(a + b) = \cos(a)\sin(b) + \cos(b)\sin(a)$*.)*

Problem 1.15. *Prove that for all* $n \geq 1$,

$$169 \mid 3^{3n+3} - 26n - 27.$$

Problem 1.16. *Prove that for all* $n \geq 1$, $(1 + \sqrt{2})^{2n} + (1 - \sqrt{2})^{2n}$ *is an even integer.*

Problem 1.17. *Prove that for all* $n \geq 1$, $(1 + \sqrt{2})^{2n} - (1 - \sqrt{2})^{2n} = k\sqrt{2}$ *for some integer* k*.*

Problem 1.18. *Prove that for all* $n \geq 1$ *and odd* k,

$$2^{n+2} \mid k^{2^n} - 1.$$

Problem 1.19. *Prove that for all* $n \geq 1$,

$$23 \mid 7^{14n+3} + 2^{n+1}.$$

Problem 1.20. *Prove that for all* $n \geq 1$,

$$\sum_{i=1}^{n} i(3i - 1) = n^2(n + 1).$$

Problem 1.21. *Prove that for all* $n \geq 1$,

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}.$$

Problem 1.22. *Prove that for all* $n \geq 1$, $\frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 - \frac{1}{30}n \in \mathbb{Z}$*.*

Problem 1.23. *Prove that for all* $n \geq 1$,

$$\sum_{i=1}^{n} (2i - 1)^2 = \frac{n(4n^2 - 1)}{3}.$$

Problem 1.24. *Prove that for all* $n \geq 1$,

$$\sum_{i=n}^{2n} i^2 = \frac{(1 + n)(n + 14n^2)}{6}.$$

Problem 1.25. *Prove that for all* $n \geq 1$,

$$\sum_{i=1}^{n} \frac{1}{((i-1)k+1)(ik+1)} = \frac{n}{nk+1}.$$

Problem 1.26. *Prove that for all* $n \geq 1$,

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

Problem 1.27. *Prove that for all* $n \geq 5$, $(n+1)! > 2^{n+3}$.

Problem 1.28. *Prove that for all* $n \geq 2$, $\sqrt{n} < 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}}$.

Principle of Strong Induction: If $S \subseteq \mathbb{N}$ such that $1 \in S$ and for all $k \in \mathbb{N}$, $(\forall l \leq k)(l \in S) \Rightarrow k+1 \in S$, then $S = \mathbb{N}$.

Class Example 1.12. Every natural number greater than 2 has a prime divisor.

Proof. For $n = 2$, 2 is prime and $2 \mid 2$, so 2 has a prime divisor.

Suppose the claim is true for all $l \leq k$ for some $k \geq 2$. Then $k+1$ is either prime or composite. If $k+1$ is prime, then again, $k+1 \mid k+1$ and thus $k+1$ has a prime divisor. Suppose $k+1$ is composite. Then there exist natural numbers r and s such that $r \cdot s = k+1$ and $r, s \neq 1$. Since neither are equal to 1, both r and s are strictly less than $k+1$. Hence $r \leq k$. So by the inductive hypothesis, r has a prime divisor. This prime also divides $k+1$. Hence $k+1$ has a prime divisor.

Thus by strong induction, every natural number greater than 2 has a prime divisor. □

Well-Ordering Principle: If $S \subseteq \mathbb{N}$ and is nonempty, then there exists a smallest element of S.

Note: Mathematical Induction, Strong Induction and the Well-Ordering Principle are all logically equivalent, i.e. if we take any one of them to be an axiom of the natural numbers, the other two can be proven as theorems. The following proof using the Well-Ordering Principle should give an indication of how it relates to induction.

Class Example 1.13. For all $n \in \mathbb{N}$,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof. Let $T = \{n \in \mathbb{N} \mid 1 + 2 + 3 + \cdots + n \neq \frac{n(n+1)}{2}\} \subseteq \mathbb{N}$. Since $1 = 1 \cdot \frac{2}{2} = \frac{1(1+1)}{2}$, $1 \notin T$. For the sake of contradiction, suppose $T \neq \varnothing$. Then, by the Well-Ordering Principle, there exists a smallest element $2 \leq t \in T$. Since t is the smallest element of T, $t - 1 \notin T$. Thus $1 + 2 + 3 + \cdots + (t-1) = \frac{(t-1)t}{2}$. But then

$$1 + 2 + 3 + \cdots + (t-1) + t = \frac{(t-1)t}{2} + t = \frac{t^2 - t}{2} + \frac{2t}{2} = \frac{t^2 + t}{2} = \frac{t(t+1)}{2}.$$

Hence $t \notin T$. So by contradiction, the set T must be empty. Thus $1+2+3+\cdots+n = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$. □

2 Real Numbers

2.1 Field Properties

Requires completion of Predicates and Quantifiers

The Real numbers, denoted $\mathbb{R}$, have two operations, called **addition** (denoted $a + b$) and **multiplication** (denoted $a \cdot b$ or ab), that satisfy the following axioms:

Axiom 1: The operations are **well-defined**: If $a = b$ then $a + c = b + c$ and $a \cdot c = b \cdot c$.

Axiom 2: The operations are **commutative**: For all $a, b \in \mathbb{R}$

$$a + b = b + a \qquad\qquad a \cdot b = b \cdot a.$$

Axiom 3: The operations are **associative**: For all $a, b, c \in \mathbb{R}$

$$a + (b + c) = (a + b) + c \qquad\qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

Axiom 4: Multiplication **distributes over** addition: For all $a, b, c \in \mathbb{R}$

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Axiom 5: Each operation has an **identity**, denoted 0 and 1, such that for all $a \in \mathbb{R}$:

$$0 + a = a \qquad\qquad 1 \cdot a = a.$$

Axiom 6: For every $a \in \mathbb{R}$ there exists an **additive inverse**, denoted $-a$, such that

$$a + (-a) = 0.$$

Axiom 7: For every real number $a \neq 0$, there exists a **multiplicative inverse**, denoted a^{-1} such that

$$a \cdot a^{-1} = 1.$$

Class Example 2.1 (Cancellation Law for Addition)**.** If $a + b = a + c$, then $b = c$.

Proof. Suppose $a + b = a + c$. By Axiom 6, there exists $-a$. Then

$$\begin{aligned} (-a) + a + b &= (-a) + a + c && \text{(by Axiom 1)} \\ 0 + b &= 0 + c && \text{(by Axiom 6)} \\ b &= c. && \text{(by Axiom 5)} \end{aligned}$$

Hence $b = c$. □

Corollary 2.1. *If $a \cdot b = a \cdot c$ and $a \neq 0$ then $b = c$.*

Problem 2.2. *Prove that the additive identity is unique.*

Corollary 2.3. *Prove that the multiplicative identity is unique.*

Problem 2.4. *Prove that the additive inverse is unique.*

Corollary 2.5. *Prove that (when it exists) the multiplicative inverse is unique.*

Problem 2.6. *Prove that given real a and b, there exists a real x such that $b + x = a$.*

Corollary 2.7. *Prove that given real a and $b \neq 0$, there exists a real x such that $b \cdot x = a$.*

Problem 2.8. *Prove that given real a and b, the real x such that $b + x = a$ is unique.*

Corollary 2.9. *Prove that given real a and $b \neq 0$, the real x such that $b \cdot x = a$ is unique.*

For real a and b, the notation $a - b$ is called **subtraction** and denotes the unique solution to $b + x = a$.

For real a and $b \neq 0$, the notation $a \div b$ or $\frac{a}{b}$ is called **division** and denotes the unique solution to $b \cdot x = a$.

Corollary 2.10. *Prove that* $0 - a = -a$.

Corollary 2.11. *Prove that* $-0 = 0$.

Corollary 2.12. *Prove if* $a \neq 0$, *then* $\frac{1}{a} = a^{-1}$.

Corollary 2.13. *Prove that* $\frac{1}{1} = 1$.

Problem 2.14. *Prove that* $-(-a) = a$.

Corollary 2.15. *Prove that if* $a \neq 0$, *then* $(a^{-1})^{-1} = a$.

Problem 2.16. *Prove* $a \cdot b - a \cdot c = a \cdot (b - c)$.

Problem 2.17. *Prove* $a \cdot 0 = 0$.

Problem 2.18. *Prove that if* $a \cdot b = 0$ *then* $a = 0$ *or* $b = 0$.

Problem 2.19. *Prove that if* $ab \neq 0$, *then* $(ab)^{-1} = a^{-1}b^{-1}$.

Problem 2.20. *Prove that* $(-a) \cdot b = -(a \cdot b)$.

Corollary 2.21. *Prove that* $(-a) \cdot b = a \cdot (-b)$.

Problem 2.22. *Prove that* $(-a) \cdot (-b) = a \cdot b$.

Problem 2.23. *Prove that* $\frac{a}{b} + \frac{c}{b} = \frac{a+c}{b}$.

Problem 2.24. *Prove that*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Problem 2.25. *Prove that*

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

Problem 2.26. *Prove that*

$$\frac{\left(\frac{a}{b}\right)}{\left(\frac{c}{d}\right)} = \frac{a \cdot d}{b \cdot c}.$$

2.2 Order Properties

Requires completion of Field Properties

There exists an **order**, $<$, on $\mathbb{R}$ that satisfies the following axioms.

Axiom 8: There is a **trichotomy**: For any $a \in \mathbb{R}$, exactly one of $0 < a$, $0 = a$, $a < 0$ is true. When $0 < a$ we say a is **positive**. When $a < 0$ we say a is **negative**.

Axiom 9: If $0 < a$ and $0 < b$ then $0 < a + b$ and $0 < ab$.

Axiom 10: If $a < b$ then $a + c < b + c$ for any $c \in \mathbb{R}$.

If $a < b$ is a false statement, then $a \not< b$ is the true negation.

Problem 2.27. *Prove: The order is* **irreflexive**: *For all real* a, $a \not< a$.

Problem 2.28. *Prove: The order is* **transitive**: *If* $a < b$ *and* $b < c$, *then* $a < c$.

Problem 2.29. *Prove: The order is* **asymmetric**: *If* $a < b$ *then* $b \not< a$.

Problem 2.30. *Prove: If* $a < b$ *and* $0 < c$, *then* $ac < bc$.

Problem 2.31. *Prove: If $a < b$ then $-b < -a$.*

Corollary 2.32. *Prove: If $a < 0$, then $0 < -a$.*

Problem 2.33. *Prove: If $a < b$ and $c < 0$, then $bc < ac$.*

Problem 2.34. *Prove: The quantity $a \cdot b$ is positive if and only if a and b are both positive or both negative.*

Corollary 2.35. *Prove: $a \cdot a \not< 0$.*

Corollary 2.36. *Prove: $0 < 1$.*

Definition 2.1. The symbols $>$, $\leq$, $\geq$ are defined in the following ways:

$$\begin{aligned} a > b &\Leftrightarrow b < a \\ a \geq b &\Leftrightarrow \neg(a < b) \\ a \leq b &\Leftrightarrow \neg(a > b) \end{aligned}$$

If $a \geq 0$ we say a is **nonnegative**.

Definition 2.2. The **absolute value** of a real number x is given by

$$|x| = \begin{cases} x & \text{if } -x \leq x \\ -x & \text{if } x < -x \end{cases}$$

Class Example 2.2. Explain why $\pm x \leq |x|$.

Class Example 2.3. Triangle Inequality For all $a, b \in \mathbb{R}$, $|a + b| \leq |a| + |b|$.

Proof. Either $|a + b| = a + b$ or $|a + b| = -(a + b) = -a + (-b)$.
Case 1: $|a + b| = a + b \leq |a| + |b|$.
Case 2: $|a + b| = -a + (-b) \leq |a| + |b|$.
So in both cases, Class Example 2.2 shows that the inequality holds. □

Definition 2.3. Let A be a subset of $\mathbb{R}$. We say u is an **upper bound** of A if $a \leq u$ for all $a \in A$. We say l is a **lower bound** if $l \leq a$ for all $a \in A$.

Definition 2.4. Let A be a subset of $\mathbb{R}$. We say s is a **least upper bound** or **supremum of** A if s is an upper bound of A and for every upper bound t of A, $s \leq t$. Likewise, we say i is a **greatest lower bound** or **infimum of** A if i is an lower bound of A and for every lower bound l of A, $i \geq l$.

Completeness Axiom: If a non-empty set $A \subseteq \mathbb{R}$ has an upper bound, it has a least upper bound.

Class Example 2.4. Consider the set

$$P = \{3, 3.1, 3.14, 3.141, 3.1415, 3.14159, ...\} \subseteq \mathbb{Q}.$$

This set is certainly bounded above by $u = 4$ and below by $l = 0$. The infimum is $i = 3$ since 3 is the smallest element of the set. But the supremum is $\pi \notin P$. Note that this example also shows that $\mathbb{Q}$ is does not have the completeness axiom: $P \subseteq \mathbb{Q}$, but the supremum $\pi \notin \mathbb{Q}$.

Example 2.1. Determine the supremum and infimum of the set $\left\{\frac{n+1}{2n+1} \mid n \in \mathbb{N}\right\}$.

Problem 2.37. *Prove: If a non-empty subset $A \subseteq \mathbb{R}$ has a lower bound, then it has an infimum.*

Class Example 2.5. (**Archimedean Principle**) If $a > 0$, then for some $n \in \mathbb{N}$ we have $a < n$.

Proof. Consider the nonempty set $S = \{n \in \mathbb{N} \cup \{0\} | n \leq a\}$. Since S has upper bound a, by the Completeness Axiom, there is a least upper bound s. Since s is the least upper bound, $s - 1$ is not an upper bound. Hence there exists $m \in S$ such that $s - 1 < m \leq a$. Since $m \in \mathbb{N} \cup \{0\}$, then $m + 1 \in \mathbb{N}$. Since s is an upper bound of S and $s < m + 1$, then $m + 1 \notin S$. Hence $a < m + 1$. □

Problem 2.38. *Prove: If $a > 0$, then for some $n \in \mathbb{N}$ we have $1/n < a$.*

Problem 2.39. *Between any two real numbers is a rational number.*

Problem 2.40. *Generalize the Class Example above to show that a real number can be defined by its decimal representation.*

3 Set Theory

3.1 Basic Set Theory

Requires completion of Predicates and Quantifiers

Definition 3.1. A **set** is a collection of distinguishable objects, called **elements**, in no particular order. If x is an element of a set X, we denote this by $x \in X$.

Definition 3.2. For some set U and a propositional statement P, the set $X = \{x \in U \mid P(x)\}$ is the set containing all elements of U that make the propositional statement true, i.e. X is the truth set of $P(x)$ in the universe of U. Notating sets in this way is called **set-builder notation**.

Class Example 3.1. The rationals can be given in set-builder notation in two ways:

$$\mathbb{Q} = \{r \in \mathbb{R} \mid (\exists a, b \in \mathbb{Z})(b \neq 0 \wedge br = a)\} = \left\{\frac{a}{b} \mid a, b \in \mathbb{Z} \wedge b \neq 0\right\}$$

Notice that the first way emphasizes the predicate whose truth set is being considered while the second way emphasizes what the actual elements look like. Both ways can be helpful in a proof.

Definition 3.3. The **empty set**, $\varnothing$, is the unique set containing no elements.

Example 3.1. Give a definition for $\mathbb{Z}$ using set-builder notation and $\mathbb{N}$.

Example 3.2. Give a definition for $\varnothing$ using set builder notation.

Definition 3.4. For sets X and Y, X is a **subset** of Y, denoted $X \subseteq Y$, if and only if $x \in X$ implies $x \in Y$.

Class Example 3.2. The following standard sets form a chain of subsets:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

Example 3.3. Consider the following two sets

$$X = \{x \in \mathbb{Z} \mid x > 3\}$$

$$Y = \{y \in \mathbb{R} \mid y > 2\}.$$

Show that $X \subseteq Y$.

Definition Given a predicate $P(x)$ and some set A in the universe of discourse, the **restriction** of A, denoted $A|_P$, is given by

$$A|_P = \{x \in A \mid P(x)\}.$$

The previous example is an example of the proposition: If $A \subseteq B$, then $A|_P \subseteq B|_P$.

Example 3.3.2 Give a nontrivial example of two sets X and Y defined with set-builder notation such that $X \subseteq Y$, but $Y \not\subseteq X$.

Problem 3.1. *Prove or disprove: If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

Problem 3.2. *Prove or disprove: If $A \subseteq B$ and $B \not\subseteq C$, then $A \not\subseteq C$.*

Definition 3.5. Two sets X and Y are **equal** if and only if $X \subseteq Y$ and $Y \subseteq X$.

Class Example 3.3. Consider the two sets $X = \{n \mid (\exists k \in \mathbb{Z})(7k = n - 31)\}$ and $Y = \{3 + 7k \mid k \in \mathbb{Z}\}$. Then $X = Y$.

Proof. Suppose $x \in X$. Then there exists $k \in \mathbb{Z}$ such that $7k = x - 31$. Hence

$$x = 31 + 7k = 3 + 28 + 7k = 3 + 7(4 + k).$$

Since $4 + k \in \mathbb{Z}$, then $x \in Y$. So $X \subseteq Y$.

Now suppose $y \in Y$. Then $y = 3 + 7k$ for some $k \in \mathbb{Z}$. Then

$$y - 31 = (3 + 7k) - 31 = -28 + 7k = 7(-4 + k).$$

Since $-4 + k \in \mathbb{Z}$, $y \in X$. Hence $Y \subseteq X$.

Thus, by definition of equal sets, $X = Y$. □

Problem 3.3. *Prove or disprove: The sets* $X = \{1 + i\sqrt{3}, 1 - i\sqrt{3}\}$ *and* $Y = \{x \in \mathbb{C} \mid x(x - 2) = -4\}$ *are equal.*

Definition 3.6. For real $a < b$, the **open interval** $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$. The **closed interval** $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$. Similar definitions for (a, ∞), $[a, \infty)$, $(-\infty, b)$, and $(-\infty, b]$.

Problem 3.4. *Show that the set* $X = [-4, 10]$ *and the set* $Y = \{x \in \mathbb{R} \mid |x - 3| \leq 7\}$ *are equal.*

Definition 3.7. For two sets X and Y, the **union** is

$$X \cup Y = \{a \mid a \in X \vee a \in Y\}.$$

the **intersection** is

$$X \cap Y = \{a \mid a \in X \wedge a \in Y\},$$

and the **difference** is

$$X - Y = \{a \mid a \in X \wedge a \notin Y\}.$$

Class Example 3.4. Consider the real intervals $[3, 8)$ and $[6, 10]$. Then

$$\begin{aligned}
[3, 8) \cup [6, 10] &= [3, 10] \\
[3, 8) \cap [6, 10] &= [6, 8) \\
[3, 8) - [6, 10] &= [3, 6) \\
[6, 10] - [3, 8) &= [8, 10]
\end{aligned}$$

Example 3.4. Give two (finite but nontrivial) sets and compute their union, intersection and difference.

Problem 3.5. *Determine if the following equality is true:* $X - (X - Y) = Y$. *If true, prove it. If the equality fails, determine whether the statement becomes true if the* $=$ *is replaced by* $\subseteq$ *or* $\supseteq$ *and then give a counterexample to the other direction.*

Problem 3.6. *Determine if the following equality is true:* $X - (Y - X) = X$. *If true, prove it.If the equality fails, determine whether the statement becomes true if the* $=$ *is replaced by* $\subseteq$ *or* $\supseteq$ *and then give a counterexample to the other direction. For sets* X *and* Y, $X - (Y - X) = X$.

Problem 3.7. *Determine if the following equality is true:* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. *If true, prove it. If the equality fails, determine whether the statement becomes true if the* $=$ *is replaced by* $\subseteq$ *or* $\supseteq$ *and then give a counterexample to the other direction.*

Problem 3.8. *Determine if the following equality is true:* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. *If true, prove it. If the equality fails, determine whether the statement becomes true if the* $=$ *is replaced by* $\subseteq$ *or* $\supseteq$ *and then give a counterexample to the other direction.*

Problem 3.9. *Determine if the following equality is true:* $A \cap (B - C) = (A \cap B) - (A \cap C)$. *If true, prove it. If the equality fails, determine whether the statement becomes true if the* $=$ *is replaced by* $\subseteq$ *or* $\supseteq$ *and then give a counterexample to the other direction.*

Problem 3.10. *Determine if the following equality is true: $A \cup (B - C) = (A \cup B) - (A \cup C)$. If true, prove it. If the equality fails, determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$ and then give a counterexample to the other direction.*

Problem 3.11. *Determine if the following equality is true: $(A \cap B) \cup (A - B) = A$. If true, prove it. If the equality fails, determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$ and then give a counterexample to the other direction.*

Problem 3.12. *Determine if the following equality is true: $A \cup B = (A - B) \cup (B - A) \cup (B \cap A)$. If true, prove it. If the equality fails, determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$ and then give a counterexample to the other direction.*

Definition 3.8. Two sets are said to be **disjoint** if and only if their intersection is empty.

Problem 3.13. *Prove or disprove: For any sets A and B, the sets $A - B$, $B - A$ and $B \cap A$ are pairwise disjoint. (Note: pairwise disjoint means every possible pair is disjoint.)*

Propositions 3.12 and 3.13 illustrate a larger idea of a partition.

Definition 3.9. Given a set A, we say a collection of nonempty subsets $\mathcal{B}$ is a **partition** of A if

i. $\displaystyle\bigcup_{B \in \mathcal{B}} B = A$

ii. The subsets are pairwise disjoint, i.e. if $B, B' \in \mathcal{B}$, then $B \cap B' = \varnothing$.

Definition 3.10. When a universe U has been specified, the **complement of** A is

$$\widetilde{A} = \{u \mid u \notin A\} = U - A.$$

Class Example 3.5. The complement of an interval can be given as a union of intervals:

$$\widetilde{(3,4]} = \mathbb{R} - (3,4] = (-\infty, 3] \cup (4, \infty).$$

Problem 3.14. *If A and B are subsets of U, show that $U - (A \cup B) = (U - A) \cap (U - B)$.*

Problem 3.15. *If A and B are subsets of U, show that $U - (A \cap B) = (U - A) \cup (U - B)$.*

Note: Propositions 3.14 and 3.15 are the set-theory versions of DeMorgan's Laws. They are sometimes written as

$$\widetilde{A \cup B} = \widetilde{A} \cap \widetilde{B},$$
$$\widetilde{A \cap B} = \widetilde{A} \cup \widetilde{B}.$$

Definition 3.11. The **power set** of a set A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.

Class Example 3.6. For the set $A = \{a, b\}$, the power set is

$$\mathcal{P}(A) = \{\varnothing, \{a\}, \{b\}, A\}.$$

Example 3.5. Give the power set of $A = \{\varnothing, \{\varnothing\}, \{\varnothing, a\}\}$.

Problem 3.16. *Prove or disprove: $\mathcal{P}(A - B) - \{\varnothing\} = \mathcal{P}(A) - \mathcal{P}(B)$.*

Problem 3.17. *Prove or disprove: If $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, then $A \subseteq B$.*

Definition 3.12. For sets A and B, the set of all ordered pairs having a first coordinate in A and a second coordinate in B is called the **Cartesian product**,

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

Class Example 3.7. A familiar example is

$$\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x \in \mathbb{R} \land y \in \mathbb{R}\} = \mathbb{R}^2.$$

Example 3.6. Give an example of two (finite but nontrivial) sets A and B and their Cartesian product $A \times B$.

Problem 3.18. *Prove or disprove: If $A \times B = A \times C$ and $A \neq \varnothing$, then $B = C$.*

Problem 3.19. *Determine if the following equality is true: $(A \times B) \cup C = (A \times C) \cup (A \times B)$. If true, prove it. If the equality fails, give a counterexample and then determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$.*

Problem 3.20. *Determine if the following equality is true: $A \times (B \cup C) = (A \times B) \cup (A \times C)$. If true, prove it. If the equality fails, determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$ and then give a counterexample to the other direction.*

Problem 3.21. *Determine if the following equality is true: $A \times (B \cap C) = (A \times B) \cap (A \times C)$. If true, prove it. If the equality fails, determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$ and then give a counterexample to the other direction.*

3.2 Extended Set Theory

Requires completion of Basic Set Theory

Definition 3.13. A set of sets is called a **family** or a **collection** of sets.

Class Example 3.8. The power set $\mathcal{P}(A)$ is a family of sets.

Definition 3.14. Given a family of sets $\mathcal{A}$, the **union over** $\mathcal{A}$ is

$$\bigcup_{A \in \mathcal{A}} A = \{a \mid (\exists A \in \mathcal{A})(a \in A)\}.$$

The **intersection over** $\mathcal{A}$ is

$$\bigcap_{A \in \mathcal{A}} A = \{a \mid (\forall A \in \mathcal{A})(a \in A)\}.$$

Example 3.7. Give an example of a family of three sets and the union and intersection over the family.

Problem 3.22. *Prove for every $B \in \mathcal{A}$, $\displaystyle\bigcap_{A \in \mathcal{A}} A \subseteq B$.*

Problem 3.23. *Prove for every $B \in \mathcal{A}$, $B \subseteq \displaystyle\bigcup_{A \in \mathcal{A}} A$.*

Problem 3.24. *The statement $\displaystyle\bigcap_{A \in \mathcal{A}} A \subseteq \bigcup_{A \in \mathcal{A}} A$ is false in one special case. Determine that case, why it's false in that case, and then prove it's true in all other cases.*

Definition 3.15. Let Δ be a nonempty set such that for each $\alpha \in \Delta$ there is a set A_α. The family $\{A_\alpha \mid \alpha \in \Delta\}$ is called an **indexed family of sets**. The set Δ is called the **indexing set** and $\alpha \in \Delta$ is call an **index**.

Class Example 3.9. Let $\Delta = \mathbb{N}$ and to each index $n \in \mathbb{N}$ associate the interval $I_n = [\frac{1}{n}, 1 + \frac{1}{n})$. Then the family of indexed sets is $\mathcal{I} = \{I_n \mid n \in \mathbb{N}\} = \{[1,2), [\frac{1}{2}, \frac{3}{2}), [\frac{1}{3}, \frac{4}{3}), \dots\}$.

Example 3.8. Compute $\bigcup\limits_{I \in \mathcal{I}} I$ and $\bigcap\limits_{I \in \mathcal{I}} I$, for $\mathcal{I}$ the family of sets in the above class example.

Problem 3.25. *Let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Delta\}$ be a nonempty indexed family of sets in the universe U. Prove that* $\widetilde{\bigcup\limits_{\alpha \in \Delta} A_\alpha} = \bigcap\limits_{\alpha \in \Delta} \widetilde{A_\alpha}$.

Problem 3.26. *Let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Delta\}$ be a nonempty indexed family of sets in the universe U. Prove that* $\widetilde{\bigcap\limits_{\alpha \in \Delta} A_\alpha} = \bigcup\limits_{\alpha \in \Delta} \widetilde{A_\alpha}$.

Problem 3.27. *Prove or disprove: For families of sets $\mathcal{A}$ and $\mathcal{B}$ indexed by Δ and Γ, respectively,*

$$\left(\bigcup_{\alpha \in \Delta} A_\alpha \right) \cap \left(\bigcup_{\beta \in \Gamma} B_\beta \right) = \bigcup_{\alpha \in \Delta} \left(\bigcup_{\beta \in \Gamma} (A_\alpha \cap B_\beta) \right).$$

Problem 3.28. *For $\mathcal{A}$ a nonempty family of sets indexed by Δ and B a set, determine if the following equality is true:*

$$B - \left(\bigcap_{\alpha \in \Delta} A_\alpha \right) = \bigcap_{\alpha \in \Delta} (B - A_\alpha).$$

If true, prove it. If the equality fails, give a counterexample and then determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$.

Problem 3.29. *For $\mathcal{A}$ a nonempty family of sets indexed by Δ and B a set, determine if the following equality is true:*

$$B - \left(\bigcup_{\alpha \in \Delta} A_\alpha \right) = \bigcup_{\alpha \in \Delta} (B - A_\alpha).$$

If true, prove it. If the equality fails, give a counterexample and then determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$.

Problem 3.30. *For $\mathcal{A}$ a nonempty family of sets indexed by Δ and B a set, determine if the following equality is true:*

$$\left(\bigcap_{\alpha \in \Delta} A_\alpha \right) - B = \bigcap_{\alpha \in \Delta} (A_\alpha - B).$$

If true, prove it. If the equality fails, give a counterexample and then determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$.

Problem 3.31. *For $\mathcal{A}$ a nonempty family of sets indexed by Δ and B a set, determine if the following equality is true:*

$$\left(\bigcup_{\alpha \in \Delta} A_\alpha \right) - B = \bigcup_{\alpha \in \Delta} (A_\alpha - B).$$

If true, prove it. If the equality fails, give a counterexample and then determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$.

3.3 Cardinality

Requires completion of Functions

4 Number Theory

4.1 Basic Number Theory

Requires completion of Basic Set Theory

Definition 4.1. An integer n is **even** if and only if there exists an integer k such that $n = 2k$.

Definition 4.2. An integer n is **odd** if and only if there exists an integer k such that $n = 2k + 1$.

Definition 4.3. Whether an integer is odd or even is called its **parity**. In other words, parity is the property of an integer that can be described as being even or odd.

Class Example 4.1. The number 10 is even since $10 = 2 \cdot 5$. Also, if a is an integer than $-6a - 7$ is odd since $-6a - 7 = 2(-3a - 4) + 1$.

Definition 4.4. An integer n is a **square** if and only if there exists $k \in \mathbb{Z}$ with $n = k^2$.

Example 4.1. If a and b are integers, is $ab - (3a + 2)(5b + 4)$ even or odd? Why?

Problem 4.1. *Prove or disprove: The sum of two even numbers is even.*

Problem 4.2. *Prove or disprove: Consecutive integers have different parity.*

Corollary 4.3. *Prove or disprove: For any integer a, $a^2 + a$ is even.*

Problem 4.4. *Prove or disprove: The product of two odd integers is odd.*

Problem 4.5. *Prove or disprove: If the product of two integers is odd, then both integers are odd.*

Problem 4.6. *Prove or disprove: The sum of two integers has the same parity as their difference.*

Definition 4.5. A positive integer n is **prime** if and only if $n > 1$ and for all positive integers r and s, if $n = rs$ then $r = 1$ or $s = 1$.

Definition 4.6. A positive integer n is **composite** if and only if there exist positive integers $r \neq 1$ and $s \neq 1$ such that $n = rs$.

Example 4.2. Is 104807 prime or composite? Explain why.

Example 4.3. Explain why if $n > 1$ is an integer, then n is either composite or prime.

Problem 4.7. *Prove or disprove: 3 is the only prime that can be written as $k^4 + k^2 + 1$ for some integer k.*

Definition 4.7. A number r is **rational** if and only if $br = a$ for some integers a and b with $b \neq 0$. In this case we can write $r = \frac{a}{b}$. The set of rationals is denoted $\mathbb{Q}$. A number that is not rational is **irrational**.

Class Example 4.2. Any finite decimal is rational. For example, $3.1415 = \frac{31415}{10000}$.

Example 4.4. Is 0.5757575757... rational or irrational? Explain why.

Example 4.5. Is every integer a rational number? Explain why or why not.

Problem 4.8. *Prove or disprove: The sum of two rational numbers is rational.*

Corollary 4.9. *Given that π is irrational, prove or disprove: For every $x \in \mathbb{R}$, either $\pi - x$ or $\pi + x$ is irrational.*

Problem 4.10. *Prove or disprove: The product of two rational numbers is rational.*

Definition 4.8. For integers n and $d \neq 0$, n is **divisible by** d if and only if there exists an integer k with $n = dk$. The property of "n is divisible by d" is also phrased as

- **n is a multiple of d,**
- **d is a factor of n,**
- **d is a divisor of n,**
- **d divides n, notated as $d \mid n$.**

The notation $d \nmid n$ denotes that d does not divide n.

Example 4.6. Prove that even numbers are divisible by 2.

Example 4.7. For which integers k does $k \mid 0$?

Example 4.8. Restate the definition of prime using the idea of divisibility.

Problem 4.11. *Prove or disprove: If a and b are positive integers with $a \mid b$, then $a \leq b$.*

Problem 4.12. *Prove or disprove: For all $a \in \mathbb{Z}$, $a \mid a$.*

Problem 4.13. *Prove or disprove: If a, b and c are integers with $a \mid b$ and $b \mid c$, then $a \mid c$.*

Problem 4.14. *Prove or disprove: If a, b and c are integers with $a \mid b$, then $a \mid bc$.*

Problem 4.15. *Prove or disprove: Any integer $n > 1$ is divisible by a prime number.*

Problem 4.16. *Prove or disprove: For $a, b, c, x, y \in \mathbb{Z}$, if $a \mid b$ and $a \mid c$, then $a \mid (xb + yc)$.*

Problem 4.17. *Prove or disprove: For $a, b \in \mathbb{Z}$, if $a \mid b$ and $b \mid a$, then $a = \pm b$.*

4.2 Congruences

Requires completion of Basic Number Theory

Definition 4.9. For $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$, we say a **is congruent to** b **modulo** m, denoted $a \equiv b \mod m$ if and only if $m \mid a - b$. Occasionally we will also write $a \equiv_m b$.

Class Example 4.3. The integers 28 and 13 are congruent mod 5 since $5 \mid 28 - 13 = 15$. So we can write $28 \equiv 13 \mod 5$.

Class Example 4.4. Applying the definition of "divides" to the above definition gives: $a \equiv b \mod m$ if and only if there exists $k \in \mathbb{Z}$ with $a = b + mk$. This is often much easier to work given that our statement now is one of equality rather than divisibility.

Class Example 4.5. The integers 28 and 13 are congruent mod 5 since $28 = 13 + 5 \cdot 3$.

Example 4.9. Rephrase the definitions of even and odd in terms of congruences.

Example 4.10. Give an alternate definition for $b \mid a$ in terms of congruency.

Example 4.11. Show that $\equiv$ is reflexive: For all $a \in \mathbb{Z}$ and $m \in \mathbb{N}$, $a \equiv a \mod m$.

Problem 4.18. *Show that $\equiv$ is symmetric: For any $m \in \mathbb{N}$, if $a \equiv b \mod m$ then $b \equiv a \mod m$.*

Problem 4.19. *Show that $\equiv$ is transitive: For any $m \in \mathbb{N}$, if $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$.*

Problem 4.20. *Suppose $d \mid m$ and $a \equiv b \mod m$. Show that $a \equiv b \mod d$.*

Problem 4.21. *Prove or disprove: If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $a + c \equiv b + d \mod m$.*

Problem 4.22. *Prove or disprove: If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $ac \equiv bd \mod m$.*

Problem 4.23. *Prove or disprove: If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $a^c \equiv b^d \mod m$.*

Problem 4.24. *Prove or disprove: If $c \not\equiv 0 \mod m$ and $ac \equiv bc \mod m$, then $a \equiv b \mod m$.*

Theorem 4.25 (Division Algorithm)**.** *Let a and b be integers with $b > 0$. Then there exists unique integers q and r such that $a = bq + r$ and $0 \leq r < b$. In this case q is called the* **quotient** *and r is called the* **remainder** *of a divided by b.*

Proof. Given a and b, consider the set $S = \{a - nb \mid n \in \mathbb{Z}\} \subseteq \mathbb{Z}$. If $a \geq 0$, then $a \in S$ is a nonnegative element. If $a < 0$, then $a - ab = -a(b-1) \geq 0$ is a nonnegative element of S. So in either case, S contains nonnegative elements. Take r to be the smallest nonnegative element of S and define q by $a - qb = r$. We need to show $0 \leq r < b$. By construction $0 \leq r$. Suppose $r \geq b$, then

$$0 \leq r - b = a - qb - b = a - (q+1)b \in S$$

and r would not be the least nonnegative element of S. Thus $0 \leq r < b$. The proof of uniqueness is left to the problems below. □

Class Example 4.6. Applying the division algorithm to $a = 13$ and $b = 5$ gives quotient $q = 2$ and remainder $r = 3$ since $13 = 5 \cdot 2 + 3$.

Example 4.12. Find q and r for the pairs $(a, b) = (29, 6)$, $(a, b) = (-23, 7)$, $(a, b) = (91, 13)$.

Example 4.13. Give an alternate definition for $b \mid a$ in terms of the Division Algorithm.

Problem 4.26. *Finish the proof of Division Algorithm by proving the uniqueness of q and r in the theorem.*

Problem 4.27. *Prove: $a \equiv b \mod m$ if and only if a and b have the same remainder when divided by m.*

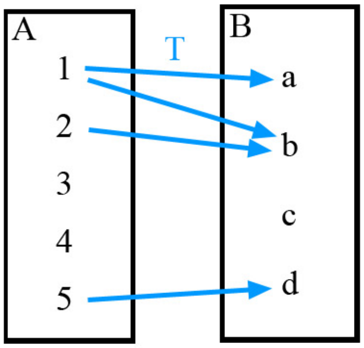
5 Relations

5.1 General Relations

Requires completion of Basic Set Theory

Definition 5.1. Let A and B be sets. R is a **relation from** A **to** B if and only if $R \subseteq A \times B$. If $(a, b) \in R$, we can also write this as $a\ R\ b$. If $(a, b) \notin R$, then we can write $a \not R\ b$. A relation from A to itself is called a **relation on** A.

Class Example 5.1. Suppose $A = \{1, 2, 3, 4, 5\}$ and $B = \{a, b, c, d\}$. Then one possible relation from A to B is $T = \{(1, a), (1, b), (2, b), (5, d)\}$. In this case we could write $2\ T\ b$. Think of the T the same way you think of $=$, $\leq$, $\subseteq$, or $\cong$ in that it states some sort of relationship exists between 2 and b.
We can represent the relation T graphically as connections between elements of two sets.



Definition 5.2. The **domain** of a relation R from A to B is the set

$$\mathrm{Dom}(R) = \{a \in A \mid (\exists b \in B)(a\ R\ b)\}.$$

Definition 5.3. The **range** of a relation R from A to B is the set

$$\mathrm{Rng}(R) = \{b \in B \mid (\exists a \in A)(a\ R\ b)\}.$$

Definition 5.4. The **inverse** of a relation R from A to B is the set

$$R^{-1} = \{(b, a) \mid (a, b) \in R\}.$$

Class Example 5.2. Using the relation T in the above example,

$$\mathrm{Dom}(T) = \{1, 2, 5\},\ \mathrm{Rng}(T) = \{a, b, d\},\ T^{-1} = \{(a, 1), (b, 1), (b, 2), (d, 5)\}.$$

Example 5.1. Consider the following relation from $\mathbb{Q}$ to $\mathbb{R}$,

$$x\ S\ y \text{ if and only if } x^2 = y^2 + y.$$

Give the set-builder notation for S, then determine the domain, range, and inverse.

Example 5.2. If R is a relation from A to B, explain why R^{-1} is a relation from B to A.

Example 5.3. If R is a relation, explain why $(R^{-1})^{-1} = R$.

Problem 5.1. *Determine if the following equality is true:* $\mathrm{Dom}(R^{-1}) = \mathrm{Rng}(R)$. *If true, prove it. If the equality fails, give a counterexample and then determine whether the statement becomes true if the* $=$ *is replaced by* $\subseteq$ *or* $\supseteq$.

Corollary 5.2. *Determine if the following equality is true:* $\mathrm{Rng}(R^{-1}) = \mathrm{Dom}(R)$. *If true, prove it. If the equality fails, give a counterexample and then determine whether the statement becomes true if the* $=$ *is replaced by* $\subseteq$ *or* $\supseteq$.

Problem 5.3. *Determine if the following equality is true:* $\mathrm{Rng}(R^{-1}) = \mathrm{Dom}(R)$. *If true, prove it. If the equality fails, give a counterexample and then determine whether the statement becomes true if the* $=$ *is replaced by* $\subseteq$ *or* $\supseteq$.

Definition 5.5. Let A be a set. Then the **identity relation** on A is $I_A = \{(a,a) \mid a \in A\}$.

Definition 5.6. Let R be a relation from A to B and S a relation from B to C. The **composition** of R and S is

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

Example 5.4. For $a, b \in A$, explain the difference between saying $a = b$ and $a \; I_A \; b$.

Example 5.5. Let $R = \{(1,5),(2,2),(3,4),(5,2)\}$ and $S = \{(2,4),(3,4),(3,1),(5,5)\}$. Compute $R \circ S$ and $R \circ R$.

Example 5.6. Give an example of nonempty relations R and S on the set $A = \{a,b,c,d\}$ such that $R \circ S = S \circ R = \varnothing$.

Problem 5.4. *Determine if the following equality is true: For relations S and R on a set A, $S \circ R = R \circ S$. If true, prove it. If the equality fails, give a counterexample and then determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$.*

Problem 5.5. *Determine if the following equality is true: $T \circ (S \circ R) = (T \circ S) \circ R$. If true, prove it. If the equality fails, give a counterexample and then determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$.*

Problem 5.6. *Determine if the following equality is true: $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$. If true, prove it. If the equality fails, give a counterexample and then determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$.*

Problem 5.7. *Determine if the following equality is true:* $\mathrm{Dom}(S \circ R) = \mathrm{Dom}(R)$. *If true, prove it. If the equality fails, give a counterexample and then determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$.*

Problem 5.8. *Determine if the following equality is true:* $\mathrm{Rng}(S) = \mathrm{Rng}(S \circ R)$. *If true, prove it. If the equality fails, give a counterexample and then determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$.*

5.2 Equivalence Relations

Definition 5.7. A relation R on a set X is **reflexive** if and only if for all $x \in X$, xRx.

Definition 5.8. A relation R on a set X is **symmetric** if and only if for all $x, y \in X$, if xRy then yRx.

Definition 5.9. A relation R on a set X is **transitive** if and only if for all $x, y, z \in X$, if xRy and yRz then xRz.

Definition 5.10. A relation R on a set X is **antisymmetric** if and only if for all $x, y \in X$, if xRy and yRx then $x = y$.

Class Example 5.3. Consider the relation of similarity $\sim$ on polygons given by $P_1 \sim P_2$ if and only if there is a constant $\lambda \neq 0$ such that every side length of P_1 is λ times the side length of P_2. Then $\sim$ is reflexive since we can take $\lambda = 1$. The relation is symmetric since if $P_1 \sim P_2$ by λ, then $P_2 \sim P_1$ by $1/\lambda$. The relation is transitive since if $P_1 \sim P_2$ by λ and $P_2 \sim P_3$ by λ', then $P_1 \sim P_3$ by $\lambda\lambda'$. The relation $\sim$ is not antisymmetric since it's possible to have $P_1 \sim P_2$ and $P_2 \sim P_1$ without $P_1 = P_2$ (just take two equilateral triangles of differing size).

Example 5.7. Complete the table of properties for familiar relations.

Relation	Reflexive	Symmetric	Transitive	Antisymmetric
$=$ on $\mathbb{R}$				
$\cong$ on geometric shapes				
$\equiv_n$ on $\mathbb{Z}$				
$\leq$ on $\mathbb{R}$				
$<$ on $\mathbb{Q}$				
$\subseteq$ on sets				
$\mid$ on $\mathbb{N}$				
$\mid$ on $\mathbb{Z}$				
$\perp$ on lines in a plane				

Problem 5.9. *Prove: A relation R on X is reflexive if and only if $I_X \subseteq R$.*

Problem 5.10. *Prove: A relation R on X is symmetric if and only if $R^{-1} = R$.*

Problem 5.11. *Prove: A relation R on X is transitive if and only if $R \circ R \subseteq R$.*

Problem 5.12. *Prove or disprove: If R is a symmetric, transitive relation on X and* $\mathrm{Dom(R) = X}$, *then R is reflexive.*

Definition 5.11. A relation R on a set X is an **equivalence relation** if it is reflexive, symmetric, and transitive.

Class Example 5.4. The relation $\sim$ in the example above was reflexive, symmetric and transitive. Thus it is an equivalence relation.

Note: Equivalence relations are a way of saying "the same". So, for example, $\sim$ is an equivalence relation because if $P_1 \sim P_2$ they are the same shape. Any relation that can be stated "xRy if and only if x and y have the same property P" is an equivalence relation. But a proof must still show the three properties.

Class Example 5.5. The relation $\equiv_n$ can be rephrased as $a \equiv_n b$ if and only if a and b have the same remainder when divided by n. This means that $\equiv_n$ is an equivalence relation. (The actual proof is given in Example 4.11 and Propositions 4.18 and 4.19.)

Example 5.8. Which of the relations in Example 5.7 are equivalence relations? (Note: It might be best to fill out the chart completely before answering this question.)

Problem 5.13. *Prove or disprove: The following relation on $\mathbb{R}$ is an equivalence relation: xVy if and only if $x = y$ or $xy = 1$.*

Problem 5.14. *Prove or disprove: The following relation on $\mathbb{R}$ is an equivalence relation: xDy if and only if $|x - y| \leq 1$.*

Problem 5.15. *Prove or disprove: The following relation on $\mathbb{R} \times \mathbb{R}$ is an equivalence relation: $(x, y)T(a, b)$ if and only if $a^2 + b^2 = x^2 + y^2$.*

Problem 5.16. *Prove or disprove: The following relation on $\mathbb{R}$ is an equivalence relation: xGy if and only if $xy > 0$.*

Problem 5.17. *Prove or disprove: The following relation on $\mathbb{Z} \times \mathbb{N}$ is an equivalence relation: $(x, y)F(z, w)$ if and only if $xw = zy$.*

Problem 5.18. *Prove or disprove: The following relation on $\mathbb{N}$ is an equivalence relation: nSm if and only if $\sqrt{n/m} \in \mathbb{Q}$.*

Definition 5.12. For an equivalence relation R on X, the **equivalence class of** x is the set $x/R = \{y \in X \mid xRy\}$. The set of all equivalence classes is called X **modulo** R and is given by $X/R = \{x/R \mid x \in X\}$. A set of **represenatives** is a subset $A \subset X$ such that $\{a/R \mid a \in A\} = X/R$ and for all $a, b \in A$, aRb if and only if $a = b$.

Class Example 5.6. For the equivalence relation $\equiv_5$, the equivalence class of 2 is the set

$$2/{\equiv_n} = \{\dots, -8, -3, 2, 7, 12, \dots\} = \{2 + 5k \mid k \in \mathbb{Z}\}.$$

Then $\mathbb{Z}$ modulo $\equiv_5$ is the set

$$\mathbb{Z}/{\equiv_5} = \{0/\equiv_5, 1/\equiv_5, 2/\equiv_5, 3/\equiv_5, 4/\equiv_5\}.$$

This set is usually denoted more simply as $\mathbb{Z}_5$. Also, a set of representatives for $\equiv_5$ is $\{0, 1, 2, 3, 4\}$.

Example 5.9. For the equivalence relation V in Proposition 5.13, a typical equivalence class looks like $x/V = \{x, \frac{1}{x}\}$. The classes $0/V$, $1/V$ and $-1/V$ only contain a single element. A complete set of representatives is then the closed interval $[-1, 1]$.

Example 5.9. For one of the equivalence relations in the previous set of problems, Give/describe a typical equivalence class (which sometimes can be achieved by saying giving the property that all members have the same) and give a complete set of representatives. (You should probably wait until a relation above has been proven to actually be an equivalence relation.)

Example 5.10. Prove that for an equivalence relation R on a set A, for all $x \in A$, $x/R \neq \varnothing$.

Problem 5.19. *Prove that for an equivalence relation R on a set A that $\bigcup\limits_{x\in A} x/R = A$.*

Problem 5.20. *Prove that for an equivalence relation R on a set A that $x \; R \; y$ if and only if $x/R = y/R$.*

Problem 5.21. *Prove that for an equivalence relation R on a set A that $x \not R \; y$ if and only if $x/R \cap y/R = \varnothing$.*

Note: The previous three propositions show that the equivalence classes of an equivalence relation on a set form a partition of the set. The next proposition shows that anytime you have a partition, you can create an equivalence relation from it.

Problem 5.22. *Suppose the family of sets $\{B_i\}$ form a partition of a set A. Define a relation R on A by xRy if and only if there exists j such that $x, y \in B_j$. Prove that R is an equivalence relation.*

5.3 Order Relations

Requires completion of General Relations

6 Functions

6.1 Basic Functions

Requires completion of General Relations

Definition 6.1. A **function from a set X to a set Y**, denoted $f : X \to Y$, is a set of ordered pairs of $X \times Y$ such that

(i.) (**well-supported**) for all $x \in X$ there is a $y \in Y$ with $f(x) = y$, i.e. $(\forall x \in X)(\exists y \in Y)((x, y) \in f)$.

(ii.) (**well-defined**) for each x there is a unique y with $(x, y) \in f$, i.e. $x_1 = x_2 \Rightarrow f(x_1) = f(x_2)$.

If $(x, y) \in f$ then this is denoted $f : x \mapsto y$ or $f(x) = y$, and $f(x)$ is called the **image of x under f**. The set X is called the **domain** and the set Y is called the **co-domain**.

Class Example 6.1. As a non-example, suppose one tried to define a function on the integers modulo 7 by $f(n) =$ (the number of letters in the English spelling of n). This is not well-defined since $8 \equiv_7 1$ but $f(8) = 5 \neq 3 = f(1)$.

Class Example 6.2. The familiar function $f(x) = x^2$ is represented as a set by $f = \{(x, x^2) \mid x \in \mathbb{R}\} \subseteq \mathbb{R}^2$.

Definition 6.2. For a function $f : X \to Y$, and $U \subseteq X$, the **image of U** is

$$f(U) = \{f(u) \mid u \in U\} = \{y \mid (\exists u \in U)(f(u) = y)\}.$$

The **range** of f is the image of X, i.e. the range is $f(X)$.

Class Example 6.3. For $f(x) = x^2$ and the interval $(-1, 1)$, we have $f((-1, 1)) = [0, 1)$.

Example 6.1. Explain why every function is a relation. Describe the roles the well-defined and well-supported conditions play in the visual interpretation of a function as a relation.

Example 6.2. Give a (small) nontrivial subset $A \subseteq \mathbb{Z}$ and a nontrivial function $f : \mathbb{Z} \to \mathbb{N}$. Compute $f(A)$.

Example 6.3. Give an example of an f with domain $\mathbb{Q}$ that is not well-supported. Give a specific instance where it fails the well-supported condition.

Example 6.4. Give an example of an f with domain $\mathbb{Q}$ that is not well-defined. Give a specific instance where it fails the well-defined condition.

Problem 6.1. *Suppose $f : A \to B$, with C and D subsets of A. Determine if the following equality is true: $f(C \cap D) = f(C) \cap f(D)$. If true, prove it. If the equality fails, give a counterexample and then determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$.*

Problem 6.2. *Suppose $f : A \to B$, with C and D subsets of A. Determine if the following equality is true: $f(C \cup D) = f(C) \cup f(D)$. If true, prove it. If the equality fails, give a counterexample and then determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$.*

Definition 6.3. For functions $f : X \to Y$ and $g : Y \to Z$, the **composition** $g \circ f$ is the function $g \circ f : X \to Z$ defined by

$$g \circ f = \{(x, z) \mid (\exists y \in Y)(f(x) = y \wedge g(y) = z)\}.$$

More informally, this is written as $(g \circ f)(x) = g(f(x))$.

Example 6.5. Give two functions $f, g : \mathbb{R} \to \mathbb{R}$ and find $g \circ f$ and $f \circ g$. What can we say in general about $g \circ f$ and $f \circ g$?

Definition 6.4. A function $f : X \to Y$ is **injective** or **one-to-one** when

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

This can also be denoted $f : X \hookrightarrow Y$.

Class Example 6.4. The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 3x + 1$ is injective.

Proof. Suppose $f(x) = f(y)$. Then

$$\begin{aligned} 3x + 1 &= 3y + 1 \\ 3x &= 3y \\ x &= y. \end{aligned}$$

Hence f is one-to-one. □

Definition 6.5. A function $f : X \to Y$ is **surjective** or **onto** when

$$(\forall y \in Y)(\exists x \in X)(f(x) = y),$$

i.e. $y \in Y \Rightarrow y \in f(X)$. This can also be denoted $f : X \twoheadrightarrow Y$.

Class Example 6.5. The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 3x + 1$ is surjective.

Proof. Suppose $y \in \mathbb{R}$. Let $x = \frac{y-1}{3}$. Then $x \in \mathbb{R}$ and

$$f(x) = f\left(\frac{y-1}{3}\right) = 3\left(\frac{y-1}{3}\right) + 1 = (y - 1) + 1 = y.$$

Thus f is onto. □

Example 6.6. Describe the role that being 1-to-1 plays in the visual interpretation of a function as a relation. Describe the role that being onto plays in the visual interpretation of a function as a relation.

Example 6.7. Give an example of a function $f : \mathbb{R} \to \mathbb{R}$ that is one-to-one, but not onto.

Example 6.8. Give an example of a function $f : \mathbb{R} \to \mathbb{R}$ that is onto, but not one-to-one.

Example 6.9. Give an example of a situation where $f : A \to B$, $D \subseteq A$, and $f(a) \in f(D)$, but $a \notin D$.

Example 6.10. Using arrow diagrams, give an example of functions f and g such that f is one-to-one, g is onto, but $g \circ f$ is neither.

Example 6.11. Using arrow diagrams, give an example of functions f and g such that f is onto, g is one-to-one, but $g \circ f$ is neither.

Problem 6.3. *Prove or disprove that* $M : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *given by* $M(x, y) = 2^{x-1}(2y - 1)$ *is onto.*

Problem 6.4. *Prove or disprove that* $M : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *given by* $M(x, y) = 2^{x-1}(2y - 1)$ *is one-to-one.*

Problem 6.5. *Prove or disprove: If* $f : A \twoheadrightarrow B$ *and* $g : B \twoheadrightarrow C$ *then* $g \circ f : A \twoheadrightarrow C$.

Problem 6.6. *Prove or disprove: If* $f : A \hookrightarrow B$ *and* $g : B \hookrightarrow C$ *then* $g \circ f : A \hookrightarrow C$.

Problem 6.7. *Prove or disprove : If* $f : A \to B$, $g : B \to C$, *and* $g \circ f : A \twoheadrightarrow C$ *then* $g : B \twoheadrightarrow C$

Problem 6.8. *Prove or disprove: If* $f : A \to B$, $g : B \to C$, *and* $g \circ f : A \hookrightarrow C$ *then* $f : A \hookrightarrow B$

Definition 6.6. Given a function $f : X \to Y$, its **inverse** is

$$f^{-1} = \{(y, x) \mid f(x) = y\}.$$

If this set satisfies the well-defined condition, then f^{-1} is the **inverse function** of f.

Class Example 6.6. Notice that for the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$, the inverse function is not well-defined since we don't know if $f^{-1}(x) = \sqrt{x}$ or $f^{-1}(x) = -\sqrt{x}$. This can be resolved somewhat by restricting the domain of the original function to $f : \mathbb{R}^{\geq 0} \to \mathbb{R}$.

Definition 6.7. For a function $f : X \to Y$, and $V \subseteq Y$, the **pre-image of** V is

$$f^{-1}(V) = \{x \in X \mid f(x) \in V\} = \{x \in X \mid (\exists v \in V)(f(x) = v)\}.$$

Class Example 6.7. Even though the inverse of $f(x) = x^2$ may not be a function, we can still compute, for example, $f^{-1}((1, 4]) = [-2, -1) \cup (1, 2]$.

Example 6.12. Give a nontrivial example of a function $f : \mathbb{R} \to \mathbb{R}$ where f^{-1} is a function, too. Make sure to prove the well-definition of your f^{-1}.

Problem 6.9. *Suppose $f : A \to B$, with C and D subsets of B. Determine if the following equality is true: $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$. If true, prove it. If the equality fails, give a counterexample and then determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$.*

Problem 6.10. *Suppose $f : A \to B$, with C and D subsets of B. Determine if the following equality is true: $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$. If true, prove it. If the equality fails, give a counterexample and then determine whether the statement becomes true if the $=$ is replaced by $\subseteq$ or $\supseteq$.*

6.2 Sequences

Requires completion of Basic Functions

Definition 6.8. A **sequence** is a function with domain $\mathbb{N}$. Instead of using the usual function notation of $a(n)$, a specific value of a sequence a is denoted a_n and can be referred to as the nth term of a. A sequence may be defined **explicitly** with a closed formula for the nth term, or it may be defined **recursively** by giving a finite number of initial terms and then relating the general nth term to the previous terms.

Class Example 6.8. Notice there is no restriction on the co-domain of a sequence. The sequence $a_n = \dfrac{1}{\sqrt{n}}$ has domain $\mathbb{N}$ but co-domain $\mathbb{R}$.

Class Example 6.9. The Fibonacci sequence is defined recursively as follows: $F_0 = 0$, $F_1 = 1$, for all $n \geq 2$,

$$F_n = F_{n-1} + F_{n-2}.$$

However, it can be shown that the Fibonacci sequence can be given explicitly by

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Example 6.13. Give the first 5 terms of the recursively defined sequence $q_1 = 2$, $q_k = \dfrac{(-1)^k(k^2+1)}{q_{k-1}}$.

Example 6.14. Give an explicit definition for the sequence that is defined recursively by $a_0 = C$, $a_n = a_{n-1} + d$.

Example 6.15. Give an explicit definition for the sequence that is defined recursively by $a_0 = C$, $a_n = ra_{n-1}$.

Problem 6.11. *Give an explicit definition for the sequence defined by $p_1 = 1$, $p_{i+1} = 2p_i + 2$. Prove your result.*

Problem 6.12. *Use induction to prove that the Fibonacci sequence satisfies*

$$F_1 + F_2 + \cdots F_n = F_{n+2} - 1.$$

Problem 6.13. *Use induction to prove that the Fibonacci sequence satisfies*

$$F_2 + F_4 + \cdots F_{2n} = F_{2n+1} - 1.$$

Problem 6.14. *Use induction to prove that the Fibonacci sequence satisfies*

$$F_1 + F_3 + \cdots F_{2n-1} = F_{2n}.$$

Definition 6.9. A sequence x of reals **has limit** L if and only if for every real $\epsilon > 0$ there exists a natural number N such that if $n > N$ then $|x_n - L| < \epsilon$. If such an L exists, we say x **converges** to L and this can be noted $\lim\limits_{n\to\infty} x_n = L$ or $x_n \to L$. If no such L exists, we say the sequence **diverges**.

Class Example 6.10. The definition of limit can be given in logical form as

$$(\exists L \in \mathbb{R})(\forall \epsilon > 0)(\exists N \in \mathbb{N})(\forall n \in \mathbb{N})(n > N \Rightarrow |x_n - L| < \epsilon).$$

Class Example 6.11. The sequence $a_n = \dfrac{1}{\sqrt{n}}$ converges.

Proof. Given $\epsilon > 0$, then $\frac{1}{\epsilon^2} > 0$. So by Archimedean Principle there exists $N \in \mathbb{N}$ with $N > \frac{1}{\epsilon^2}$. Now suppose $n > N$. Then

$$\begin{aligned} n &> \frac{1}{\epsilon^2} \\ \frac{1}{n} &< \epsilon^2 \\ \frac{1}{\sqrt{n}} &< \epsilon \end{aligned}$$

Thus $|a_n - 0| = \frac{1}{\sqrt{n}} < \epsilon$. Hence the limit is 0 and so a_n converges. □

Class Example 6.12. The sequence $a_n = \dfrac{n-1}{n+1}$ converges.

Thought process: We know from Calculus that the limit is $L = 1$. So we need to get $\left|\frac{n-1}{n+1} - 1\right| < \epsilon$. Algebra gives $\frac{2}{n+1} < \epsilon$. We could at this point possibly use $n > \frac{2}{\epsilon} - 1$, but this expression might not be positive for $\epsilon > 2$. Instead we notice that $\frac{2}{n+1} < \frac{2}{n}$. So if $n > \frac{2}{\epsilon}$ that will suffice.

Proof. Take $L = 1$. let $\epsilon > 0$. By the Archimedean Principle there exists $N \in \mathbb{N}$ with $N > \frac{2}{\epsilon}$. Now suppose $n > N > \frac{2}{\epsilon}$. Then $\frac{2}{n} < \epsilon$ and hence

$$\left|\frac{n-1}{n+1} - 1\right| = \left|\frac{(n-1)-(n+1)}{n+1}\right| = \left|\frac{2}{n+1}\right| < \left|\frac{2}{n}\right| < \epsilon.$$

□

Class Example 6.13. The sequence $a_n = (-1)^n$ diverges.
Note: Here we use the negation of the limit definition:

$$(\forall L \in \mathbb{R})(\exists \epsilon > 0)(\forall N \in \mathbb{N})(\exists n \in \mathbb{N})(n > N \wedge |a_n - L| \geq \epsilon).$$

Proof. Let $L \in \mathbb{R}$. Take $\epsilon = 1$. Suppose $N \in \mathbb{N}$.
Case 1. If $L \geq 0$, let $n = 2N + 1$. Then $a_n = (-1)^{2N+1} = -1$. So $|-1 - L| = 1 + L \geq 1$.
Case 2. If $L < 0$, let $n = 2N$. Then $a_n = (-1)^{2N} = 1$. So $|1 - L| = 1 + (-L) > 1$.
In both cases, $n > N$ but $|a_n - L| \geq 1$. Thus a_n diverges. □

Example 6.16. Prove: A constant sequence, i.e. $x_n = k$, converges.

Problem 6.15. *Prove or disprove: The sequence* $x_n = \dfrac{6}{2^n}$ *converges.*

Problem 6.16. *Prove or disprove: The sequence* $x_n = \dfrac{\cos(n)}{n}$ *converges.*

Problem 6.17. *Prove or disprove: The sequence* $x_n = n^2$ *converges.*

Problem 6.18. *Prove or disprove: The sequence* $x_n = \dfrac{3n}{n^2-1}$ *converges.*

Problem 6.19. *Prove or disprove: The sequence* $x_n = \dfrac{3n^2}{n-1}$ *converges.*

Problem 6.20. *Prove or disprove: The sequence* $x_n = \dfrac{3n^2}{n^2+1}$ *converges.*

Class Example 6.14. If a sequence converges, the limit is unique.
Note: Here we get to use the assumption that the sequence converges to prove another fact. This means we can pick any $\epsilon > 0$ and the rest of the definition of the limit should hold. In the following proof, we choose just the right value of ϵ to draw the appropriate contradiction.

Proof. For sake of contradiction, suppose $x_n \to L$ and $x_n \to M$ with $L \neq M$. Let $\epsilon = \frac{1}{3}|L-M| > 0$. Since $x_n \to L$, then there is $N_1 \in \mathbb{N}$ so that $n > N_1$ implies $|x_n - L| < \epsilon$. Likewise since $x_n \to M$, then there is $N_2 \in \mathbb{N}$ so that $n > N_2$ implies $|x_n - M| < \epsilon$. Let $N = N_1 + N_2$ and suppose $n > N$. Then

$$\begin{aligned}
|L-M| &= |(L-x_n)+(x_n-M)| \\
&\leq |L-x_n| + |x_n-M| \\
&= |x_n-L| + |x_n-M| \\
&< \epsilon + \epsilon \\
&= \frac{2}{3}|L-M|.
\end{aligned}$$

Hence $L \neq M$ implies $|L-M| < \frac{2}{3}|L-M|$ which is a contradiction. Thus $L = M$ and the limit is unique. □

Problem 6.21. *Prove that if the sequence x converges and r is a constant, then the sequence z defined by $z_n = rx_n$ converges.*

Problem 6.22. *Prove that if sequences x and y converge, then the sequence z defined by $z_n = x_n + y_n$ converges.*

Problem 6.23. *Prove that if sequences x and y converge, then the sequence z defined by $z_n = x_n y_n$ converges.*

Problem 6.24. *Prove that if the sequence $x \to L$, then there is a natural number N such that if $n \geq N$, then* $|x_n| > \dfrac{|L|}{2}$.

Problem 6.25. *Prove that if $x \to L$ and $y \to M \neq 0$ with $y_n \neq 0$ for all n, then the sequence z defined by* $z_n = \dfrac{x_n}{y_n}$ *converges.*

7 Algebraic Structure

7.1 Algebraic Systems

Requires completion of Basic Functions

Definition 7.1. A **binary operation** on a set A is a function $f : A \times A \to A$.

Class Example 7.1. Addition is a binary operation on the integers. It takes two integers as input and outputs a single integer. If we wanted to be pedantic we could say $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ and say, for example, $+(3, 4) = 7$. No one actually does this. Instead we write $3 + 4 = 7$. So usually the symbol for a binary operation is place between the two elements. Note, though, there is a big difference between relations and binary operations. If R is a relation on $\mathbb{Z}$ and $\boxplus$ is an operation on $\mathbb{Z}$, then $3\ R\ 4$ is a statement that is either true or false. Whereas $3 \boxplus 4$ is a way of writing some integer value.

Class Example 7.2. Other examples of binary operations: $\cdot$ on $\mathbb{Q}$, $\circ$ on functions, matrix multiplication of square matrices.

Definition 7.2. An **algebraic system** is a set A with at least one binary operation and a (possibly empty) set of relations. Often an algebraic system is denoted as a tuple of the set, operations, and relations.

Class Example 7.3. Take $\mathbb{Z}$ with operations $+$ and $\cdot$ and the relation $\equiv_n$. We can denote this as $(\mathbb{Z}, +, \cdot, \equiv_n)$. This is the algebraic system of the integers mod n. It is more often denoted $\mathbb{Z}_n$.

Definition 7.3. If $B \subseteq A$ and $(A, *)$ is an algebraic system, then B is **closed with respect to** $*$ if and only if $x, y \in B$ implies $x * y \in B$.

Class Example 7.4. $\mathbb{Z} \subset \mathbb{R}$ and is closed under addition since the sum of two integers is an integer.

Example 7.1. Give an example of an infinite subset of $\mathbb{Z}$ that is not closed under addition.

Problem 7.1. *Consider the set* $5\mathbb{Z} = \{5n \mid n \in \mathbb{Z}\}$*. Show that* $5\mathbb{Z}$ *is closed under addition.*

Definition 7.4. A **Cayley Table** is an array of all possible inputs and outputs of a binary operation. The left column represents the first argument of the function, the top row the second.

Class Example 7.5. The following is the Cayley Table for $\mathbb{Z}_4$ under addition.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Example 7.2. Give the Cayley Table for $\mathbb{Z}_6$ under multiplication.

Example 7.3. Give the Cayley Table for $\wedge$ on the set $\{F, T\}$.

Example 7.4. Use the following Cayley Table to compute $(3 \boxplus 2) \boxplus (1 \boxplus 0)$.

$\boxplus$	0	1	2	3
0	3	2	1	3
1	3	2	3	2
2	1	2	1	1
3	3	0	2	1

Definition 7.5. A binary operation $*$ on a set A is **commutative** if and only if for all $x, y \in A$, $x * y = y * x$.

Class Example 7.6. Usual $+$ on $\mathbb{Z}$ is commutative because $n + m = m + n$ for all integers m and n.

Definition 7.6. A binary operation $*$ on a set A is **associative** if and only if for all $x, y, z \in A$, $x * (y * z) = (x * y) * z$.

Class Example 7.7. Function composition is associative since for all x in the domain

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = (f \circ (g \circ h))(x).$$

Definition 7.7. For a binary operation $*$ on a set A, an element $e \in A$ is the **identity** if and only if for all $x \in A$, $e * x = x * e = x$.

Class Example 7.8. The element 0 is the identity for $(\mathbb{R}, +)$ since $0 + x = x$ for all $x \in \mathbb{R}$.

Definition 7.8. For a binary operation $*$ on a set A with identity e, an element $y \in A$ is the **inverse** of $x \in A$ if and only if $y * x = e$.

Class Example 7.9. Since 0 is the identity for $(\mathbb{R}, +)$, then the inverse of 4 is -4 since $-4 + 4 = 0$.

Example 7.5. For the operation in Example 7.4, show that it is not commutative or associative. Explain also why there is not an identity or inverses.

Example 7.6. Prove that if $(A, *)$ has an identity then it is unique.

Class Example 7.10. If $e \in (A, *)$ is the identity of an associative algebraic system and for all $x \in A$ there is an inverse $y_x \in A$ (such that $y_x * x = e$), then for all $x \in A$, $x * y_x = e$.

Proof. Let $x \in A$. Then by assumption there is $y_x \in A$ with $y_x * x = e$. Also, since $x * y_x \in A$, by hypothesis there is $z \in A$ with $z * (x * y_x) = e$. Then

$$x * y_x = e * x * y_x = z * (x * y_x) * x * y_x = z * x * (y_x * x) * y_x = z * x * e * y_x = z * (x * y_x) = e.$$

So y_x also acts as an inverse on the other side. □

Problem 7.2. *Prove that if $(A, *)$ is associative and has an identity and $x \in A$ has an inverse, then the inverse is unique.*

Example 7.7. Give an example of an algebraic system with an identity where the inverse is not unique.

Example 7.8. Let U be a nonempty set. Consider the binary operation on $\mathcal{P}(U)$ given by $A \nabla B = (A \cup B) - (A \cap B)$. Prove or disprove that ∇ is commutative.

Problem 7.3. *Let U be a nonempty set. Consider the binary operation on $\mathcal{P}(U)$ given by $A \nabla B = (A \cup B) - (A \cap B)$. Prove or disprove that ∇ is associative.*

Problem 7.4. *Let U be a nonempty set. Consider the binary operation on $\mathcal{P}(U)$ given by $A \nabla B = (A \cup B) - (A \cap B)$. Prove or disprove that ∇ has an identity.*

Problem 7.5. *Let U be a nonempty set. Consider the binary operation on $\mathcal{P}(U)$ given by $A \nabla B = (A \cup B) - (A \cap B)$. Prove or disprove that every subset of A has an inverse.*

Problem 7.6. *Consider the binary operation on positive reals given by $x \otimes y = x^{\ln y}$. Prove or disprove that $\otimes$ is commutative.*

Problem 7.7. *Consider the binary operation on positive reals given by $x \otimes y = x^{\ln y}$. Prove or disprove that $\otimes$ is associative.*

Example 7.9. Consider the binary operation on positive reals given by $x \otimes y = x^{\ln y}$. Prove or disprove that $\otimes$ has an identity.

Problem 7.8. *Consider the binary operation on positive reals given by $x \otimes y = x^{\ln y}$. Prove or disprove that every positive real has an inverse.*

Example 7.10. Consider the binary operation on reals given by $x@y = \ln(e^x + e^y)$. Prove or disprove that @ is commutative.

Problem 7.9. *Consider the binary operation on reals given by $x@y = \ln(e^x + e^y)$. Prove or disprove that @ is associative.*

Problem 7.10. *Consider the binary operation on reals given by $x@y = \ln(e^x + e^y)$. Prove or disprove that @ has an identity.*

Example 7.11. Consider the binary operation on reals given by $x@y = \ln(e^x + e^y)$. Prove or disprove that every real has an inverse.

Example 7.12. Consider the binary operation on nonconstant differentiable functions that go through the origin $f \omega g = \int f'(x)g'(x)\ dx$. Prove or disprove that ω is commutative.

Example 7.13. Consider the binary operation on nonconstant differentiable functions that go through the origin $f \omega g = \int f'(x)g'(x)\ dx$. Prove or disprove that ω is associative.

Problem 7.11. *Consider the binary operation on nonconstant differentiable functions that go through the origin $f \omega g = \int f'(x)g'(x)\ dx$. Prove or disprove that ω has an identity.*

Problem 7.12. *Consider the binary operation on nonconstant differentiable functions that go through the origin $f \omega g = \int f'(x)g'(x)\ dx$. Prove or disprove that every nonconstant differentiable function has an inverse.*

Definition 7.9. For a binary operation $*$ on a set A with identity e, the **units of** A is the subset of all elements with an inverse.

Class Example 7.11. The units for $(\mathbb{R}, \cdot)$ is denoted $\mathbb{R}^{\times} = \{x \in \mathbb{R} \mid x \neq 0\}$.

Example 7.14. Determine the units of $(\mathbb{Z}, \cdot)$, where $\cdot$ is regular multiplication.

Example 7.15. Suppose $(A, *)$ is an algebraic system with identity e. Prove or disprove: e is a unit.

Problem 7.13. *Suppose $(A, *)$ is an algebraic system with identity e. Prove or disprove: The units of A are closed with respect to $*$.*