Introduction to mathematical reasoning

Chris Woodward
Rutgers University, New Brunswick

Copyright 2013, All right reserved.

CONTENTS

1. Introduction 2
2. Propositions and Connectives 2
2.1. Propositions 2
2.2. Connectives and compound propositions 3
2.3. Propositional Forms 4
2.4. Conditionals and biconditionals 6
2.5. Smullyan’s logic puzzles 7
3. Predicates and Quantifiers 9
3.1. Universal and existential quantifiers 9
3.2. Working with quantifiers 10
3.3. Quantifiers and numbers 11
3.4. Divisors and primes 12
3.5. Inequalities 13
4. Proofs by inference 14
4.1. Inference and a few other rules 14
4.2. More rules of inference 16
5. Proof by deduction and contradiction 18
5.1. Proof by deduction 18
5.2. Proof by contradiction 19
5.3. Arithmetic proofs by deduction or contradiction 21
6. Proofs involving quantifiers 22
6.1. Universal instantiation and existential generalization 22
6.2. Universal generalization and existential instantiation 24
6.3. Proofs of inequalities 26
6.4. More rules about quantifiers 27
7. Introduction to sets 28
7.1. Roster form and defining form 28
7.2. Subsets 29
7.3. Intersections and unions 29
7.4. Sets of subsets 31
7.5. Qualified quantifiers 31
7.6. Smullyan’s logic puzzles using sets 31
8. Proofs involving sets 32
8.1. Proving set containment and set equality 32
8.2. The set definition and roster axioms 33
8.3. Problems with naive set theory 36
9. Proof strategies and styles 37
9.1. Working backwards 37
9.2. Proof summaries 39
9.3. Writing proof summaries 39
9.4. Breaking proofs into pieces 41
10. Ordered pairs and relations 43
10.1. Ordered pairs and relations 43
10.2. Proofs involving relations 46
11. Functions 47
11.1. Functions 47
11.2. Injections, surjections, and bijections 48
11.3. Proofs involving functions 49
11.4. Sequences and convergence to infinity 50
11.5. Operations 51
12. Equivalence relations and partitions 53
12.1. Equivalence relations 53
12.2. Partitions and quotient sets 55
12.3. Cardinality 56
13. Natural numbers and induction 58
13.1. The induction axiom 58
13.2. The remainder theorem and base representation 60
13.3. The Peano axioms 62
14. Integers and primes 62
14.1. Properties of the integers 62
14.2. Prime numbers and prime factorizations 63
14.3. Common divisors 64
14.4. Fundamental theorem of arithmetic 65
14.5. Construction of the integers 67
14.6. Modular arithmetic 68
1. Introduction

These notes cover what is often called an “introduction to proof” course. In fact the main difficulty for students is translating their intuitive ideas about what should be true into precise statements, especially ones involving quantifiers. The beginning of the course, is inspired by an approach that I learned from B. Kaufman, and described in the Elements of Mathematics series he co-authored [3].

Some of the idiosyncrasies of the notes are as follows. First, every rule of inference is given an abbreviation, but I don’t ask students to memorize the abbreviations. Second, I couldn’t bring myself to completely identify \( P \vdash Q \), \( Q \) can be derived from \( P \), with the conditional statement \( P \implies Q \); which are not the same by Gödel. I note there is a difference, but say that students may identify the two notions for the purposes of the course. Third, I mostly assume standard properties of the natural numbers, integers etc. The Peano axioms, and construction of the integers and rationals as equivalence classes, are covered, but in a non-crucial way. So for example, natural numbers are introduced before sets, in an informal way in order to practice proofs; then as a set later.

Induction does not appear until Section 13.

Not all of the material is covered in a standard one-semester course. In most years, I skip the material in the subsections on operations, groups, the well-ordering principle and cardinality, although I talk briefly about countability near the end of the course.

Finally, a warning about my conventions: 0 is a natural number, and \((f \circ g)(x) = g(f(x))\).

2. Propositions and Connectives

2.1. Propositions. A statement that is either true or false will be called a proposition. The truth value of a proposition is either true or false, depending on which it is.

Here are some examples of statements, propositions, and truth values.

<table>
<thead>
<tr>
<th>Statement</th>
<th>Proposition?</th>
<th>Truth Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2 + 2 = 4 )</td>
<td>Yes</td>
<td>True</td>
</tr>
<tr>
<td>When ice melts, it turns into steam</td>
<td>Yes</td>
<td>False</td>
</tr>
<tr>
<td>Chris Woodward played for the New York Mets</td>
<td>Yes</td>
<td>True</td>
</tr>
<tr>
<td>Alexander Hamilton was a U.S. President</td>
<td>Yes</td>
<td>False</td>
</tr>
<tr>
<td>She is secretary of state</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>( x^2 = 36 )</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>This sentence is false</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

The fifth and sixth are not propositions because they are not sufficiently precise to have a definite truth value. That is, we don’t know whether \( x^2 = 36 \) is true or false until we know what \( x \) is. The last statement is not a proposition because it cannot be either true or false. It is called self-referential because it refers to itself. (Some self-referential statements can sometimes be considered propositions, but this isn’t one of them.)

Whether a given sentence is a proposition can be, in some situations, very debatable, depending on people agree on the meaning or not. For example, \( I \ never \ make \ spelling \ mistakes \) could be considered a proposition, if everyone agrees that ‘I’ means the author of these notes. The proposition, if it is one, is false. However, for the most part we will be able to agree on which statements are propositions.
A statement can be a proposition regardless of whether we know its truth value. For an off-beat example, consider that the statement *Columbus was the first person to arrive in North America* is definitely false, and off by about ten thousand years. *Columbus was the first European to arrive in North America* is also false, because of the Viking expedition to Newfoundland. But the statement *Columbus was Jewish* seems to be unknown, even if we can agree what it means. Statements about the future or far past tend to have unknown truth-values.

**Problem 2.1.** Which of the following are propositions? (Some are debatable.) Of those that are propositions, which have unknown (to you) truth values?

(1) It rained on Columbus’ fifth birthday in Madrid.
(2) It will rain on Barack Obama’s sixtieth birthday in Hawaii.
(3) It is raining.
(4) If it is raining, then it is cloudy.

**2.2. Connectives and compound propositions.** A *compound proposition* is a proposition formed from simpler propositions by the use of connectives such as *and*, *or* and *not*. For example, *the author of these notes is the greatest teacher ever, or the Tampa Bay is going to win the world series,* is a compound proposition. It might even be true! The statement *The author of this book is an American and the Devil Rays are a baseball team* is a compound proposition, which happens to be true, because of the two simple propositions that make up the compound the proposition both happen to be true.

Some propositions are true or false because of the assertions they make about external reality, while others are true or false because of their internal logical structure. The statement *It is Tuesday and it is not Tuesday* is a special kind of propositional, called a *tautology*. It is true because of its internal logical structure, and not because of external reality. The statement *It is Tuesday and it is not Tuesday* is a *contradiction*; it is false because of its internal logical structure.

**Problem 2.2.** (From [1]) Which of the following are propositions, in your opinion? (Some are slightly debatable.) Comment on the truth values of all the propositions you encounter; if a sentence fails to be a proposition, explain why.

(1) All swans are white.
(2) The fat cat sat on the mat. Look in thy glass and tell whose face thou viewest. My glass shall not persuade me I am old.
(3) Father Nikolsky penned his dying confession to Patriarch Arsen III Charnoyevich of Pe in the pitch dark, somewhere in Poland, using a mixture of gunpowder and saliva, and a quick Cyrillic hand, while the innkeeper’s wife scolded and cursed him through the bolted door.
(4) 1,000,000,000 is the largest integer.
(5) There is no largest integer. There may or may not be a largest integer.
(6) Intelligent life abounds in the universe.
(7) This definitely is a proposition.
(8) The speaker is lying.
(9) This is exercise number 12.
(10) This sentence no verb.
(11) ”potato” is spelled p-o-t-a-t-o-e.
Problem 2.3. Which of the following are propositions? (Some are slightly debatable.) Explain. For each that is, describe the truth value and explain.

(1) Washington was the first US president, and Jefferson was second.
(2) Washington was the first US president or Jefferson was second.
(3) It is not true that Washington was the first US president or Jefferson was second.
(4) It is not true that Washington was the first US president and Jefferson was second.
(5) Washington was the first US president but Jefferson was not the second.

Propositional Forms. Sentences in English can have ambiguous compound structure. For instance, the meaning of I am not paranoid is clear enough. I am not paranoid or distrustful probably means It is not true that I am paranoid or distrustful, which is equivalent to I am not paranoid and I am not distrustful. But what does you can have soup or salad and sandwich mean? Of course there are many other kinds of ambiguity in English. (Headlines: Police help dog bite victim. Drunk gets nine months in violin case.)

Propositional forms represent the structure of propositions more precisely than we can in English.

Definition 2.4. A propositional variable is a (usually capital) letter representing a proposition. A propositional form is an expression of propositional variables involving connectives, formed according to the following rules:

1. If P is a propositional form then (NOT P) is a proposition.
2. If P, Q are propositional forms then (P OR Q), (P AND Q) are propositional forms.

For example, the proposition form of It is Monday and it is not raining is (P AND (NOT Q)) where P = It is Monday and Q = It is raining.

Problem 2.5. Find a propositional form for the following sentences, involving at least two symbols each.

(1) He loves me not.
(2) He loves her but can’t seem to commit.
(3) You can’t have your cake and eat it too.
(4) He can’t play violin or cello.

Answer to (c) NOT (P AND Q) where P is “You can have your cake” and Q is “You can eat it too”.

Note that each propositional variable represents a proposition with a definite truth value. A common mistake is to say, in the previous example, Q = “eat it too”. But “eat it too” is neither true nor false, and so not a proposition.

Problem 2.6. Which of the following are propositional forms?

(1) (P AND (NOT Q))
(2) (P AND Q OR S)
(3) (P NOT AND S)
(4) ((NOT P) AND (NOT Q))
(5) (NOT (NOT P))
(6) NOT (NOT P)

We won’t always be consistent about using the parentheses in this way, for example, we often drop the outside parentheses which are somewhat redundant. We can also drop the inside parentheses if there is no confusion. For example, (P AND Q) AND R is the same as P AND (Q AND R), so we write it as P AND Q AND R. However, (P AND Q) OR R is not the same as P AND (Q OR R) (as in for example the soup and salad example above) so we have to keep the parentheses.

Any propositional form has a truth table, which lists the truth values of the form depending on the truth values of the variables. The truth tables for AND, OR, NOT are

<table>
<thead>
<tr>
<th>P</th>
<th>NOT P</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

Figure 2. Truth table for NOT

There are actually two kinds of or in English usage. The first, inclusive or, is true if both are true, while exclusive or is false if both or true. For example, Biden is vice president or Biden is president of the senate is false under exclusive or, since both statements are true. Exclusive or is sometimes written XOR, and has the truth table in Figure 5.
When we use or in English, we often mean exclusive or. For example, if the waiter says *it comes with a soup or salad* he probably means that you can choose on or the other, but not both. In mathematics, we always mean **inclusive or**, unless explicitly stated. For example, if we say that *ab is even then a is even or b is even*, we mean that both are possibly even.

When writing larger truth table, it helps to have symbols for the connectives AND, OR, NOT are \( \land, \lor, \neg \). For example, the propositional form P AND (NOT Q) is written \( P \land (\neg Q) \).

To obtain a truth table for a compound expression, we make a table with a column for each of its constituents, and a row for each possible set of truth values for the propositional variables. For example, the truth table for \( (P \land (\neg Q) \land R) \) is

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>R</th>
<th>( (\neg Q) )</th>
<th>( (P \land (\neg Q)) )</th>
<th>( (P \land (\neg Q) \land R) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

How do you know what to put in the columns of a truth table? One way to solve this is to write the expression in **tree form**. Figure 7 shows the tree form for \( (P \land (\neg Q) \land R) \).

When writing larger truth table, it helps to have symbols for the connectives AND, OR, NOT are \( \land, \lor, \neg \). For example, the propositional form P AND (NOT Q) is written \( P \land (\neg Q) \).

To obtain a truth table for a compound expression, we make a table with a column for each of its constituents, and a row for each possible set of truth values for the propositional variables. For example, the truth table for \( (P \land (\neg Q) \land R) \) is

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>R</th>
<th>( (\neg Q) )</th>
<th>( (P \land (\neg Q)) )</th>
<th>( (P \land (\neg Q) \land R) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

How do you know what to put in the columns of a truth table? One way to solve this is to write the expression in **tree form**. Figure 7 shows the tree form for \( (P \land (\neg Q) \land R) \).

In tree form, each vertex corresponds to an operation ADD, OR, NOT. The highest level operation, in this case AND, is at the top.

**Problem 2.7.** Find the tree form for

1. \( (P \land Q) \lor (\neg (R \land S)) \).
(2) NOT (NOT (P AND Q))
(3) NOT (P AND (Q OR R))

Two propositional forms are called equivalent if they have the same truth values.

Problem 2.8. Which of the following are equivalent forms?

(1) P, ¬(¬P)
(2) ¬(P ∧ Q), (¬P) ∨ (¬Q)
(3) ¬(P ∨ Q), (¬P) ∧ (¬Q)
(4) (¬Q) ∨ P, ¬((Q ∧ (¬P))

Answer: (1),(2),(3). The first equivalence is double negation. The second and third equivalences are called de Morgan’s laws. For example, an example of (3) is that the statement He can’t play violin or cello, or put another way, it’s not true that he can play violin or cello, is equivalent to He can’t play violin and he can’t play cello.

Problem 2.9. Find a propositional form for the following sentences, involving at least two symbols each. Write the meaning of each variable clearly, as a proposition.

(1) He left and ran away without paying the bill.
(2) He left but he’s coming back.
(3) He ran away and he’s not coming back.
(4) He didn’t have the money, or he forgot.
(5) You can have a sandwich and either soup or salad.

Problem 2.10. Find the truth table for the propositional forms (i) P ⇒ Q (ii) P ⇒ P. (iii) (P ∧ Q) ∨ (P ∧ R). (iv) (P ⇒ Q) ⇔ (¬P ∨ Q). (v) P ∨ Q (vi) P ⇔ ¬P. (vii) (P ∧ Q) ∨ R (x) (P ⇒ (Q ∧ R)) ⇒ (P ⇒ Q) ∧ (P ⇒ R). Identify any tautologies or contradictions.

2.4. Conditionals and biconditionals. Let’s introduce two new connectives. The first new connective is the conditional: P IMPLIES Q or IF P THEN Q is written P ⇒ Q. Its truth table is

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>P ⇒ Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

For example, x = 2 ⇒ x² = 4 is true, because of the hypothesis x = 2 is true then so is the conclusion x² = 4. But an implication is automatically true if the hypothesis is false: for example, if pigs can fly, then the moon is made of cheese is true! The statement if the moon is made of cheese, then George W. Bush is a great president says nothing about the author’s political views.

An equivalent form of P ⇒ Q is (¬P) ∨ Q.

The second new connective is the biconditional: P IF AND ONLY IF Q or P IFF Q or P ⇔ Q for short. It’s truth table is

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>P ⇔ Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

In other words, P ⇔ Q is true if and only if P and Q are equivalent forms.

P ⇒ Q is equivalent to (P ⇒ Q) ∧ (Q ⇒ P).

P ⇒ Q is equivalent to (¬Q) ⇒ (¬P). For example, if it’s raining, then it’s cloudy is equivalent to if it’s sunny, then it’s not raining.

Problem 2.11. Your chia pet is kidnapped. The ransom note reads, If you don’t pay the ransom, you will never see your chia again! Is there anything you can do to save your chia? (From [3].)

Thinking that P ⇒ Q is the same as (¬P) ⇒ (¬Q) is called the error of the converse. It is the most common error among students learning to write proofs.

Problem 2.12. Write the truth tables for

(1) Q ⇔ Q
(2) (P ⇒ Q) ⇔ (Q ⇒ P)
(3) (P ⇔ Q) ⇔ (Q ⇔ P).

A propositional form is a tautology if its truth values are all true, and a contradiction if its truth values are all false. For example, P ∨ (¬P) is a tautology, while P ∧ (¬P) is a contradiction.

Problem 2.13. Which of the following are tautologies? Contradictions? Explain your answer briefly, or write out a truth table.
One common source of tautologies is equivalent forms. $P$ and $Q$ are equivalent propositional forms, if and only if $P \iff Q$ is a tautology. For example, the first de Morgan’s law says that $(\neg(P \land Q))$ is equivalent to $(\neg P) \lor (\neg Q)$. So $(\neg(P \land Q)) \iff ((\neg P) \lor (\neg Q))$ is a tautology.

In practice, rather than writing out the truth table, you will want to try out an example.

**Problem 2.14.**

1. Guess whether $((P \land Q) \implies R) \iff (P \implies R) \land (Q \implies R)$ is a tautology by writing out the English sentence, substituting it rains for $P$, I forget my umbrella for $Q$ and I get wet for $R$. Do the same problem another way by writing out an equivalent form of $(P \land Q) \implies R$ by changing the implies to an or and using de Morgan’s law.

2. Guess whether $((P \lor Q) \implies R) \implies (P \implies R) \land (Q \implies R)$ is a tautology by writing out the English sentence, substituting it’s Saturday for $P$, it’s Sunday for $Q$ and it’s the weekend for $R$. We will come back to this example at the end of the next section.

3. Guess whether $(P \implies (Q \land R)) \iff ((P \implies Q) \land (P \implies R))$ is a tautology by writing out an example in English. Check your answer by writing out an equivalent form, changing the implication to an or.

2.5. Smullyan’s logic puzzles. Here is a puzzle from the books of R. Smullyan, whose inclusion in these knots is inspired by an approach that I learned from B. Kaufman, and described in the Elements of Mathematics series he co-authored [3].

An island has two kinds of inhabitants:

- **Knights** always tell the truth.
- **Knaves** always lie.

Two of the island’s inhabitants, A and B, were talking together. A observed, at least one of us is a knave. What are A and B?

We can reason as follows:

- **A is a knight**
  - A is telling the truth
  - A is a knave or B is a knave
  - B is a knave

- **A is a knave**
  - A is lying
  - neither A nor B is a knave
  - A is a knight
  - contradiction.

A must be a knight and B a knave.

Let’s try another puzzle. Two of the island’s inhabitants, A and B, were talking to a stranger. A says, Either I am a knave or B is a knight. What are A and B?

- **A is a knight**
  - A is telling the truth
  - A is a knave or B is a knight
  - B is a knight

- **A is a knave**
  - A is lying
  - A is a knight AND B is a knave
  - contradiction!

So A and B are knights.

Finally, our last puzzle. Three of the island’s inhabitants A, B, and C were talking together. A: B is a knave. B: A,C are the same type. What is C?

- **A is a knight**
  - A is telling the truth
  - B is a knave
  - B is lying
  - A,C are not the same type
  - C is a knave

- **A is a knave**
  - A is lying
  - B is a knight
  - B is telling the truth
  - C is a knave

Let’s identify some of the kinds of reasoning we used above.

**Reasoning by deduction:** If one statement implies a second and the first statement holds, then the second does as well. For example, if “B is a knight implies B is telling the truth” holds and “B is a knight” then we know that “B is telling the truth”.
**Reasoning by cases:** If there are only finitely many possibilities, we can examine each one separately.

**Reasoning by contradiction:** If some assumption leads to a contradiction, then the opposite of that assumption must be true.

For puzzles such as the ones above, there is a fool-proof method to find the answer: enumerate all the possible cases, and determine which are consistent with the assumptions. However, enumerating all the cases can take a lot of time. We are more interested in reasoning which establishes the answer without enumerating all the cases.

**Problem 2.15.** (Smullyan via [3])

1. An island has two kinds of inhabitants, knights and knaves. Naves always lie, and knights always tell the truth. Two of the island’s inhabitants A and B were talking together. A remarked, "I am a knave, but B isn’t." What are A and B?
2. Three of the island’s inhabitants A, B, and C were talking together. A said, "All of us are knaves." Then B remarked, "Exactly one of us is a knave." What is C?
3. Two of the islanders A and B exactly one of whom is a werewolf, make the following statements: A: The werewolf is a knight. B: The werewolf is a knave. Which one is the werewolf?
4. There is exactly one werewolf in the group and he is a knight. The other two members of the group are knaves. Only one person makes a statement: B: C is a werewolf. Who is the werewolf? (Hint: Argue that B must be a knave by showing that it is impossible for him to be a knight.)

**Problem 2.16.** (Smullyan via [3])

1. Two of the island’s inhabitants A and B were talking together. A remarked, "I am a knave, but B isn’t." What are A and B?
2. Three of the island’s inhabitants A, B, and C were standing together in a garden. A stranger passed by and asked A, "Are you a knight or a knave?" A answered, but rather indistinctly, so the stranger could not make out what he said. The stranger then asked B, "What did A say?" B replied, "A said that he is a knave." At this point the third man, C, said, "Don’t believe B; he is lying!". The question once again is, what are B and C?
3. Three of the island’s inhabitants A, B, and C were talking together. A remarked, "B is a knave." Whereupon B commented, "A and C are of the same type." What is C?
4. A stranger came across three of the island’s inhabitants A, B, and C. A volunteered this information: "B and C are of the same type." The stranger then asked C, "Are A and B of the same type?" What was C’s answer?
5. A stranger came across two of the island’s inhabitants A and B resting under a tree. He asked A, "Is either of you a knight?" A responded and, as a result, the stranger knew the answer to his question. What are A and B?
6. A stranger came across two of the island’s inhabitants A and B lying in the sun. He asked A, "Is B a knight?" A answered either "Yes" or "No." Then the stranger asked B, "Is A a knight?" B also answered either "Yes" or "No." Are A’s and B’s answers necessarily the same?
7. Inhabitants of Bahava are knights, knaves, or normal people (who sometimes lie and sometimes tell the truth.) Three inhabitants of Bahava A, B, and C are having a conversation. The group includes one knight, one knave, and one normal person. They make the following statements: A: I am normal. B: That is true. C: I am not normal. What are A, B, and C?
8. Three inhabitants of Bahava A, B, and C are having a conversation. The group includes one knight, one knave, and one normal person. They make the following statements:
   - A: I am normal. B: That is true. C: I am not a knight.
   - A: I am normal. B: That is true. C: I am not a knight.
   What are A, B, and C?
9. Two inhabitants of Bahava A and B are talking to a stranger. They make the following statements:
   - A: B is a knight. B: A is not a knight.
   Can the stranger be sure that at least one of A and B is a normal person who is telling the truth?
(11) Two inhabitants of Bahava A and B are talking to a stranger. They make the following statements:
   A: B is a knight. B: A is a knave.
   Can the stranger be sure that at least one of A and B is a normal person?

(12) Two inhabitants of Bahava A and B are talking to a stranger. They make the following statements:
   A: I am of lower rank than B. B: That’s not true!
   What are A and B? Are they telling the truth?

(13) Three inhabitants of Bahava A, B, and C are talking to a stranger. The three Bahavans include one knight, one knave, and one normal person. Two of them make the following statements:
   A: B is of higher rank than C. B: C is of higher rank than A.
   The stranger then asked C, "Who has higher rank, A or B?"
   What was C’s response?

(14) A married couple of Bahavans Mr. and Mrs. A are talking to a stranger. They make the following statements:
   Mr. A: My wife is not normal. Mrs. A: My husband is not normal.
   What are Mr. and Mrs. A?

(15) A married couple of Bahavans Mr. and Mrs. A are talking to a stranger. They make the following statements:
   Mr. A: My wife is normal. Mrs. A: My husband is normal.
   What are Mr. and Mrs. A?

(16) Two married Bahavan couples Mr. and Mrs. A and Mr. and Mrs. B are talking to a stranger. Three of them make the following statements:
   Mr. A: Mr. B is a knight. Mrs. A: My husband is right; Mr. B is a knight. Mrs. B: That’s right. My husband is indeed a knight.
   What are each of the four people, and which (if any) of the three statements are true?

(17) Two of the islanders A and B exactly one of whom is a werewolf, make the following statements:
   A: The werewolf is a knight. B: The werewolf is a knave.
   Which one is the werewolf? [Hint: B is either a knight or a knave. Consider the implications of each of these two possibilities.]

3. Predicates and Quantifiers

3.1. Universal and existential quantifiers. Some statements are not propositions because they contain unknowns. For example, the sentence she loves that kind of ice-cream is not a proposition because she and that kind are unknown.

A collection of possible values for an unknown variable is called a universe. For example, my daughters Sophie, Julia is a universe for she. mint chocolate chip, strawberry is a universe for that kind.

A statement containing unknowns that becomes a proposition after substitute a value for each unknown is a predicate.

For example, the statement \( P(x) \) given by \( x^2 = 4 \) is a predicate statement. If we substitute \( x = 2 \), then the predicate becomes a proposition, which happens to be true.

Besides substitution, another way of turning a predicate into a proposition is by adding a quantifier. The two kinds of quantifiers are

<table>
<thead>
<tr>
<th>technical name</th>
<th>meaning</th>
<th>notation</th>
<th>other meanings</th>
</tr>
</thead>
<tbody>
<tr>
<td>universal</td>
<td>for all</td>
<td>( \forall )</td>
<td>for every</td>
</tr>
<tr>
<td>existential</td>
<td>there exists</td>
<td>( \exists )</td>
<td>there is, there are some</td>
</tr>
</tbody>
</table>

For example, suppose that \( P(x) \) is the predicate \( x \) likes chocolate, and \( x \) is an unknown representing one of my daughters Sophie, Julia.

\( \forall x, P(x) \) means all my daughters like chocolate. \( \exists x, P(x) \) means one of my daughters likes chocolate, or there exists a daughter that likes chocolate.

The truth value of a proposition involving a quantifier depends on the universe for the unknown(s). For example, if \( P(x) \) is \( (x^2 = 4) \implies x = 2 \), then \( \forall x, P(x) \) is true if the universe for \( x \) is positive integers, but false if the universe for \( x \) is all integers.

Problem 3.1. Find the truth value of the propositions below where \( P(x, y) \) is the predicate given by \( y = x^2 + 3 \).

(1) \( P(2, 7) \)
(2) \( P(2, 8) \)
(3) \( \forall x, y, P(x, y) \)
(4) \( \exists x, y, P(x, y) \)
(5) \( \forall x, \exists y P(x, y) \)
(6) \( \exists x, \forall y P(x, y) \)
Everyone was rested and relaxed means Everyone was rested and everyone was relaxed.

A proposition that is obtained from a universally quantified proposition by substitution is called an instance of the quantified proposition. For example, all prime numbers greater than 2 are odd can be written $\forall n, n \text{ prime } \land n \geq 2 \implies n \text{ odd}$. 5 is odd is an instance of that proposition.

**Problem 3.2.** Consider the statement $P(x, y)$, for all integers $x, y$: $P(x, y)$ if $x^k \leq y^2$. Which of the following are instances of $P(x, y)$?

1. $2^3 \leq 3^2$.
2. $2^2 \leq 2^2$.
3. $2^2 \leq 3^3$

Answer: Only (1),(2). (1) is an instance with $x = 2, y = 3$; 2 is an instance with $x = 2, y = 2$. (3) is not an instance.

**Problem 3.3.** Consider the statement $P(n, a)$, for all integers $n$ and any prime number $a$: $P(n, a)$ if $a$ is a divisor of $n^a - n$. Which of the following are instances of $P(n, a)$? (From M. Saks)

1. 5 is a divisor of $4^5 - 4$.
2. 3 is a divisor of $8^3 - 3$.
3. 4 is a divisor of $5^4 - 5$.

**Problem 3.4.** In each case find a predicate statement so that each of the statements below is an instance of it.

1. $2|3 \iff \exists x, 2x = 3$. $2|4 \iff \exists x, 2x = 4$. $2|5 \iff \exists x, 2x = 5$.
2. $2|3 \iff \exists x, 2x = 3$. $2|4 \iff \exists x, 2x = 4$. $3|4 \iff \exists x, 3x = 4$.
3. $3|4 \land 3|7 \iff 3|3$. $4|5 \land 4|8 \iff 4|3$. $5|10 \land 5|25 \iff 5|15$.

**Problem 3.5.** In each problem find a predicate statement so that each of the statements three statements is an instance of the single predicate statement.

1. $2^2 \cdot 3^2 = 2^5$. $3^2 \cdot 3^3 = 3^5$. $10^2 \cdot 10^3 = 10^5$.
2. $2^2 \cdot 4^2 = 2^6$. $3^2 \cdot 3^3 = 3^5$. $10^2 \cdot 10^{-1} = 10^1$.
3. $2^3 \cdot 2^4 = 2^4$. $3^2 \cdot 3^3 = 3^6$. $3^n \cdot 3 = 3^{n+1}$.

**3.2. Working with quantifiers.** In some cases, one can distribute quantifiers over connectives. For example,

1. Everyone was rested and relaxed is the same as Everyone was rested and everyone was relaxed.

(2) Someone was singing or humming means Someone was singing or someone was humming.

(3) Someone was singing and humming is not the same as Someone was singing and someone was humming.

(4) Everyone was singing or humming is not the same as Everyone was singing or everyone was humming.

More formally, for any predicate statements $P(x), Q(x)$,

1. $\forall x, (P(x) \land Q(x)) \iff (\forall x P(x)) \land (\forall x Q(x))$
2. $\exists x, (P(x) \lor Q(x)) \iff (\exists x P(x)) \lor (\exists x Q(x))$

There is no rule for distributing $\forall$ over $\lor$, or $\exists$ over $\land$.

A negation can be moved on the inside of a quantifier, if the type of quantifier is changed: For example, “there does not exist a perfect person” is the same as “all people are not perfect”, and “there exists a person who is not perfect” is the same as “not all people are perfect”. We call this rule “quantifier conversion”. More formally,

1. $\neg(\forall x, P(x)) \iff (\exists x, \neg P(x))$
2. $\neg(\exists x, P(x)) \iff (\forall x, \neg P(x))$

**Problem 3.6.** Use quantifier conversion on each of the following statements:

1. Not all math books are correct.
2. All math books are not correct.
3. Some math teachers don’t know what they are talking about.
4. There does not exist a math professor who can teach well.

Answer to (i) There exists a math book that is not correct.

We write a negation of a quantifier by using a slash through the quantifier. For example, “there does not exist a direct flight from New York to Marseille” is written $\nexists f, f$ is a direct flight from New York to Marseille.

If a predicate contains more than one unknown, then the order that the quantifiers is added makes a difference. For example, suppose that $P(x, y)$ means $x$ likes flavor $y$ of ice cream. $\forall x, \exists y P(x, y)$ means that everyone likes some flavor. What does $\exists y, \forall x P(x, y)$ mean?

**Problem 3.7.** (From [1]) Suppose that $P(x, y)$ means astronaut $x$ will visit planet $y$. What is the predicate form of

1. Some planets will be visited by every astronaut.
Every good girl deserves fruit.
Good boys deserve fruit always.
All cows eat grass.
No cows eat grass.
Some cows are birds but no cows are fishes.
Although some city drivers are insane, Dorothy is a very sane city driver.

Problem 3.8. Translate into English the predicate forms

1. $\forall x, \forall y F(x, y)$
2. $\exists y, \forall x F(x, y)$
3. $\forall x, \exists y F(x, y)$
4. $\exists x, \exists y F(x, y)$

where $F(x, y)$ means $x$ is friends with $y$. (We won’t bother specifying a universe for these variables, if you like it can be all living people.)

Problem 3.9. Find the predicate form of “Just because I am paranoid doesn’t mean that no one is following me.”

Answer. Let $P$ be “I am paranoid” and $Q$ be “someone is following me”. Then “no one is following me” is $\neg Q$ and “Just because I am paranoid doesn’t mean that no one is following me” is the same as “It is not true that because I am paranoid means that no one is following me”. The words “means” has the same logical meaning as “implies”, so we get $\neg(P \implies \neg Q)$. One can break it down even more: suppose that $R(x)$ means $R(x)$ is following me, then we get $\neg(\forall x (\neg R(x)))$.

Problem 3.10. Find the equivalent form of $\neg(\forall x (\exists y, R(x)))$ obtained by distributing the $\neg$ as much as possible.

Sometimes we wish to say not only that there exists a value of $x$ such that $P(x)$ is true, but also that the value is unique. In that case, we write $\exists! x, P(x)$. An equivalent form is

$$\exists x, P(x) \land \forall y (y \neq x \implies \neg P(y)).$$

Problem 3.11. Translate each of the sentences into a statement in the predicate calculus. (From [1])

1. Every good girl deserves fruit.
2. Good boys deserve fruit always.
3. All cows eat grass.
4. No cows eat grass.
5. Some cows are birds but no cows are fishes.
6. Although some city drivers are insane, Dorothy is a very sane city driver.
7. Even though all mathematicians are nerds, Woodward is not a nerd.
8. If one or more lives are lost, then all lives are lost.
9. If every creature evolved from lower forms, then you and I did as well.
10. Some numbers are larger than two; others are not.
11. Every number smaller than 6 is also smaller than 600

Problem 3.12. Translate the statements into words. (From [1].)

1. $\forall x (R(x) \implies S(x))$; $R = "$is a raindrop," $S = "$makes a splash.$
2. $\exists y (C(y) \implies M(y))$; $C = "$is a cowboy," $M = "$is macho.$
3. $\exists z (D(z) \land W(z))$; $D = "$is a dog," $W = "$whimpers.$
4. $\exists z (D(z) \land \neg W(z))$; $D = "$is a dog," $W = "$whimpers.$
5. $\forall x (D(x) \implies \neg W(x))$; $D = "$is a dog," $W = "$whimpers.$
6. $\neg \forall x (D(x) \implies W(x))$; $D = "$is a dog," $W = "$whimpers.$
7. $\exists y (C(y) \land C(y) \land W(z) \land \neg W(y))$; $C = "$is a cat," $W = "$whimpers.$
8. $\forall x (P(x) \implies \exists y (P(y) \land L(x, y)))$, $P = "$is a person," $L(x, y) = "$y is older than x.$

Problem 3.13. Let $P(x)$ be “$x$ is a fast food joint” $Q(x)$ be “$x$ serves hamburgers”, $R(x)$ be “$x$ is open only to truckers” and $S(x)$ be “$x$ is open all night”. Translate the following into good English sentences. Based on your knowledge of fast food joints, say whether each statement is true or false.

(i) $\forall x, P(x) \implies Q(x)$
(ii) $\exists x, P(x) \land Q(x)$
(iii) $\forall x, P(x) \implies R(x)$
(iv) $\exists x, P(x) \land S(x)$

3.3. Quantifiers and numbers. In this section we begin to investigate mathematical statements involving quantifiers. The numbers here are either natural numbers $0, 1, 2, 3, \ldots$ or integers $\ldots, -2, -1, 0, 1, 2, \ldots$. By definition

$$2 = 1 + 1, 3 = 2 + 1, 4 = 3 + 1, \ldots, 10 = 9 + 1.$$

Some authors do not include 0 as a natural number. If you’re unsure, it’s best to say which convention you are using.
Addition and multiplication are operations on the natural numbers, written + and ·. For example,

\[ 2 + 3 = 5, \quad 2 \cdot 3 = 6. \]

Sometimes the symbol for multiplication is omitted if the meaning is clear. The first two natural numbers 0, 1 are the additive unit and multiplicative unit respectively, so that

\[ 0 + x = x = 0, \quad 1x = x1 = x \]

for any integer \( x \). For the moment we assume the standard properties of addition and multiplication:

**Assumption 3.14.** For all integers \( x, y, z \)

1. \( 0 + x = x = 0 + x \)
2. \( x + y = y + x \)
3. \( x + (y + z) = (x + y) + z \)
4. \( x + z = y + z \implies x = y \)
5. \( 0 = x + y \implies x = 0 \land y = 0 \)
6. \( 0x = x0 = 0 \)
7. \( xy = yx \)
8. \( x(yz) = (xy)z \)
9. \( 0 = xy \implies x = 0 \lor y = 0 \)
10. \( x(y + z) = xy + xz \)

Propositions involving natural numbers are often expressed using quantifiers. However, it can be difficult to go from the English sentence that one typically uses to the symbolic form.

**Example 3.15.** Find the symbolic form of the propositions

1. 11 is not the square of any integer.
2. 13 is the sum of two integers bigger than 5.

For (a), we note that 11 is the square of another integer, call it \( x \), iff \( x^2 = 11 \). The English phrase “not any” is the same as “there does not exist”. So the symbolic form is \( \neg \exists x, x^2 = 11 \).

For (b), to say that 13 is the sum of two integers bigger than 5 means that 13 is the sum of some two integers bigger than 5. Some is the same as “there exists”. So the symbolic form is \( \exists x, y, x \geq 5 \land y \geq 5 \land x + y = 13 \).

We say that an integer is square if it is the square of some integer.

**Problem 3.16.** Write the following mathematical statements using only symbols. Are the statements true?

1. The sum of any integer with itself is twice that integer.
2. Every integer is one plus some other integer.
3. The only integer which squares to zero is zero.
4. If two positive integers have the same square, then they are equal.
5. Three is not square.
6. One is square.

**3.4. Divisors and primes.** We say \( a \) divides \( b \), or is a divisor of \( b \), and write \( a \mid b \) iff \( \exists c, ac = b \) and say \( a \) is a divisor of \( b \). For example, \( 2 \mid 4 \) but \( \neg (2 \mid 5) \). The divisors of 12 are 1, 2, 3, 4, 6, 12. A common mistake is to write \( 2 \mid 4 \) using a horizontal or slanted line. Note that \( \frac{2}{4} \) is a number, namely one-half, while \( 2 \mid 4 \) is a proposition which is true or false (in this case true.)

**Problem 3.17.** Which of the following are numbers? Which are propositions? Which are just badly formed? Of the propositions, which are true?

1. \( 2 \mid 4 \)
2. \( 2 \mid 4 \)
3. \( 4 \mid 2 \)
4. \( 4 \mid 2 \)
5. \( 4 \mid 2 \)
6. \( 2 \mid 4 \Rightarrow 2 \mid 6 \)
7. \( 2 \mid 4 \Rightarrow 2 \mid 6 \)
8. \( 2 \mid 4 > 2 \mid 6 \).

**Problem 3.18.** Write the following mathematical statements using only symbols. Are the statements true?

1. 3 divides 9.
2. 2 and 3 are divisors of 12.
3. Any integer divides its square.
4. 1 divides any integer.
5. Every integer divides zero.

An answer to (2) is \( 2 \mid 12 \land 3 \mid 12 \); true.

**Definition 3.19.** An integer \( n \) is even if \( 2 \mid n \), and \( n \) is odd if \( 2 \mid (n + 1) \). Equivalently, \( n \) is odd iff \( n - 1 \) is even.
For example, 6 is even iff $2|6$ which is true.

**Definition 3.20.** An integer $n$ is square iff $\exists m, m^2 = n$.

For example, 9 is square iff $\exists m, m^2 = 9$ which is true, namely, $m = \pm 3$.

A natural number $p$ is prime iff its only divisors are 1 and itself and $p \neq 1$. For example, 2, 3, 7 are prime. More formally, $p$ is prime if and only if

$$p \neq 1 \land \forall d, (d|p \implies d = 1 \lor d = p).$$

**Problem 3.21.** Write the following mathematical statements using only symbols. Are the statements true?

1. 5 is an odd integer.
2. 16 is a square integer.
3. Any integer is even or odd.
4. The square of an odd integer is odd.
5. Any square integer greater than 4 is odd.
6. 9 is a prime number.

An answer to (1) is $\exists c, 2c + 1 = 5$; true.

**Problem 3.22.** (From P.F. Reynolds, Jr.) Express the following statements in English, and find their truth value. Let $P(x)$ be the statement $x$ is an odd integer and $Q(x)$ the statement $x$ is a prime integer, and $R(x)$ the statement $3x$ is an odd integer.

1. $\forall x, Q(x) \land P(x)$.
2. $\forall x, Q(x) \implies R(x)$.
3. $\exists x, P(x) \land R(x)$.

Sometimes a universally proposition is false, but can be made true after changing the hypotheses slightly. For example, all prime numbers are odd can be written $\forall p, p$ prime $\implies p$ odd. This is false, but can be made true by adding the hypothesis that $p$ is at least 3: $\forall p, p$ prime $\land p \geq 3 \implies p$ odd.

We say that $a$ is a $k$-th root of $b$ if $a^k = b$. For example, 2 and $-2$ are square $k$-th roots of 4 for $k = 2$.

**Problem 3.23.** Find the predicate form of the statement “4 has a unique positive square root”.

Answer: $(\exists x, x^2 = 4 \land x > 0) \land \forall y, y \neq 0, (x^2 = 4 \land y^2 = 4 \land x > 0 \land y > 0) \implies x = y$. The first part says there is a square root and the second part says that the square root is unique.

**Problem 3.24.** Find a predicate form of the following statements. (Hint: each of your answers should contain a quantifier.)

1. 11 is even.
2. 11 is prime.
3. 9 is divisible by 3.
4. $x^2 - 6x + 9 = 0$ has a solution.
5. 9 has a positive square root.
6. $-5$ does not have a 4-th root.
7. 9 has a unique positive square root. (Please do not use the symbol $\exists!$ for this problem.)
8. $x^2 - 6x + 9 = 0$ has a unique solution.

Determine which statements are true or false.

### 3.5. Inequalities

From the rest of this section, we work only with natural numbers. We define $x \leq y \iff \exists z, x + z = y$ and $x < y \iff (\exists z, x + z = y \land z \neq 0)$.

For example, $2 \leq 6 \iff \exists x, 2 + x = 6$

where the universe for $x$ is all natural numbers. This is true since $2 + 4 = 6$.

We will assume for the moment standard properties of $\leq$ for all natural numbers $x, y, z$:

1. $0 \leq x$
2. $x \leq x$
3. $x \leq y \land y \leq z \implies x \leq z$
4. $x \leq y \lor y \leq x$
5. $x \leq y \implies xz \leq yz$
6. $x \leq y \implies x + z \leq y + z$

We say that $x$ is the largest (or smallest) natural number with a given property if all other natural numbers with that property are smaller.
Problem 3.25. Find the predicate form of “There is a largest even natural number”.

Answer: “There is” means $\exists$. “Largest even number” means that all other even numbers are less than that it. So an equivalent English formulation is, “there exists an even number so that all other even numbers are less than it”. Or equivalently, “there exists an even number such that all even numbers are at most equal to it”. Even means divisible by two. So in English, “there exists a number divisible by two, such that all other numbers divisible by two are less than or equal to it”. In predicate form, $\exists a, 2|a \land \forall b, 2|b \implies b \leq a$.

Problem 3.26. Find the predicate form of “There is no largest even number”.

Answer: “There is no largest number” means “It is not true that there is a largest number”. So the predicate form is $\neg \exists a, 2|a \land \forall b, 2|b \implies b \leq a$.

Problem 3.27. Find the predicate form of the following statements; each answer should contain at least one quantifier.

(1) 100 is the largest natural number.
(2) 0 is the smallest natural number.
(3) There is no largest natural number.
(4) There is no smallest even natural number.
(5) There is no largest prime number.
(6) There is no smallest prime number.

Determine which statements are true or false.

Problem 3.28. Determine the truth of the following statements about the integers.

(1) $\forall x, \exists y, x \leq y$.
(2) $\exists y, \forall x, x \leq y$.
(3) $\forall x, \neg \forall y, x \leq y$.
(4) $\forall x, \forall y, \neg (x \leq y)$.
(5) $\exists x, \neg \exists y, x \leq y$.

Problem 3.29. In Problem 2.14 (2), we talked about the sentence “If it’s the weekend, then it’s Saturday or it’s Sunday”. There are actually two possible meanings, depending on the meaning of it. Does it mean today, or does it mean any day? If the second meaning holds, then the predicate form is $\forall d, \text{weekend}(d) \implies (\text{sat}(d) \lor \text{sun}(d))$ where $\text{sat}(d)$ means $d$ is Saturday etc. This is not equivalent to saying that “If it’s the weekend, then it’s Saturday, or if it’s the weekend, then it’s Sunday, which has predicate form, ($\forall d, \text{weekend}(d) \implies \text{sat}(d)$) $\lor$ ($\forall d, \text{weekend}(d) \implies \text{sat}(d)$). To see why not, let’s change the implies to an or: $\forall d, \neg \text{weekend}(d) \lor (\text{sat}(d) \lor \text{sun}(d))$. It’s not allowed to distribute a universal quantifier over an or, so this is not the same as $(\forall d, \neg \text{weekend}(d) \lor \text{sat}(d)) \lor (\forall d, \neg \text{weekend}(d) \lor \text{sat}(d))$.

4. PROOFS BY INFERENCE

Now we discuss how to prove mathematical propositions. The truth of propositional forms can always be established by writing out the truth table. For more complicated propositions, such as predicates, we can never write out all the possibilities, and so if we want to establish their truth we have to use proofs. Informally, a proof is a sequence of statements with justifications which establish the truth of a proposition from a set of hypotheses.

4.1. Inference and a few other rules. The most common method of proof is proof by inference, also called modus ponens in Latin. The basic pattern of inference goes like this:

If my alarm clock is ringing, then it is time to wake up.
My alarm clock is ringing.
Therefore it is time to wake up.

Using propositional variables,

$P \implies Q$. $P$. Therefore $Q$.

$P$ is called the premise or hypothesis and $Q$ is the conclusion. Note that both the statements $P$ and $Q$ used in inference can be complicated propositions. For example, the reasoning “If someone stole the cookies and it wasn’t me, then it was you and you’re going to jail. Someone stole the cookies and it wasn’t me. It was you and you’re going to jail” has propositional form
\[(P \land Q) \implies (R \land S). P \land Q. \text{Hence } R \land S.\]

**Problem 4.1.** Write the conclusion of reasoning by inference in each of the following examples, if possible.

1. If it is Memorial Day, then the post office is closed. It is Memorial Day.
2. If it is raining and I don’t have an umbrella, I will get wet. It is raining and I don’t have an umbrella.
3. \((P \land Q) \implies R. P \land Q. \text{Hence } R \land S.\)
4. \(P \lor (Q \implies R). P \lor Q.\)
5. \((P \implies Q) \implies R. P.\)

In the case of propositional forms, we can be completely precise about what we mean by a proof. In the following, for the moment a *statement* means a propositional form; later it will be a mathematical proposition or once we introduce more rules, a predicate statements.

**Definition 4.2.** (Proof) Suppose that \(H_1, \ldots, H_n, Q\) are statements. A sequence \(P_1, \ldots, P_k\) of statements is a *proof* (or *demonstration*) of \(Q\) from hypotheses \(H_1, \ldots, H_n\) if and only if

1. The last statement \(P_k\) is \(Q\); and
2. each statement \(P_1, \ldots, P_k\) is either
   a. one of the hypotheses;
   b. a tautology;
   c. follows by inference from two earlier statements.

If \(n = 0\), that is, there are no hypothesis, then \(P_1, \ldots, P_k\) is a *hypothesis-free proof*. If there is a proof of \(Q\) using \(H_1, \ldots, H_n\), we write \(H_1, \ldots, H_n \vdash Q\), and say \(Q\) *can be deduced from* \(H_1, \ldots, H_n\), or \(\vdash Q\) if \(Q\) has a hypothesis-free proof.

The most important thing about the above definition to notice is that you cannot write down a statement until you know it is true. For example, suppose that you are trying to show that 16 is not prime given a collection of hypotheses. The statement 16 is not prime is the last, not the first statement in the proof.

The symbol \(\vdash\) translates as “from which it follows that”, or “from which can be proved that”. For the purposes of this course it will turn out to be the same as the symbol \(\implies\) for “implies”. For the moment, let’s keep the two notions separate. \(^1\)

When writing proofs, it is helpful to write the justification in the second column. Later on, we will move to a more informal style.

**Problem 4.3.** Show \((P \land Q) \vdash P.\)

1. \(P \land Q\) hypothesis
2. \((P \land Q) \implies P\) tautology
3. \(P\) inf on 1,2

**Problem 4.4.** Show \(P, Q \vdash P \land Q.\)

1. \(P\) hyp (hypothesis)
2. \(Q\) hyp
3. \(P \implies (Q \implies (P \land Q))\) taut (tautology)
4. \((Q \implies (P \land Q))\) inf on 1,3
5. \((P \land Q)\) inf on 2,4

**Problem 4.5.** Show that \(P \implies Q, Q \implies R \vdash P \implies R.\)

Some of the proofs above will be used over and over. We introduce names for them, so that we don’t have to repeat the argument. The names for the rules are not so important; you could make up your own, for example, conjunctive simplification could be called “simplifying and”.

\(^1\)The two notions can be different: \(P \implies Q\) means that \(Q\) is true whenever \(H_1, \ldots, H_n\) is true. \(P \vdash Q\) means that \(Q\) can be derived from \(H_1, \ldots, H_n\) by some set of rules that have to be specified. In the 1940’s Gödel showed that there are some statements that are true given a set of hypotheses, but that can never be derived from the hypotheses, in any system of logic “sufficient to reproduce elementary arithmetic.”. So in general, \(\implies\) is not the same as \(\vdash\).
Definition 4.6. (More rules of inference)

\[ P \land Q \vdash P \text{ (or } P \land Q \vdash Q) \] will be called conjunctive simplification (cs).
\[ P, Q \vdash P \land Q \] will be called conjunctive inference (ci).
\[ P \vdash P \lor Q \] will be called disjunctive inference (di).
\[ P \Rightarrow Q, Q \Rightarrow R \vdash P 
\Rightarrow R \] will be called transitivity of implication (ti).
\[ (P \land (Q \lor R)) \vdash (P \land Q) \lor (P \land R) \] or vice-versa or \((P \lor (Q \land R)) \vdash (P \lor Q) \land (P \lor R) \) and vice-versa will be called distribution of conjunction and disjunction (distrib).
\[ P \Rightarrow Q \vdash (\neg Q) \Rightarrow (\neg P) \] will be called contrapositive inference or contra inf for short.

Problem 4.7. Which of the following represent valid reasoning? If so, what is the rule?

1. \( P, Q \land R \vdash P \land (Q \land R) \)
2. \( P \vdash P \land Q \)
3. \( P \vdash P \lor (Q \Rightarrow R) \)
4. \( Q \Rightarrow R \vdash P \lor (Q \Rightarrow R) \)
5. If it's Sunday then it's the weekend \( \vdash \) If it's the weekend then it's Sunday.
6. \( P \Rightarrow \neg(Q \Rightarrow R) \vdash (Q \Rightarrow R) \Rightarrow \neg P \).

Problem 4.8. Show \( S \land P, P \Rightarrow Q, Q \Rightarrow R \vdash R \).

\[
\begin{align*}
1 & \quad S \land P \quad \text{hyp} \\
2 & \quad P \quad \text{cs on 1} \\
3 & \quad P \Rightarrow Q \quad \text{hyp} \\
4 & \quad Q \quad \text{inf on 2,3} \\
5 & \quad Q \Rightarrow R \quad \text{hyp} \\
6 & \quad R \quad \text{inf on 4,5}
\end{align*}
\]

Problem 4.9. Show that \( P, P \Rightarrow Q \vdash P \land Q \).

Remark 4.10. If you don't know how to start, start by writing down all the hypotheses. For the most part, we won't be doing problems with unnecessary hypotheses, so you might as well write down all the hypotheses at the beginning.

Problem 4.11. Prove the statements (using the tautologies and inference).

\[ 1 \quad Q, S, (Q \land S) \Rightarrow R \vdash R. \]
\[ 2 \quad P, Q \land S \vdash P \land S. \]
\[ 3 \quad P, (P \lor R) \Rightarrow S \vdash S. \]
\[ 4 \quad (P \Rightarrow Q) \vdash ((P \Rightarrow Q) \lor (P \Rightarrow R)). \]
\[ 5 \quad ((P \land Q) \lor (\neg(P \land Q))) \Rightarrow R \vdash R. \]
\[ 6 \quad P, (P \leftrightarrow Q) \vdash Q. \]
\[ 7 \quad ((P \land Q) \lor (\neg(P \land Q))) \Rightarrow R \vdash R. \]
\[ 8 \quad P, (P \leftrightarrow Q) \vdash Q. \]
\[ 9 \quad (\neg(P \land (\neg P))) \Rightarrow Q \vdash Q. \]
\[ 10 \quad P, (\neg Q) \vdash (\neg(P \Rightarrow Q)). \]
\[ 11 \quad P, Q, R, ((P \land Q) \Rightarrow S), ((S \land R) \Rightarrow T) \vdash T. \]
\[ 12 \quad (P \land Q) \vdash Q. \]
\[ 13 \quad (P \Rightarrow (Q \land R)), (P \land Q) \vdash R. \]
\[ 14 \quad (P \Rightarrow Q) \vdash ((\neg Q) \Rightarrow (\neg P)). \]
\[ 15 \quad Q \vdash (P \Rightarrow Q). \]

4.2. More rules of inference. We now introduce some more rules. The first is contrapositive inference: if \( P \) implies \( Q \) and \( Q \) is not true, then \( P \) cannot be true either. For example, if we know that rain means the presence of clouds, and it is not cloudy, then it cannot be raining. Or to give a more amusing example: “If he doesn’t get out of bed, nothing bad will happen to him. Something bad happened to him. So he got out of bed.” (The first proposition is an excellent reason never to attend class.) Contrapositive inference is also called modus tollens, or contra inf for short. In symbols, \( P \Rightarrow Q, \neg Q \vdash \neg P \). A proof using modus ponens \(^2\) is

\[
\begin{align*}
1 & \quad P \Rightarrow Q \quad \text{hyp} \\
2 & \quad (P \Rightarrow Q) \Rightarrow (\neg Q \Rightarrow \neg P) \quad \text{taut.} \\
3 & \quad \neg Q \Rightarrow \neg P \quad \text{inf on 1,2} \\
4 & \quad \neg Q \quad \text{hyp} \\
5 & \quad \neg P \quad \text{inf on 3,4}
\end{align*}
\]

Problem 4.12. Show \( \neg R, P \Rightarrow Q, Q \Rightarrow R \vdash \neg P \). (2) \( \neg P \Rightarrow Q, Q \Rightarrow R \vdash \neg R \). (2) \( \neg P \Rightarrow Q, Q \Rightarrow R \vdash \neg R \).

Problem 4.13. (From [3]) Translate the following into a proof. “If the basketball team’s fast break runs well, the team will win. If the center

\(^2\) It will not always be the case that we can always deduce the new rules we want from previously introduced rules; a rule that cannot be so deduced is usually called an axiom.
rebounds well, the fast break will work. So if the team loses, the center did not rebound well.

**Remark 4.14.** There are many different forms of contrapositive inference. You might wonder how to justify the following reasoning:

1. $P \implies Q$ (hyp)  
2. $\neg Q \implies \neg P$ (???)

Strictly speaking, you should write out some more steps

1. $P \implies Q$ (hyp)  
2. $(P \implies Q) \implies (\neg Q \implies \neg P)$ (taut)  
3. $\neg Q \implies \neg P$ (inf on 1,2)

However, in a little while, we will become more informal, and then a single line of justification will be enough:

1. $P \implies Q$ (hyp)  
2. $\neg Q \implies \neg P$ (equiv form of 1)

The second rule we will call

\textit{disjunctive conversion (dc):} $P \implies Q \equiv (\neg P) \lor Q$.

A proof is

1. $P \implies Q$ (hyp)  
2. $(P \implies Q) \implies ((\neg P) \lor Q)$ (taut)  
3. $\neg P \lor Q$ (inf on 1,2)

By \textit{distributing negation} (also called \textit{de Morgan’s law}) we mean the rule of inference

$\neg (P \land Q) \equiv (\neg P) \lor (\neg Q)$

or vice-versa. The proof uses the tautology $\equiv (\neg (P \land Q)) (\neg P) \lor (\neg Q)$.

\textit{Inference by cases (ic):} $S \implies U, T \implies U \lor (S \lor T) \implies U$. A proof is

1. $S \implies U$ (hyp)  
2. $T \implies U$ (hyp)  
3. $((\neg S) \lor U)$ (dc on 1)  
4. $((\neg T) \lor U)$ (dc on 3)  
5. $((\neg S) \lor U) \land ((\neg T) \lor U)$ (ci on 3,4)  
6. $((\neg S) \land (\neg T)) \lor U$ (distrib on 5)  
7. $(S \lor T) \implies U$ (dc on 6)

A particularly useful trick is to use that $P \lor (\neg P)$ is always true. This implies something that might be closer to what we really mean by inference by cases:

**Problem 4.15.** Show

1. $P \implies Q, \neg P \implies Q \equiv Q$.
2. $P \implies (Q \lor R), Q \implies S, R \implies S \lor (P \implies S)$.
3. $S \implies Q, (R \implies Q) \implies (P \land T), R \implies S \lor T$.
4. $Q \implies S, (\neg R) \implies Q, R \implies S \lor S$.

We also find it useful to give a name to the reasoning $P \lor Q, \neg P \implies Q$. We call it the \textit{disjunctive alternative} (da).

It’s also useful to note that $(P \implies (Q \lor R) \equiv (P \implies Q) \lor (P \implies R)$ or vice-versa or $(P \implies (Q \land R) \equiv (P \implies Q) \land (P \implies R)$ and vice-versa will be called \textit{distribution of implication over conjunction or disjunction}.

Finally, we have rules of inference for the biconditional that are similar to those for the conditional:

\textit{Transitivity of the biconditional} (tb) is $P \iff Q, Q \iff R \iff R$.

\textit{Inference (Modus Ponens) for the biconditional} (inf) is $P \iff Q, P \iff Q$.

\textit{Modus Tollens for the biconditional} (contra infb) is $P \iff Q, \neg Q \iff P$.

\textit{Symmetry (of the biconditional)} (sbc) is $(P \iff Q) \equiv (Q \iff P)$.

Technically speaking, one should also use symmetry to justify the rules $P \lor Q \iff Q \lor P$ and $P \land Q \iff Q \land P$.

**Problem 4.16.** (From [3]) Show that

1. $(S \implies Q), (R \implies Q) \implies (P \land T), (R \implies S) \lor T$.
2. $(Q \iff S), (R \iff Q), (R \iff S) \lor S$.
3. $(Q \implies R) \land P), ((Q \implies R) \equiv (\neg T) \equiv (\neg T)$.
4. $(Q \iff R), ((\neg P) \equiv Q), (\neg P) \equiv P$.
5. $(\neg R) \iff (S), (S \iff P \land Q), (R \iff T), (\neg T) \iff Q$.
6. $(Q \iff S), (\neg S), (R \iff S) \lor (\neg Q) \lor (\neg R))$.
7. $(R \lor S), (P \iff (Q \land T)), (P \iff (R \iff (Q \lor T))) \iff Q$.
8. $(S \land R), (Q \iff T), (R \iff (\neg T)) \lor (\neg Q) \lor S)$.
9. $(\neg S \iff \neg (P \lor (\neg T))), (T \iff (Q \lor R), (\neg S) \lor (R \lor Q)$.
This means that I will repeat it over and over, not that you necessarily will.

$$Q \implies P \vdash (P \iff Q).$$

$$(- (\neg P) \land (-Q)), (S \implies (-Q)), (\neg (\neg P) \lor S) \vdash (Q \iff (-P)).$$

$$P \implies Q, (R \implies S), (Q \implies R) \vdash (P \implies S).$$

$$P \implies Q, P, (Q \implies R) \vdash R.$$

$$(- (\neg P) \implies Q), (R \implies Q) \implies S), (\neg S) \lor T), (R \implies (-P)) \vdash (T \lor V).$$

**Problem 4.17.** Translate into propositional form: (From [3].)

1. I can’t go to Mary’s party and go to Jim’s party. If I go to Jim’s party, Mary will be upset. I won’t upset Mary, but I will go to one of the parties. So, I will go to Mary’s party.

2. If Bill doesn’t play baseball, then Pete will be the shortstop. If Mike doesn’t pitch, then Pete won’t play shortstop. Therefore, if Bill doesn’t play, Mike will pitch.

3. If mathematics is important as an experience in thinking, then we should study it. If it is important as a tool for other subjects, we should also study it. Mathematics is important either as an experience in thinking or as a tool for other subjects. So, we should study mathematics.

5. **Proof by deduction and contradiction**

Next we introduce several methods for proving if-then statements. A mathematical example is the following: *if a given integer is even, then its square is also even*. To prove such a statement, we have two choices: we can assume that the given integer is even, and deduce that its square is also even; this is called *proof by deduction*. Or we can assume that its square is *not* even, and deduce that the integer is not even either. This is called *proof by contradiction*.

5.1. **Proof by deduction.** *Proof by deduction* means that in order to show that $P$ implies $Q$, it suffices to assume $P$ and prove $Q$. The statement $P$ is called a *temporary hypothesis*.

It might seem intuitive that “$P$ implies $Q$” is the same as “$Q$ follows from $P$”. For example, $x + 1 = 2$ implies $x = 1$ is the same as saying that $x = 1$ follows from $x + 1 = 2$. This is the content of the *deduction theorem* of Herbrand-Tarski, at least for propositional forms, which is a more formal version of the *proof by deduction* principle:

**Theorem 5.1** (Deduction Theorem). For any propositional forms $S, H_1, \ldots, H_n, T, S, H_1, \ldots, H_n \vdash T$ if and only if $H_1, \ldots, H_n \vdash S \implies T$. In particular, $S \vdash T$ is the same as $S \implies T$.

In English, this takes the form of the mantra\(^4\)

*Mantra: to prove that $S \implies T$, first assume $S$, and then deduce $T$.*

When I use the deduction theorem, I will use the abbreviation *temp hyp* for *temporary hypothesis*. Here is an example of the theorem in action:

**Problem 5.2.** Show $S, ((S \land P) \implies Q) \vdash (P \implies Q)$.

1. $S$ hyp
2. $(S \land P) \implies Q$ hyp
3. $P$ temp hyp
4. $(S \land P)$ ci on 1,3
5. $Q$ inf on 2,4
6. $S, P, (S \land P) \implies Q \vdash Q$ 1-5
7. $S, (S \land P) \implies Q \vdash P \implies Q$ deduc on 6

**Remark 5.3.** The last line of the proof is no longer the conclusion, so technically only lines 1-5 above form a proof (of line 6). The last two lines explain that we are using proof by deduction. Usually we will note the use of proof by deduction at the beginning, rather than the end.

**Problem 5.4.** Prove $((-R) \implies P), ((P \land (-S)) \implies Q) \vdash ((- (R \lor S)) \implies Q)$.

1. $-(R \lor S)$ hyp
2. $-R \land -S$ de Morgan’s 1
3. $-R$ cs 2
4. $-R \implies P$ hyp
5. $P$ inf 3,4
6. $P \land -S$ cs,ci 2,5
7. $(P \land -S) \implies Q$ hyp
8. $Q$ inf 6,7
9. $(- (R \lor S)) \implies Q$ deduc 1-8

\(^3\)Most mathematicians take this for granted. The reason is that situations where $\vdash$ is not the same as $\implies$ are so rare. What is true under any consistent axiom system for mathematics is that if $P \vdash Q$, then $P \implies Q$.

\(^4\)This means that I will repeat it over and over, not that you necessarily will.
Problem 5.5. Show \( \vdash ((P \implies Q) \land (Q \implies R)) \implies (P \implies R) \).

Problem 5.6. (From [3]) Using inference by cases or the deduction theorem, show

\[
\begin{align*}
(1) & \quad (P \implies (Q \land S)) \vdash (P \implies (Q \lor S)). \\
(2) & \quad (P \implies (Q \iff S)), (Q, (R \implies (Q \iff S)) \vdash ((P \lor R) \implies S) \\
(3) & \quad ((\neg Q) \implies (R \lor S)), (S \iff (P \lor R)), (\neg P) \vdash ((R \implies Q) \\
(4) & \quad (P \implies R), (Q \implies T), ((R \land T) \iff S) \vdash ((P \land Q) \implies S). \\
(5) & \quad (S \implies P), (Q \implies R), S \vdash ((P \implies Q) \implies R) \\
(6) & \quad (R \implies T), ((\neg T) \iff S), ((R \land (\neg S)) \implies (\neg Q)) \vdash (R \implies (\neg Q)) \\
(7) & \quad (P \implies R), ((P \land R) \implies S), ((\neg S) \lor Q) \vdash (P \implies Q) \\
(8) & \quad (P \iff S), (Q \iff T) \vdash ((P \land Q) \iff (S \land T)). \\
(9) & \quad ((\neg P) \land S) \iff R), ((\neg P) \iff S), (\neg P) \vdash (\neg (P \lor (\neg R))). \\
(10) & \quad ((\neg P) \iff Q), (Q \iff R), R \implies (\neg P) \\
(11) & \quad (Q \iff S), (R \iff (\neg S)), (P \iff (\neg R)) \vdash (P \iff (\neg Q)). \\
(12) & \quad (Q \iff R), ((\neg P) \iff Q), (\neg R) \vdash P \\
(13) & \quad (P \iff (\neg S)), (Q \iff S) \vdash (P \implies (\neg Q)).
\end{align*}
\]

5.2. Proof by contradiction. Everyone is familiar with reasoning by contradiction: John Doe cannot be guilty of the murder. For suppose he did it, ...... which is usually followed by arguments that he was on the other side of the country, playing golf, etc. The advantage of proof by contradiction is that it gives one more hypothesis to play with. The informal version of the proof by contradiction is:

To show a statement \( C \), assume its opposite and show a contradiction.

A more formal version is:

\[ \neg C \vdash \bot \]

Theorem 5.7 (Contradiction Theorem). Suppose that \( H_1, \ldots, H_n, S, C \) are propositions, and \( C \) is a contradiction. Then \( H_1, \ldots, H_n \vdash S \) is equivalent to \( H_1, \ldots, H_n, \neg S \vdash C \).

Here are two examples.

Problem 5.8. Prove by contradiction that \( Q \implies \neg P, ((\neg R) \implies (P \land Q)) \vdash R \).

1. \( Q \implies \neg P \) \quad hyp
2. \( (\neg R) \implies (P \land Q) \) \quad hyp
3. \( \neg R \) \quad temp hyp
4. \( P \land Q \) \quad inf 2,3
5. \( Q \) \quad cs 4
6. \( \neg P \) \quad inf 1,5
7. \( P \) \quad cs 4
8. \( P \land \neg P \) \quad ci 6,7, contra
9. \( R \) \quad proof by contra, 3-8

Problem 5.9. Prove by contradiction \( P \implies (\neg S), S \lor (\neg R), \neg(Q \lor (\neg R)) \vdash \neg P \).

Here is a harder example:

Problem 5.10. \( P \lor Q, (\neg R) \implies (\neg S)), ((Q \lor P) \implies S), ((\neg (T \land U)) \implies (\neg R)) \vdash (U \land T) \)

1. \( \neg (U \land T) \) \quad temp hyp
2. \( \neg (T \land U) \implies \neg R \) \quad hyp
3. \( \neg R \) \quad inf 1,2
4. \( \neg R \implies \neg S \) \quad hyp
5. \( \neg S \) \quad inf 3,4
6. \( Q \lor P \implies S \) \quad hyp
7. \( \neg (Q \lor P) \) \quad contra inf 5,6
8. \( \neg Q \land \neg P \) \quad dm (de Morgan’s) 7
9. \( \neg P \) \quad cs 8
10. \( P \lor Q \) \quad hyp
11. \( Q \) \quad da 9,10
12. \( \neg Q \) \quad cs 8
13. \( Q \land \neg Q \) \quad ci 11,12, contra
14. \( U \land T \) \quad proof by contra 1-13

Proof by contradiction is often easier than a direct proof, because it increases the number of hypotheses. This gives a

Mantra: If you’re stuck, try proof by contradiction.

Often, but not always, proofs by contradiction can be made into shorter direct proofs afterwards.

Problem 5.11. (From [3]) Determine, for each of the following five claims, whether or not it is a logical consequence of the following three
assumptions. Assumptions: 1. If Jim’s arm hurts, he pitches badly. 2. If Jim pitches badly, the team loses. 3. If Jim pitches badly or the team loses, the crowd does not applaud. Claims: 1. If the crowd applauds, then Jim’s arm does not hurt. 2. If the team loses, Jim’s arm hurts. 3. If the crowd does not applaud, then the team loses. 4. If Jim pitches badly, then his arm hurts and the crowd applauds. 5. If Jim’s arm does not hurt and he pitches badly and the crowd applauds, then the team loses.

**Problem 5.12.** (From [3]) Using the deduction theorem, proof by contradiction, etc show that

\[
\begin{align*}
(1) \; & ((\neg P) \Rightarrow (Q \land R)), \; (P \Rightarrow (\neg S)) \vdash (S \Rightarrow Q). \\
(2) \; & (P \Rightarrow Q), \; (((\neg P) \lor R) \Rightarrow S) \vdash (Q \lor S). \\
(3) \; & ((\neg P) \Rightarrow Q), \; (Q \Rightarrow (R \land (\neg S))) \vdash ((S \lor (\neg Q)) \Rightarrow P). \\
(4) \; & ((\neg R) \Rightarrow P), \; ((P \land (\neg S)) \Rightarrow Q) \vdash ((\neg (R \lor S) \Rightarrow Q). \\
(5) \; & (P \Rightarrow (Q \Rightarrow R)) \vdash (Q \Rightarrow (P \Rightarrow R)) \\
(6) \; & (Q \Rightarrow R) \vdash (((\neg Q) \Rightarrow (\neg P)) \Rightarrow (P \Rightarrow R)). \\
(7) \; & (P \Rightarrow Q), \; (Q \Rightarrow (\neg R)), \; (R, \; (S \Rightarrow P) \vdash (\neg S). \\
(8) \; & (S \Rightarrow (P \land (\neg Q))), \; ((\neg S) \Rightarrow (\neg R)), \; R \vdash ((\neg Q) \land P). \\
(9) \; & (P \Rightarrow Q), \; (Q \Rightarrow R), \; ((P \Rightarrow R) \Rightarrow (\neg S)), \; ((\neg S) \Rightarrow T) \Rightarrow T. \\
(10) \; & (T \Rightarrow Q), \; (P \Rightarrow Q), \; (R \Rightarrow Q) \vdash (((P \lor R) \lor T) \Rightarrow Q). \\
(11) \; & (R \Rightarrow S), \; ((R \Rightarrow (\neg P)) \Rightarrow Q), \; (S \Rightarrow (\neg P)), \; T \vdash (Q \land T). \\
(12) \; & (P \Rightarrow Q), \; (R \Rightarrow S), \; (P \lor R), \; (\neg Q) \Rightarrow S. \\
(13) \; & (P \land Q), \; ((\neg R) \Rightarrow (\neg S)), \; ((Q \land P) \Rightarrow S), \; ((\neg (T \land U) \Rightarrow (\neg R)) \vdash (U \land T). \\
(14) \; & ((\neg P) \Rightarrow (\neg R)), \; (\neg S), \; (P \Rightarrow S), \; (\neg (R) \Rightarrow Q) \vdash Q. \\
(15) \; & (\neg P), \; (\neg Q), \; (R \Rightarrow P) \vdash (\neg (Q \lor R)). \\
(16) \; & ((\neg (T \land R)), \; ((\neg T) \Rightarrow S), \; ((\neg R) \Rightarrow S) \vdash S. \\
(17) \; & ((Q \land R) \Rightarrow S), \; ((\neg S) \land R) \vdash (\neg Q). \\
(18) \; & ((S \land P) \Rightarrow Q) \vdash (S \Rightarrow ((\neg P) \lor (Q \lor R))). \\
(19) \; & (P \Rightarrow ((R \land T) \Rightarrow S)), \; R, \; (S \Rightarrow Q), \; (\neg (T \Rightarrow Q)) \vdash (\neg P). \\
(20) \; & (R \Rightarrow (\neg P)), \; (R \Rightarrow U), \; (Q \Rightarrow (S \Rightarrow T)), \; ((U \land (\neg P)) \Rightarrow ((\neg S) \lor T) \vdash ((R \lor Q) \Rightarrow (S \Rightarrow T)). \\
(21) \; & (\neg P), \; (S \Rightarrow (P \lor Q)), \; (Q \Rightarrow R), \; ((S \Rightarrow Q \land T) \Rightarrow U) \vdash (S \Rightarrow Q) \iff (T \Rightarrow U). \\
(22) \; & (P \Rightarrow S), \; (R \Rightarrow (\neg S)), \; R \vdash (\neg P). \\
(23) \; & (S \land (\neg T)), \; (S \Rightarrow (\neg R)), \; ((\neg P) \Rightarrow Q) \vdash (R \Rightarrow Q). \\
(24) \; & (R \Rightarrow (\neg S)), \; (Q \Rightarrow R) \vdash (S \Rightarrow (\neg Q)). \\
(25) \; & (P \Rightarrow (\neg Q)), \; ((\neg R) \Rightarrow Q) \vdash (P \Rightarrow R). \\
(26) \; & (R \Rightarrow (\neg Q)), \; (((\neg P) \Rightarrow S) \Rightarrow R), \; ((\neg Q) \Rightarrow (\neg S)), \; (\neg P) \vdash (\neg ((\neg P) \Rightarrow S)). \\
(27) \; & (R \Rightarrow (\neg Q)), \; (\neg (S \land (\neg R))) \vdash (Q \Rightarrow (\neg S)). \\
(28) \; & (((\neg P) \Rightarrow Q), \; (Q \Rightarrow (R \Rightarrow S)), \; (\neg S) \vdash (R \Rightarrow P). \\
(29) \; & ((\neg P) \Rightarrow (\neg S)), \; (P \Rightarrow R), \; (R \Rightarrow (\neg T)) \vdash (S \Rightarrow (\neg T)). \\
(30) \; & (R \lor S), \; (P \lor (\neg R)), \; (P \iff Q) \vdash S.
\end{align*}
\]

Some proofs can involve both proof by contradiction and proof by deduction.

**Example 5.13.** Show that \( P \Rightarrow Q, \; (Q \land S) \Rightarrow R, \; \neg R \vdash S \Rightarrow \neg P. \)

1. \( S \) temp hyp
2. \( P \) temp hyp
3. \( P \Rightarrow Q \) hyp
4. \( Q \) inf on 1,3
5. \( Q \land S \) ci on 1,4
6. \( (Q \land S) \Rightarrow R \) hyp
7. \( R \) inf on 5,6
8. \( \neg R \) hyp
9. \( R \land \neg R \) ci on 7,8, contra
10. \( P \) proof by contra on 2-9
11. \( S \Rightarrow \neg P \) proof by deduc on 1-10

The temporary hypotheses introduced have to be removed in opposite order. That is, if you introduce \( S \) and then \( P \) as temporary hypotheses, then \( P \) has to be removed as a temporary hypothesis by citing proof by contradiction or deduction, and then \( S \) has to be removed as a temporary hypothesis by proof by contradiction or deduction as well.

Unfortunately once we allow proof by deduction and contradiction, we have to change our definition of proof, for the following reason. Suppose one uses proof by deduction to show that some proposition \( P \) implies proposition \( Q \). So line 1 reads \( P \) hyp. Following the proof by deduction, one can write on the next line \( P \Rightarrow Q \). Now, one cannot use line 1 in the lines following \( P \Rightarrow Q \), because this was a temporary assumption, which holds only up to the line \( P \Rightarrow Q \). This leads to a change in our Definition 4.2 of proof:
Definition 5.14. (Proof by Deduction and Contradiction) Suppose that $H_1, \ldots, H_n, Q$ are propositional forms. A sequence $P_1, \ldots, P_k$ of propositional forms is a proof (or demonstration) of $Q$ from hypotheses $H_1, \ldots, H_n$ if and only if

1. The last statement $P_k$ is $Q$; and
2. each statement $P_1, \ldots, P_k$ is either
   a) one of the hypotheses;
   b) a tautology;
   c) a temporary hypothesis;
   d) follows by inference, proof by deduction or contradiction from earlier statements not used in proof by deduction or contradiction.

Table 1 contains a summary of the rules of inference and methods of proof we have developed so far. Note that the last two, proof by deduction and contradiction, are in a different class than the previous rules; they require a “metalanguage” to state formally.

5.3. Arithmetic proofs by deduction or contradiction.

Problem 5.15. Show the following statements using proof by deduction. You may assume basic arithmetic and algebraic facts. For each answer, write out a summary of the proof.

1. $x^2 = 9 \iff x = \pm 3$.
2. $x = \pm \sqrt{9}$.
3. $x = \sqrt{9}$.
4. $x^2 = 9$.
5. $x = 3$.
6. $x = -3$.
7. $x = 0$.
8. $x = 0$.
9. $x = 0$.
10. $x = 0$.

Table 1. Some rules of propositional calculus

<table>
<thead>
<tr>
<th>Rule</th>
<th>Name (Abbrev)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P, P \implies Q \vdash Q$</td>
<td>$\inf$</td>
</tr>
<tr>
<td>$P \implies Q, \neg Q \vdash \neg P$</td>
<td>$\contra inf$</td>
</tr>
<tr>
<td>$P \lor Q \vdash P \land Q$</td>
<td>$\conj inf$</td>
</tr>
<tr>
<td>$P \land Q \vdash P$</td>
<td>$\conj si inf$</td>
</tr>
<tr>
<td>$P \vdash P \lor Q$</td>
<td>$\disj inf$</td>
</tr>
<tr>
<td>$\neg(P \land Q) \vdash Q$</td>
<td>$\disj alt$</td>
</tr>
<tr>
<td>$P \implies Q, Q \implies R \vdash (P \lor Q) \implies R$</td>
<td>$\inf by cases$</td>
</tr>
<tr>
<td>$P \implies Q, Q \implies R \vdash P \implies R$</td>
<td>$\trans of impl$</td>
</tr>
<tr>
<td>$P \equiv Q \equiv ((P \implies Q) \land (Q \implies P))$</td>
<td>$\def of bicond$</td>
</tr>
<tr>
<td>$P, P \equiv Q \vdash Q$</td>
<td>$\bicond inf$</td>
</tr>
<tr>
<td>$P \equiv Q, Q \equiv R \vdash P \equiv R$</td>
<td>$\trans of bicond$</td>
</tr>
<tr>
<td>$-P \lor Q, Q \lor -P \vdash R$</td>
<td>$\de Morgan’s$</td>
</tr>
<tr>
<td>$P, Q \lor -P \equiv (P \lor Q) \lor (Q \lor -P)$</td>
<td>$\de Morgan’s$</td>
</tr>
<tr>
<td>$(P \lor Q) \lor R \equiv (P \lor R) \lor (Q \lor R)$</td>
<td>$\distrib of \lor over \lor$</td>
</tr>
<tr>
<td>$(P \land Q) \lor R \equiv (P \lor R) \land (Q \lor R)$</td>
<td>$\distrib of \land over \lor$</td>
</tr>
<tr>
<td>$(P \lor Q) \land R \equiv (P \land R) \lor (Q \land R)$</td>
<td>$\cond conversion$</td>
</tr>
<tr>
<td>$(P, H_1, \ldots, H_n \vdash Q) \equiv (H_1, \ldots, H_n \vdash P \equiv Q)$</td>
<td>$\Proof by Deduc$</td>
</tr>
<tr>
<td>$(H_1, \ldots, H_n, S \vdash C) \equiv (H_1, \ldots, H_n \vdash S)$</td>
<td>$\Proof by Contra$</td>
</tr>
</tbody>
</table>

We can also write out the argument in English. The summary might go like this: Suppose that $x^2 = 9$ and $x \geq 0$. Since $x^2 = 9$, we must have $x = 3$ or $x = -3$. But since $x \geq 0$, $x \neq -3$. Hence $x = 3$.

There are many ways of writing the proof, at various levels of detail. Once you get comfortable with proof, you would naturally compress the above argument. But for now, we want to break everything down. A
good way of figuring out how much detail to give is that each line should have a separate reason. For example, I could write on the third line directly \( x = 3 \vee x = -3 \), by arithmetic. But that is not really accurate, because I would be using arithmetic and line 2.

**Problem 5.16.** Prove that \( x^2 = 144 \vdash x \neq 5 \) (where the universe for \( x \) is integers) by contradiction.

An answer:
1. \( x^2 = 144 \) hyp
2. \( x = 5 \) temp hyp
3. \( x = 5 \implies x^2 = 25 \) arith hyp
4. \( x^2 = 25 \) inf on 1,3
5. \( x^2 = 144 \wedge x^2 = 25 \) ci on 2.4; contra
6. \( x \neq 5 \) proof by contra on 1-5

**Problem 5.17.** In the following the universe for the variable \( x \) is all integers.

1. Prove that \( x^3 = 64 \implies x \neq 3 \) by contradiction.
2. Prove that \( (x = 3 \vee x = -3) \implies x^2 = 9 \) by cases.
3. Prove that \( (2 + 2 = 5 \wedge 2 + 2 = 4) \implies 1 = 0 \).

### 6. Proofs involving quantifiers

In this section we introduce methods for proving statements involving quantifiers. The idea is simple: For statements involving a variable with a universal (for all) quantifier, we have to prove the statement for the variable without assumptions. For statements involving a variable with an existential (for some) quantifier, we just have to give a value of the variable for which the statement is true.

For example, suppose we want to show that for all integers \( x \), the product \( x(x + 1) \) is even. A possible proof is as follows: Let \( x \) be an integer. Then \( x \) is either odd or even. In the first case, \( x + 1 \) is even, while in the second, \( x + 1 \) is odd. So \( x(x + 1) \) is the product of an odd and an even number, or an even number and an odd number. In both cases, \( x(x + 1) \) is even. Hence, for all integers \( x \), the product \( x(x + 1) \) is even.

This kind of argument will be called *universal generalization*: if there is no assumption on the integer \( x \), then any statement proved holds for all integers \( x \).

The technique for proving statements involving existential quantifiers is called *existential generalization*. For example, suppose we want to show that for some integer \( x \), the product \( x(x + 1) \) is even. A possible proof is as follows: Let \( x = 2 \). Then \( x + 1 = 3 \) and so \( x(x + 1) = 6 \), which is even. Hence, for some integer \( x \), the product \( x(x + 1) \) is even.

There also rules that go the other way: Given a statement involving a universal or existential quantifier, we can deduce a statement that does not involve a quantifier. These rules are called *universal instantiation* and *existential instantiation*. In the case of existential instantiation, the variable name that is used must be a new variable name, and one has to keep track in the proof that it is a particular instance of the variable in the statement with the quantifier, not an unrestricted variable. Here is an example: *Some integer divides 145. Let \( y \) be such an integer*. For the rest of the proof \( y \) is not just any integer, it is a specific integer, which divides 145. Below we describe the rules more formally.

#### 6.1. Universal instantiation and existential generalization

More formally, for proofs involving predicate forms and quantifiers, we have the following rules which we already introduced before in Section 3.

- \( \forall x. P(x) \iff \exists x. \neg P(x) \) quantifier conversion (qc)
- \( \forall x \forall y P(x, y) \iff \forall y \forall x P(x, y) \) commutativity of univ. quant. (cuq)
- \( \exists x \exists y P(x, y) \iff \exists y \exists x P(x, y) \) commutativity of exist. quant. (ceq)

We also have rules which allow us to deduce specific instances from a universal statement, and an existential statement from a specific instance. *Universal instantiation* (ui) deduces the truth of an instance from a universal statement. An example of universal instantiation would be the following reasoning: *All people make mistakes. Therefore, the author makes mistakes.* In more symbolic form, this reasoning looks as follows:

1. \( \forall x. x \text{ makes mistakes.} \) hyp
2. The author makes mistakes. univ inst on 1

The rule is valid because the author is in the universe for \( x \), which is all people. More formally, we write universal instantiation for a predicate statement \( P(x) \) as

\[ \forall x. P(x) \vdash P(y) \text{ universal instantiation (ui)} \]

Here is a more mathematical example:

**Problem 6.1.** Show \( 3 | a \implies 9 | a^2 \), assuming \( \forall x, y, x | y \implies x^2 | y^2 \).
Answer: The first problem here is to write the statement precisely in terms of quantifiers:

\[ \exists m, n, m \text{ are odd} \land 26 = m + n. \]

To prove such an existential statement, it's enough to come up with specific values for \( m, n \). A proof is:

1. \( 26 = 15 + 11 \)  \( \text{arith} \)
2. \( 15 = 2(7) + 1 \)  \( \text{arith} \)
3. \( 11 = 2(5) + 1 \)  \( \text{arith} \)
4. \( \exists k, 15 = 2k + 1 \)  \( \text{exist gen 2} \)
5. \( \exists k, 11 = 2k + 1 \)  \( \text{exist gen 3} \)
6. \( 15 \text{ is odd} \)  \( \text{def odd, 4} \)
7. \( 11 \text{ is odd} \)  \( \text{def odd, 5} \)
8. \( 15 \text{ is odd} \land 11 \text{ is odd} \land 26 = 15 + 11 \)  \( \text{cs 1,6,7} \)
9. \( \exists m, n, n, m \text{ are odd} \land 26 = m + n \)  \( \text{exist gen 8} \)

Summary: By arithmetic \( 26 = 15 + 11 \). Since \( 15 = 2(7) + 1 \) and \( 11 = 2(5) + 1 \), we have \( \exists k, 15 = 2k + 1 \) and \( \exists k, 11 = 2k + 1 \). Hence 15 and 11 are odd, and \( 26 = 15 + 11 \). Hence 26 is the sum of two odd integers.

Problem 6.5. Using existential generalization prove that

1. 7 is odd.
2. 30 is the sum of two odd numbers.
3. 26 is the sum of two even numbers.
4. 26 is the sum of two square numbers.
5. \( \exists x, x^3 = 27 \).

In each case, give an summary of your proof.

Problem 6.6. Prove that 7 does not divide 29, assuming 29 is prime.

Answer:

1. 29 is prime  \( \text{hyp} \)
2. 29 is prime iff \( 29 \neq 1 \land \forall x, x | 29 \implies (x = 29 \lor x = 1) \)  \( \text{def prime} \)
3. \( 29 \neq 1 \land \forall x, x | 29 \implies (x = 29 \lor x = 1) \)  \( \text{inf on 1,2} \)
4. \( \forall x, x | 29 \implies (x = 29 \lor x = 1) \)  \( \text{cs on 3} \)
5. \( 7 | 29 \implies (7 = 29 \lor 7 = 1) \)  \( \text{univ inst on 4} \)
6. \( \neg(7 = 29 \lor 7 = 1) \)  \( \text{def of 1,7,29} \)
7. \( \neg(7 | 29) \)  \( \text{contra inf on 5,6} \)
More formally, the two rules are the following:

1. **Existential instantiation** = 1) sub 8, 7
2. **Universal generalization** = 1)

**Theorem 6.7.** 

\[ p \text{ is not prime iff } \exists x, y, p = xy \land x > 1 \land y > 1. \]

We'll give a proof with some steps condensed.

1. \( p \) is prime iff \( p \neq 1 \land \forall a, (a|p \implies a = 1 \lor a = p) \)
   
   \[ \text{def prime} \]

2. \( p \) is not prime iff \( \neg(p \neq 1 \land \forall a, (a|p \implies a = 1 \lor a = p)) \)
   
   \[ \text{negation of 1} \]

3. \( p \) is not prime iff \( p = 1 \lor \neg\forall a, (a|p \implies a = 1 \lor a = p)) \)
   
   \[ \text{de Morgan’s on 2} \]

4. \( p \) is not prime iff \( p = 1 \lor \exists a, \neg(a|p \implies a = 1 \lor a = p)) \)
   
   \[ \text{q.e.d. on 3} \]

5. \( p \) is not prime iff \( p = 1 \lor \exists a, \neg(\neg a|p \lor a = 1 \lor a = p)) \)
   
   \[ \text{universal generalization} \]

6. \( p \) is not prime iff \( p = 1 \lor \exists a, (a|p \wedge a \neq 1 \land a \neq p)) \)
   
   \[ \text{de Morgan’s on 5} \]

7. \( p \) is not prime iff \( p = 1 \lor \exists a, (a|p \wedge a \neq 1 \land a \neq p)) \)
   
   \[ \text{universal generalization} \]

8. \( p \) is not prime iff \( p = 1 \lor \exists a, b, ab = p \wedge a \neq 1 \land a \neq p \)
   
   \[ \text{universal generalization} \]

9. \( ab = p \wedge a \neq p \iff ab = p \wedge a \neq 1 \land b \neq 1 \)
   
   \[ \text{universal generalization} \]

10. \( p \) is not prime iff \( p = 1 \lor \exists a, b, ab = p \wedge a \neq 1 \land a \neq 1 \)
    
    \[ \text{sub 8, 7} \]

Notice that this isn’t a complete proof, because e.g. we didn’t justify the fact in line 8. We will do that later in Problem 13.25.

We can’t give any serious examples yet of universal instantiation, because we haven’t developed any properties of numbers etc.

**6.2. Universal generalization and existential instantiation.** The next two rules involving quantifiers are harder because they involve the notion of **restricted** and **unrestricted** variables.

A **restricted variable** means a variable which has already been assigned a value, even if the value itself is unknown. An **unrestricted variable** has not been assigned a value.

**Universal generalization**, says the following: in order to prove a statement with a universal quantifier, it suffices to prove it for a variable without any assumptions. For example, to prove the square of any even number is even, suppose that \( x \) is an even number. Then \( x = 2a \) for some number \( a \), and \( x^2 = (2a)^2 = 4a^2 \). So \( x^2 = 2b \) where \( b = 2a^2 \), so \( x^2 \) is even. Since \( x \) is unrestricted, we’ve shown that any even number has an even square.

**Existential instantiation** allows us to drop the existential quantifier, as long as we keep in mind that we are talking about a particular instance \( y \) of \( x \), not a general one. For example, suppose the police find a murdered man, call him John Doe. John Doe’s wallet is missing, and the police begin trying to find the murderer using further reasoning. The only thing to remember is that if a name or symbol appears first via existential instantiation, it cannot be used later in universal generalization. For example, in the above argument the conclusion “All people are dead” by universal generalization on “John Doe is dead” is false, because John Doe is a particular person, not an arbitrary person. Similarly, the reasoning “There exists a practically perfect person. Call her \( p \). All people \( p \) are practically perfect” is obviously fallacious: \( p \) refers to a particular person, say Mary Poppins, not a person in general.

More formally, the two rules are the following:
Problem 6.8. Prove that for all integers $a$, there exists an integer $b$ such that $a + b = 10$.

Answer:
1 $a$ is an integer
2 $(a) + (10 - a) = 10$
3 $10 - a$ is an integer
4 $\exists b, b$ is an integer $\land a + b = 10$
5 $a$ is an integer $\implies$
   $\exists b, b$ is an integer $\land a + b = 10$
6 $\forall a, a$ is an integer $\implies$
   $\exists b, b$ is an integer $\land a + b = 10$

Summary: Let $a$ be an integer. We have $a + (10 - a) = 10$. Therefore, there exists an integer $b$ such that $a + b = 10$. Thus for all integers $a$, there exists an integer $b$ such that $a + b = 10$.

Warning 6.1. When doing exist. inst., you cannot use a variable that has already been used. (Imagine in a murder investigation, there are two dead men whose names are unknown. You should not call them both John Doe.)

For example, an integer $n$ is even iff $\exists m, 2m = n$ where the universe for $m$ is all integers. An integer $n$ is odd iff $\exists m, 2m + 1 = n$.

Problem 6.9. Prove that if $x$ is an odd integer and $y$ is an odd integer then $x + y$ is even.

Answer:
1 $x$ is an odd integer
2 $\exists k, x = 2k + 1$
3 $x = 2l + 1$
4 $y$ is an odd integer
5 $\exists k, y = 2k + 1$
6 $y = 2m + 1$
7 $x + y = 2l + 2m + 2$
8 $x + y = 2(l + m + 1)$
9 $\exists k, x + y = 2k$
10 $x + y$ is even

Summary: Suppose that $x$ and $y$ are odd integers. Then there exist integers $k, l$ such that $x = 2l + 1$ and $y = 2m + 1$. Then $x + y = 2l + 2m + 1 + 1 = 2(l + m + 1)$. So there exists an integer $k$ such that $2k = x + y$. Hence $x + y$ is even.

Problem 6.10. Prove that if $n$ is an even integer, then so is $n^2$.

Answer:
1 $n$ is an even integer
2 $n$ is even $\implies \exists m, 2m = n$
3 $\exists m, 2m = n$
4 $2l = n$
5 $(2l)(2l) = n^2$
6 $2(2l^2) = n^2$
7 $\exists m, 2m = n^2$
8 $n^2$ is an even integer

Summary: Suppose that $n$ is an even integer. By definition of even, there exists an integer $m$ such that $2m = n$. Then $(2m)^2 = n^2 = 2(2m^2)$. So there exists an integer $n$ such that $2m = n^2$. Hence $n^2$ is also an even integer.

Problem 6.11. Prove that if 3 divides integers $x$ and $y$ then 3 divides $2x + y + 6$.

Answer:
1 $3|x \land 3|y$
2 $3k, 3k = x \land (\exists k, 3k = y)$
3 $3m = x \land 3n = y$
4 $2x + y + 6 = 6m + 3n + 6$
5 $2x + y + 6 = 3(2m + n + 3)$
6 $\exists k, 3k = 2x + y + 6$
7 $3|(2x + y + 6)$

Summary: Suppose $3|x \land 3|y$. Then there are integers $m, n$ such that $3m = x$ and $3n = y$. Then

$$2x + y + 6 = 6m + 3n + 6 = 3(2m + n + 3).$$

So there exists an integer $k$ such that $3k = 2x + y + 6$. Hence $3|2x + y + 6$.

Here is an example of how re-using a variable name can give a wrong answer:
Problem 6.12. Find what is wrong with the following proof that the sum of any two even integers is divisible by 4. Given an example showing the statement is false.

To show: $2|x \land 2|y \implies 4|(x + y)$.
1. $2|x \land 2|y$ hyp
2. $\exists k, 2k = x \land \exists k, 2k = y$ def divides
3. $4k = x + y$ exist inst, arith on 2
4. $\exists k, 4k = x + y$ exist gen on 3
5. $4|(x + y)$ def divides

Problem 6.13. Using universal generalization prove that

1. For any integer $n$, $2n + 3$ is odd.
2. For any odd integer $n$, $n^3 + 1$ is even.
3. For any even integer $n$, $n^2$ is even.

6.3. Proofs of inequalities. Recall from several sections ago that we assumed basic properties of addition and multiplication, but we defined what it means for one number to be less than or equal to another: for natural numbers $x, y, z$,

$$x \leq y \iff \exists z, x + z = y$$

and

$$x < y \iff (\exists z, x + z = y \land z \neq 0).$$

This means that we can prove basic properties of ordering of natural numbers:

Problem 6.14. Show that (where the universe for any variable below is natural numbers)

1. $\forall x, 0 \leq x$
2. $\forall x, x \leq x$
3. $\forall x, y, z, x \leq y \land y \leq z \implies x \leq z.$
4. $\forall x, y, z, x \leq y \implies xz \leq yz.$
5. $\forall x, y, z, x \leq y \implies x + z \leq y + z.$

Here is a proof for the first item.

1. $0 \leq x \iff \exists y, 0 + y = x$ def $\leq$
2. $0 + x = x$ def $0$
3. $\exists y, 0 + y = x$ exist inst on 2
4. $0 \leq x$ inf on 1, 3
5. $\forall x, 0 \leq x$ univ gen on 1, 4

Here is a proof for the last item.

1. $x \leq y$ temp hyp
2. $\exists a, x + a = y$ def $\leq$ on 1
3. $x + a = y$ exist inst on 2
4. $x + z + a = y + z$ add $z$ to both sides of 3
5. $\exists b, x + z + b = y + z$ exist gen on 4
6. $x + z \leq y + z$ def $\leq$ on 5
7. $\forall x, y, z, x + z \leq y + z$ univ gen on 6

Recall that summation notation means

$$\sum_{i=1}^{n} f(i) := f(1) + f(2) + \ldots + f(n).$$

Problem 6.15. Find the following.

1. $\sum_{i=1}^{3} i$
2. $\sum_{i=1}^{4} i$
3. $\sum_{i=1}^{3} 2^i$
4. $\sum_{i=1}^{3} 2^i$
5. $\sum_{i=1}^{n} 2^i = \sum_{i=1}^{n} 2^i.$

Problem 6.16. Prove that

1. $\forall n, 3|4n - 1 \implies 3|4^{n+1} - 1$
2. $\forall n, 9|4n + 15n - 1 \implies 9|4^{n+1} + 15(n + 1) - 1$
3. $\forall n, \sum_{i=1}^{n} i = n(n + 1)/2 \implies \sum_{i=1}^{n+1} i = (n + 1)(n + 2)/2.$
4. $\forall n, 2^n > n \implies 2^{n+1} > n + 1$

Problem 6.17. Prove that there is no largest odd integer.

Answer: First we translate this into mathematical language. $x$ is the largest odd integer if $x$ is odd and if for any other odd integer $y$, $x \geq y$. That is, $2|x + 1 \land \forall y, 2y + 1 \implies x \geq y$. So, there is no largest integer iff $\exists x, 2|x + 1 \land \forall y, 2y + 1 \implies x \geq y$. The method is proof by contradiction:
1. \( \exists x, 2|x + 1 \land \forall y, 2|y + 1 \implies x \geq y \) hyp
2. \( 2|x + 1 \land \forall y, 2|y + 1 \implies x \geq y \) exist inst on 1
3. \( 2x + 1 \) def odd
4. \( \exists k, 2k = x + 1 \) def divides
5. \( 2l = x + 1 \) exist inst on 4
6. \( 2(l + 1) = (x + 2) + 1 \) arith on 5
7. \( 2(x + 2) + 1 \) def divides, 6
8. \( 2(x + 2) + 1 \implies x \geq x + 2 \) cs, Univ inst on 2 with \( y = x + 2 \)
9. \( x \geq x + 2 \) inf 7, 8, contra
10. \( \neg \exists x, 2|x + 1 \land \forall y, 2|y + 1 \implies x \geq y \) proof by contra 1-7

Proof summary: Suppose that \( x \) is the largest even integer. Then for any other even integer \( y \), we have \( y \leq x \). But consider \( x + 2 \). Since \( x \) is even and 2 is even, so is \( x + 2 \). But \( x + 2 > x \), which is a contradiction.

**Problem 6.18.** Show that \( \neg \exists a, 2|a \land \forall b, 2|b \implies b \leq a \) is equivalent to \( \forall a, (2|a) \implies \exists b, (2|b) \land a < b \).

**Problem 6.19.** Write out a symbolic version of each statement. (i.e. no words.) Then prove or disprove. In each case, provide an summary of your proof.

1. \( 100 \) is the largest natural number.
2. \( 0 \) is the smallest natural number.
3. There is no largest natural number.
4. There is no smallest even natural number.
5. There is no smallest prime number.
6. There is no largest odd number.
7. If \( n \) is odd, then \( n^2 - 1 \) is divisible by 8.
8. No integer larger than 1 divides consecutive integers.

6.4. **More rules about quantifiers.** Finally, we mention that a quantifier that appears in one part of a conjunction or disjunction can be moved outside, if the other parts of the conjunction make no reference to that variable. For example, if \( \text{it is Tuesday and it is somebody's birthday} \) is the same as \( \text{there is a person whose birthday is today and it is Tuesday} \), because the phrase “It is Tuesday” makes no reference to the person. More formally,

\[
(\forall x, P(x)) \iff (P \land (\forall x, Q(x)))
\]

\[
(\forall x, P \lor Q(x)) \iff (P \lor (\forall x, Q(x)))
\]

\[
(\exists x, P(x)) \iff (P \land (\exists x, Q(x)))
\]

\[
(\exists x, P \lor Q(x)) \iff (P \lor (\exists x, Q(x)))
\]

**Example 6.20.**

1. \( \exists x, y, x^2 = 16 \land x = y^2 \) is equivalent to \( \exists x, (x^2 = 16 \land \exists y, x = y^2) \).
2. \( \forall x, y, x^2 \geq 0 \land y^4 \geq 0 \) is equivalent to \( \forall x, (x^2 \geq 0 \land \forall y, y^4 \geq 0) \).
3. \( \forall x, y(x = y^2 \implies x \geq 0) \) is NOT the same as \( \forall x, (\forall y, x = y^2) \implies x \geq 0 \).

Here is a summary of our commonly-used rules on quantifiers:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Name (Abbrev)</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \neg \forall x, P(x) \iff \exists x, \neg P(x) )</td>
<td>quantifier conversion (qc)</td>
</tr>
<tr>
<td>( \forall x \forall y P(x, y) \iff \forall y \forall x P(x, y) )</td>
<td>commutativity univ quant</td>
</tr>
<tr>
<td>( \exists x \exists y P(x, y) \iff \exists y \exists x P(x, y) )</td>
<td>commutativity exist quant</td>
</tr>
<tr>
<td>( \forall x, P(x) \vdash P(y) )</td>
<td>universal instantiation (ui)</td>
</tr>
<tr>
<td>( P(y) \vdash \exists x, P(x) )</td>
<td>existential generalization (exist. gen.)</td>
</tr>
<tr>
<td>( P(y), y \text{ unrestricted} \vdash \forall x, P(x) )</td>
<td>universal generalization (ug)</td>
</tr>
<tr>
<td>( \exists x, P(x) \vdash P(y), y \text{ restricted} )</td>
<td>existential instantiation (exist inst )</td>
</tr>
</tbody>
</table>

**Problem 6.21.** (i) Prove that if \( R(x, y) \) is any predicate form, then \( (\exists y, \forall x, R(x, y)) \implies (\forall x, \exists y, R(x, y)) \). (ii) Give an example of a predicate form \( R(x, y) \) so that the converse is not true.

**Problem 6.22.** (Adapted from Charles Dodgson aka Lewis Carroll)

Turn the following into a formal proof.

1. (a) All babies are illogical.
   (b) Nobody is despised who can manage a crocodile.
   (c) Illogical persons are despised.
   (d) Therefore, no baby can manage a crocodile.
2. (a) No interesting poems are unpopular among people of real taste
   (b) No modern poems is free from affectation
   (c) All your poems are on the subject of soap-bubbles
   (d) No affected poems are popular among people of real taste
   (e) No ancient poems are on the subject of soap-bubbles
   (f) Therefore, all your poems are uninteresting.
We would like to have a way of talking about membership in a collection, such as the collection of students in a class, or the set of numbers with a certain property. The technical name for a collection is called a set and a member of the set is called an element of that set.

7.1. Roster form and defining form. Sets can be identified in roster form by listing their elements:

(1) the set $I$ of integers from 1 to 5 is \{1, 2, 3, 4, 5\}.
(2) If John has two daughters named Jill and Jane, then the set $D$ of John’s daughters is $D = \{\text{Jill, Jane}\}$.
(3) The equation $S = \{2, 3, 5, 6\}$ is read in English as $S$ is the set consisting of 2, 3, 5 and 6.

The ordering of the elements of the set is irrelevant, and the additional of duplicates does not change the set.

Example 7.1. The set of baseball players who played shortstop for the New York Mets in 2006 is

$$M = \{\text{Hernandez, Reyes, Chris Woodward}\} = \{\text{Hernandez, Reyes, Reyes, Woodward}\} = \{\text{Woodward, Hernandez, Reyes}\}$$

which is the order I like it in.

If $x$ is an element of a set $S$ we write $x \in S$ for short, or if $x$ is not an element of a set we write $x \notin S$.

Example 7.2. Woodward $\in M$ means Woodward played shortstop for the Mets in 2006, which happens to be true. George Bush $\notin M$ means George Bush did not play shortstop for the Mets in 2006.

Problem 7.3. Find the truth value for each of the following. (From Kaufman et al.)

(1) 1 $\in \{1, 2\}$.
(2) 1 $\notin \{2, 3\}$.
(3) 6 $\in \{1, 4, 6\}$.
(4) 2 $\notin \{x | 2 < x < 5\}$.
(5) 4/2 $\in \{4, 2, 1\}$.
(6) \{2\} $\in \{1, \{2\}\}$.
(7) \{1\} $\in \{1, \{2\}\}$.

Problem 7.4. Find, if possible, a roster name for the given set.

(1) The set of the first four even natural numbers.
(2) The set of the first ten positive prime integers.
(3) The set of the first three months of the year.

The following are notations for standard sets of numbers.

Definition 7.5. (1) $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ is the set of natural numbers.
(2) $\mathbb{N}_+ = \{1, 2, 3, \ldots\}$ is the set of positive natural numbers.
(3) $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is the set of integers.
(4) $\mathbb{Q} = \{\ldots, 0, 1, 1/2, 1/3, 2/3, -1/2, \ldots\}$ is the set of rational numbers.
(5) $\mathbb{R}$ is the set of real numbers.
Some authors use \( \mathbb{N} \) to denote positive integers, while others use \( \mathbb{W} \) to denote positive integers. Unfortunately, even among professional mathematicians there is no standard convention.

Sets can also be identified by a defining property, for example,

\[
I = \{x | x \in \mathbb{Z} \land 1 \leq x \leq 5\}
\]

means that \( I \) is the set of integers between one and five. The symbol \( \{ \) means such that, the left brace \( \{ \) is read as the set of all.

\[
D = \{y | y \text{ is my daughter}\}
\]

means that \( D \) is the set of my daughters.

**Problem 7.6.** (From [3]) Find a defining form for the following sets.

1. \( \{5, 6, 7, 8, 9\} \).
2. \( \{5, 20\} \).
3. \( \{11, 13, 15, 17, 19\} \).
4. \( \{8\} \).

**Problem 7.7.** Give a roster form for the following sets of natural numbers.

1. \( \{x | x \in \mathbb{N} \land x \text{ is prime } \land x \text{ is even }\} \).
2. \( \{y | y \in \mathbb{N} \land (y | 7 \land y > 1)\} \).
3. \( \{x | x \in \mathbb{N} \land (x = 5 \lor 2x + 4 = 14)\} \).
4. \( \{y | y \in \mathbb{N} \land (3y = y \lor y = 3y - 2)\} \).

### 7.2. Subsets

Let \( S \) and \( T \) be sets. We say that \( S \) is a subset of \( T \), and write \( S \subseteq T \), if every element of \( S \) is an element of \( T \). More formally,

\[
S \subseteq T \iff (\forall x, x \in S \implies x \in T).
\]

\( S \) equals \( T \) if they have the same elements, that is,

\[
S = T \iff (\forall x, x \in S \iff x \in T).
\]

We say \( S \) is a proper subset of \( T \), and write \( S \subset T \), if \( S \) is a subset of, but not equal to, \( T \):

\[
(S \subset T) \iff (S \subseteq T) \land (S \neq T).
\]

A common error is to omit quantifiers. For example, \( A \subseteq B \iff (x \in A \implies x \in B) \) is incorrect, because you haven’t specified which \( x \) you are talking about.

**Example 7.8.**

1. \( \{1, 3\} \subseteq \{1, 3, 5\} \).
2. \( \{1, \text{apple}\} \subseteq \{1, \text{orange, apple}\} \).
3. \( \{x | x^2 = 9\} = \{3, -3\} \), assuming that the universe for \( x \) is all integers.
4. \( \{2, 4\} \subset \{x | x \text{ is even }\} \), assuming that the universe for \( x \) is all integers.

Note the difference between being a subset and being an element. Both represent a general notion of one thing being inside or contained in the other, but in different ways. For example \( \{1\} \) is a subset of \( \{1, 2, 3\} \), but \( \{1\} \) is not element of \( \{1, 2, 3\} \), because the elements of \( \{1, 2, 3\} \) are 1, 2 and 3. That is, you should not read \( \{1, 2\} \subseteq \{1, 2, 3\} \) as the set consisting of 1, 2 is contained in the set consisting of 1, 2, 3, because the English word contained is ambiguous as to whether it means element of or subset of.

**Problem 7.9.** (from [3].) Determine the truth value of each of the following.

1. \( \{1\} \subseteq \{1, \{1\}\} \).
2. \( \{0\} \subseteq \{0, 1, 2\} \).
3. \( \{1, 2\} \subseteq \{2, 1\} \).
4. \( \{1\} \subseteq \{2, 1\} \).
5. \( \{1, 2\} \in \{3, 1, \{1, 2\}\} \).

**Problem 7.10.** Determine the truth value of each of the following.

1. \( \mathbb{N} \subseteq \mathbb{N}_+ \).
2. \( \mathbb{N} \subseteq \mathbb{Z} \).
3. \( \mathbb{Q} \subseteq \mathbb{R} \).
4. \( \mathbb{Z} \subseteq \mathbb{R} \).
5. \( \mathbb{R} \subseteq \mathbb{N}_+ \).

**Problem 7.11.** Write the symbolic form of the following statements. Comment on their truth value.

1. The sum of any two rational numbers is rational.
2. The sum of any two irrational numbers is irrational.
3. The sum of a rational number and an irrational number is irrational.

### 7.3. Intersections and unions

The intersection \( S \cap T \) of \( S \) and \( T \) is the set of common elements. For example,

\[
\{1, 3, 5\} \cap \{3, 5, 7\} = \{3, 5\}.
\]
The union $S \cup T$ of $S$ and $T$ is the set of elements in either $S$ or $T$, for example,

$$\{1, 3, 5\} \cup \{3, 5, 7\} = \{1, 3, 5, 7\}.$$ 

More formally,

$$S \cup T = \{x|x \in S \lor x \in T\}, S \cap T = \{x|x \in S \land x \in T\}.$$ 

The complement $S - T$ of $T$ in $S$ is the set of elements of $S$ that are not in $T$, for example,

$$\{1, 3, 5\} - \{3, 5, 7\} = \{1\}.$$ 

Note that it does not mean subtract the elements of $T$ from those of $S$. Formally

$$S - T = \{x|x \in S \land x \notin T\}.$$ 

**Problem 7.12.** Suppose that $A$ has five members, $B$ has three members, and $C$ has two members. What is the maximum number of members that $A \cup B, A \cap (A \cap B) \cup C$, and $A - B$ could have?

The relations between the intersections, unions, and complements of various sets are often drawn in terms of Venn diagrams: For example, the following diagram shows $(A \cap B) \cup C$:

![Venn Diagram](image)

**Problem 7.13.** Draw the Venn diagram for

1. $(A \cap B) \cup C - (A \cap B \cap C)$.
2. $(A \cup B) - C$.
3. $(A \cap B) \cup (B \cap C) \cup (C \cap A)$.

An empty set is a set with no elements, that is,$A$ is empty $\iff \nexists x, x \in A \iff \forall x, x \notin A$.

For example $\{x|x \neq x\}$ is empty. Any two empty sets are equal since $A, B$ empty $\implies \forall x, x \notin A \land x \notin B \implies \forall x, (x \in A \iff x \in B)$

since both $x \in A$ and $x \in B$ are always false. We denote the empty set by the symbol $\emptyset$, so that

$$A = \emptyset \iff \nexists x, x \in A \iff \forall x, x \notin A.$$ 

**Problem 7.14.** Which of the following statements are true?

1. $\{x|x^2 = 1 \land x^3 = 8\} = \emptyset$.
2. $\{p\mid p \land 3p\} = \emptyset$.
3. $\{p\mid 5p \land 7p \land p \leq 20\} = \emptyset$.

**Problem 7.15.** If $A = \{2, 4, 6, 16\}, B = \{2, 6, 10, 14\}, C = \{6, 10, 14\}$ and $D = \{2, 4, 6, 8, 10, 12, 14\}$, determine each of the following.

1. $D - A$.
2. $B - B$.
3. $B - \emptyset$.
4. $D - (D - A)$.
5. $D - (B \cup C)$.
6. $D - (B \cap C)$.
7. $D - (A - D)$.
8. $\emptyset - A$.

**Problem 7.16.** Which of the following are propositions for sets $A, B, C$? Explain your answers in one sentence each.

1. $A \subseteq B$.
2. $A \implies B$.
3. $\forall x, x \in A \implies x \in B$.
4. $(A \cap B) \subseteq C$.
5. $A \cap (B \subseteq C)$.
6. $(A = A) \land (B \subseteq C)$.
7. $(A \subseteq B) \implies (A \subseteq B \cup C)$.
8. $\forall x, x \in A \land B$.

**Problem 7.17.** List all subsets of

1. $\{1\}$
(2) \{1, 2\}.
(3) \{1, 2, 3\}.

**Problem 7.18.** Rephrase the following statements in terms of intersection, union, and complement using \(E\) as the set of even numbers \(\emptyset\) as the set of odd numbers, \(P\) as the set of primes, and \(S\) is the set of numbers bigger than 5. (Example: Some prime numbers are even is the same as \(P \cap E \neq \emptyset\).) Determine whether the statements are true or false.

(1) The only even prime number is 2.
(2) Every natural number is even or odd.
(3) Some odd natural numbers are prime.
(4) No prime number is even and bigger than five.
(5) If \(2^n - 1\) is prime then \(n\) is prime.

Answer to (a): \(E \cap \mathbb{P} = \{2\}\).

7.4. **Sets of subsets.** We can also talk about sets whose elements are themselves sets. A particularly important example is the set of all subsets of a given set \(S\), which is denote \(\mathcal{P}(S)\). Formally,
\[ \mathcal{P}(S) = \{T, T \subseteq S\}. \]

**Example 7.19.** If \(S = \{1, 3, 5\}\) then
\[ \mathcal{P}(S) = \{\emptyset, \{1\}, \{3\}, \{5\}, \{1, 3\}, \{1, 5\}, \{3, 5\}, \{1, 3, 5\}\}. \]

**Problem 7.20.** Find \(\mathcal{P}(S)\) where

(1) \(S = \{1, 2, 3\}\)
(2) \(S = \{0, 1\}\)
(3) \(S = \emptyset\)
(4) \(S = \{1, 2, 3\}\).

**Problem 7.21.** Determine whether the following statements are true or false.

(1) \(\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)\).
(2) \(\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)\).
(3) \(A \subseteq B \implies \mathcal{P}(A) \subseteq \mathcal{P}(B)\).

7.5. **Qualified quantifiers.** We use \(\forall x \in A\), to mean \(\forall x, x \in A \implies \). This simplifies many statements a lot. For example, the square of any odd integer is odd can be written \(\forall x, x \in \mathbb{O} \implies x^2 \in \mathbb{O}\), or more simply
\(\forall x \in \mathbb{O}, x^2 \in \mathbb{O}\). (Recall \(\mathbb{O}\) is the set of odd integers.)

We will call the use of the quantifier in \(\forall x \in \mathbb{O}\), a *qualified quantifier*. It means that we specify the universe for the variable in the quantifier notation. From now on, we should try to avoid using unqualified quantifiers, as in \(\forall x, x \in \mathbb{N} \implies 4x \in \mathbb{E}\).

**Problem 7.22.** Write out predicate form of the following, specifying the universe as part of the quantifier.

(1) Any even natural number is followed by an odd natural number.
(2) The square of any odd natural number is odd.
(3) The square of any integer is non-negative.
(4) There is no largest odd natural number.

Answer to (1): \(\forall e \in \mathbb{E}, e + 1 \in \mathbb{O}\).

7.6. Smullyan’s logic puzzles using sets. Consider the following problem. On the island of knights and knaves, either \(A\) or \(B\) is a werewolf. \(A\): The werewolf is a knight. \(B\): The werewolf is a knave. Who is the werewolf?

In English, you can reason like this: If the werewolf is \(B\) then \((B\) is a knight iff \(B\) is telling the truth iff \(B\) is a knave). This is a contradiction, so \(A\) is the werewolf.

We can formalize this in propositional calculus as follows.

For hypotheses, we take
\[ P \quad A\text{ is a knight} \]
\[ Q \quad B\text{ is a knight} \]
\[ R \quad \text{the werewolf is a knight} \]
\[ S \quad A\text{ is the werewolf} \]

Then the hypotheses become \(P \iff R, Q \iff \neg R\) (that knights always tell the truth and knaves always lie). But we also have to add the hypotheses \(S \implies (P \iff R), \neg S \implies (Q \iff R)\). Then our proof becomes

1. \(\neg S\) temp hyp
2. \(\neg S \implies (Q \iff R)\) hyp
3. \(Q \iff R\) inf
4. \(Q \iff \neg R\) hyp
5. \(R \iff \neg R\) tb on 3,4, contra
6. \(S\) proof by contra on 1-4
The problem with this reasoning is that it is somewhat longer than the reasoning in English we had above. To get closer to the kind of reasoning we would like to use, let’s introduce a set $K$, whose elements are knights. Let $w$ denote the werewolf, and $a, b$ the residents in the puzzle.

Our hypotheses are now $a = w \lor b = w$ (one of them is the werewolf) $b \in K \iff w \notin K$ (what $b$ says) $a \in K \iff w \in K$ (what $a$ says).

Our proof is

1. $w \neq a$ temp hyp
2. $a = w \lor b = w$ hyp
3. $b = w$ da on 1,2
4. $b \in K \iff w \notin K$ hyp
5. $w \in K \iff w \notin K$ substitution on 3,4
6. $w = a$ proof by contra on 1-5

**Problem 7.23.** (a) Write the following sets in the form $\{x|P(x)\}$. (i) $\{2, 4, 6, 8\}$. (ii) $\{\text{red, orange, yellow, green, blue, violet}\}$.

(b) Write a roster name for the following sets (i) $\{x \in \mathbb{N} | x \leq 20 \land y \in \mathbb{N} \land 5y = x\}$ (ii) $\{x \in \mathbb{N} | x \leq 20 \land \exists y(y \in \mathbb{N} \land 4y = x\}$.

(c) Find the (i) intersection and (ii) union of the sets in (b).

**Problem 7.24.** Consider the following problem on the island of knights and knaves. Recall that knights always tell the truth, and knaves always lie. Three of the island’s inhabitants $A$, $B$, and $C$ were talking together. $A$ said, ”All of us are knaves.” Then $B$ remarked, ”Exactly one of us is a knight.” Give an argument for the identities of $A$, $B$, and $C$, in English. Then translate it into a proof.

Negations of statements involving sets can be tricky:

**Problem 7.25.** All of the following statements are false. Fix them so they are true.

1. $x \notin A \cap B \iff (x \notin A \land x \notin B)$.
2. $A \neq B \iff (\forall x, x \notin A \iff x \notin B)$.
3. $A \neq \emptyset \iff (\forall x, x \in A)$.

8. **Proofs involving sets**

In proofs involving sets, we have the following rules, most of which we mentioned in the last section.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A = B \iff (\forall x, x \in A \iff x \in B)$</td>
<td>Definition of Set Equality</td>
</tr>
<tr>
<td>$A \subseteq B \iff (\forall x, x \in A \Rightarrow x \in B)$</td>
<td>Definition of Subset</td>
</tr>
<tr>
<td>$A = B \iff (A \subseteq B) \land (B \subseteq A)$</td>
<td>Theorem about set equality</td>
</tr>
<tr>
<td>$A \cap B = {x</td>
<td>x \in A \land x \in B}$</td>
</tr>
<tr>
<td>$A \cup B = {x</td>
<td>x \in A \lor x \in B}$</td>
</tr>
<tr>
<td>$A - B = {x</td>
<td>x \in A \land x \notin B}$</td>
</tr>
<tr>
<td>$\emptyset = {x \neq x}$</td>
<td>Definition of Empty Set</td>
</tr>
<tr>
<td>$\forall x, x \in A$</td>
<td>Characterization of Empty Set</td>
</tr>
</tbody>
</table>

**Definition 8.1.** (Proofs involving sets) A proof involving sets is a sequence of statements, each formed out of

1. the symbols $\{, \}, =, \notin, \subseteq, \cap, \cup, \\neg, \exists, \forall$
2. symbols for sets $S, T, \ldots$, and
3. symbols for elements $x, y, \ldots$

such that each statement is either

1. a tautology,
2. a hypothesis, or
3. deduced from the statements above by one of the rules of inference, proof by contradiction or deduction (statements used in proof by contradiction or deduction cannot be used afterwards),

or set-theoretic rules above.

8.1. **Proving set containment and set equality.** Let’s start with proving that one set is a subset of another.

**Mantra:** To prove $S \subseteq T$ you should show that a general element of $S$ belongs also to $T$.

For example,

**Problem 8.2.** Prove that for any sets $A, B, C$, $A \subseteq B, B \subseteq C \vdash A \subseteq C$.

1. $A \subseteq B$ hyp
2. $B \subseteq C$ hyp
3. $A \subseteq B \iff \forall x, x \in A \Rightarrow x \in B$ def subset
4. $\forall x, x \in A \Rightarrow x \in B$ inf on 1,3
5 \( B \subseteq C \iff \forall x, x \in B \implies x \in C \) def subset
6 \( \forall x, x \in B \implies x \in C \) inf on 2.5
7 \( y \in A \implies y \in B \) univ inst on 4
8 \( y \in B \implies y \in C \) univ inst on 6
9 \( y \in A \implies y \in C \) ti on 7,8
10 \( \forall x, x \in A \implies x \in C \) univ gen on 9
11 \( A \subseteq C \iff \forall x, x \in A \implies x \in C \) def subset
12 \( A \subseteq C \) inf on 10,11

Summary of proof: Suppose that \( A \subseteq B \) and \( B \subseteq C \). By definition of subset, this means that (i) \( x \in A \implies x \in B \) and (ii) \( x \in B \implies x \in C \). Now \( A \subseteq C \) iff \( x \in A \implies x \in C \). To prove this, suppose that \( x \in A \). Then \( x \in B \) by (i) and \( x \in C \) by (ii). Hence \( x \in A \implies x \in C \), so \( A \subseteq C \).

**Problem 8.3.** Prove that for any sets \( A, B \),

1. \( A \subseteq B \vdash A \cup B \subseteq B \).
2. \( A \subseteq B \vdash A \subseteq A \cap B \).

In each case provide a summary of your proof.

To prove set equality, you should prove that the first set is contained in the second, and vice versa:

**Mantra:** To prove \( S = T \) you should show that a general element of \( S \) belongs also to \( T \), and a general element of \( T \) belongs to \( S \).

**Problem 8.4.** Prove that for any sets \( A, B \), \( A \cap B = B \cap A \).

1 \( x \in A \cap B \) hyp
2 \( x \in A \land x \in B \) def int on 1
3 \( x \in B \land x \in A \) commut of and, 2
4 \( x \in B \cap A \) inf on 2,3
5 \( x \in A \cap B \implies x \in B \cap A \) deduc on 1-4
6 \( x \in B \cap A \) hyp
7 \( x \in B \land x \in A \) def int on 1
8 \( x \in A \land x \in B \) commut of and, 2
9 \( x \in A \cap B \) inf on 2,3
10 \( x \in B \cap A \implies x \in A \cap B \) deduc on 1-4
11 \( x \in A \cap B \iff x \in B \cap A \) ci on 5,10
12 \( A \cap B = B \cap A \) def set equality on 11

Summary of proof: We have \( A \cap B = B \cap A \) iff \( x \in A \cap B \implies x \in B \cap A \) and vice versa. If \( x \in A \cap B \) then \( x \in A \land x \in B \), so \( x \in B \land x \in A \) so \( x \in B \cap A \). Conversely, if \( x \in B \cap A \) then \( x \in B \land x \in A \) so \( x \in A \land x \in B \) so \( x \in B \cap A \). Hence \( A \cap B = B \cap A \).

We are not claiming that this is the shortest proof: it is not hard to see that you can combine both directions into one using biconditionals. Here is the summary of the shorter proof: We have \( A \cap B = B \cap A \) iff \( x \in A \land x \in B \iff x \in B \land x \in A \). Now \( x \in A \cap B \) iff \( x \in A \land x \in B \) iff \( x \in B \land x \in A \) iff \( x \in B \cap A \). By transitivity \( x \in A \cap B \) iff \( x \in B \cap A \). Hence \( A \cap B = B \cap A \).

8.2. The set definition and roster axioms. There are two new rules in the list above. The first is sometimes called the set definition axiom. In abbreviated form it says that

\[ x \in \{ y : P(y) \} \iff P(x). \]

Here are some examples:

\[ x \in \{ y : y^4 = y \} \iff x^4 = x \]

\[ x \in \{ y : y \in A \land y \in B \} \iff x \in A \land x \in B. \]

\[ x \in \{ z : z - 5 \in A \} \iff x - 5 \in A. \]

The set definition property can be combined with the definitions of union, intersection and complement as follows

\[ x \in A \cap B \iff x \in A \land x \in B. \]

\[ x \in A \cup B \iff x \in A \lor x \in B. \]

\[ x \in A - B \iff x \in A \land x \notin B. \]

For example, the first is obtained applying transitivity of the biconditional to

\[ x \in A \cap B \iff x \in \{ y : y \in A \land y \in B \} \iff x \in A \land x \in B. \]

**Problem 8.5.** Use the set definition property to simplify the following statements (which may be false).

1. \( 2 \in \{ x : x^2 \neq 5 \} \)
2. \( 3 \in \{ p : p \text{ is prime} \} \)
3. \( \{ 2, 3 \} \in \{ S : S \cap \{ 1, 2 \} = \emptyset \} \)
4. \( x \in B \cup C. \)
5. \( x \in B - C. \)
Problem 8.6. Prove that for any sets $A, B, A \subseteq A \cup B$.

1. $A \subseteq A \cup B \iff \forall x, x \in A \implies x \in A \cup B$ (def subset)
2. $x \in A$ (temp hyp)
3. $x \in A \cup B \iff x \in A \lor x \in B$ (def union)
4. $x \in A \lor x \in B$ (da on 2)
5. $x \in A \cup B$ (inf on 3,4)
6. $x \in A \implies x \in A \cup B$ (proof by deduc on 2-5)
7. $\forall x, x \in A \implies x \in A \cup B$ (univ gen on 6)
8. $A \subseteq A \cup B$ (inf on 1,7)

Problem 8.7. Fill in the blanks in the following proof that $A \cap B \subseteq A$.

1. $x \in A \cap B \iff \underline{x \in A \cap B}$ (def intersection)
2. $x \in A \land x \in B \implies x \in A$ (ti on 1,2)
3. $\underline{x \in A \land x \in B \implies x \in A}$ (on 3)
4. $\forall x, x \in A \land x \in B \implies x \in A$ (def subset)

Problem 8.8. Show that $A \cap B \subseteq A \cup B$.

The second rule is the roster axiom.

(1) $S = \{s_1, \ldots, s_k\} \vdash x \in S \iff (x = s_1 \lor x = s_2 \lor \ldots \lor x = s_k)$.

For example, $x \in \{1,2,3\} \iff x = 1 \lor x = 2 \lor x = 3$.

Here is an example of the set definition axiom and roster axiom in a proof:

Problem 8.9. Show that $\{x|x^3 = x\} \subseteq \{-1, 0, 1\}$.

1. $y \in \{x|x^3 = x\}$ (hyp)
2. $y^3 = y$ (set def on 1)
3. $y^2 - y = 0$ (algebra on 2)
4. $(y^2 - 1)y = 0$ (algebra on 3)
5. $(y - 1)(y + 1)y = 0$ (algebra on 4)
6. $xyz = 0 \implies (x = 0 \lor y = 0 \lor z = 0)$ (assumption 15.1 (9))
7. $y = 0 \lor y + 1 = 0 \lor y - 1 = 0$ (modus ponens, subst on 5,6)
8. $y = 0 \lor y = -1 \lor y = 1$ (algebra on 7)
9. $y \in \{-1, 0, 1\}$ (roster axiom on 8)
10. $y \in \{x|x^3 = x\} \implies y \in \{-1, 0, 1\}$ (deduc on 1-9)
11. $\{x|x^3 = x\} \subseteq \{-1, 0, 1\}$ (def subset)

Problem 8.10. Show that

1. $\{1, 2\} \subset \{x|x \leq 4\}$.
2. $\{x \in \mathbb{N}|x^2 \leq 4\} \subset \{1, 2, 3\}$.
3. $\{x \in \mathbb{N}|x^2 \leq 4\} \subset \{x \in \mathbb{N}|x^2 \leq 9\}$

Problem 8.11. Show that $\{3, 5\} \subset \{y|y \text{ is odd}\}$.

1. $x \in \{3, 5\}$ (temp hyp)
2. $x = 3 \lor x = 5$ (roster axiom on 1)
3. $x = 3$ (temp hyp)
4. $x = 2(1) + 1$ (arith)
5. $\exists k, x = 2k + 1$ (exist gen on 4)
6. $x$ is odd (def odd on 5)
7. $x = 5$ (temp hyp)
8. $x = 2(2) + 1$ (arith)
9. $\exists k, x = 2k + 1$ (exist gen on 8)
10. $x$ is odd (def odd on 9)
11. $x = 3 \implies x$ is odd (deduc on 3-6)
12. $x = 5 \implies x$ is odd (deduc on 7-10)
13. $x = 3 \lor x = 5 \implies x$ is odd (cases on 11,12)
14. $x$ is odd (inf on 2,13)
15. $x \in \{x|x \text{ is odd}\}$ (set def axiom on 14)
16. $x \in \{3, 5\} \implies x \in \{y|y \text{ is odd}\}$ (deduc on 1-15)
17. $\{3, 5\} \subset \{y|y \text{ is odd}\}$ (def subset on 16)

Here is a table including the roster and set definition axioms, as well as a two more “obvious” rules on equality and substitution.
Problem 8.12. Prove that \(-1, 0, 1\} = \{x | x^3 = x\}.

We already showed one direction in Problem 8.9, you should in addition show that \(-1, 0, 1\} \subseteq \{x | x^3 = x\}. To do this, use the set definition property in reverse.

\[
\begin{array}{ll}
11 & (-1)^3 = (-1) \\
12 & (1)^3 = (1) \\
13 & (0)^3 = (0) \\
14 & -1 \in \{x | x^3 = x\} & \text{set def prop on 11} \\
15 & 1 \in \{x | x^3 = x\} & \text{set def prop on 12} \\
16 & 0 \in \{x | x^3 = x\} & \text{set def prop on 13} \\
17 & y = -1 \implies y \in \{x | x^3 = x\} & \text{subst on 14} \\
18 & y = 1 \implies y \in \{x | x^3 = x\} & \text{subst on 15} \\
19 & y = 0 \implies y \in \{x | x^3 = x\} & \text{subst on 16} \\
20 & y = -1 \lor y = 1 \lor y = 0 \implies y \in \{x | x^3 = x\} & \text{ic on 17-19} \\
21 & y \in \{-1, 1, 0\} \implies y = -1 \lor y = 0 \lor y = 1 & \text{roster def} \\
22 & y \in \{-1, 1, 0\} \implies y \in \{x | x^3 = x\} & \text{ti on 20,21} \\
23 & \{-1, 10\} \subseteq \{x | x^3 = x\} & \text{def of subset on 22} \\
24 & \{-1, 10\} = \{x | x^3 = x\} & \text{def equality on 10,23}
\end{array}
\]

Actually, we have omitted a few steps in going from 14 to 17; we leave it to you to fill these in. In practice, we tend to omit the tedious steps 14-20.

Remark 8.13. It might be hard to accept that there is a definition of =, and that one should use the definition to get rid of =. This is not surprising: usually, once one has gotten an =, one wants to hold onto it, not get rid of it!

Problem 8.14. One of the following statements is true. Identify which one, and prove it.

1. For any sets \(A, B\), \(A \cap B \subseteq C \implies A \subseteq C\)
2. For any sets \(A, B\), \(A \cup B \subseteq C \implies A \subseteq C\)

To figure out which one, we draw the Venn diagrams as in Figure 11. The diagram on the left shows that if \(A \subseteq B\) is inside \(C\), then \(A\) is not necessarily inside \(C\). On the other hand, the diagram on the right shows that if \(A \cup B\) is inside \(C\), then \(A\) must be inside \(C\).

**Figure 11.** \(A \cap B\) and \(A \cup B\)

The formal proof is:

1. \(A \cup B \subseteq C\) \hspace{1cm} \text{hyp}
2. \(\forall x, x \in A \cup B \implies x \in C\) \hspace{1cm} \text{def subset}
3. \(x \in A \vee x \in B \implies x \in C\) \hspace{1cm} \text{univ inst, def union on 2}
4. \(A \subseteq C \iff (\forall x, x \in A \implies x \in C)\) \hspace{1cm} \text{def subset}
5. \(x \in A \implies x \in A \vee x \in B\) \hspace{1cm} \text{tautology}
6. \(x \in A \implies x \in C\) \hspace{1cm} \text{ti on 3,5}
7. \(x \in A \implies x \in C\) \hspace{1cm} \text{univ gen 6}
8. \(A \subseteq C\) \hspace{1cm} \text{inf on 4,7}

Problem 8.15. For each statement provide a proof and a proof summary. Let \(A, B, C\) be sets.

1. \(A \cup B = B \cup A\).
2. \((A \cup B) \cap C = A \cup (B \cap C)\).
3. \((A \cap B) \cup C = A \cap (B \cup C)\).
4. \(A \cup B = A \implies B \subseteq A\).
5. \(A \cap B = A \implies A \subseteq B\).

Proofs involving the emptyset are particularly tricky. This is because there are several definitions of the emptyset, e.g., the roster form \(\emptyset = \{\}\), but it is not particularly helpful to use this definition. Instead it is more helpful to expand the definition of \(\emptyset\), that is,

\[A = \emptyset \iff \forall x, x \notin A.\]
Example 8.16. Show that \( A \cup B = \emptyset \implies A = \emptyset \land B = \emptyset \).

1. \( A \cup B = \emptyset \) hyp
2. \( \forall x, \neg(x \in A \cup B) \) def emptiness
3. \( \forall x, \neg(x \in A \lor x \in B) \) def union
4. \( \forall x, x \notin A \land x \notin B \) distribute not
5. \( \forall x, x \notin A \lor \forall x, x \notin B \) distribute for all
6. \( A = \emptyset \land B = \emptyset \) def emptiness

Problem 8.17. For each statement provide a proof and a proof summary. Let \( S, A, B \) be sets.

1. \( S = \emptyset \iff \forall y, y \notin S \).
2. \( A = A - B \iff A \cap B = \emptyset \).
3. \( \emptyset \subseteq A \) for any \( A \).

The main point in proofs of this type is to unravel the definitions. Notice that each definition in the above list can be used in a proof to get rid of some jargon. For example, the set definition property can be used to get rid of the notation \( \{ x \mid \} \). To prove a statement involving jargon, first you have to use the definitions to get rid of the jargon and find the underlying statement. How do you know which definition to unravel first? As with logical statements, each set-theoretic statement has a tree form. For example, the tree form of \( (A - B) \cup (A \cap B) = A \) is shown in Figure 12.

![Figure 12](image)

The highest level operation, =, is at the top. This means that probably you will want to expand the definition of = first.

Example 8.18. Prove that for sets \( A, B \), \( A \cap B = \emptyset \iff A - B = A \).

1. \( A \cap B = \emptyset \iff \forall x, x \notin A \land x \notin B \) def emptiness
2. \( \iff \forall x, x \notin A \lor \forall x, x \notin B \) def union
3. \( \iff \forall x, x \notin A \lor \forall x, x \notin B \) def subset
4. \( \iff \forall x, x \notin A \lor \forall x, x \notin B \) distrib implies
5. \( \iff \forall x, x \in A \lor \forall x, x \notin B \) taut, \( P \lor \neg P \) is always true

Problem 8.19. For each statement, provide a proof and a proof summary. Let \( A, B, C \) be sets.

1. \( A \cup B = B \cup A \)
2. \( A \cup (B \cup C) = (A \cup B) \cup C \)
3. \( \forall y, y \notin \emptyset \)
4. \( A \neq \emptyset \iff \exists y, y \in A \)
5. \( A \cup \emptyset = A \)
6. \( (A \subseteq B) \implies (A \cup C \subseteq B \cup C) \)
7. \( (A - B) \cup (A \cap B) = A \)
8. \( A - (B \cap C) = (A - B) \cup (A - C) \)
9. \( A - (B \cup C) = (A - B) \cap (A - C) \)
10. \( (A \cap B) \subseteq (A \cup B) \)
11. \( (A \cup B) \cap (A \cup C) = A \cup (B \cap C) \)
12. \( (A \subseteq B) \implies (A - B = \emptyset) \)
13. there is a unique set \( C \) such that \( C \cup (C \cap A) = A \).
14. \( (\mathcal{P}(A) \subseteq \mathcal{P}(B)) \iff (A \subseteq B) \).

8.3. Problems with naive set theory. We have to be careful about asserting the existence of sets containing themselves as elements. The following example is known as Russell’s paradox:

Problem 8.20. Suppose that \( S \) is the set of all sets that do not contain themselves, \( S = \{ T, T \notin T \} \). Prove that such a set cannot exist. (Hint: does \( S \) contain itself?)
In the standard ZFC (Zermelo-Fraenkel with axiom of Choice) axioms of set theory, the set of all sets does not exist. ZFC is widely believed to a consistent axiom system, although by Gödel incompleteness it can never be proved so, if it is. Such collections are called classes, they are admissible in the NBG (Von Neumann-Bernays-Gödel set theory) axiom system. But that is the topic for a more advanced course.\footnote{Which the author of these notes would not be qualified to teach.}

9. Proof strategies and styles

9.1. Working backwards. When doing proofs in practice the most common technique is to work backwards from the statement one is trying to prove. The trick here is not to assume what one is trying to prove. Rather, use biconditional or conditional statements to unravel the definitions before one starts thinking too hard.

Problem 9.1. Prove that 4 is not prime.

Summary of proof: By definition 4 is prime iff its only divisors are 1 and 4. So 4 is not prime if one of its divisors is not 1 or 4. At this point, you can see what you are trying to prove: that 4 has a divisor that is not 1 or 4. Continuing: 2(2) = 4, so 2 divides 4. Therefore, 4 has a divisor that is not 1 or 4. So 4 is not prime.

Mantra: Do not start a proof by thinking. Rather, unravel the definitions, then think.

Here is the same proof in symbolic form.

1. $4$ is prime $\iff (4 \neq 1 \land \forall x, x|4 \implies (x = 4 \lor x = 1))$ def prime
2. $4$ is not prime $\iff \neg(4 \neq 1 \land \forall x, x|4 \implies (x = 4 \lor x = 1))$ negation of 1
3. $4$ is not prime $\iff \begin{cases} 4 = 1 \lor \exists x, \neg(x|4 \implies (x = 4 \lor x = 1)) \end{cases}$ dm, qc on 2

At this point, you can see what you are trying to prove, namely the statement in the box. In order for 4 not to be prime, it either has to equal 1 (which it obviously does not) or there has to be a number not equal to 1 or 4 which divides it. In order to prove the existence of such a number, it suffices to give an example.

4. $2|4$ arith
5. $\neg(2 = 4 \lor 2 = 1)$ fact
6. $2|4 \land \neg(2 = 4 \lor 2 = 1)$ ci 4,5
7. $\neg(2|4 \implies (2 = 4 \lor 2 = 1))$ de Morgan’s, cc on 6
8. $\exists x, \neg(x|4 \implies (x = 4 \lor x = 1))$ eg on 7
9. $4$ is not prime inf on 3,8

Here is a set-theoretic example.

Problem 9.2. Prove that $A \subseteq B \land B \subseteq C \implies A \subseteq C$.

Summary of proof: Suppose that $A \subseteq B$ and $B \subseteq C$. Then (i) $x \in A \implies x \in B$ and (ii) $x \in B \implies x \in C$. Now $A \subseteq C$ iff $x \in A \implies x \in C$.

At this point you can see what you are trying to prove. It is an implies statement. So assume that $x \in A$. Continuing,

Let $x \in A$. Then $x \in B$, by deduction on (i), and $x \in C$, by deduction on (ii). So $x \in A$ implies $x \in C$, hence $A \subseteq C$.

Here is the formal proof:

1. $A \subseteq B \text{ hyp}$
2. $B \subseteq C \text{ hyp}$
3. $\forall x, x \in A \implies x \in B \text{ def subset 1}$
4. $\forall x, x \in B \implies x \in C \text{ def subset 2}$
What next? Don't panic yet! One possibility is to write out the definition of the goal, $A \subseteq C$.

5 $A \subseteq C \iff \forall x, x \in A \implies x \in C$ def subset

We cannot write either side of the iff by itself, since we don't know whether either side is true yet. At this point it is helpful to circle what you are trying to prove. I put it into a box, which is easier to typeset.

Now you can panic. Once you are done panicking, look at what you are trying to prove again. If it is a conditional statement, you will often want to assume the hypothesis. (We did it a different way in the last section.) The rest of the proof is not that hard.

6 $x \in A$ temp hyp
7 $x \in B$ exist inst, inf on 3
8 $x \in C$ exist inst, inf on 4
9 $\forall x, x \in A \implies x \in C$ deduc on 6-8, univ gen
10 $A \subseteq C$ inf on 5, 9

Note that any temporary hypothesis is in force for only part of the proof. That is, you should be able to say where the temporary hypothesis begins and ends, and afterwards should be followed either by a “proof by deduction” line or a “proof by contradiction” line. In this case, the temporary hypothesis is in force from lines 6 to 8.

Problem 9.3. Prove $A \cap B = \emptyset \implies A - B = A$.

1 $A \cap B = \emptyset$ hyp
2 $\forall x, x \notin A \cap B$ char emptyset
3 $\forall x, \neg(x \in A \cap x \in B)$ def intersection
4 $\forall x, x \notin A \lor x \notin B$ de Morgan's

Don't panic yet! Write what you are trying to prove, as a biconditional.

5 $A - B = A \iff \forall x, x \in A - B \iff x \in A$ def set equality

Now we can unravel the definitions in this statement.

6 $A - B = A \iff \forall x, x \in A \land x \notin B \iff x \in A$ def set equality

Now you can panic. It helps again to circle what you are trying to prove. It happens to be a biconditional. To prove a biconditional, you have to prove the implication both ways. The first way is easy:

7 $x \in A \land x \notin B \implies x \in A$ taut

In fact, this is the tautology which is the basis of the cs rule. The other direction is harder. We start by assuming the hypothesis, and then deduce the conclusion.

8 $x \in A$ temp hyp
9 $x \notin B$ univ inst, da on 4
10 $x \in A \land x \notin B$ ci on 7, 8
11 $\forall x, x \in A \land x \notin B \iff x \in A$ cs on 7.10, univ gen
12 $A - B = A$ inf on 6, 11

Note that the temporary hypothesis is in force from lines 7 to 9, and is followed by a proof by deduction line.

Problem 9.4. Prove that for integers $x, y, z$, $x \mid y \lor x \mid z \implies x \mid yz$.

To prove a statement of this form, you will want to use inference by cases. Actually, the reasoning for both cases is the same, so we omit the steps for the second.

1 $x \mid y$ hyp
2 $\exists k, xk = y$ def divides
3 $xl = y$ ei 2

Now we unravel the definitions in what we are trying to prove.

4 $x \mid yz \iff \exists k, xk = yz$ def divides

We see that we need to find a number $k$, so that $xk$ is $yz$. To get that number, we multiply line 3 by $z$.

5 $xlz = yz$ arith 3
6 $\exists k, xk = yz$ exist gen 5
7 $x \mid yz$ deduc 1-6
8 $x \mid y \implies x \mid yz$ deduc 1=7

Next we do the second case. We omit the reasoning since it is the same.

9 $xz$ temp hyp
10 $x \mid yz$ same reasoning as in 4-8
11 $xz \implies x \mid yz$ deduc on 9-10
12 $x \mid y \lor x \mid z \implies x \mid yz$ ic on 8, 11

Problem 9.5. Let $A, B$ be sets. Show that $A - (A - B) = A \cap B$.

There are no hypotheses here, so we must work backwards, unravelling the definitions.
Write down a first line of a proof for each of the following problems. Minus one hundred points for writing down something that is equivalent to what you are trying to prove.

1. Let $A, B, C$ be sets. Prove that $B - (B \cap C) = B - C$
2. Let $n$ be an integer. Prove that if $n$ is square and $2$ divides $n$ then $4$ divides $n$.
3. Prove that the sum of two odd natural numbers is even.
4. Prove that any prime greater than $5$ is odd.
5. Prove that if the product $ab$ of integers $a, b$ is odd then $a$ is odd and $b$ is odd.

Problem 9.7. Prove the following by working backwards. In each case, give a formal proof, then a proof summary.

1. Let $B, C$ be sets. Prove that $B - (B \cap C) = B - C$
2. Let $n$ be an integer. Prove that if $n$ is square and $2$ divides $n$ then $4$ divides $n$.
3. Prove that the sum of two odd natural numbers is even.
4. Prove that any prime greater than $5$ is odd.
5. Prove that if the product $ab$ of integers $a, b$ is odd then $a$ is odd and $b$ is odd.

9.2. Proof summaries. In practice, it quickly becomes cumbersome to give formal two-column proofs. A proof summary is an outline of how one might construct a formal proof. A proof summary must be written in complete English sentences.

Here is an example. A formal proof that $2|6$ is the following:

1. $A - (A - B) = A \cap B \iff \forall x,$
2. $x \in A - (A - B) \iff x \in A \cap B \quad \text{def} =$
3. $(x \in A \land (x \in A \cup x \notin B)) \iff (x \in A \cap x \in B) \quad \text{def } -, \cap \text{ on 1}$
4. $(x \in A \land (x \in A \cup x \notin B)) \iff$
5. $(x \in A \land x \notin A \cup x \notin B) \quad \text{taut}$
6. $x \in A \land x \notin B \quad \text{inf on 3-4}$
7. $A - (A - B) = A \cap B \quad \text{univ gen on 5, inf on 2}$

A proof summary that $2|6$ is the following: By definition of divides, $2$ divides $6$ if and only if there exists an integer $x$ such that $2x = 6$. In fact, $2\cdot 3 = 6$. So, there exists an integer $x$, namely $x = 3$, such that $2x = 6$. Hence $2|6$.

9.3. Writing proof summaries. Here is a rough dictionary for how to construct a proof summary from a formal proof. It should be composed of complete English sentences, but it should also contain the key equations of the formal proof.

<table>
<thead>
<tr>
<th>formal proof</th>
<th>proof summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>hyp</td>
<td>Let, assume, suppose</td>
</tr>
<tr>
<td>mp on 1,2</td>
<td>By equations 1,2</td>
</tr>
<tr>
<td>mp on previous line</td>
<td>Hence, therefore, so, this shows</td>
</tr>
<tr>
<td>def</td>
<td>By definition of</td>
</tr>
</tbody>
</table>

Usually in summary form we do not mention the logical rules inf, contra inf, ic, di, ti, da, etc., because everyone who is working with summary proofs already is familiar with basic logic.

Problem 9.8. Translate the following proof that if $n$ is an even integer, then so is $n^2$, into summary form.

1. $n$ is even
2. $n$ is even $\implies \exists m, 2m = n$ def of even
3. $\exists m, 2m = n$ inf on 2
4. $2l = n$ exist inst on 3, $l$ an instance of $m$
5. $(2l)(2l) = n^2$ arithmetic on 4
6. $2(2l^2) = n^2$ arithmetic on 5
7. $\exists m, 2m = n^2$ exist gen on 6, $2l^2$ an instance of $m$
8. $n^2$ is even def of even

Answer: Let $n$ be an even integer. By definition of even, there exists an integer $m$ such that $2m = n$. Then $(2m)^2 = n^2$, and so $n^2 = 2(2m^2)$. Let $l = 2m^2$. Then $n^2 = 2l$. Hence there exists an integer $l$ such that $n^2 = 2l$, so $n^2$ is even.

Note that each new notation is introduced, either through a “Let” which makes it an unrestricted element of some set, through a temporary
hypothesis which makes it a restricted element of some set, or through an existential instantiation.

Problem 9.9. Translate the following proof that $\forall x, y, z, x|y \land x|z \implies x|y + z$ into summary form.

<table>
<thead>
<tr>
<th>Step</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$x</td>
</tr>
<tr>
<td>2</td>
<td>$\exists k, xk = y \land \exists k, xk = z$</td>
</tr>
<tr>
<td>3</td>
<td>$xl = y \land xm = z$</td>
</tr>
<tr>
<td>4</td>
<td>$x(l + m) = y + z$</td>
</tr>
<tr>
<td>5</td>
<td>$\exists k, xk = y + z$</td>
</tr>
<tr>
<td>6</td>
<td>$x</td>
</tr>
<tr>
<td>7</td>
<td>$x</td>
</tr>
<tr>
<td>8</td>
<td>$\forall x, y, z \in \mathbb{Z}, x</td>
</tr>
</tbody>
</table>

Answer: Let $x, y$ and $z$ be integers. Suppose that $x$ divides $y$ and $x$ divides $z$. By definition of divides, there exist integers $l, m$ such that $xl = y$ and $xm = z$. Hence $x(l + m) = y + z$, so $x$ divides $y + z$. 

Problem 9.10. For each of the variables $x, y, z, l, m$, identify the place where the variable is introduced. Is each introduced as a general or restricted element of the set of integers?

Here is a translation of a formal proof that $A \cup B \subseteq C \implies A \subseteq C$ into a proof summary. Recall the formal proof:

<table>
<thead>
<tr>
<th>Step</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$A \cup B \subseteq C$</td>
</tr>
<tr>
<td>2</td>
<td>$\forall x, x \in A \cup B \implies x \in C$</td>
</tr>
<tr>
<td>3</td>
<td>$x \in A \lor x \in B \implies x \in C$</td>
</tr>
<tr>
<td>4</td>
<td>$A \subseteq C \iff (\forall x, x \in A \implies x \in C)$</td>
</tr>
<tr>
<td>5</td>
<td>$x \in A \implies x \in A \lor x \in B$</td>
</tr>
<tr>
<td>6</td>
<td>$x \in A \implies x \in C$</td>
</tr>
<tr>
<td>7</td>
<td>$\forall x, x \in A \implies x \in C$</td>
</tr>
<tr>
<td>8</td>
<td>$A \subseteq C$</td>
</tr>
</tbody>
</table>

Here is the proof summary: Suppose that $A, B, C$ are sets and $A \cup B \subseteq C$. By definition of subset $\forall x, x \in A \cup B \implies x \in C$. Using this and the definition of union, $\forall x, x \in A \lor x \in B \implies x \in C$. Now tautologically, $\forall x, x \in A \implies x \in A \lor x \in B$. By transitivity of implication, $\forall x, x \in A \implies x \in C$. By definition of subset, $A \subseteq C$.

Problem 9.11. Translate the following proof that $x|y \lor x|z \implies x|yz$ into summary form, by filling in the blanks.

<table>
<thead>
<tr>
<th>Step</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$x</td>
</tr>
<tr>
<td>2</td>
<td>$\exists k, xk = y$</td>
</tr>
<tr>
<td>3</td>
<td>$xl = y$</td>
</tr>
<tr>
<td>4</td>
<td>$xlz = yz$</td>
</tr>
<tr>
<td>5</td>
<td>$\exists k, xk = yz$</td>
</tr>
<tr>
<td>6</td>
<td>$x</td>
</tr>
<tr>
<td>7</td>
<td>$x</td>
</tr>
<tr>
<td>8</td>
<td>$x</td>
</tr>
<tr>
<td>9</td>
<td>$\exists k, xk = z$</td>
</tr>
<tr>
<td>10</td>
<td>$xl = z$</td>
</tr>
<tr>
<td>11</td>
<td>$xl = yz$</td>
</tr>
<tr>
<td>12</td>
<td>$\exists k, xk = yz$</td>
</tr>
<tr>
<td>13</td>
<td>$x</td>
</tr>
<tr>
<td>14</td>
<td>$x</td>
</tr>
<tr>
<td>15</td>
<td>$x</td>
</tr>
</tbody>
</table>

Answer: Suppose that $x, y$ are integers and $x | y$. By definition of $x | y$, there exists an integer $k$ such that $y = kx$. Hence $yz = x(kz)$, so $x$ divides $yz$. By the same argument, if $x | z$ then $x$ divides $yz$. Hence if either $x | y$ or $x | z$ then $x$ divides $yz$.

Problem 9.12. Translate the following proof that $A \subseteq B, B \subseteq C \implies A \subseteq C$ into summary form, by filling in the blanks.

<table>
<thead>
<tr>
<th>Step</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$A \subseteq B$</td>
</tr>
<tr>
<td>2</td>
<td>$B \subseteq C$</td>
</tr>
<tr>
<td>3</td>
<td>$A \subseteq B \iff \forall x, x \in A \implies x \in B$</td>
</tr>
<tr>
<td>4</td>
<td>$\forall x, x \in A \implies x \in B$</td>
</tr>
<tr>
<td>5</td>
<td>$B \subseteq C \iff \forall x, x \in B \implies x \in C$</td>
</tr>
<tr>
<td>6</td>
<td>$\forall x, x \in B \implies x \in C$</td>
</tr>
<tr>
<td>7</td>
<td>$y \in A \implies y \in B$</td>
</tr>
<tr>
<td>8</td>
<td>$y \in B \implies y \in C$</td>
</tr>
<tr>
<td>9</td>
<td>$y \in A \implies y \in C$</td>
</tr>
<tr>
<td>10</td>
<td>$\forall x, x \in A \implies x \in C$</td>
</tr>
<tr>
<td>11</td>
<td>$A \subseteq C \iff \forall x, x \in A \implies x \in C$</td>
</tr>
<tr>
<td>12</td>
<td>$A \subseteq C$</td>
</tr>
</tbody>
</table>

Answer: Suppose that $A, B, C$ are sets such that $A \subseteq B$ and $B \subseteq C$. By definition of $A \subseteq B$ and $B \subseteq C$, for all $x, x \in A \implies x \in B$,
and \( x \in B \implies x \in C \). Since \( \star \) is transitive, \( x \in A \implies x \in C \). By definition of \( \star \), \( A \subseteq C \).

Note we skipped several steps in the proof above; for example, the last step really uses universal generalization as well as the definition of subset.

Later in the course we will drop formal proofs completely and work only with proof summaries.

**Suggestions for proof summaries:**

1. If the statement is an implication, your proof should start with an “Assume”, “Suppose” or “Let” followed by the hypothesis.
2. A proof by contradiction, you would say something like “Suppose, by way of contradiction, that ...”, or “The proof is by contradiction. Suppose ...”.
3. If the proof is a universal statement, for example, a statement about all integers, your proof should start with a “Let ...”. For example, if you want to show that for any even integer \( x \), \( 4 \) divides \( 2x \), you would start by “Let \( x \) be an even integer.”
4. If your statement is an existential statement, you have to show that there is at least one solution. For example, to prove that \( \exists x, x^2 = 9 \), your proof might start with “Let \( x = 3 \). Then ... “.

**Problem 9.13.** Use the following proof summary that there is no largest even natural number to construct a formal proof.

**Proof summary:** Suppose, by way of contradiction, that there is a largest even integer, call it \( x \). Then \( x + 2 \) is also an even integer, and must be less than or equal to \( x \). But then subtracting \( x \) from both sides gives \( 2 \leq 0 \), which is a contradiction. Hence, there is no largest even integer.

1. \( \exists x \) \( \forall y \) \( y \leq x \) temp hyp
2. \( \forall y, y \leq x \) exist inst on 1
3. \( 2|x + 2 \) \( \iff \) \( x \) \( \leq \) \( x \) exist inst on 2
4. \( 2|x \)
5. \( 2|x + 2 \)
6. \( \inf 3,4, \text{ contra} \)
7. \( \exists x, \forall y, 2|y \iff y \leq x \) proof by contra 1-5

**Problem 9.14.** Fill in the blanks in the following proof summary and proofs that for all sets \( A, B \), \( B - A = B \implies A \cap B = \emptyset \).

**Proof summary:** Suppose that \( A, B \) are sets such that \( \star \). By definition of \( \star \) and \( \star \), for all \( x, x \in B \land x \notin A \implies x \in B \). Hence given \( x, x \in B \) implies \( \star \) or equivalently, \( \star \) or \( x \notin A \). By de Morgan’s law, \( \neg(x \land x) \). By definition of intersection, \( x \notin \star \).

Hence \( A \cap B = \star \), by characterization of the empty set.

1. \( B - A = B \)
2. \( \forall x, x \in B \land x \notin A \iff x \in B \)
3. \( x \in B \iff x \notin A \)
4. \( (x \notin B \lor x \notin A) \)
5. \( \text{de Morgan’s} \)
6. \( x \notin A \cap B \)
7. \( \forall x, x \notin A \cap B \)
8. \( \star \) char empty set

**Rules for writing proof summaries:**

1. Proof summaries have to be in complete English sentences, in particular, there should be verbs and punctuation.
2. Each step in the proof should be justified, at least with a “Hence” to indicate it follows from the previous line or lines.
3. You cannot use a variable before you introduce it, or use it with a quantifier. For example, you cannot write “Suppose that \( x \) is even. Then \( x = 2k \).” Instead, write “Suppose that \( x \) is even. Then \( x = 2k \) for some integer \( k \).”
4. Check to make sure you haven’t assumed something that is equivalent to what you are trying to prove.
5. Is it clear where you have used hypotheses? If not, the proof isn’t clearly written.
6. Have you used the definitions of the terms and symbols used in the statement you are trying to prove? If not, you can’t have proved it.
7. If the proof is too long, try to break part of it out into a separate proof.
8. If you used proof by contradiction, try to simplify your proof so that you are arguing directly. Often times, once you have found a proof by contradiction you can simplify the argument.

9.4. **Breaking proofs into pieces.** Part of the art of writing good proofs is to finding the structure of the argument. Suppose for example,
in the course of proving a statement, you encounter a statement that you would like to assume, for the moment. You may want to prove the separate statement as a lemma; this is Greek for something that is taken or assumed. In other situations, you might realize that the statement that you want to prove is a consequence of a more general statement. In that case, you may want to prove the more general statement as a theorem, which is Greek for to consider, and give your statement as a corollary (Greek for a small garland of flowers given as a gift). A proposition is a statement whose importance is somewhere in between a lemma and a theorem.

Here is an example, which we will use later in the proof of the fundamental theorem of arithmetic.

Problem 9.15. Prove that \( \forall d, n \in \mathbb{N}, d|n! + 1 \implies d \notin \{2, \ldots, n\} \).

Let’s first give a proof, without breaking anything out, by contradiction.

1. \( d \in \{1, \ldots, n\} \)  
   hyp
2. \( d|n(n-1)(n-2)\ldots1 \)  
   inference by cases
3. \( n! = n(n-1)(n-2)\ldots1 \)  
   def factorial
4. \( d|n! \)  
   sub 2,3
5. \( d|n! + 1 \)  
   temp hyp
6. \( d|(n! + 1) - n! \implies d|y \wedge x|z \implies x|y - z \)
7. \( d|1 \)  
   arithmetic on 6
8. \( d = 1 \)  
   def divides
9. \( d \notin \{2, \ldots, n\} \)  
   since 1 \( \neq 2 \) etc., contra
10. \( \neg(d|n! + 1) \)  
    proof by contra, 5-9

In the proof, we used that \( x|y \wedge x|z \implies x|y - z \). This is the sort of thing you might want to break out into a lemma.

Lemma 9.16. \( \forall x, y, z \in \mathbb{Z}, x|y \wedge x|z \implies x|y - z \).

1. \( x, y, z \in \mathbb{Z} \)  
   hyp
2. \( x|y \)  
   hyp
3. \( x|z \)  
   hyp
4. \( \exists k, xk = y \)  
   def divides
5. \( \exists l, xl = z \)  
   def divides
6. \( y - z = x(k - l) \)  
   arithmetic, exist inst on 4,5
7. \( \exists m, xm = y - z \)  
   exist gen on 6
8. \( x|y - z \)  
   def divides on 7

Then on line 7 of your original proof you could write instead

\[ d|(n! + 1) - n! \]  
by Lemma below

Looking at your proof, you might realize that it is obscuring the following basic fact: no natural number greater than one can divide two consecutive numbers. This is the basic theorem, and the statement you are being asked to prove is really a consequence of that, namely, if \( d \) divides \( n! \) then it cannot divide \( n! + 1 \). So you might want to structure your argument like this:

Lemma 9.17. For all integers \( x, y, z \), if \( x \) divides \( y \) and \( x \) divides \( z \) then \( x \) divides \( y - z \).

Proof: Suppose that \( x, y, z \) are integers such that \( x \) divides \( y \) and \( x \) divides \( z \). Then there exist natural numbers \( k, l \) such that \( y = kx \) and \( z = lx \). Subtracting gives \( y - z = (k - l)x \), hence \( x \) divides \( y - z \).

Theorem 9.18. No natural number greater than one divides two consecutive natural numbers. That is, \( \forall d, n \in \mathbb{N}, d > 1 \implies \neg(d|n \wedge d|n + 1) \).

Proof: Let \( d, n \in \mathbb{N} \) and \( d > 1 \). Suppose, by way of contradiction, that \( d \) divides \( n \) and \( n + 1 \). By the lemma, \( d \) divides 1. Since the only divisor of 1 is itself, \( d = 1 \), which is a contradiction. Hence \( d \) does not divide both \( n \) and \( n + 1 \).

Corollary 9.19. If \( d \in \{1, \ldots, n\} \) then \( d \) does not divide \( n! + 1 \).

Proof: Suppose that \( d \in \{1, \ldots, n\} \). Then \( d \) divides \( n! \), since \( n! = n(n-1)\ldots1 \). By the Theorem, \( d \) does not divide both \( n! \) and \( n! + 1 \). Since \( d \) divides \( n! \), \( d \) cannot divide \( n! + 1 \), which proves the corollary.

Hints for writing proof summaries:

1. Write down your hypotheses.
2. Break down your hypotheses using definitions.
3. Proof is an art, not a science. Mess around a little.
4. If you are stuck, try proof by contradiction.
5. If you can, try some examples. Don’t confuse an example with a proof, but still, it helps to do examples.
6. Still stuck? Try to break it down into cases.

Problem 9.20. Write proof summaries of the following statement.

1. The sum of two odd integers is even.
(2) Any square natural number is not prime.
(3) There is no largest natural number divisible by 7.
(4) \( A - (B \cup C) = (A - B) \cap (A - C) \) for any sets \( A, B, C \).
(5) If \( A \cap B \) is empty then \( A - B = A \).
(6) \( 58 \) is the sum of two square natural numbers.
(7) If \( x \) divides \( z \) and \( x \) divides \( y \) then \( x \) divides \( y - z \).
(8) If \( A \subset C \) and \( B \subset C \) then \( A \cup B \subset C \).

10. ORDERED PAIRS AND RELATIONS

In this section we introduce a way of defining mathematical relations via set theory.

10.1. ORDERED PAIRS AND RELATIONS.

Definition 10.1. Suppose that \( A \) and \( B \) are sets. An ordered pair is a pair of elements \((a, b)\) with \( a \in A \) and \( b \in B \), called the components of the pair. Two ordered pairs \((a, b)\) and \((a', b')\) are equal if \( a = a' \) and \( b = b' \).

Example 10.2. The components of \((jill, jack)\) are jill and jack. The components of \((-100, \text{my bank account})\) are \(-100\) and \(\text{my bank account}\). The components of \((\{1\}, \{2, 3\})\) are \(\{1\}\) and \(\{2, 3\}\). The components of \((1, (0, 1))\) are 1 and \((0, 1)\).

Problem 10.3. Find the components of the ordered pairs \((1) (1, (2, 3)) \) \((2) ((1, 2), 3) \) \((3) ((1, 2), \{3\})\).

Answer to (1): The components are 1 and \((2, 3)\).

The set of all ordered pairs whose first component lies in a set \( A \) and whose second component lies in \( B \), also called the Cartesian product, is denoted \( A \times B \).

Example 10.4. The Cartesian product of \(\{1, 2, 3\}\) and \(\{4, 5\}\) is \(\{1, 2, 3\} \times \{4, 5\} = \{(1, 4), (2, 4), (3, 4), (1, 5), (2, 5), (3, 5)\}\). Similarly the product \(\{s, j\} \times \{v, c\} = \{(s, v), (s, c), (j, v), (j, c)\}\).

Problem 10.5. Find the Cartesian product of \{apples, oranges\} with \{frogs, grandmothers\}.

The square of a set \( A \) is the product \( A^2 = A \times A \). For example, \(\{\text{apples}\}^2 = \{\text{apples, apples}\}\) while
\[
(2) \quad \{\text{frogs, grandmothers}\}^2 = \{(\text{frogs, frogs}), (\text{frogs, grandmothers}),
\quad \quad \quad \quad \quad (\text{grandmothers, frogs}), (\text{grandmothers, grandmothers})\}.
\]

We can also talk about ordered triples, ordered quadruples etc. For example, if \( A = \{1\}, B = \{2\}, C = \{3\}\) then \(A \times B \times C = \{(1, 2, 3)\}\), the set consisting of the ordered triple \((1, 2, 3)\). Note that
\[
A \times (B \times C) \neq (A \times B) \times C \neq A \times B \times C.
\]
Indeed, in the example above, \(A \times (B \times C) = \{(1, (2, 3))\}\) while \((A \times B) \times C = \{((1, 2), 3)\}\). Both consist of a single ordered pair, and since the components of the ordered pair are not equal, the ordered pairs are not equal.

If \( A = \mathbb{R} \) are the real numbers, then we often think of \( A^2 = \mathbb{R}^2 \) as the Cartesian plane, with the first number giving the horizontal position and the second number the vertical.

Definition 10.6. A relation on \( A, B \) is a subset of \( A \times B \). If \((a, b) \in R\), we write \(aRb\) for short.

Example 10.7. If \( R = \{(1, 2), (1, 3)\}\) then \(1R2\) but \(\neg(2R1)\).

Example 10.8. If \( A \) is the set of my daughters abbreviated \(s, j\) and \( B \) is the set of ice cream flavors \(v\) for vanilla and \(c\) for coffee, then the set of ordered pairs \((a, b)\) such that \(a\) likes flavor \(b\) is a relation, which happens to be \(R = \{(s, v), (j, v)\}\). In other words, the kids don’t like coffee ice cream, which is great for me! In this case the notation \(sRv\) means \(s\) likes flavor \(v\).

An important class of relations are the order relations on numbers. For example, we say that \(x \leq y\) iff \(\exists z \in \mathbb{N}, x + z = y\), and \(x < y\) iff \(\exists z \in \mathbb{N}, x + z = y \land z \neq 0\). The relations \(\geq\) and \(>\) are defined similarly. Note that \(\leq\) is a subset of \(\mathbb{N} \times \mathbb{N}\), whose elements include \(\{(0, 0), (0, 1), (1, 1), (1, 2), \ldots\}\).

Example 10.9. The relation \(\geq\) is the set of ordered pairs \(\geq = \{(0, 0), (1, 0), (1, 1), (2, 0), (2, 1), \ldots\}\).

Problem 10.10. Give a roster form of the relation
(1) \( \leq \) on the set \( \{1, 2, 3\} \).
(2) \( < \) on the set \( \{1, 2, 3\} \).
(3) \( xRy \iff x = y^2 \) on the set \( \{1, -1, 2\} \).

**Problem 10.11.** True or false? Justify your answer.

1. \( \cup \geq = \mathbb{N} \times \mathbb{N} \)
2. \( \cup \geq = \mathbb{N} \times \mathbb{N} \)
3. \( \geq \cap \leq = \emptyset \)

Answer to (3): False, \( \leq \cap \leq = \{(x, y) \in \mathbb{N} \mid x \geq y \land y \geq x\} = \{(x, y) \in \mathbb{N} \mid x = y\} \).

**Problem 10.12.** (1) Prove that \( x \leq y \implies xz \leq yz \) for all \( x, y, z \in \mathbb{N} \).
(2) Prove that \( x \leq y \implies x + z \leq y + z \) for all \( x, y, z \in \mathbb{N} \).

Answer to the first part: Let \( x, y, z \in \mathbb{N} \), and suppose that \( x \leq y \). Then \( y - x \geq 0 \), so \( z(y - x) \geq 0 \). But \( z(y - x) = yz - xz \) so \( yz - xz \geq 0 \), hence \( xz \leq yz \).

**Definition 10.13.** The *divides relation* on \( \mathbb{N} \) as follows. We say \( a \) divides \( b \), or is a divisor of \( b \), or \( b \) is divisible by \( a \), and write \( a|b \) iff \( \exists c, ac = b \) and say \( a \) is a divisor of \( b \).

**Example 10.14.** \( 2|4 \) by \( \neg(2|5) \). The divisors of 12 are 1, 2, 3, 4, 6, 12. 25 is divisible by 1, 5 and 25.

**Problem 10.15.** Prove that \( \forall a, b, c \in \mathbb{N}, a|b \lor a|c \implies a|bc \), and \( \forall a, b, c \in \mathbb{N}, a|b \land a|c \implies a|b + c \).

Here is a formal proof:

1. \( a|b \land a|c \) hyp
2. \( \exists k \in \mathbb{N}, ak = b \land \exists l \in \mathbb{N}, al = c \) 1, def | 2
3. \( ak = b \land al = c \) exist inst on 2
4. \( ak + al = b + c \) arithmetic on 3
5. \( a(k + l) = b + c \) distributive prop on 4
6. \( \exists m, am = b + c \) exist gen on 5
7. \( a|b + c \) 6, def of |

There are two common ways of picturing relations. The first is *graph form*, in which we write the first set horizontally, the second vertically, and draw a dot for each element of the relation. For example, the relation above is shown in Figure 14.

**Figure 14.** Graph form of “she likes that flavor”

The second is *arrow form*, where we draw an arrow between each pair of dots in the relation, as in Figure 15.

**Figure 15.** Arrow form of “she likes that flavor”

**Problem 10.16.** Let \( R = \{(x, y), x^2 = y\} \) where the universe for \( x \) is \( -2, -1, 0, 1, 2 \) and the universe for \( y \) is \( 0, 1, 4 \). Draw \( R \) in both arrow and graph forms.

**Definition 10.17.** The *domain* of a relation \( R \) is the set of \( a \) such that \( (a, b) \in R \), or formally, \( \text{dom}(R) = \{a, \exists b, (a, b) \in R\} \).

The *range* of a relation \( R \) is the set of \( b \) such that \( (a, b) \in R \), or formally, \( \text{rng}(R) = \{b, \exists a, (a, b) \in R\} \).
Example 10.18. The range of \( \{(1,3)(2,3)(2,5)\} \) is \( \{3,5\} \), while the domain is \( \{1,3\} \). The range of \( R = \{(x,y) | y = x^2\} \) is the set of non-negative integers, if the universe for \( x \) is all integers.

Problem 10.19. Describe the domain and range of the following relations.

1. \( R = \{(s,v),(j,v)\} \).
2. \( R = \{(x,y) \in \mathbb{Z}^2 | y^2 = x\} \).
3. \( R = \{(x,y) | y \) is the genetic father of \( x\}\). (Describe the answer in English).

Problem 10.20. Describe the domain and range of the following relations. (1) \( \{(1,2),(2,3),(3,4),(2,4)\} \). (2) \( R = \{(x,y) \in \mathbb{Z}^2 | 2y = x\} \). (3) \( R = \{(apples, oranges),(apples, frogs)\} \).

Definition 10.21. If \( R \subseteq A \times B \) is a relation, the inverse relation \( R^{-1} \subseteq B \times A \) is the relation obtained by switching order:

\[
R^{-1} = \{(b,a) | (a,b) \in R\}.
\]

That is,

\[
xR^{-1}y \iff yRx.
\]

Example 10.22. If \( R = \{(1,3),(2,3)(2,5)\} \) then \( R^{-1} = \{(3,1),(3,2),(5,2)\} \). If \( R = \{(x,y) \in \mathbb{Z}^2 | x = y^2\} \) then \( R^{-1} = \{(y,x) \in \mathbb{Z}^2 | x = y^2\} = \{(x,y) \in \mathbb{Z}^2 | y = \pm \sqrt{x}\} \).

In arrow form, the inverse is obtained by reversing the directions of all the arrows. In graph form, the inverse relation is obtained by reflecting the graph over the diagonal.

Definition 10.23. Suppose that \( A, B, C \) are sets, and \( R \subseteq A \times B \) and \( S \subseteq B \times C \) are relations. The composition of \( R \) and \( S \) is the set of pairs \( (a,c) \) that can be connected through \( B \), that is,

\[
R \circ S = \{(a,c) | \exists b, (a,b) \in R \land (b,c) \in S\}.
\]

Example 10.24. If \( R = \{(1,3),(2,3)(2,5)\} \) and \( S = \{(3,4),(4,5),(5,6)\} \) then \( R \circ S = \{(1,4),(2,4),(2,6)\} \). You can see this by finding all pairs of ordered pairs such that the last component of the first matches the first component of the second. Then we cross off the matching components to get the ordered pair for the composition:

\[
R \circ S = \{(1,3)(2,4),(2,3)(4,4),(2,6)(5,6)\}.
\]

In arrow form, this means that the arrows for \( R \circ S \) are obtained by joining together the arrows for \( R \) and those for \( S \), see Figure 16.

![Figure 16. Composition of relations](image)

Problem 10.25. (1) Let \( R = \{(1,3),(2,3)(2,5)\} \) and \( S = \{(3,4),(4,5),(5,6)\} \). Find \( R \circ S \) and \( S \circ R \).

(2) Let \( R = \{(1,3),(3,4)(2,5)\} \) and \( S = \{(2,3),(4,5),(5,6)\} \). Find \( S \circ R \) and \( S \circ R \).

(3) Let \( R = \{(1,3)(2,5)\} \) and \( S = \{(2,3),(5,6)\} \). Find \( R \circ S \) and \( R \circ S^{-1} \).

Remark 10.26. Unfortunately there are two conventions for composition, depending on whether \( R \) or \( S \) is applied first. The other convention, \( R \circ S = \{(a,c) | \exists b, aSb \land bRc\} \) has the advantage that \( (R \circ S)(a) = R(S(a)) \), if \( R, S \) are functions. The first convention fits better with the arrow picture of relations. If you want to be clear, say which convention you are using.
Problem 10.27. Suppose that $R$ is the relation $aRb$ iff $a$ is the child of $b$, and $S$ is the relation $aSb$ iff $a$ is the sibling of $b$. Find the meaning in English of the relations

1. $R \circ S$
2. $S \circ R$
3. $R \circ R$
4. $S \circ S$
5. $R^{-1}$
6. $S^{-1}$
7. $R \circ R^{-1}$
8. $R^{-1} \circ R$
9. $(R \circ S)^{-1}$

10.2. Proofs involving relations. Proofs involving relations are the same as those for sets, except that we use the definitions for relations, compositions, and inverses. One important trick which shortens the proofs considerable is the following: since an element of a relation is an ordered pair, always use ordered pairs in the definition of equality and subsets. That is, by definition of set equality, if $R$ and $S$ are relations, then

$$(R = S) \iff \forall x, x \in R \iff x \in S.$$

But it’s better to write

$$(R = S) \iff \forall (x, y), (x, y) \in R \iff (x, y) \in S$$

since the elements of $R, S$ are ordered pairs. The following example shows how this is used in practice.

Problem 10.28. Let $R$ be the relation on the natural numbers defined by $xRy \iff (x|y)$. Prove

1. $R \neq R^{-1}$
2. $R \circ R = R$.

A good strategy for these types of proofs is working backwards, as in Section 9.1. To start the proof of the first part, write

1. $R \neq R^{-1}$

\[ \neg \forall (x, y), (x, y) \in R \iff (x, y) \in R^{-1} \quad \text{def equality} \]

Note that you cannot write either of the sides of this biconditional by themselves, since you do not know yet whether either side is true.

At this point you are done unravelling the definitions, and you have to examine the statement that you are trying to prove. I have put it in a box. To prove an exists statement, it suffices to give an example. In this case, you want to give an example where $x/y \iff y|x$ does not hold, that is, an example where one side is true and the other false.

2. $R \neq R^{-1}$

$\exists (x, y), \neg ((x, y) \in R \iff (y, x) \in R)$

def $R$ on 2

At this point you are done unravelling the definitions, and you have to examine the statement that you are trying to prove. I have put it in a box. To prove an exists statement, it suffices to give an example. In this case, you want to give an example where $x/y \iff y|x$ does not hold, that is, an example where one side is true and the other false.

3. $R \neq R^{-1}$

$\exists (x, y), \neg (x | y \iff y | x)$

exist gen on 4

Proof summary: $R \neq R^{-1}$ means that there is a pair of numbers $x, y$ such that $(x, y) \in R$ but $(x, y) \notin R^{-1}$, that is, $xRy$ but not $xR^{-1}y$, that is, $xRy$ but not $yRx$. Since $R$ is the divides relation, it suffices to give a pair of numbers $x, y$ such that $x|y$ but not $y|x$. For example 2|4 but not 4|2. Hence $R \neq R^{-1}$.

In the answer to the second part, the first line unravels the definition of what you are trying to prove. Since it is a conditional, the next line takes the assumption of the conditional as temporary hypothesis.

1. $R \circ R \subseteq R \iff \forall (x, y), (x, y) \in R \implies (x, y) \in R$\text{ def subset}$

2. $(x, y) \in R \circ R \implies (x, y) \in R$\text{ temp hyp}$

3. $\exists z, (x, z) \in R \wedge (z, y) \in R$\text{ def composition,2}$

4. $x|z \wedge z|y$\text{ def divides}$

5. $\exists k, xk = z \wedge \exists k, zk = y$\text{ def divides}$

6. $xm = z \wedge zn = y$\text{ exist inst on 3}$

7. $x(mn) = y$\text{ algebra on 6}$

8. $\exists k, xk = y$\text{ exist gen on 7, } k = mn$

9. $(x, y) \in R$\text{ def divides, R}$

10. $(x, y) \in R \circ R \implies (x, y) \in R$\text{ deduction 2-9}$

11. $R \circ R \subseteq R$\text{ inf on 1,10}$

Problem 10.29. Let $R$ be the relation on the natural numbers defined by $xRy \iff (x \leq y)$. Prove

1. $R \neq R^{-1}$
2. $R \circ R = R$.
Problem 10.30. Let $R$ be the relation on the natural numbers defined by $xRy \iff (x \leq y)$. Let $S$ be the relation on the natural numbers defined by $xRy \iff (x \geq y)$. Prove

1. $R = S^{-1}$.
2. $R \circ S = \mathbb{N}^2$.

Problem 10.31. Prove that for any composable relations $R, S, T$,

1. $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.
2. $R \circ (S \circ T) = (R \circ S) \circ T$.

In each case, provide a proof summary.

Problem 10.32. Prove that $B \subseteq C \implies A \times B \subseteq A \times C$, and provide a proof summary.

1. $B \subseteq C$ hyp
2. $B \subseteq C \iff (\forall x, x \in B \implies x \in C)$ def subset
3. $\forall x, x \in B \implies x \in C$ inf on 1,2
4. $(x, y) \in A \times B$ temp hyp
5. $(x, y) \in A \times B \iff (x \in A \land y \in B)$ def product
6. $x \in A \land y \in B$ inf on 4,5
7. $y \in B$ cs on 7
8. $y \in B \implies y \in C$ univ inst on 3
9. $y \in C$ inf on 7,8
10. $x \in A \land y \in C$ ci on 8,9
11. $(x, y) \in A \times C \iff (x \in A \land y \in C)$ def product
12. $x \in A \times C$ inf on 10,11
13. $(x, y) \in A \times B \implies (x, y) \in A \times C$ ded from 6-12
14. $(A \times B \subseteq A \times C) \iff $(\forall x, y, (x, y) \in A \times B \implies (x, y) \in A \times C)$ def subset
15. $A \times B \subseteq A \times C$ inf on 13,14

Some proofs, especially those involving the emptyset, can be very awkward, for example:

Problem 10.33. Show that $A \times \emptyset = \emptyset$.

1. $A \times \emptyset = \emptyset \iff \forall x, x \in A \times \emptyset \iff x \in \emptyset$ def set equality
2. $(a, b) \in A \times \emptyset \iff a \in A \land b \in \emptyset$ def product
3. $b \in \emptyset \iff b \neq b$ def emptyset
4. $(a, b) \in A \times \emptyset \iff a \in A \land b \neq b$ sub 2,3
5. $a \in A \land b \neq b \iff (a, b) \neq (a, b)$ taut
6. $(a, b) \neq (a, b) \iff (a, b) \in \emptyset$ def emptyset
7. $(a, b) \in A \times \emptyset \iff (a, b) \in \emptyset$ sub 5,6
8. $A \times \emptyset = \emptyset$ inf on 1,7

Problem 10.34. Prove that if $R$ is the relation defined by $xRy$ iff $x-y \geq 2$, then $R \neq R^{-1}$.

Problem 10.35. Give formal proofs that

1. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
2. $((A \subseteq B) \land (C \subseteq D)) \implies (A \times C) \subseteq (B \times D)$
3. $\forall x, x \in A \implies x \in A$ def subset

Problem 10.36. Give proofs that if $R, S$ are relations in $A \times B$ and $B \times C$ respectively then

1. $\text{dom}(R \circ S) \subseteq \text{dom}(R)$
2. $\text{rng}(R \circ S) \subseteq \text{rng}(S)$

11. Functions

A function is a particular kind of relation, namely a relation with a unique value for each element of the domain.

11.1. Functions.

Definition 11.1. A function is a relation $R \subseteq A \times B$ such that assigns to each element of the domain a unique value of $B$, that is,

$\forall a \in A, b, b' \in B, aRb \land aRb' \implies b = b'$.

Example 11.2. $\{(1,2), (2,2), (3,1)\}$ is a function, while $\{(1,2), (1,1), (3,1)\}$ is not. Another example: The relation defined by $xRy \iff y = x^2$ is a function from the $\mathbb{R}$ to $\mathbb{R}$, but the relation $R^{-1}$ defined by $xR^{-1}y \iff x = y^2$ is not, because it assigns to e.g. $x = 4$ the values $2, -2$ of $y$. The relation $\{(x, y) : y \text{ is the genetic father of } x\}$ is a perfectly good function.

Problem 11.3. Which of the following is a function?
Problem 11.4. List all

(1) functions from \{1, 2\} to itself.
(2) functions with domain \{1, 2, 3\} and image \{1, 2\}.

Some functions can be given as algebraic rules (as in the latter example) while other functions cannot. Thus the actual definition of function in mathematics is somewhat different from the one usually given in calculus (a rule that assigns to any number, another number) both because there is not necessarily any finite algebraic rule, and because the notion of function has nothing to do with numbers, but rather has to do with sets and ordered pairs.

Graphically, a relation is a function if it passes the vertical line test: there is at most one point in the intersection of the graph of \(R\) with each vertical line. If \(F \subseteq A \times B\) is a function, and \(a \in \text{dom}(F)\), then the value of \(F\) at \(a\) is the unique element \(F(a) \in B\) such that \((a, F(a)) \in F\). For example, if \(F = \{(x, y) \mid y = x^2\}\) then the value of \(F\) at \(-3\) is \(F(-3) = 9\).

Even though we usually talk about functions depending on a number, any set of ordered pairs may or not be a function. For example: \(F = \{(\text{George Bush}, \text{Dick Cheney}), (\text{Bill Clinton}, \text{Al Gore})\}\) is a function, while \(G = \{(\text{George Bush}, \text{Dick Cheney}), (\text{Bill Clinton}, \text{Al Gore}), (\text{Nixon}, \text{Agnew}), (\text{Nixon}, \text{Ford})\}\) is not.\(^7\) For the first function, we write \(F(\text{Clinton}) = \text{Gore}\), that is, Gore is the value of \(F\) at Clinton. More common examples of functions involving people are the “genetic father” or “genetic mother” functions of people.

Problem 11.5. Which of the following are functions?

1. The relation from people to flavors defined by \(F = \{(\text{sophie}, \text{vanilla}), (\text{julia}, \text{vanilla})\}\).
2. The relation from people to flavors defined by \(F = \{(\text{sophie}, \text{vanilla}), (\text{julia}, \text{vanilla}), (\text{chris}, \text{vanilla}), (\text{chris}, \text{coffee})\}\).
3. \(F = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x | y\}\).
4. \(F = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x | y \land y | x\}\).

\(^7\)The situation gets worse for F.D. Roosevelt, who had three vice-presidents.

Problem 11.6. Construct a function \(F : \{1, 2, 3\} \to \{1, 2, 3\}\) with the given properties (give the function in roster form.)

(1) \(F\) is increasing, that is, if \(x < y\) then \(F(x) < F(y)\).
(2) \(F\) is decreasing.
(3) \(F\) is neither increasing nor decreasing.

11.2. Injections, surjections, and bijections.

Definition 11.7. A function \(F : A \to B\) is called one-to-one or injective or an injection if each \(b \in B\) is the value of at most one \(a \in A\), that is,

\[
\forall a, a' \in A, \; F(a) = F(a') \implies a = a'.
\]

A function \(F\) is called onto or surjective or a surjection if each \(b \in B\) is the value of at least one \(a \in A\), that is,

\[
\forall b \in B, \exists a \in A, \; F(a) = b.
\]

A function \(F : A \to B\) is called a one-to-one correspondence or bijective or a bijection if it is both one-to-one and onto. Note that a one-to-one correspondence is not the same as a one-to-one function. To avoid this confusion, many mathematicians prefer the terminology injection, surjection, bijection.

Example 11.8. (1) The function \(f = \{(1, 1)(2, 2), (3, 2)\}\) is surjective onto \(\{1, 2\}\) but not injective, since \(f(2) = f(3) = 2\).
(2) The function \(f = \{(1, 1), (2, 2), (3, 4)\}\) is injective into \(\{1, 2, 3, 4\}\), but not surjective since there is no \(x\) such that \(f(x) = 3\).
(3) The function \(f(x) = 2^x\) from real numbers to real numbers is injective, since \(2^x = 2^y\) implies \(x = y\) but not surjective since if \(y\) is negative then there is no \(x\) such that \(2^x = y\).

Problem 11.9. Determine whether the following functions are injective resp. surjective resp. bijective.

(1) \(xFy\) if \(y\) is the genetic father of \(y\) and \(F \subset A \times B\) where \(A\) and \(B\) are both the set of all people.
(2) \(xFy\) if \(x\) has natural hair color \(y\) and \(A\) is the set of people and \(B\) is the set of colors yellow, brown, blue.
(3) \(xFy\) if \(y\) is the birthday of \(x\), \(B\) is the set of days of the week, and \(A\) is the set of all people.
Problem 11.10. Determine whether the following functions of a real variable are injective, surjective, or bijective. If they are not surjective, determine the range.

1. \( f(x) = x^2 \)
2. \( f(x) = x^3 \)
3. \( f(x) = x^3 + 3x^2 + 3x + 1 \).
4. \( f(x) = 2^x \).
5. \( f(x) = 2x^2 \).

Problem 11.11. Construct a function \( F : \{1, 2, 3\} \to \{1, 2, 3\} \) with the given properties (give the function in roster form.)

1. \( F = F^{-1} \) and \( F \) is not bijective.
2. \( F(1) = F(2) \).
3. \( F \) is bijective, \( F = F^{-1} \) and \( F(1) = 2 \).

Definition 11.12. The pre-image (also known as inverse image) of a value \( b \) of \( f \) is the set

\[ f^{-1}(b) = \{a, f(a) = b\}. \]

More generally, if \( B \) is a subset of \( f \) then the pre-image of \( B \) is the set of elements that map to \( B \), given by

\[ f^{-1}(B) = \{a | f(a) \in B\}. \]

Somewhat confusingly, \( f^{-1}(b) \) is a subset of \( A \) while \( f(a) \) is an element of \( b \). If \( f^{-1} \) is a function, then unfortunately the notation \( f^{-1}(b) \) is also used for the value of \( f^{-1} \) at \( b \). For example, if \( f(x) = 2^x \) then \( f^{-1}(2) = \log_2(2) \) and \( f^{-1}(4) \) could mean either 2 or \{2\}, depending on the context. The difference is usually not that important so doesn’t tend to cause problems.

Example 11.13. The pre-image of 0 under \( f(x) = x^4 - x^2 \) is \( f^{-1} = \{1, 0, -1\} \). The pre-image of \( -10 \) is \( f^{-1}(-10) = \emptyset \). The pre-image of \((\infty, 0)\) is \((-1, 0) \cup (0, 1)\).

Problem 11.14. Find the inverse image of 4 and the set \{0, 1, 2\} under the function from \( \mathbb{N} \times \mathbb{N} \) to \( \mathbb{N} \) defined by \( f(x, y) = x + y \).

Problem 11.15. (1) Find the domain and range of the relation \( R = \{(1,2),(2,2),(5,6),(7,6)\} \).
(2) Find its inverse \( R^{-1} \).
(3) Determine whether \( R, R^{-1} \) are functions.

(4) Find the pre-image of 2 under \( R \) and under \( R^{-1} \).
(5) Find the compositions \( R \circ R^{-1} \) and \( R^{-1} \circ R \).

11.3. Proofs involving functions. Proofs involving functions are the same as those involving relations, except that we have a few more definitions.

Problem 11.16. Show that the relation defined by \( xFy \iff y = x^3 \) is a function.

1. \( \forall x, y, xFy \iff y = x^3 \)
2. \( F \) is a function iff \( \forall x, z, xFy \land xFz \implies y = z \)
3. \( xFy \land xFz \)
4. \( y = x^3 \land z = x^3 \)
5. \( y = z \)
6. \( \forall x, y, z, xFy \land xFz \implies y = z \)
7. \( F \) is a function

Problem 11.17. Show that the function \( F(x) = x^3 \) is one-to-one.

1. \( \forall x, F(x) = x^3 \)
2. \( F \) is 1-1 \( \iff \forall x, y \in A \)
3. \( F(x) = F(y) \implies x = y \)
4. \( F(x) = x^3 \)
5. \( F(y) = y^3 \)
6. \( x^3 = y^3 \)
7. \( x = y \)
8. \( F(x) = F(y) \implies x = y \)
9. \( F \) is 1-1

You might wonder whether step 7 is really valid; since we haven’t introduce properties of numbers yet, we don’t really know which properties we can use. It might be better in this case to insert a few more steps, along the following lines: \( x^3 - y^3 = (x^2 + xy + y^2)(x - y) \). Since \(|xy| \leq x^2 + y^2 \), the first factor can never be zero, so if \( x^3 - y^3 = 0 \) we must have \( x - y \). Formally one could insert

6.1 \( x^3 - y^3 = 0 \)
6.2 \( (x^2 + xy + y^2)(x - y) = 0 \)
6.3 \( x - y = 0 \lor x^2 + xy + y^2 = 0 \)
6.4 \( x^2 + xy + y^2 > 0 \)
6.5 \( x - y = 0 \)
Of course, this still uses facts about numbers we haven’t talked about very much yet.

**Problem 11.18.** Show that for any function $F$ from $A$ to $B$,

1. $F$ is onto iff $\text{rng}(F) = B$.
2. $F$ is one-to-one iff $F^{-1}$ is a function.
3. if $F$ and $G$ are functions from $A$ to $B$ and from $B$ to $C$ respectively then $F \circ G$ is a function from $A$ to $C$.

**Problem 11.19.** Prove that

1. For any function $f$, $\forall a \in A, f^{-1}(f(a)) = \{a\} \iff f$ is one-to-one.
2. For any functions $f : A \to B$ and $g : B \to C$, if $f$ and $g$ are injective then so is $f \circ g$.
3. For any functions $f : A \to B$ and $g : B \to C$, if $f$ and $g$ are surjective then so is $f \circ g$.

Answer to part (b) in summary form. Suppose that $f : A \to B$ and $g : B \to C$ are injective. $f \circ g$ is injective if and only if for all $a_1, a_2 \in A$, $(f \circ g)(a_1) = (f \circ g)(a_2)$ implies $a_1 = a_2$. So suppose that $(f \circ g)(a_1) = (f \circ g)(a_2)$. Then $(f \circ g)(a_1) = g(f(a_1)) = (f \circ g)(a_2) = g(f(a_2))$ by definition of composition. Since $g$ is injective, $f(a_1) = f(a_2)$. Since $f$ is injective, $a_1 = a_2$. Hence, $(f \circ g)(a_1) = (f \circ g)(a_2)$ implies $a_1 = a_2$, so $f \circ g$ is injective.

Here is a summary of our definitions for relations and functions:

### 11.4. Sequences and convergence to infinity.

**Definition 11.20.** (Sequences) Let $S$ be a set.

1. A **finite sequence of elements of $S$** of length $k$ is a function $F$ from $\{1, \ldots, k\}$ to $S$.
2. An **infinite sequence of elements of $S$** is a function $F$ from $\mathbb{N}$ to $S$.

**Example 11.21.** For example, $2, 3, 4, 5$ is a sequence of length 4. $2, 4, 8, 16, 32$ is a sequence of length five. $4, 7, 10, 13, 16, 19$ is a sequence of length six. The Fibonacci sequence $1, 1, 2, 3, 5, 8, 13, \ldots$ is an infinite sequence.

The first and third of the example above are called **arithmetic sequences**; the next number in the sequence is given by adding a given number $1$ resp. $3$. The second example is a **geometric sequence**: the next number in the sequence is given by multiplying by a given number, in this case $2$. That is,

**Definition 11.22.** (Arithmetic and geometric sequences) $n_1, \ldots, n_k$ is an arithmetic resp. geometric sequence iff $\exists r, \forall k, n_{k+1} = n_k + r$ resp. $\exists r, \forall k, n_{k+1} = rn_k$.

**Problem 11.23.** Which of the following are arithmetic resp. geometric sequences? Identify $r$ in each case, if possible.

1. $2, 4, 6, 8$
2. $2, 6, 10, 15$
3. $5, 10, 15, 20$
4. $1, -1, 1, -1, 1$

**Problem 11.24.** Prove that the (i) sum of arithmetic (ii) product of geometric sequences is also an arithmetic reps. geometric sequence.

One of the most important definitions we want to make rigorous is that of a **limit**. This is because the notion of limit appears in the definition of a derivative, which is one of the most important concepts in mathematics (and science generally, because it represents an instantaneous rate of change; for example, instantaneous velocity is defined as a limit). The definition of limit is somewhat difficult to work with, because it involves several quantifiers. In this section, we start with a special case, the notion of a sequence having **limit equal to infinity**.

**Definition 11.25.** (Convergence to infinity) A sequence $x(0), x(1), x(2), \ldots$ of integers converges to infinity or has limit equal to infinity and write $\lim_{n \to \infty} x(n) = \infty$ iff $\forall e \in \mathbb{R}, \exists d \in \mathbb{Z}, \forall n \in \mathbb{Z}, n \geq d \implies x(n) \geq e$.

**Problem 11.26.** Which of the following sequences converges to infinity? (Use your intuition to decide how the sequence continues.) Explain your answer.

1. $0, 1, 1, 2, 2, 2, 3, 3, 3, 3, \ldots$
2. $0, 1, 0, 2, 0, 3, 0, 4, 0, 5, \ldots$
3. $0, 1, \sqrt{2}, \sqrt{3}, \sqrt{4}, \ldots$
4. $0, 1, 0, 1, 2, 0, 1, 2, 3, 0, 1, 2, 3, 4, \ldots$

**Example 11.27.** The sequence $1, 4, 9, 16, \ldots$ converges to infinity. Here is a proof, assuming basic facts about real numbers that we will explain in more detail later.
1. \( (\lim_{n \to \infty} n^2 = \infty) \iff \forall e \in \mathbb{Z}, \exists d \in \mathbb{Z}, \forall n \in \mathbb{Z}, n \geq d \implies n^2 \geq e \) def of limit
2. \( \forall n \in \mathbb{Z}, n \geq \sqrt{e} \implies n^2 \geq e \) basic fact
3. \( \exists d \in \mathbb{Z}, \forall n \in \mathbb{Z}, n \geq d \implies n^2 \geq e \) exist gen on 2
4. \( \forall n \in \mathbb{Z}, \exists d \in \mathbb{Z}, \forall n \in \mathbb{Z}, n \geq d \implies n^2 \geq e \) univ gen on 3
5. \( \lim_{n \to \infty} n^2 = \infty \) inf on 1, 4

**Example 11.28.** If \( x(n) \) converges to infinity, then so does \( x(n)^2 \). Proof:

1. \( \lim_{n \to \infty} x(n) = \infty \) temp hyp
2. \( \forall e \in \mathbb{Z}, \exists d \in \mathbb{Z}, \forall n \in \mathbb{Z}, n \geq d \implies x(n) \geq e \) def lim
3. \( \lim_{n \to \infty} x(n)^2 = \infty \iff \forall e \in \mathbb{Z}^+, \exists d \in \mathbb{Z}, \forall n \in \mathbb{Z}, n \geq d \implies x(n)^2 \geq e^2 \) def lim
4. \( x(n)^2 \geq e^2 \iff x(n) \geq \sqrt{e^2} \) algebra
5. \( \exists d \in \mathbb{Z}, \forall n \in \mathbb{Z}, n \geq d \implies x(n) \geq \sqrt{e} \) univ inst on 2, \( e = \sqrt{e^2} \)
6. \( \lim_{n \to \infty} x(n)^2 = \infty \) inf on 3, 5

When prove facts about limits, it helps to keep in mind that you only have to estimate the size of \( x(n) \), for example, bound it from below by something that is easier and still enough to show convergence.

**Example 11.29.** Prove that \( x(n) = n^n \) converges to infinity.

1. \( (\lim_{n \to \infty} n^n = \infty) \iff \forall e \in \mathbb{Z}, \exists d \in \mathbb{Z}, \forall n \in \mathbb{Z}, n \geq d \implies n^n \geq e \) def of limit
2. \( n \geq 1 \implies n^n \geq nn^{n-1} \geq n \) basic fact
3. \( n \geq e \land n \geq 1 \implies n^n \geq e \) transitivity \( \geq, 2 \)
4. \( \exists d \in \mathbb{Z}, \forall n \in \mathbb{Z}, n \geq d \implies n^n \geq e \) exist gen on 3
5. \( \forall n \in \mathbb{Z}, \exists d \in \mathbb{Z}, \forall n \in \mathbb{Z}, n \geq d \implies n^2 \geq e \) univ gen on 4
6. \( \lim_{n \to \infty} n^n = \infty \) inf on 1, 5

**Problem 11.30.** In each case, prove or disprove the convergence to infinity.

1. \( x(n) = n^2 \).
2. \( x(n) = (-1)^n n^3 \).
3. \( x(n) = n! \).

**Problem 11.31.** Prove that if \( x(n) \) and \( y(n) \) converge to infinity, then so do the sequences (a) \( x(n) + y(n) \) (b) \( 2x(n) \) (c) \( x(n)y(n) \).

**Problem 11.32.** Prove that if \( x(n) \) converges to infinity and \( \forall n \in \mathbb{N}, x(n) \leq y(n) \) then \( y(n) \) also converges to infinity.

### 11.5. Operations

An operation is a function from the product of a set with itself to the set. Examples include addition and multiplication of numbers, composition of functions etc.

**Definition 11.33.** An operation on a set \( S \) is a function \( S \times S \to S \). An operation \( f : S \times S \to S \) is **commutative** if \( f(x, y) = f(y, x) \) and associative if \( f(f(x, y), z) = f(x, f(y, z)) \). Given an operation \( f \) and an element \( x \in S \), we say that an element \( e \in S \) is a **unit** if \( f(y, e) = f(e, y) = y \) for all \( y \in Y \). Given a unit \( e \in S \) and an element \( x \in X \), an inverse for \( x \) is an element \( y \in Y \) so that \( f(x, y) = f(y, x) = e \).

For example, \( \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (3, 2), (3, 3)\} \) is an operation on the set \{1, 2\}. You might notice that the operation takes as input a pair of numbers and outputs the maximum of them; however, an operation does not necessarily have to have a rule.

#### 11.5.1. Addition and multiplication

**Addition**

\[ + : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (x, y) \mapsto x + y \]

**Multiplication**

\[ \cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (x, y) \mapsto xy \]

are examples of operations on the natural numbers. The additive unit is 0, while the multiplicative unit is 1. The additive inverse of \( x \) is \(-x\), while the multiplicative inverse of \( x \) is \(1/x\), if \( x \) is non-zero.

**Problem 11.34.** For \( f \) equal to (a) addition and (b) multiplication on the natural numbers find (i) three elements of \( f \) (ii) \( f^{-1}(0) \) (iii) the image of \( f \).

#### 11.5.2. Subtraction and division

Subtraction is an operation not on the natural numbers but rather on the integers. The first few elements are \( ((0, 0), 0), ((1, 0), 1), ((0, 1), -1) \) etc. Division is an operation on non-zero rational numbers.

#### 11.5.3. Minimum and maximum

The **minimum** and **maximum** of two natural numbers \( a, b \) are the operations defined by

\[ a \leq b \implies \min(a, b) = a \land \max(a, b) = b \]
\[ b \leq a \implies \min(a, b) = b \land \max(a, b) = a. \]

**Problem 11.35.** Show that given integers \( a, b, \)
(1) \(\min(a, b) \max(a, b) = ab.\)
(2) \(\min(a, b) + \max(a, b) = a + b.\)

11.5.4. And and Or. Let \(S\) be the set of all propositional forms. Then conjunction

\[
\land : S \times S \to S, (P, Q) \mapsto P \land Q
\]

is an operation on \(S\). Similarly \(\lor\) and \(\Rightarrow\) are operations on \(S\). For example, some elements of \(\land\) are \(((P, Q), P \land Q), ((P \lor S, Q), (P \lor S) \land Q)\).

**Problem 11.36.** Which of the following are elements of \(\lor\)? (a) \(((P, Q), P \lor Q), ((P \Rightarrow S, Q), (P \Rightarrow S) \lor Q)((P, Q) \Rightarrow P), (c) (P \lor Q) \Rightarrow P).\)

**Problem 11.37.** Which of \(\land, \lor, \Rightarrow\) are commutative? associative?

11.5.5. Composition.

**Definition 11.38.** The composition of relations is an operation on relations:

\[
\text{Rel}(S, S) \times \text{Rel}(S, S) \to \text{Rel}(S, S), \quad (f, g) \mapsto f \circ g.
\]

The identity relation

\[
\text{Id}_S := \{(x, x) \mid x \in S\}
\]

is an identity with respect to this operation:

\[
\forall f \in \text{Rel}(S, S), f \circ \text{Id}_S = \text{Id}_S \circ f = f.
\]

A permutation of a set \(S\) is a bijection from \(S\) to itself. The set of permutations is denoted \(\text{Perm}(S)\).

**Example 11.39.** (1) \(\{(1, 3), (2, 1), (3, 2)\}\) is a permutation of \(\{1, 2, 3\}\).
(2) \(\text{Perm}([1, 2]) = \{\{(1, 1), (2, 2)\}, \{(2, 1), (2, 2)\}\}\).

**Problem 11.40.** Find \(\text{Perm}([1, 2, 3])\).

**Problem 11.41.** Which of the following are permutations of the set of integers?

(1) \(f(x) = x + 1\)
(2) \(f(x) = x - 1\)
(3) \(f(x) = x^2\)
(4) \(f(x) = -x\)
(5) \(f(x) = x, \text{ if } x \text{ is odd, or } f(x) = x + 2, \text{ if } x \text{ is even.}\)

For permutations of a finite set \(\{1, 2, 3, \ldots, k\}\) there is a special notation for permutations called cycle notation. Each number is followed by the number it maps to, and a parenthesis is used to indicate when the cycle stops. Any sequence within a parenthesis is called a cycle. If an element maps \(k\) to itself under a permutation, we omit it from the notation, or write simply \((k)\).

**Example 11.42.** \((123)(4)\) means the permutation that maps 1 to 2, 2 to 3 and 3 to 1, and 4 to itself. We also write this permutation simply as \((123)\). \((12)(34)\) means the permutation that switches 1 with 2 and 3 with 4. The permutation that maps each element to itself is \((1)(2)(3)(4)\).

Composition of permutations defines an operation \(\circ\) on \(\text{Perm}(S)\). Indeed, if \(f\) and \(g\) are permutations then \(f \circ g\) are bijections from \(S\) to itself. By Problem 11.19, so is \(f \circ g\). Hence \(f \circ g\) is a permutation of \(S\).

![Figure 17. The permutation (1236)(45)](image_url)

**Problem 11.43.** Find the composition of the following permutations of \(\{1, 2, 3, 4\}\).

(1) \((12) \circ (12)\).
(2) \((12) \circ (23)\).
(3) \((12) \circ (34)\).
(4) \((12)(34) \circ (34)\).
(5) \((123) \circ (123) \circ (123)\).

Answer to (b): 1 maps to 2 under the first, then to 3 under the second. 3 maps to 3 under the first and then 2 under the second. 2 maps to 1.
Suppose the places in a deck of cards are numbered from 1 to 52. Find the permutation corresponding to a perfect shuffle (alternating between two halves of the deck).

Problem 11.45. Find all commutative operations on the set \{1, 2\} with \(f(1, 2) = 1\).

Answer: Since \(f\) is commutative \(f(1, 2) = f(2, 1) = 1\) while \(f(2, 2)\) can be either 1 or 2. So the possibilities are \{((1, 1), 1), ((1, 2), 1), ((2, 1), 1), ((2, 2), 1)\} and \{((1, 1), 1), ((1, 2), 1), ((2, 1), 1), ((2, 2), 2)\}.

Problem 11.46. Consider the operation defined by \(f(x, y) = xy + 3\). Show that \(f\) is commutative but not associative.

Here is the proof of commutativity:

1. \(\forall f, f\) is commutative iff \(\forall x, y, f(x, y) = f(y, x)\) def commutative
2. \(f(x, y) = xy + 3\) def \(f\)
3. \(f\) is commutative iff \(\forall x, y, xy + 3 = yx + 3\) sub 2 in 1
4. \(xy = yx\) commutative of mult
5. \(xy + 3 = yx + 3\) add 3 to 4
6. \(\forall x, y, xy + 3 = yx + 3\) univ gen on 5
7. \(f\) is commutative inf on 6,3

Problem 11.47. Find an operation that is associative but not commutative.

12. Equivalence relations and partitions

An equivalence relation is a particular kind of relation which expresses similarity between objects. An example of an equivalence relation is the notion of similarity in geometry, where two figures are congruent if one can be transformed to the other by a rigid motion and a dilation.

12.1. Equivalence relations. In the previous section, we studied functions, which are a very special kind of relation. In this section, we study another special kind, called equivalence relations. A typical example is the relation on the set of people defined by \(xRy\) iff \(x\) is blood related to \(y\).

Definition 12.1. A relation \(R \subset A \times A\) is

1. transitive iff \(\forall a, b, c \in A, aRb \land bRc \implies aRc\)
2. symmetric iff \(\forall a, b \in A, aRb \iff bRa\)
3. reflexive iff \(\forall a \in A, aRa\).

These properties only make sense when \(R\) is a relation from a set \(A\) to itself. For example, if \(R\) is the blood relation on people, then \(R\) is transitive (if you are related to him and he is related to her, then you are related to her), symmetric (if he is related to her, then she is related to him), and reflexive (you are related to yourself), and so an equivalence relation. If \(R\) is the relation \(xRy\) iff \(y\) is the genetic father of \(x\), then \(R\) is not transitive, symmetric, or reflexive. If \(R\) is the relation \(xRy\) iff \(y\) is a sibling of \(x\), then \(R\) is transitive and symmetric, but probably (depending on convention) not reflexive (Would you say that you are your own brother/sister?)

In the arrow picture, a relation \(R\) is reflexive iff each point is connected to itself by a loop; symmetric if each arrow has an arrow going the other way; and transitive if for any two consecutive arrows there is an arrow going directly from the first to third point.

![Diagram showing reflexive, symmetric, and transitive relations](image)

Definition 12.2. A relation \(R\) is an equivalence relation if \(R\) is transitive, symmetric, and reflexive.

Example 12.3. The relation between people defined by \(xRy\) if \(x, y\) have the same birthday is an equivalence relation. The relation between
people defined by \( xRy \) if \( y \) is older than \( x \) is not an equivalence relation, because it is not symmetric or reflexive.

**Problem 12.4.** Which of the following are equivalence relations? In each case say which of the three properties (transitive, symmetric, reflexive) hold.

1. \( xRy \) if \( x \) is born in the same year as \( y \).
2. \( xRy \) if \( x \) has the same hair color as \( y \).
3. \( xRy \) if \( x \) is the spouse of \( y \).
4. \( xRy \) if \( x \) is taller than \( y \).

**Problem 12.5.** Determine whether the relations

1. \( \leq \)
2. \( < \)
3. \( | \)

are reflexive, symmetric, or transitive. Draw the

1. graph
2. arrow picture

of each for the numbers less than 3.

**Problem 12.6.** Consider the relation on \( A = \{1\} \) given by \( R = \{(1,1)\} \). Determine whether \( R \) is (i) reflexive, (ii) symmetric, (iii) transitive.

**Problem 12.7.** Prove that if \( R \) is transitive and symmetric and \( \text{dom}(R) = A \), then it is reflexive, hence an equivalence relation.

Define a relation on \( \mathbb{Z} \) as follows.

**Definition 12.8.** We say that \( a \) is equivalent mod \( k \) to \( b \) and write \( a \equiv_k b \) iff \( k|b-a \), that is, their difference is a multiple of \( k \).

**Example 12.9.** \( 2 \equiv_2 4 \equiv_2 6 \equiv_2 8 \ldots \) and \( 1 \equiv_2 3 \equiv_2 5 \equiv_2 7 \). \( 2 \equiv_{10} 12 \) but \( \neg(2 \equiv_9 12) \).

**Problem 12.10.** (1) Find 3 numbers equivalent to \( 2 \) mod 3.
(2) Find 3 numbers equivalent to \( 2 \) mod 10.
(3) Are all numbers equivalent mod 1?
(4) For which \( k \geq 1 \) are \( 0, 1, 2, 3 \) not equivalent mod \( k \)?

**Problem 12.11.** Show that

1. \( a \equiv_6 b \implies a \equiv_2 b \land a \equiv_3 b \).

(2) \( a \equiv_9 b \implies a \equiv_3 b \).

**Problem 12.12.** Give a proof summary that \( \equiv_k \) is an equivalence relation on \( \mathbb{Z} \).

Here is the beginning of a two-column proof:

1. \( \equiv_k \) is an equiv reln iff \( \equiv_k \) is refl, symm, and tran def equiv reln
2. \( \equiv_k \) is refl iff
   \[ \forall x \in \mathbb{Z}, x \equiv_k x \] def reflexive
3. \( x \equiv_k x \iff k|(x-x) \] def \( \equiv_k \)
4. \( x-x = 0 \)
5. \( k|0 \) easy
6. \( x \equiv_k x \)
7. \( \equiv_k \) is reflexive
   \[ \text{mp, sub 3,4,5} \]
   \[ \text{univ gen, inf on 6,2} \]

Here is the beginning of a proof summary: Let \( k \) be an integer. The relation \( \equiv_k \) is an equivalence relation iff it is reflexive, symmetry and transitive. It is reflexive iff \( \forall x \in \mathbb{Z}, x \equiv_k x \iff k|(x-x) \). Since \( x-x = 0 \) and \( k|0 \), \( \equiv_k \) is reflexive.

**Problem 12.13.** Prove that if \( R, S \) are equivalence relations on \( A \), then so is \( R \cap S \).

**Definition 12.14.** Let \( R \) be an equivalence relation on a set \( A \), and \( a \in A \). The equivalence class of \( a \) is the set of \( b \in A \) equivalent to \( a \), and denoted \( \overline{a} \). Formally,
\[ \overline{a} = \{ b \in A, bRa \} \]

**Example 12.15.** In the equivalence relation shown in arrow form in Figure 19, there are two equivalence classes of size one, two of size two, and two of size three.

**Example 12.16.** Suppose that \( R \) is the relation on people given by \( xRy \) iff \( x \) is related by blood to \( y \). The equivalence class of \( x \) is the set \( \overline{x} \) of (blood) relations, that is, the family (by blood) of \( x \).

**Example 12.17.** Suppose that \( R \) is the relation on people given by \( xRy \) iff \( x \) has the same birthday as \( y \). The equivalence class of \( x \) is the set \( \overline{x} \) of people with the same birthday as \( x \).

Hint: one of the equivalence classes \( \{10, 15\} \). There are two more.
**Example 12.18.** Prove that \( a \cap b \neq \emptyset \implies a \sim b \).

1. \( R \) is an equiv relation \quad \text{hyp}
2. \( R \) is ref, symm, and trans \quad \text{def equiv reln}
3. \( \forall a, aRa \land \forall b, aRb \Rightarrow bRa \)
   \( \land \forall c, bRc \Rightarrow cRb \) \quad \text{def ref, symm, trans}
4. \( a \cap b \neq \emptyset \) \quad \text{hyp}
5. \( \neg (a \cap b = \emptyset) \) \quad \text{def} \neq
6. \( \neg (\neg \exists x, x \in a \cap b) \) \quad \text{two wrongs make a right in 6}
7. \( \exists x, x \in a \cap b \) \quad \text{exist inst, def intersection on line 7}
8. \( x \in a \land x \in b \) \quad \text{def } a, b, \text{ line 8}
9. \( xRa \land xRb \) \quad \text{def } a, \overline{b}, \text{ line 8}
10. \( aRx \land xRb \) \quad \text{using line 9, symmetry from 3}
11. \( aRb \) \quad \text{using line 10, transitivity from 3}

**Problem 12.19.** Give a (a) formal proof and (b) proof summary that \( a \equiv b \) \iff \( a \sim b \).

The problem can be translated, in the case that \( R \) means blood relation, as saying that two people have the same families (by blood) if and only if they are related (by blood).

---

**Definition 12.20.** Let \( A \) be a set. A partition of \( A \) is a set \( S \) of subsets \( S \subseteq A \) such that each element of \( A \) occurs in exactly one element \( S \) of \( S \). That is,

1. Any two elements of \( S \) are disjoint or equal: \( S_1, S_2 \in S \iff S_1 = S_2 \lor S_1 \cap S_2 = \emptyset \). (This is another way of saying that each element appears in at most one subset in the partition.)
2. The union of the elements of \( S \) is \( A \), that is,

\[
\bigcup_{S \in S} S = A
\]

. (This is another way of saying that each element appears in at least one subset of the partition.)
For example, a partition of $A = \{a, b, c, d, e\}$ is $\{\{a, b, e\}, \{c, d\}\}$. Another example is $\{\{a\}, \{b\}, \{c\}, \{d\}, \{e\}\}$. The set $\{\{a, c\}, \{b, c\}, \{d, e\}\}$ is not a partition, because $c$ occurs twice. $\{\{a, c\}, \{b, d\}\}$ is not a partition of $A$ because $e$ does not occur at all. $\{\{1\}, \{2, 3\}, \{4\}\}$ is a partition of $\{1, 2, 3, 4\}$, while $\{\{ \text{Cheney, Biden} \}, \{ \text{Bush, Obama} \}\}$ is a partition of $\{ \text{Cheney, Biden, Bush, Obama} \}$ (into the subsets of vice-presidents and presidents).

The notation $\bigcup_{S \in \mathcal{S}} S$ means the union of elements of $\mathcal{S}$. It is similar to the sum or product notation.

Example 12.21.

\[
\bigcup_{S \in \{\{1\}, \{2, 3\}, \{4\}\}} S = \{1\} \cup \{2, 3\} \cup \{4\} = \{1, 2, 3, 4\}.
\]

If $T = \{3, 4, 5\}$ then

\[
\bigcup_{S \in \{\{1\}, \{2, 3\}, \{4\}\}} T - S = \{3, 4, 5\} \cup \{4, 5\} \cup \{3, 5\} = \{3, 4, 5\}.
\]

Problem 12.22. List all partitions of

1. $\{1\}$
2. $\{1, 2\}$
3. $\{1, 2, 3\}$

Problem 12.23. Show that if $R$ is an equivalence relation, then the set $S$ of equivalence classes of $R$ is a partition of $S$.

Here is a proof summary. Suppose that $R$ is an equivalence relation, and that $S$ is the set of equivalence classes. We claim that $S$ is an partition. We must first show that any two equivalence classes $\overline{a}, \overline{b}$ are equal or have empty intersection. Suppose their intersection is not empty. Then there exists an element $c$ with $c \in \overline{a} \cap \overline{b}$. Hence $c \in \overline{a}$ and $c \in \overline{b}$, and so $cRa$ and $cRb$. By transitivity, $aRb$, which implies $\overline{a} = \overline{b}$. Hence, the intersection $\overline{a} \cap \overline{b}$ is empty, or $\overline{a} = \overline{b}$. Next we must show that the union of the equivalence classes is all of $A$. Now, an element $a$ lies in the union of equivalence classes, if and only if it lies in some equivalence class. But $aRa$ by reflexivity, hence $a \in \overline{a}$, hence $a$ lies in the union of equivalence classes. By universal generalization, any $a \in A$ lies in the union of equivalence classes, hence $A$ is contained in the union of equivalence classes. Conversely, any element of an equivalence class is contained in $A$, so the union of equivalence classes is also contained in $A$. Hence, $A$ is equal to the union of equivalence classes.

As you might guess, this is a little long to write out in two-column format. Conversely, suppose we are given a set $\mathcal{S}$ of subsets of $A$. Define a relation $R$ form $S$ to $S$ by $aRb$ if $\exists S \in \mathcal{S}, a \in S \land b \in S$.

Answer to (1a): $R = \{(1, 1), (1, 3), (3, 3), (3, 1), (2, 2), (2, 5), (5, 2), (5, 5)\}$.

Problem 12.24. If $S$ is a partition of $A$, then the relation defined $R$ def by $aRb$ if $\exists S \in \mathcal{S}, a \in S \land b \in S$ is an equivalence relation.

Here is the start of a formal proof.

1. $S$ is a partition of $A$.
2. $\forall a, b, aRb \iff \exists S \in \mathcal{S}, a \in S \land b \in S$ \quad \text{hyp}
3. $R$ is an equiv reln iff $R$ is refl, symm, and tran \quad \text{def equiv reln}
4. $R$ is refl iff $\forall a \in A, aRa$ \quad \text{def reflexive}
5. $a \in A$ \quad \text{hyp}
6. $\exists S \in \mathcal{S}, a \in S$ \quad \text{def partition}
7. $\exists S \in \mathcal{S}, a \in S \land b \in S$ \quad \text{exist inst,ci, exist gen on 6}
8. $\forall a \in A, aRa$ \quad \text{univ inst, mp, univ gen on 2,7}
9. $R$ is reflexive \quad \text{inf on 4,8}

The previous two problems show the following:

Theorem 12.25. There is a one-to-one correspondence between equivalence relations on a set $A$ and partitions of $A$.

Problem 12.26. Suppose that $A = \{1, 2, 3, 4, 5\}$. Write the relation $R$ for each of the following sets of subsets $\mathcal{S}$ in (a) roster form and (b) arrow form.

1. $S = \{\{1, 3\}, \{2, 5\}\}$.
2. $S = \{\{1, 2, 3\}, \{2, 4, 5\}\}$.
3. $S = \{\{1, 2, 3\}, \{4, 5\}\}$.

Definition 12.27. Let $R$ be an equivalence relation on a set $A$. The quotient set $A/R$ is the corresponding partition, that is, the set of equivalence classes of $R$.

For example, if $R$ is the informal relation related to on the set $A$ of all people, then the quotient $A/R$ is the set of families.

12.3. Cardinality. We say that $S$ and $T$ have the same cardinality and write $S \sim T$, iff there is a bijection between $S$ and $T$. We say that a set
Problem 12.28. Determine the order of the following sets.

(1) \{1, 2, 3, 4\}
(2) \{1, 3, 5, 7, 9\}
(3) \{2, 3, 5, 7, 11, 13\}
(4) \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}
(5) \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{x \neq x\}\}
(6) \{x \mid x \in \mathbb{N} \land 0 \leq x \leq 5\}
(7) \{(x, y) \mid x \in \mathbb{N} \land y \in \mathbb{N} \land x + y \leq 4\}
(8) The set of all subsets of \{1, 2, 3\}.
(9) The set of functions from \{1, 2, 3\} to \{0, 1\}.
(10) The set of relations from \{1, 2, 3\} to \{0, 1\}.
(11) The set of equivalence relations on \{1, 2, 3\}.

Theorem 12.29. A set \(S\) is finite with order \(k\), if and only if \(S\) can be written in roster form \(S = \{s_1, \ldots, s_k\}\) with \(s_1, \ldots, s_k\) distinct.

Proof: If \(F: S \to \{1, \ldots, k\}\) is a bijection, let \(s_j\) denote the inverse image of \(j\). Then \(S = \{s_1, \ldots, s_k\}\) and these are distinct. Conversely, if \(S = \{s_1, \ldots, s_k\}\) with \(s_1, \ldots, s_k\) distinct then define a function \(F: S \to \{1, \ldots, k\}\) by \(F(s_j) = j\). Then clearly \(F\) is onto and \(F\) is 1-1 since \(F(s_j) = F(s_k) \implies j = k \implies s_j = s_k\).

Problem 12.30. Prove that \(S = \{n \in \mathbb{N} \mid 2n + 1 \leq 10\}\) has order 5.

Proof: Consider the function \(F: S \to \mathbb{N}\) defined by \(F(n) = n + 1\). We claim that \(F\) is a bijection onto the set \(\{1, \ldots, 5\}\). \(F\) is 1-1: If \(F(n) = F(m)\), then \(n + 1 = m + 1\) so \(n = m\). \(F\) is onto: If \(1 \leq y \leq 5\) then \(y = F(n) = n + 1\) where \(n \leq 4\) and so \(2n + 1 \leq 10\).

Problem 12.31. Prove that the set of prime numbers less than 10 has order 4.

Problem 12.32. Prove that the relation \(\sim\) given by the existence of a bijection is an equivalence relation.

Problem 12.33. Prove that if \(A\) has the same cardinality as \(B\) and \(C\) has the same cardinality as \(D\) then

1. \(|A \times C| = |B \times D|\),
2. \(|\text{Fun}(A, C)| = |\text{Fun}(B, D)|\),
3. \(|\mathcal{P}(A)| = |\mathcal{P}(B)|\).

Problem 12.34. Prove that

1. \(|A \times B| = |A||B|\) (in particular, both are either infinite or finite.)
2. \(|A \cup B| = |A| + |B| - |A \cap B|\).
3. \(|\text{Fun}(A, B)| = |A||B|\). (this is the set of functions from \(A\) to \(B\).)
4. \(|\text{Perm}(A, A)| = |A|!\). (this is the set of permutations of \(A\), that is, bijections from \(A\) to itself)
5. \(|\mathcal{P}(A)| = 2^{|A|}\). (this is the set of subsets of \(A\).)

Proof of (i). Suppose that \(|A| = k\) and \(|B| = l\) are both finite. By definition of order, there exists a bijection from \(A\) to \(\{0, \ldots, k - 1\}\) and from \(B\) to \(\{0, \ldots, l - 1\}\). By the previous problem, \(|A \times B| = |\{0, \ldots, l - 1\} \times \{0, \ldots, k - 1\}|\). Define a function from \(\{0, \ldots, k - 1\} \times \{0, \ldots, l - 1\}\) to \(\{0, \ldots, kl - 1\}\) by \(F(x, y) = lx + y\). We claim that \(F\) is a bijection. \(F\) is onto: For any \(z \in \mathbb{N}\) with \(z \leq kl - 1\) can be written as \(lz + y\) for some \(y \in \mathbb{N}\) with \(y \leq l - 1\), by the remainder theorem. \(F\) is 1-1: If \(F(x, y) = F(x', y')\) then \(lx + y = lx' + y'\) and by the remainder theorem \(x = x'\) and \(y = y'\). Hence \(F\) is a bijection, so \(\{0, \ldots, k - 1\} \times \{0, \ldots, l - 1\}\) has cardinality \(kl\). Hence \(|A \times B| = kl\), by the previous problem. The case that \(|A|\) or \(|B|\) is infinite is left as an exercise.

Definitions for Relations and Functions

| inverse relation: \(R^{-1} = \{(b, a) \mid (a, b) \in R\}\). |
| composed relation: \(R \circ S = \{(a, c) \mid \exists b, (a, b) \in R \wedge (b, c) \in S\}\). |
| \(f: A \to B\) injective \(\iff \forall a, a' \in A\), \(f(a) = f(a') \implies a = a'\). |
| \(f: A \to B\) surjective \(\iff \forall b \in B\), \(\exists a \in A\), \(f(a) = b\). |
| \(f: A \to B\) bijective \(\iff f\) injective \& \(f\) surjective. |
| pre-image: \(f^{-1}(b) = \{a \mid f(a) = b\}\). |
| domain: \(\text{dom}(R) = \{a, \exists b, (a, b) \in R\}\). |
| range: \(\text{rng}(R) = \{b, \exists a, (a, b) \in R\}\). |
| \(R \subseteq A \times A\) is transitive iff \(\forall a, b, c \in A\), \(aRb \land bRc \implies aRc\). |
| \(R \subseteq A \times A\) is symmetric iff \(\forall a, b \in A\), \(aRb \iff bRa\). |
| \(R \subseteq A \times A\) is reflexive iff \(\forall a \in A\), \(aRa\). |
| \(R \subseteq A \times A\) is an equivalence relation iff \(R\) is reflexive, symmetric, and transitive. |
| congruence mod \(k\): \(a \equiv_k b \iff k|b - a\). |
| equivalence class: \(\bar{a} = \{b \in A, bRa\}\). |
| order: \(|S| = k \iff \exists \text{ bijection } F: S \to \{1, \ldots, k\}\). |
13. Natural numbers and induction

In this section we develop the properties of the natural numbers. In particular, we introduce a method of proving statements about the natural numbers called induction.

13.1. The induction axiom. We have already made the following assumptions on natural numbers:

**Assumption 13.1.** There exists a set \( \mathbb{N} = \{0, 1, 2, \ldots \} \) of natural numbers equipped with operations of addition
\[
\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}, \quad (n, m) \mapsto n + m.
\]
and multiplication
\[
\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}, \quad (n, m) \mapsto nm.
\]
satisfying the axioms in Assumption 15.1.

There is another axiom we will assume on the natural numbers, called induction, that allows us to prove statements about all natural numbers at once. The term induction is used in mathematics somewhat differently from common English, in which it means concluding the truth of a proposition on the basis of the truth for a collection of special cases.

**Induction Axiom, Informally:** If some property of natural numbers is such that

- (1) it’s true for \( n = k \), and
- (2) if it’s true for some number \( n \), then it’s true for the next number \( n+1 \);

then it’s true for all natural numbers \( n \geq k \).

**Induction Axiom, Formally:** Suppose that \( P(n) \) is a property of a natural number \( n \in \mathbb{N} \). If \( P(n) \) holds for \( n = k \), and \( P(n) \implies P(n+1) \), then \( P(n) \) holds for all \( n \geq k \).

A typical example of the induction axiom is the proof that \( 1+\ldots+n = n(n+1)/2 \) for all \( n \geq 1 \). (Note that you can see this geometrically by seeing the sum on the left as the number of integer pairs in a right triangle with side length \( n \); doubling the number of such pairs you get a rectangle with side lengths \( n \) and \( n+1 \), as in Figure ??). One can also see the statement is true by noting that the average of the numbers is \( (n+1)/2 \), so the sum is the number of terms times the average, or \( n(n+1)/2 \).

Here is the proof using induction:

\[
\begin{align*}
1 & \quad P(n) \iff 1 + \ldots + n = n(n+1)/2 \quad \text{hyp} \\
2 & \quad P(1) \iff 1 = 1(2)/2 \quad \text{subst in 1} \\
3 & \quad 1 = 1 \quad \text{equality axiom} \\
4 & \quad P(1) \quad \text{inf on 4,2} \\
5 & \quad P(n) \quad \text{ind hyp} \\
6 & \quad 1 + \ldots + n = n(n+1)/2 \quad \text{inf on 1,5} \\
7 & \quad 1 + \ldots + n + (n+1) = n(n+1)/2 + (n+1) \quad \text{arith on 6} \\
8 & \quad 1 + \ldots + (n+1) = (n+1)(n/2 + 1) \quad \text{distrib on 7} \\
9 & \quad 1 + \ldots + (n+1) = (n+1)(n+2)/2 \quad \text{arith on 8} \\
10 & \quad P(n+1) \quad \text{subst on 1, inf} \\
11 & \quad P(n) \implies P(n+1) \quad \text{deduc on 5-10} \\
12 & \quad \forall n \geq 1, P(n) \quad \text{induc on 4,11} \\
13 & \quad \forall n \geq 1, 1 + \ldots + n = n(n+1)/2 \quad \text{subst on 12,1}
\end{align*}
\]

Here is the proof summary: Let \( P(n) \) be the statement \( 1 + \ldots + n = n(n+1)/2 \). Then \( P(1) \iff 1 = 1(2)/2 \) which is true. Suppose \( P(n) \), so \( 1 + \ldots + n = n(n+1)/2 \). Then \( 1 + \ldots + n + (n+1) = (1 + \ldots + n) + (n+1) = n(n+1)/2 + (n+1) = n(n+1)/2 + 2(n+1)/2 = (n+2)(n+1)/2 \), which is \( P(n+1) \). Hence \( P(n) \implies P(n+1) \) for all \( n \geq 1 \). By the induction axiom, \( P(n) \) is true for all \( n \geq 1 \).

**Problem 13.2.** (From [2]) Each of the following statements is of the form \( \forall n, P(n) \), for some statement \( P(n) \). For each, write (a) the corresponding statement \( P(n) \); (b) the statement \( P(n+1) \) (c) the statement \( P(1) \).

- (1) \( 1 + 3 + 5 + \ldots + (2n-1) = n^2 \) for all \( n \geq 1 \).
- (2) \( 3 + 11 + 19 + \ldots + (8n-5) = 4n^2 - n \).
- (3) \( \forall n \in \mathbb{N}, \sum_{i=1}^n 2^i = 2^{n+1} - 2 \).
- (4) \( \forall n, x \in \mathbb{N}, x \geq 2, n \geq 0, \sum_{i=0}^n x^i = (x^{n+1} - 1)/(x - 1) \).
- (5) \( \sum_{i=1}^n i^3 = (\sum_{i=1}^n i)^2 \).

Answer to (i) : (a) \( P(n) \iff 1 + 3 + 5 + \ldots + (2n-1) = n^2 \) for all \( n \geq 1 \). (b) \( P(n+1) \iff 1 + 3 + 5 + \ldots + (2n+1) = (n+1)^2 \). (c) \( P(1) \iff 1 = 1 \).

**Example 13.3.** Show that 9 divides \( 4^n + 6n - 1 \), for all \( n \geq 1 \).
1 ∃n, P(n) ↔ 9|4^n + 6n - 1 \hspace{0.5cm} \text{temp hyp}
2 P(1) ↔ 9|4^1 + 6 - 1 ↔ 9|9 \hspace{0.5cm} \text{univ inst on 1 with n = 1}
3 P(1) \hspace{0.5cm} 9 \text{ divides 9, inf on 2}
4 P(n) \hspace{0.5cm} \text{temp hyp}
5 9|4^n + 6n - 1 \hspace{0.5cm} \text{univ inst, inf on 1,4}
6 \exists k, k = 4^n + 6n - 1 \hspace{0.5cm} \text{def divides on 5}
7 P(n + 1) ↔ 9|4^{n+1} + 6(n + 1) - 1 \hspace{0.5cm} \text{univ inst on 1}
\hspace{1cm} \rightarrow 9|4^n + 6n + 5 \hspace{0.5cm} \text{arith}
\hspace{1cm} \rightarrow 9(9k - 6n + 1) + 4 + 6n + 5 \hspace{0.5cm} \text{subst, ei from 6}
\hspace{1cm} \rightarrow 9|36k - 24n + 4 + 6n + 5 \hspace{0.5cm} \text{arith on 9}
\hspace{1cm} \rightarrow 9|36k - 18n + 9 \hspace{0.5cm} \text{arith on 10}
8 9|36k - 18n + 9 \hspace{0.5cm} \text{since 9 divides each term}
9 P(n + k) \hspace{0.5cm} \text{inf on 8, 7}
10 \forall n, P(n) \Rightarrow P(n + 1) \hspace{0.5cm} \text{deduction on 4-9, univ gen}
11 \forall n \geq 1, P(n) \hspace{0.5cm} \text{induction on 3, 10}

Problem 13.4. (From [2]) Using induction give proof summaries for the following statements:

1) 1 + 3 + 5 + \ldots + (2n - 1) = n^2 \quad \text{for all } n \geq 1.
2) 3 + 11 + 19 + \ldots + (8n - 5) = 4n^2 - n.
3) \forall n \in \mathbb{N}, \sum_{i=1}^{n} 2^i = 2^{n+1} - 2
4) \forall n, x \in \mathbb{N}, x \geq 2, n \geq 0, \sum_{i=0}^{n} x^i = (x^{n+1} - 1)/(x - 1).
5) \sum_{i=1}^{n} i^3 = (\sum_{i=1}^{n} i)^2.

Problem 13.5. Prove that

1) every natural number is even or odd.
2) for n \in \mathbb{N}, either n, n + 1 or n + 2 is divisible by 3.
3) for n \in \mathbb{N}, either n is even or n - 1 is divisible by 4 or n + 1 is divisible by 4. (Hint: use inference by cases.)

Here is a possible answer to (1). Note that again, we start out by defining P(n) so that we can use the notation.

Proof Summary: Let P(n) be the statement that n is either odd or even. Now 0 is even, so P(0). Suppose P(n), so n is either odd or even. If n is even then n + 1 is odd, and if n is odd then n + 1 even. Since n is either odd or even, so is n + 1. Hence P(n) \Rightarrow P(n + 1) for all n \geq 0. By induction, P(n) for all n \geq 0. So for natural numbers n, n is either odd or even.

Two column proof:

1 P(n) \leftrightarrow (2|n + 2|(n - 1)) \hspace{0.5cm} \text{hyp}
2 2|0 \hspace{0.5cm} \text{arith}
3 P(0) \hspace{0.5cm} \text{subst, di on 1,2}
4 P(n) \hspace{0.5cm} \text{ind hyp}
5 (2|n \vee (2|(n - 1))) \hspace{0.5cm} \text{inf on 1}
6 2|n \hspace{0.5cm} \text{temp hyp}
7 2|(n + 1) - 1 \hspace{0.5cm} \text{arith on 6}
8 2n \Rightarrow 2|((n + 1) - 1) \hspace{0.5cm} \text{deduc on 6,7}
9 2|(n - 1) \hspace{0.5cm} \text{temp hyp}
10 \exists l, 2l = n - 1 \hspace{0.5cm} \text{def |}
11 2l = n - 1 \hspace{0.5cm} \text{ei on 10}
12 2l + 2 = n + 1 \hspace{0.5cm} \text{arith on 11}
13 2l + 1 = n + 1 \hspace{0.5cm} \text{arith on 12}
14 \exists k, 2k = n + 1 \hspace{0.5cm} \text{eg on 13}
15 2|n + 1 \hspace{0.5cm} \text{def |, 14}
16 (2|n - 1) \Rightarrow (2|n + 1) \hspace{0.5cm} \text{ded on 9-15}
17 (2|n \vee 2|n - 1) \Rightarrow ((2|(n + 1) - 1) \vee 2|n + 1)) \hspace{0.5cm} \text{ic, di on 8,16}
18 (2|n + 1) - 1 \vee (2|n + 1) \hspace{0.5cm} \text{deduc on 6-17}
19 P(n + 1) \hspace{0.5cm} \text{subst on 18}
20 P(n) \Rightarrow P(n + 1) \hspace{0.5cm} \text{ded on 4-19}
21 \forall n \geq 0, P(n) \hspace{0.5cm} \text{induc on 2-20}
22 \forall n \geq 0, 2|n \vee 2|n - 1 \hspace{0.5cm} \text{sub on 1,21}

Problem 13.6. Write out the previous proof in proof summary form.

The preceding proof could have been much shorter, I just tried to write it out in the form that one usually sees in induction proofs. The following is a generalization of the fact that any number is even or odd.

Problem 13.7. Using induction prove that \forall n \geq 1 (from Lewis et al at Cornell)

1) 3|4^n - 1
2) 4|5^n - 1
3) 5|4^n - 1
4) 3|n^3 + 5n + 6
5) 2|3n^2 + 5n
6) 4|3^{2n-1} - 1.
7) 133|11^{n+1} + 12^{2n-1}.
8) n^3/3 + n^5/5 + 7n/15 is an integer.
9) 4^n + 15n - 1 is divisible by 9.
(10) \( 1 + nh \leq (1 + h)^n \).

(11) \( 1(1!) + 2(2!) + \ldots + n(n!) = (n + 1)! - 1 \).

(12) If \( n \) is odd then \( n^2 - 1 \) is divisible by 8.

(13) \( 2^n > n \).

(14) \( n! < n^n \) for \( n > 1 \).

Here is the answer to (9).

1 \( \forall n, P(n) \iff 9|4^n + 15n - 1 \) def \( P(n) \)
2 \( 4^1 + 15 - 1 = 18 \) arith
3 \( P(1) \) univ inst, inf on 1,2
4 \( P(n) \) ind hyp
5 \( 9|4^n + 15n - 1 \) from 1
6 \( P(n + 1) \iff 9|4^{n+1} + 15(n + 1) - 1 \) from 1
7 \( 4^{n+1} + 15(n + 1) - 1 = 4(4^n + 15n - 1) - 4(15n - 1) + 15(n + 1) - 1 \) arith
8 \( 4^n + 15(n + 1) - 1 = 4(4^n + 15n + 1) - 45n + 18 \) arith on 7
9 \( 9|45n + 18 \) arith
10 \( 9|4^n + 15n + 1) - 45n + 18 \) \( x|y \land x|z \implies x|y + z \)
11 \( P(n + 1) \) inf 10, 6
12 \( P(n) \implies P(n + 1) \) deduc 4-11
13 \( P(1) \land \forall n, P(n) \implies P(n + 1) \) ci, univ gen 2,12
14 \( \forall n, n \geq 1 \implies P(n) \) induc on 13

**Problem 13.8.** (From Lewis et al from Cornell and Sumner from South Carolina) Define the Fibonacci numbers \( F_n \) by \( F_{n+1} = F_n + F_{n-1} \), \( F_1 = F_2 = 1 \). Show that for all \( n \geq 1 \)

1 \( F_{3n} \) is divisible by 2.
2 \( F_{4n} \) is divisible by 3.
3 \( F_{n+1}/F_n \in (1, 2) \)
4 \( F_{n}^2 = F_{n-1}F_{n+1} + (-1)^{n+1} \).

**Problem 13.9.** Identify what is wrong with the following reasoning:
Any group of horses has the same color. Indeed, any group of 1 horse has the same color. If any group of \( n \) horses has the same color, then any group of \( n + 1 \) horses has the same color. By induction, any group of horses has the same color.

**Problem 13.10.** Given a collection of \( n \) lines in a plane such that no two lines are parallel and no more than two lines intersect in any point, into how many regions do the lines divide the plane? Justify your answer using induction.

**Problem 13.11.** How many ways are there to cover the squares of a \( 2 \times n \) board by \( n \) dominoes (that is, 2 by 1 tiles?) Justify your answer using induction.

For example, the number of ways of covering a \( 2 \times 2 \) board with 2 dominoes is two: the dominoes can go in vertically or horizontally.

An equivalent formulation of the axiom of induction is the

**Theorem 13.12.** (Well-ordering principle) any non-empty subset of \( \mathbb{N} \) has a smallest element:

\[ \forall S, S \subseteq \mathbb{N} \land S \neq \emptyset \implies \exists s \in S, \forall s' \in S, s' \geq s. \]

**Problem 13.13.** Using the well-ordering principle prove that \( \forall n \geq 1 \),

1 \( 3|4^n - 1 \)
2 \( 4|5^n - 1 \)
3 \( 5|2^{2n} - 1 \)
4 \( 3|n^3 + 5n + 6 \)
5 \( 2|3n^2 + 5n \).

Here is the answer to (a), in summary form. Suppose the statement is false, so that the set \( S \) of numbers \( n \) such that 3 does not divide \( 4^n - 1 \) is non-empty. Let \( s \) be the smallest number such that 3 does not divide \( 4^s - 1 \). Then \( s > 1 \), and so 3 does divide \( 4^{s-1} - 1 \). But \( 4^s - 1 = 4(4^{s-1}) - 1 = 4(4^{s-1} - 1) + 3 \). Since \( 4^{s-1} - 1 \) is divisible by 3, so is \( 4(4^{s-1} - 1) \) and \( 4(4^{s-1} + 3) \), which is a contradiction. Hence \( S \) is empty, which proves the statement.

### 13.2. The remainder theorem and base representation

Every integer is either even or odd. Similarly, any integers is either a multiple of three, one more than multiple of three, or two more than a multiple of three. The remainder theorem below generalizes this to multiples of an arbitrary number. The proof is via induction.

**Theorem 13.14.** (Remainder Theorem) Let \( b \) be a positive natural number. Any natural number \( n \) has a unique remainder \( r \) modulo \( b \), that is,

\[ \forall n \in \mathbb{N}, \exists !, r \in \mathbb{N}, n = bl + r \land 0 \leq r < b. \]
Example 13.15. \(5 = 2(2) + 1\) so 1 is the remainder of 5 mod 2. 111 has remainders 1 mod 10 and 11 mod 100.

The proof is somewhat long to write out in two-column format, so here it is in summary form. Fix \(k \in \mathbb{N}\) and let \(P(n)\) be the statement \(\exists l, r \in \mathbb{N}, n = kl + r \land 0 \leq r \leq k - 1.\) Then \(0 = k(0) + 0, \) so \(P(0)\) holds. Now suppose that \(P(n)\) holds, so that \(n = kl + r\) for some \(r\) between 0 and \(k - 1.\) If \(r < k - 1,\) then \(n + 1 = kl + (r + 1),\) so \(P(n + 1)\) holds. If \(r = k - 1,\) then \(n + 1 = kl + k = k(l + 1) + 0,\) so \(P(n + 1)\) holds in this case as well. By inference by cases, \(P(n + 1)\) holds, so \(P(n) \implies P(n + 1)\) by induction. Hence \(P(n)\) holds for all \(n \geq 0,\) by induction on \(n.\) To show uniqueness, suppose that \(kl + r = kl' + r'\) for some \(l, l', r, r'\) with \(r, r'\) between 0 and \(k - 1.\) Then \((l - l')k + r - r' = 0.\) Now \(|r - r'| < k\) and so \(k\) cannot divide \(r - r'\) unless \(r - r' = 0\) Hence \(r - r' = 0,\) that is, \(r = r'\) and we have \((l - l')k = 0.\) Since \(k\) is not zero, we have \(l = l'.\)

Problem 13.16. Show that for any integer \(n,\)

1. Find the remainder for 100 mod 9.
2. Find the remainder for 100 mod 11.
3. If the remainder for \(n\) is \(r\) and \(r^2 < b,\) then the remainder for \(n^2\) is \(r.\)
4. If the remainder for \(n\) is \(r\) and \(2r < b,\) then the remainder for \(2n\) is \(r.\)

Using the remainder theorem we explain the correspondence between sequences of digits and natural numbers. If we have a sequence of digits \(d_k \ldots d_1\) then the corresponding natural number (following the Hindu-Arabic system developed around 500 AD) is

\[
n = \sum_{j=0}^{k} d_j 10^j.
\]

For example, by 321, that is the sequence if digits \(d_2 = 3, d_1 = 2, d_0 = 1\) we mean the number \(310^2 + 210^1 + 1.\)

More generally, the number 10 in the above can be replaced by any positive integer \(b.\) In computer science, one often uses binary, that is, \(b = 2.\) a sequence of bits \(b_k \ldots b_0 \in \{0, 1\}\) describes the number \(b_k 2^k + \ldots + b_0.\)

Example 13.17. 1101 in base 2 is the number 13 in base 10 since

\[
1101_{\text{base}2} = 1(2)^3 + 1(2)^2 + 0(2)^1 + 1(2)^0 = 8 + 4 + 1 = 13.
\]

Let’s find the number 27 in base 2. To find it, we repeatedly apply the remainder theorem, starting with the largest power of 2 smaller than 24:

\[
27 = 1(16) + 9
\]

\[
9 = 1(8) + 1
\]

\[
1 = 0(4) + 1
\]

\[
1 = 0(2) + 1
\]

\[
1 = 1(1).
\]

The sequence 11001 is the base 2 representation of 27.

The hexadecimal system \(b = 16\) is also frequently used in computer science, with digits replaced by the symbols \(\{0, 1, 2, \ldots, 9, A, B, C, D, E, F\}\) for the numbers 0 through 15. For example, 10 in hexadecimal means \(1(16) + 0 = 16\) in decimal while \(FF\) means \(15(16) + 15 = 255.\) A byte is a pair of hexadecimals, which you might recognize from descriptions of the amount of memory in your computer.

Problem 13.18. Find the

1. (1) decimal representation of the binary number 11111
2. (2) binary representation of the binary number 100
3. (3) hexadecimal representation of the decimal number 1024
4. (4) decimal representation of the hexadecimal number 10A.

Theorem 13.19. For any base \(b,\) there is a bijection \(\rho_b\) between finite sequences of elements of \(\{0, \ldots, b - 1\}\) such that the first element is non-zero, and the positive natural numbers, defined by

\[
n_0, \ldots, n_k \mapsto \sum_{j=0}^{k} b^j n_j.
\]

Proof. Clearly 1 is in the image of a unique sequence, the sequence containing 1 as the unique element. Suppose by induction that we have shown that all positive natural numbers less than \(b^k\) are in the image of \(b,\) and each such number is the image of a unique sequence \(n_0, \ldots, n_{k-1}\). Suppose that \(x\) is at least \(b^k\) but less than \(b^{k+1}.\) By the remainder theorem, \(x = n_k b^k + r\) for some unique \(n_k \in \{1, \ldots, b - 1\}\) and remainder \(r < b^k.\) By the inductive hypothesis, \(r = \rho_b(n_0, \ldots, n_{k-1})\) for some unique sequence \(n_0, \ldots, n_{k-1},\) so \(x = \rho(n_0, \ldots, n_k)\) and the sequence \(n_0, \ldots, n_k\) is the unique sequence with this property. \(\square\)
13.3. The Peano axioms. The axioms for natural numbers we gave in Assumption 15.1 are very redundant. Peano introduced a much smaller axioms for the natural numbers \( \mathbb{N} \), the first of which is the induction axiom.

Assumption 13.20 (Peano Axioms). There is a set \( \mathbb{N} \) equipped with a successor function \( S : \mathbb{N} \rightarrow \mathbb{N}, n \mapsto n + 1 \) and a distinguished element \( 0 \in \mathbb{N} \) so that

\[
\forall n \in \mathbb{N}, S(n) \neq 0 \quad \text{(Zero is not a successor of anything)}
\]

\[
S(n) = S(n') \implies n = n' \quad \text{(Cancellation Property)}
\]

\[
(P(0) \land \forall n \in \mathbb{N}, P(n) \implies P(n + 1)) \implies \forall n \in \mathbb{N}, P(n) \quad \text{(Induction)}
\]

From this, addition, multiplication can be defined and their properties can all be deduced. Addition is defined by

\[
\forall x, x + 0 = x + x = x\quad \text{(Zero is an additive identity)}
\]

\[
S(x) + y = x + S(y) = S(x + y)\quad \text{(recursive definition)}
\]

Multiplication is defined by

\[
\forall x, x0 = 0x = 0
\]

\[
S(x)y = xy + y, xS(y) = xy + x\quad \text{(recursive definition)}
\]

Inequality is defined by \( a \leq b \iff \exists c, a + c = b \).

Problem 13.21. Using only the Peano axioms, prove that \( \forall a, b \in \mathbb{N}, a + b = b + a \).

Answer: The proof is by induction on \( b \). Let \( P(b) \iff a + b = b + a \). Then \( P(0) \iff a + 0 = 0 + a \) and \( P(1) \iff a + 1 = 1 + a \) which hold by definition of addition. Suppose that \( P(b) \) holds. Then \( a + (b + 1) = (a + b) + 1 \) by associativity, which equals \( (b + a) + 1 = b + (a + 1) = b + (1 + a) = (b + 1) + a \). This shows \( P(b + 1) \), hence \( P(b) \iff P(b + 1) \).

By induction, \( \forall b \in P(b) \), that is, \( \forall b \in \mathbb{N}, a + b = b + a \).

Problem 13.22. Write the previous proof in two-column format, using only symbols.

Problem 13.23. Using the Peano axioms, prove that

1. \( \forall a \in \mathbb{N}, 1a = a1 = a \).
2. \( \forall a, b \in \mathbb{N}, (a + b) + c = (a + b) + c \).

Using induction one can also:


Hint. Suppose that \( H_1, \ldots, H_n \vdash (S \implies T) \). Then \( H_1, \ldots, H_n, S \vdash S, S \implies T \) and so \( H_1, \ldots, H_n, S \vdash T \) by modus ponens. Conversely, suppose that \( H_1, \ldots, H_n, S \vdash T \) by a proof with lines \( R_1, \ldots, R_k = T \). Hence in particular, \( H_1, \ldots, H_n, S \vdash R_j, j \leq k \). Suppose that we have shown that \( H_1, \ldots, H_n \vdash (S \implies R_j) \) for \( j < k \). The statement \( T \) is either a hypothesis, a tautology, or follows by modus ponens from two previous statements, say \( R_i, R_i \implies T \). If \( T \) is a hypothesis, or \( T \) is a tautology, we are done. Finally, if \( T \) follows from modus ponens on \( R_i, R_i \implies T \), then \( S \implies R_i, S \implies (R_i \implies T) \) by hypothesis, and \( ((S \implies R_i) \land (S \implies (R_i \implies T))) \implies (S \implies T) \) is a tautology. By modus ponens, \( S \implies T \). Hence \( H_1, \ldots, H_n \vdash S \implies T \), by induction on the length of the proof.

Problem 13.25. Prove that for any positive integer \( c \) and integers \( a, b, ab = c \land a \neq c \land a \neq 1 \iff ab = c \land a \neq 1 \land b \neq 1 \).

Answer: Suppose that \( ab = c \) and \( a \neq c \) and \( a \neq 1 \). If \( b = 1 \) then \( a = c \) which is a contradiction, hence \( b \neq 1 \). Hence \( ab = c \) and \( a \neq 1 \) and \( b \neq 1 \). Conversely, suppose \( ab = c \) and \( a \neq 1 \) and \( b \neq 1 \). If \( a = c \) then \( cb = c \) so \( c(b - 1) = 0 \). By Assumption 15.1 (9), either \( c = 0 \) or \( b = 1 \). But \( c \neq 0 \) by assumption so \( b = 1 \), which completes the proof.

14. Integers and primes

In this section we develop properties of the integer numbers. In particular, we prove the fundamental theorem of arithmetic which states that any integer greater than one has a unique factorization into prime numbers.

14.1. Properties of the integers. The following theorem summarizes properties of the integer numbers. A proof that this theorem based on properties of the natural numbers is given at the end of the section.

Theorem 14.1. There exists a set \( \mathbb{Z} \) of integers contains the natural numbers \( \mathbb{N} \) as a subset, and equipped with operations

\[
+: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad \cdot : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}
\]

and a permutation \( - : \mathbb{Z} \rightarrow \mathbb{Z} \), with the following properties.

1. \( 0 + x = x + 0 = x \)
(2) \( x + y = y + x \)
(3) \( x + (y + z) = (x + y) + z \)
(4) \( x + z = y + z \implies x = y \)
(5) \( 0 = x + y \iff x = -y \)
(6) \( -(x + y) = (-x) + (-y) \)
(7) \( x \in \mathbb{N} \land -x \in \mathbb{N} \iff x = 0 \)
(8) \( 1x = x1 = x \)
(9) \( xy = yx \)
(10) \( x(yz) = (xy)z \)
(11) \( -(xy) = (-x)y = x(-y) \)
(12) \( 0 = xy \implies x = 0 \lor y = 0 \)
(13) \( x(y + z) = xy + xz \)
(14) \( \forall x \in \mathbb{Z}, \exists n, m \in \mathbb{N}, x = n + (-m). \)

We define subtraction as the operation
\[-: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \ (n, m) \mapsto n + (-m).\]

**Problem 14.2.** Prove that

(1) \( \forall x, y, z \in \mathbb{Z}, x - (y + z) = (x - y) - z. \)
(2) \( \forall x, y, z \in \mathbb{Z}, x(y - z) = xy - xz. \)
(3) \( \forall x, y \in \mathbb{Z}, x - y = 0 \iff x = y. \)

We define a relation \( \leq \) on the integers by \( x \leq y \iff \exists z \in \mathbb{N}, x + z = y. \)

**Problem 14.3.** Show that

(1) \( x \leq x. \)
(2) \( x \leq y \land y \leq z \implies x \leq z. \)
(3) \( x \leq y \land y \leq x \implies x = y. \)

### 14.2. Prime numbers and prime factorizations.
A natural number \( p \) is prime iff its only divisors are 1 and itself and \( p \neq 1 \). More formally, let \( \mathbb{P} \subseteq \mathbb{N} \) denote the subset of prime numbers. Then
\[ p \in \mathbb{P} \iff p \neq 1 \land \forall a \in \mathbb{N}, (a|p \implies a = 1 \lor a = p). \]
The first few prime numbers are 2, 3, 5, 7, 11, 13. Prime numbers (in particular, the difficult of factoring numbers into primes) play an important role in data encryption. Many basic questions about primes are unknown. For example, it is unknown whether there are infinitely many primes whose difference is two. (11 and 13, 17 and 19, etc.)

It is not hard to see that any number can be written as a product of primes. Recall that a way of writing a number as a product of primes is called a *prime factorization*. One can find a prime factorization by finding non-trivial divisors, and forming a tree as in the pictures below:

![Prime Factorization Trees]

**Problem 14.4.** Find the prime factorization of

(1) 12
(2) 144
(3) 30
(4) 10,000

There are several ways of writing prime factorizations. One is to order the primes in non-increasing order, e.g.

\[ 60 = (2)(2)(3)(5). \]

Another way is to use exponents:

\[ 60 = 2^235. \]

Below we will show that any natural number \( n \geq 2 \) has a unique prime factorization that is, \( n \) can be written uniquely as a product of primes \( p_1, \ldots, p_s \) with \( p_1 \leq p_2 \leq \ldots \leq p_s \), or alternatively there exists a unique finite sequence of distinct, increasing primes \( p_1, \ldots, p_k \), and positive natural numbers \( a_1, \ldots, a_k \) such that \( n = p_1^{a_1} \cdots p_k^{a_k} \).

**Problem 14.5.** Using the prime factorization you found above for 60, find the prime factorization (in exponent form) for

(1) 120
(2) 180
(3) 300
(4) 420
Problem 14.6. Suppose that the prime factorization of \( x \) is \( p_1^{r_1} \cdots p_k^{r_k} \) for some primes \( p_1, \ldots, p_k \) and exponents \( r_1, \ldots, r_k \). Find the prime factorization for
\[
\begin{align*}
(1) & \quad x^2, \\
(2) & \quad x^3, \\
(3) & \quad 2x, \text{ assuming } p_1 = 2, \\
(4) & \quad 6x, \text{ assuming } p_1 = 2, p_2 = 3.
\end{align*}
\]

Proposition 14.7. Any number greater than one has a prime factorization.

We show that the factorization is unique in Theorem 14.23.

Proof. By induction on \( n, n \geq 2 \). Let \( P(n) \) be the statement that for all \( k < n, k \) is a product of primes. Clearly 2 is prime, hence \( P(2) \).

Suppose \( P(n) \). Either \( n + 1 \) is prime, or \( n + 1 \) is not prime, in which case \( p \) has a divisor not equal to 1 or itself, call it \( a \). Since \( a|p, ab = p \) for some \( b \in \mathbb{N} \). Since \( 1 < a < p \), we must have \( 1 < b < p \) as well. Hence \( a \) and \( b \) are both products of primes, by the inductive hypothesis, and so \( p = ab \) is a product of primes as well. \( \square \)

Problem 14.8. (Euclid) Show there is no largest prime.

Here is a start to the answer: Suppose that there is a largest prime, call it \( p \). Let \( n = p! + 1 \). Then by Theorem 14.7, there exists a prime \( q \) dividing \( n \). What can you say about how large \( q \) could be?

14.3. Common divisors.

Definition 14.9. \( d \) is a common divisor of two integers \( a, b \) if \( d|a \) and \( d|b \). The greatest common divisor of \( a, b \) is denoted \( \gcd(a, b) \), that is,
\[
\gcd(a, b) = d \iff (d|a) \land (d|b) \land \forall c \in \mathbb{N}, (c|a) \land (c|b) \implies c \leq d.
\]

Two numbers \( a, b \) are relatively prime if \( \gcd(a, b) = 1 \).

\( m \) is a common multiple of two integers \( a, b \) if \( a|m \) and \( b|m \). The least common multiple is defined by
\[
\text{lcm}(a, b) = m \iff (a|m) \land (b|m) \land \forall c \in \mathbb{N}, (a|c) \land (b|c) \implies m \leq c.
\]

The existence of the least common multiple is a consequence of the well-ordering principle.

Problem 14.10. Find the gcd and lcd of the following pairs of natural numbers. (1) 24 and 15 (2) 100 and 120 (3) 60 and 122

Problem 14.11. Prove that gcd and lcd are commutative and associative.

The Euclid algorithm is an algorithm for finding the gcd, by repeatedly applying the remainder theorem. The last non-zero remainder is the gcd: Write
\[
\begin{align*}
a & = bq_1 + r_1 \\
b & = r_1q_2 + r_2 \\
r_1 & = r_2q_3 + r_3 \\
& \vdots \\
r_{k-2} & = r_{k-1}q_k + r_k, \\
r_{k-1} & = r_kq_{k+1} + 0.
\end{align*}
\]

For example,
\[
\begin{align*}
102 & = 30(4) + 12 \\
30 & = 2(12) + 6 \\
12 & = 2(6) + 0
\end{align*}
\]

Hence the greatest common divisor of 102, 30 is 6.

Theorem 14.12. (Euclid algorithm) If \( a, b \) are natural numbers with \( a > b \) and \( r_1, \ldots, r_k \) are the iterated remainders as above then \( r_k = \gcd(a, b) \).

Proof: We will first show that \( r_k \) divides \( a \) and \( b \). Indeed, \( r_k \) divides \( r_{k-1} \) and \( r_k \), by the last line. Suppose \( r_k \) divides \( r_j \) and \( r_{j-1} \). Then by the \( j \)-th line \( r_{j-1} = r_jq_{j+1} + r_{j+1} \), \( r_k \) divides \( r_{j-1} \). By induction, \( r_k \) divides all remainders, hence in particular \( r_1 \) and \( r_2 \). But then the second line implies that \( r_k \) divides \( b \) and \( r_1 \), hence by the first line \( r_k \) divides \( a \).

Suppose that \( d \) is a divisor of \( a \) and \( b \). By the first line, \( d \) divides \( r_1 \), hence by the second line \( d \) divides \( r_2 \). Continuing in this way we see that \( d \) divides \( r_k \), hence \( d \leq r_k \).

Problem 14.13. Find the greatest common divisor of
\[
\begin{align*}
(1) & \quad 1001, 300 \\
(2) & \quad 41, 103
\end{align*}
\]
(3) 120, 333

using Euclid’s algorithm.

**Definition 14.14.** An integral combination of \( a \) and \( b \) is a number of the form \( ka + lb \) for some \( k, l \in \mathbb{Z} \).

**Example 14.15.** The combinations of 36 and 20 include 20, 36, 56 = 20 + 36, -16 = 20 - 36, 16 = 36 - 20, 4 = 2(20) - 36.

**Problem 14.16.** Show that

1. If an integer \( d \) divides integers \( a \) and \( b \) then \( d \) divides any integer combination of \( a, b \).
2. If \( x \) and \( y \) are integer combinations of \( a, b \) then so is \( x + y \).

**Corollary 14.17.** For any \( a, b \in \mathbb{N} \), the number \( \gcd(a, b) \) is an integral combination of \( a \) and \( b \), that is, there exists \( k, l \in \mathbb{Z} \) such that \( \gcd(a, b) = ka + lb \). Furthermore, every positive number \( n \) such that \( n = ka + lb \) for some \( k, l \in \mathbb{Z} \) is divisible by \( \gcd(a, b) \).

**Example 14.18.** Let \( a = 20 \) and \( b = 36 \). Then integer combinations of \( a \) and \( b \) include 20, 36, 56 = 20 + 36, -16 = 20 - 36, 16 = 36 - 20, 4 = 2(20) - 36, the least of which has absolute value 4 which is the greatest common divisor. The integral combinations of \( a \) and \( b \) are exactly the multiples of 4.

Here is an informal proof. Looking at the first line of Euclid’s algorithm, we see that \( r_1 = ka + lb \) for some \( k, l \in \mathbb{Z} \). But then \( r_2 = b - r_1q_1 = -ka + (1 - q_1l)b \) is also a combination of \( a, b \). Continuing down the list, we see finally that \( r_k = \gcd(a, b) \) is combination of \( a \) and \( b \). Suppose that \( n = ka + lb \). Then \( \gcd(a, b) \) divides \( a \) and \( b \) and so \( n \) as well.

**Definition 14.19.** Two natural numbers \( a, b \) are relatively prime iff \( \gcd(a, b) = 1 \).

For example, 12 and 25 are relatively prime, while 14 and 21 are not (7 is a common divisor.)

**Problem 14.20.** Show that for any prime \( p \) and natural number \( n \), \( p \) is relatively prime to \( n \) if and only if \( p \) does not divide \( n \).

**Problem 14.21.** Show that if \( p \) is prime and \( p|ab \) then \( p|a \lor p|b \).

Here is a start of proof: Suppose that \( p|ab \), but \( p \nmid a \). Then \( \gcd(p, a) = 1 \), so there exists \( k, l \in \mathbb{N} \) such that \( kp + la = 1 \). Then \( b = kpb + lab \). We claim that \( p \) divides \( kpb + lab \)....

**14.4. Fundamental theorem of arithmetic.**

**Theorem 14.22.** If \( a_1, \ldots, a_r \) is any sequence of integers, \( p \) is prime, and \( p|a_1 \ldots a_r \), then there exists \( j \in \{1, \ldots, r\} \) such that \( p|a_j \).

**Proof:** By induction on \( r \). The theorem holds for \( r = 2 \), by Proposition 14.21. Suppose it holds for \( r \). Suppose \( p \) is prime, and \( a_1, \ldots, a_{r+1} \) are integers, and \( p|a_1 \ldots a_{r+1} \). By Proposition 14.21, either \( p|a_1 \ldots a_r \) or \( p|a_{r+1} \). If \( p|a_1 \ldots a_r \), then by the inductive hypothesis, there exists \( j \in \{1, \ldots, r\} \) such that \( p|a_j \). Hence in either case, there exists \( j \) such that \( p|a_j \).

We can now prove

**Theorem 14.23.** (Fundamental Theorem of Arithmetic) Any natural number \( n \geq 2 \) can be written uniquely as a product of primes, up to reordering.

**Proof of Theorem:** We showed that there exists a prime factorization in Theorem 14.7. To show uniqueness of the prime factorization, let \( S \subseteq \mathbb{N} \) denote the subset of numbers \( n \) such that the expression in terms of primes is not unique, that is,

\[ n = p_1 \ldots p_k = q_1 \ldots q_l. \]

for two sequences of primes \( p_1, \ldots, p_k, q_1, \ldots, q_l \) and \( q_1, \ldots, q_l \) is not a reordering of \( p_1, \ldots, p_k \). Suppose that \( n \) is the smallest element of this set, which exists by the well-ordering principle. If some \( p_i \) is equal to some \( q_j \), then we could divide both sides by \( p_i \) to obtain a smaller number with two prime factorizations, which is a contradiction. By Theorem 14.21, \( p_1 \) divides one of \( q_1, \ldots, q_l \). Since these are prime, \( p_1 \) equals some \( q_j \), which is a contradiction.

**Problem 14.24.** Show that if \( p_1, \ldots, p_r \) are primes and \( q_1, \ldots, q_s \) are primes and \( q_1 \ldots q_s \) divides \( p_1 \ldots p_r \), then for each \( i \) there exists an index \( j(i) \) such that \( q_i = p_{j(i)} \), and the indices \( j(i), i = 1, \ldots, s \) are all distinct.

**Problem 14.25.** Show that
(1) If \( n \) is a square number, then \( 3|n \) implies \( 9|n \). (A square number is one that equals \( m^2 \), for some \( m \in \mathbb{N} \).) 
(2) If \( n \) is a square number, then \( 6|n \) implies \( 4|n \). 
(3) If \( n \) is a square number, then \( 6|n \) implies \( 9|n \). 
(4) If \( 2|m^2 \) then \( 8|m^3 \).

Here is the answer to (2). First the summary: Let \( n \) be a square number. Then \( n = m^2 \) for some natural number \( y \). Suppose \( 6|n \). Then since \( 2|6 \), also \( 2|n \). Hence \( 2|m^2 \). Since \( 2 \) is prime, \( 2|m^2 \) implies \( 2|m \) or \( 2|m \). Hence \( 2|m \). But then \( 4|m^2 \) so \( 4|n \).

Here is a more formal proof.

1. \( n \) is square
2. \( \exists m \in \mathbb{Z}, n = m^2 \)
3. \( 6|n \)
4. \( 2|6 \)
5. \( 2|n \)
6. \( 2|m^2 \)
7. \( \forall p, a, b \in \mathbb{N}, p \in \mathbb{P} \land p|ab \implies p|a \lor p|b \)
8. \( 2 \in \mathbb{P} \land 2|(m)(m) \)
9. \( 2|m \lor 2|m \)
10. \( 2|m \)
11. \( \exists k, 2k = m \)
12. \( 4k^2 = m^2 \)
13. \( 4|m^2 \)
14. \( 4|n \)

If \( n \) has prime factorization \( p_1^{i_1} \cdots p_r^{i_r} \) then we call \( i_j \) the multiplicity of \( p_j \) in \( n \) and denote it \( m_{p_j}(n) \).

Example 14.26.  (1) Since \( 60 = (2^2)(3)(5) \) the multiplicity of the prime \( 2 \) in \( 60 \) is \( 2 \) while the multiplicity of \( 3 \) is \( 1 \). 
(2) Since \( 10 = 2(5) \) the multiplicity of \( 2 \) in \( 10 \) is \( 1 \). 
(3) The multiplicity of \( 2 \) in \( 600 = 10(60) \) is \( 2 + 1 = 3 \). 
(4) The multiplicity of \( 2 \) in \( 3600 = (60)(60) \) is \( 2 + 2 = 4 \).

Proposition 14.27. Let \( xy \geq 2 \) be integers and \( p \) a prime.

1. \( m_p(xy) = m_p(x) + m_p(y) \).
2. For any integer \( n \geq 1, m_p(x^n) = nm_p(x) \).
3. The multiplicity of \( p \) in \( x \) is the largest exponent of \( p \) which divides \( x \).

Proof. (a) If \( x = p_1^{a_1} \cdots p_k^{a_k} \) and \( y = p_1^{b_1} \cdots p_k^{b_k} \) then 
\[ xy = p_1^{a_1+b_1} \cdots p_k^{a_k+b_k} \]
so 
\[ m_{p_j}(xy) = a_j + b_j = m_{p_j}(x) + m_{p_j}(y) \].
(b) is similar. (c) If \( p^a \) divides \( x \) then for some \( q \) we have \( p^aq = x \) and so 
\[ m_p(p^a) + m_p(q) = a + m_p(q) = m_p(x) \]
so \( a \leq q \). By definition if \( a = m_p(x) \) then \( p^a \) does divide \( x \). So \( a \) is the largest power of \( p \) dividing \( x \). \( \square \)

A similar argument shows the following:

Theorem 14.28. Suppose \( n \) has prime factorization \( p_1^{i_1} \cdots p_r^{i_r} \). The divisors of \( d \) are precisely the numbers of the form \( p_1^{j_1} \cdots p_r^{j_r} \) where each \( j_k \) satisfies \( 0 \leq j_k \leq i_k \).

Problem 14.29. Show that if \( a \) and \( b \) are relatively prime then \( a|c \) and \( b|c \) implies \( ab|c \).

Problem 14.30. Show that if \( p^r \) appears in the prime factorization of \( a \) and \( p^q \) appears in the prime factorization of \( b \) then \( p_{\min(x,y)} \) appears in the prime factorization of \( \gcd(a, b) \) and \( p_{\max(x,y)} \) appears in the prime factorization of \( \lcm(a, b) \).

Problem 14.31. Show that if \( 10|n \) and \( 4|n \) then \( 20|n \).

Proof summary: Suppose \( 10|n \) and \( 4|n \). Since \( 5|10, 5|n \). Since \( 5 \) and \( 4 \) are relatively prime, \( 20|n \).

Problem 14.32. Show that if \( 6|n \) and \( 10|n \) then \( 30|n \).

Let’s turn to the least common multiple.

Theorem 14.33. \( \lcm(a, b) = ab/\gcd(a, b) \). Furthermore, the common multiples of \( a \) and \( b \) are the multiples of \( \lcm(a, b) \).

Proof: By the fundamental theorem of arithmetic, it suffices to show that the prime factorizations of \( a \) and \( b \) and \( \gcd(a, b) \) are equal. By Proposition 14.30, if \( p^r \) appears in \( a \) and \( p^q \) appears in \( b \) then \( p^{r+y} = p_{\max(x,y)}p_{\min(x,y)} \) appears in both \( ab \) and \( \gcd(a, b) \) which proves \( ab = \gcd(a, b)\lcm(a, b) \). If \( m_1, m_2 \) are common multiples of \( a, b \), then so is \( \gcd(m_1, m_2) \), since by Corollary 14.17 \( \gcd(m_1, m_2) \) is a combination
with integer coefficients of \( m_1, m_2 \). If \( m_1 \) is the least common multiple, it follows that \( \gcd(m_1, m_2) = m_1 \) for any other common multiple \( m_2 \), hence \( m_2 \) is a multiple of \( m_1 \).

**Problem 14.34.** Prove that for all primes \( p > 3 \),

1. \( p^2 \equiv_3 1 \) (Hint: factor. What can you say about whether 3 divides \( p - 1, p, p + 1 \)?)
2. \( p^2 \equiv_{24} 1 \). (Hint: showing \( p^2 \equiv_{12} 1 \) is not that hard, getting the extra factor of two is harder.)

**Problem 14.35.** Prove that

1. the product of any three consecutive integers is divisible by three.
2. the product of any four consecutive integers is divisible by eight.

**Problem 14.36.** The greatest common divisor is an associative operation: For any natural numbers \( a, b, c \), \( \gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c)) \).

The fundamental theorem of arithmetic states that any number greater than one is a product of prime numbers. In symbolic form, we can write that \( \text{any number greater than one has a prime factorization as} \)

\[
\forall n, n > 1 \implies \exists p_1, \ldots, p_k, n = p_1 \cdot \ldots \cdot p_k \wedge \forall j, 1 \leq j \leq k \implies p_j \in \mathbb{P}.
\]

**Problem 14.37.** Which of the following are equivalent forms of the existence part of the fundamental theorem of arithmetic?

1. Any integer is a product of prime numbers.
2. Any integer greater than one has a unique factorization as a product of prime numbers.
3. Any integer greater than one has a unique factorization as a product of powers of increasing prime numbers.

The uniqueness part of the fundamental theorem is even harder to state formally. It says that \( \text{any prime factorization is unique up to equivalence.} \) In other words, \( \text{any two prime factorizations of the same number are equivalent, or} \)

\[
\forall p_1, \ldots, p_r, q_1, \ldots, q_s, (p_1 \ldots p_r = q_1 \ldots q_s \wedge \forall i, 1 \leq i \leq r \implies p_i \text{ is prime} \wedge

\forall j, 1 \leq i \leq s \implies q_j \text{ is prime}) \implies r = s \wedge \exists n_1, \ldots, n_r, \]

\( n_1, \ldots, n_r \) is a permutation sequence \( \wedge \forall i, 1 \leq i \leq r \implies p_i = q_{n_i} \).

14.5. **Construction of the integers.** We now partially prove Theorem 14.1. The idea is that any integer \( x \) can be written as a difference \( a - b \) of natural numbers \( a, b \), although not uniquely so. Define a relation \( \sim \) on \( \mathbb{N} \times \mathbb{N} \) by \( (a, b) \sim (c, d) \iff a + d = b + c \).

**Problem 14.38.** Show that \( \sim \) is an equivalence relation.

Here is the proof that \( \sim \) is reflexive. By definition of reflexive \( \sim \) is reflexive if and only if \( (a, b) \sim (a, b) \) for all \( (a, b) \in \mathbb{N} \times \mathbb{N} \). By definition of \( \sim \), \( (a, b) \sim (a, b) \) if and only if \( a + b = a + b \), which holds by the equality axiom. Hence \( \sim \) is reflexive.

**Definition 14.39.** The set of integers \( \mathbb{Z} \) is defined as the set of equivalence classes of \( \sim \). Informally, if \( x = n - m \) then \( x \) is the equivalence class of \( (n, m) \).

**Example 14.40.** The integer \(-2\) is the equivalence class

\([-2] = \{ (3, 5), (4, 6), (5, 7), \ldots \}\)

representing all the ways of writing \(-2\) as a difference of natural numbers. The integer \(1\) is the equivalence class

\(1 = \{ (1, 0), (2, 1), (3, 2), \ldots \} \).

Addition of integers is the operation defined by

\[ \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (a, b) + (c, d) = (a + c, b + d). \]

That is, we define the sum of the sum of two integers \( x, y \) by writing \( x \) as the difference of natural numbers \( a - b \) and similarly \( y \) as the difference of natural numbers \( c - d \), and defining \( x + y \) as the difference of the natural numbers \( a + c \) and \( b + d \). What we have to check is that the definition didn’t depend on how we chose \( a, b, c, d \), in other words, the choice of representatives \( (a, b), (c, d) \) for the equivalence classes \( \overline{(a, b)}, \overline{(c, d)} \).

Often we want to define operations or functions on sets of equivalence classes by choosing representatives. If the operation or function is independent of the choice of representative, we say it is well-defined. For example, if we define a plus-one function \( f : \mathbb{Z} \to \mathbb{Z} \) by \( f((a, b)) = (a + 1, b) \), then we can check it is well-defined as follows; if \( (a, b) \sim (a', b') \) then \( a + b' = b + a' \), and so \( a + 1 + b' = b + a' + 1 \), so \( (a + 1, b) \sim (a' + 1, b') \).

**Proposition 14.41.** Addition operation on integers \( + : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \) is well-defined, that is, independent of the representative chosen.
Proof: Suppose that \((a, b)\) is equivalent to \((a', b')\), so that \(a + b' = a' + b\). Then \((a + c, b + d)\) is equivalent to \((a' + c, b' + d)\) since \(a + c + b' + d = c + d + (a + b') = c + d + (a' + b)\).

More formally, one could define a relation from \(\mathbb{Z} \times \mathbb{Z}\) to \(\mathbb{Z}\) by \((x, y) \mapsto \mathbb{Z}\) if \(\exists a, b, c, d, x = (a, b), y = (c, d), \) and \(z = (a + c, b + d)\). Then to say addition is well-defined means that this relation is actually a function, that is, there is a unique output for every input.

Multiplication of integers is the operation defined by

\[
\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (a, b)(c, d) = (ac + bd, ad + bc).
\]

Additive inverses are defined by

\[
- : \mathbb{Z} \to \mathbb{Z}, \quad (a, b) \mapsto (b, a)
\]

Finally, subtraction is defined by \(x + y = x + (-y)\)

**Problem 14.42.** Show that

1. multiplication
2. additive inverses

are well-defined, that is, independent of the representative of the equivalence class chosen.

**Problem 14.43.** Prove properties

1. (1) - (2)
2. (3) - (4)
3. (5) - (6)

of Assumption 14.1, using the definition just given of the integers.

**14.6. Modular arithmetic.** Modular arithmetic is a kind of arithmetic in which integers are replaced by their congruence classes modulo some integer. An example is clock arithmetic in which one works with integers modulo multiples of 12. For example, in clock arithmetic, 11 plus 2 is 1.

Recall that \(\equiv_k\) is the relation defined by \(x \equiv_k y \iff k|y - x\). The set of equivalence classes of \(\equiv_k\) is denoted \(\mathbb{Z}_k\). By the Remainder Theorem 13.14, any integer is equivalent to one (and only one) element of the set \(\{0, \ldots, k - 1\}\). Hence

**Corollary 14.44.** \(\mathbb{Z}_k = \{0, 1, \ldots, k - 1\}\).

When there will be no confusion, we drop the bar and write \(\mathbb{Z}_k = \{0, \ldots, k - 1\}\). Addition and multiplication induce operations

\[
+ : \mathbb{Z}_k \times \mathbb{Z}_k \to \mathbb{Z}_k, \quad a + b = a + b
\]

\[
\cdot : \mathbb{Z}_k \times \mathbb{Z}_k \to \mathbb{Z}_k, \quad a \cdot b = ab.
\]

This means that if we take any two representatives of the equivalence classes of \(a\) and \(b\), add or multiply them, and then take the corresponding equivalence class, the result is independent of which representatives we chose. In other words,

**Problem 14.45.** Show that for any \(a, a', b, b' \in \mathbb{Z}\), if \(a \equiv_k a'\) and \(b \equiv_k b'\) then \(a + b \equiv_k a' + b'\) and \(ab \equiv_k a'b'\).

When working modulo \(k\), we often drop the bar from the notation for equivalence class, the result is independent of which representatives we chose. In other words,

**Problem 14.46.** Write out the tables for addition and multiplication mod 3 are

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>\cdot</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

**Problem 14.47.** Solve the following equations in the given \(\mathbb{Z}_k\).

1. \(3x = 1\) for \(x \in \mathbb{Z}_{11}\).
2. \(3 + x = 1\) for \(x \in \mathbb{Z}_{11}\).
3. \(x^2 = 1\) in \(x \in \mathbb{Z}_8\).
4. \(x^2 + 4x + 4 = 0\) for \(x \in \mathbb{Z}_8\).

**Problem 14.48.** How many zeroes occur in the (i) addition and (ii) multiplication table for \(\mathbb{Z}_{12}\)? (Try to do this problem without writing out the multiplication table.)

Arithmetic modulo 12 is sometimes called clock arithmetic, e.g. 8 o’clock plus 6 hours is 2 o’clock.

**Problem 14.49.** Find the solution to

1. \(21x \equiv_{17} 7\).
2. \(9x \equiv_{13} 2\).

**Problem 14.50.** Show that any two inverses for an element are equal.
Problem 14.51. Find the units for the composition operation on functions.

Theorem 14.52. Consider \( \cdot_k \) as an operation on \( \mathbb{Z}_k \). The units for \( \cdot_k \) are the conjugacy classes \( \pi \) such that \( n, k \) are relatively prime.

Proof: By Corollary 14.17 to Euclid's algorithm, if \( n, k \) are relatively prime then \( an + bk = 1 \) for some \( a, b \). Hence \( \pi a = \frac{1}{a} \cdot \frac{1}{b} = 1 \) which shows that \( \pi \) is a unit. Conversely, if \( \pi \) is a unit then \( na = 1 \) for some \( a \in \mathbb{N}_+ \), in which case \( na = 1 - bk \) for some \( b \). So \( na + bk = 1 \) and \( gcd(n, a) = 1 \) by the same corollary.

Corollary 14.53. \( k \) is prime iff every non-zero element of \( \mathbb{Z}_k \) is a unit.

Problem 14.54. Show that every non-zero element of \( \mathbb{Q} \) has a multiplicative inverse.

The set of non-zero equivalence classes of \( \cong_p \) for \( p \) prime is an example of a group:

Definition 14.55. A group is a set \( G \) with an operation \( \cdot \) such that

1. \( \cdot \) is associative,
2. there exists an identity \( e \in G \),
3. every element in \( G \) has an inverse.

Example 14.56. Let \( S \) be a set. The set \( G = \text{Perm}(S) \) of permutations of \( S \), with operation given by composition \( o : G \times G \to G \), is a group. The identity is the identity permutation, \( i(s) = s \). Inverses exist because the inverse of a permutation is a permutation.

Problem 14.57. Show that \( \mathbb{Z}_n^* = \mathbb{Z}_n - \{0\} \) with modular multiplication is a group if and only if \( n \) is prime.

Problem 14.58. Show that (1) \( (\mathbb{Q}, +) \) and (2) \( (\mathbb{Q} - \{0\}, \cdot) \) are groups.

Problem 14.59. Show that if \( G \) is a group and \( x, y \in G \) then

1. \( (xy)^{-1} = y^{-1}x^{-1} \).
2. \( xy = xz \implies y = z \)

A subset \( H \) of a group \( G \) with operation \( \cdot \) is a subgroup if \( (H, \cdot) \) is itself a group. For example,

1. \( (\mathbb{Z}, +) \) is a subgroup of \( (\mathbb{Q}, +) \).

(2) \( \{1, -1\}, \cdot \) is a subgroup of \( (\mathbb{Q} - \{0\}, \cdot) \).

In other words, \( H \) is a subgroup if and only if

1. (closure under multiplication) \( \forall h_1, h_2 \in H, h_1 \cdot h_2 \in H \).
2. (closure under inverse) \( \forall h \in H, h^{-1} \in H \).

Problem 14.60. Which of the following are subgroups?

1. \( \mathbb{N} \subset \mathbb{Z} \) with addition
2. \( \{1\} \subset \mathbb{Q} - \{0\} \) with multiplication
3. \( \{(123), (321), (1)(2)(3)\} \subset \text{Perm}(\{1, 2, 3\}) \).
4. \( \{(1)(2)(3), (12), (23)\} \subset \text{Perm}(\{1, 2, 3\}) \).

15. Rational numbers

In this section we develop properties of the rational numbers. In particular, we develop techniques to show that certain polynomial equations do not have rational solutions, and that certain sets do not have least upper bounds. These deficiencies are solved using real numbers in following sections.

15.1. Properties of the rational numbers. The following theorem summarizes the properties of the rational numbers. A proof based on the previous theorem on the integers is given at the end of the section.

Theorem 15.1. There exists a set \( \mathbb{Q} \) of rational numbers, containing the integers \( \mathbb{Z} \) as a subset, and equipped with operations

\[ + : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \quad \cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} \]

a permutation \( - : \mathbb{Q} \to \mathbb{Q}, \) and a permutation \( -1 : \mathbb{Q} - \{0\} \to \mathbb{Q} - \{0\} \), with the following properties.

1. \( 0 + x = x + 0 = x \)
2. \( x + y = y + x \)
3. \( x + (y + z) = (x + y) + z \)
4. \( x + z = y + z \implies x = y \)
5. \( 0 = x + y \iff x = -y \)
6. \( 1x = x \)
7. \( xy = yx \)
8. \( x(yz) = (xy)z \)
9. \( 0 = xy \implies x = 0 \lor y = 0 \)
10. \( x(y + z) = xy + xz \).
(11) \(1 = xy \iff x = y^{-1}\)
(12) \(\forall x \in \mathbb{Q}, \exists p, q \in \mathbb{Z}, x = p/q.\)

We usually write \(1/q\) for \(q^{-1}\). For example, \(1/2\) means \(2^{-1}\).

**Proposition 15.2.**
(1) \((1/q)(1/s) = (1/q)\).
(2) \((p/q)(r/s) = pr/qs.\)
(3) \(1/(p/q) = q/p.\)
(4) \(p/q = r/s \iff ps - qr = 0.\)

**Proof.**
(1) \((1/q)(1/s)qs = (1/q)q(1/s)s = 11 = 1\) so \((1/q)(1/s) = 1/qs\) by Assumption (12). (2) \((p/q)(r/s) = p(1/q)r(1/s) = pr(1/q)(1/s) = pr/qs.\)
(3) \((p/q)(q/p) = (p/p)(q/q) = 1\) by (2), Assumption (12). (4) \(p/q = r/s \iff ps - qr = 0.\)

**Problem 15.3.** Show that \(3/6 = 1/2.\)

Answer: \(3/6 = 1/2\) iff \(3(2) = 6(1)\) by 19.2 (4), which is true.

**Theorem 15.4.** Any rational numbers has the form \(x = p/q\) for a unique pair of relatively prime integers \(p,q\).

The proof depends on the following

**Lemma 15.5.** For any integers \(a,b\), there exists unique integers \(c,d\) such that \(ad = bc\) and \(c,d\) are relatively prime.

**Proof.** To show existence, define \(c = a/gcd(a,b)\) and \(d = b/gcd(a,b)\). We claim that \(c,d\) are relatively prime. Suppose that \(e\) is a common divisor of \(c,d\). Then \(egcd(a,b)\) is a common divisor of \(a,b\), which shows that \(e\) must equal \(1.\) Hence \(c,d\) are relatively prime. To show uniqueness, suppose that \(c_1,d_1\) and \(c_2,d_2\) are two pairs of integers with this property. Then \(ad_1 = bc_1\) and \(ad_2 = bc_2\) implies \(d_1c_2 = d_2c_1.\) But then \(d_1c_2\) has the same prime factorization as \(d_2c_1.\) Any prime appearing in the prime factorization must appear in \(d_2\), and vice versa, since \(c_1,d_1\) and \(c_2,d_2\) are relatively prime. Hence \(d_1 = d_2\) and from this it follows that \(c_1 = c_2.\)

The Theorem follows from the lemma, since \(x = p/q = p'/q' \iff pq' = qp'.\)

**Problem 15.6.** (a) Show that there is no rational number such that \(q^2 = 2\), that is, prove that \(\sqrt{2}\) is irrational. (b) Prove that \(\sqrt{10}\) is irrational.

Answer: (a) Suppose otherwise, that is, that \(q \in \mathbb{Q}\) satisfies \(q^2 = 2.\) By definition of rational number, there exist integers \(a,b\) such that \(q = a/b.\) Squaring gives \(2 = a^2/b^2\) hence \(a^2 = 2b^2.\) Now the multiplicity \(m_2(a)\) of 2 (the number of times 2 appears in the prime factorization) in \(a^2\) is twice the multiplicity of 2 in \(a\) by Proposition 14.27, and so is even. On the other hand

\[ m_2(2b^2) = m_2(2) + m_2(b^2) = m_2(2) + 2m_2(b) = 2m_2(b) + 1 = 0.\]

But

\[ m_2(10b^2) = m_2(10) + m_2(b^2) = m_2((2)(5)) + 2m_2(b) = 1 + 2m_2(b)\]

is odd while

\[ m_2(a^2) = 2m_2(a)\]

is even, which is a contradiction.

**Problem 15.7.** Prove that
(1) \(\sqrt{2}/2\) is irrational.
(2) \(\sqrt{6}\) is irrational.
(3) \(\sqrt{6} + x\) is irrational.
(4) \(\sqrt{2} + \sqrt{3}\) is irrational. (Note: the sum of irrational numbers is not necessarily irrational. Instead, try squaring the given number.)

15.2. **Construction of the rational numbers.** An integer can be defined as a difference of natural numbers. Similarly, a rational number is by definition a ratio of integers. However, there are many different ways of writing a given rational number, that is, \(1/2 = 2/4 = 5/10\) etc. This means that a rational number is an equivalence class of pairs of integers. More formally, define an equivalence relation \(\sim\) on \(\mathbb{Z} \times (\mathbb{Z} - \{0\})\) by

\[(a,b) \sim (c,d) \iff ad = bc.\]

(Tsing of \((a,b)\) as \(a/b).\) Define

\[\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} - \{0\}))/\sim.\]

We write the equivalence class of \((a,b)\) as \([a,b]\). Addition is the operation defined by combining denominators,

\[\mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}, \ [a,b] + [c,d] = [ad + bc, bd].\]
Problem 15.8. Prove that addition of rational numbers is well-defined, that is \([a, b] + [c, d] = [a', b'] + [c', d']\) if \([a, b] = [a', b']\) and \([c, d] = [c', d']\).

Multiplication of rational numbers

\[Q \times Q \to Q, \quad [a, b][c, d] = [ac, bd]\]

is defined by multiplying numerators and denominators. Non-negative rational numbers are defined by \([a, b] \geq 0\) iff \(ab \geq 0\). We say \([a, b] \geq [c, d]\) iff \([a, b] - [c, d] \geq 0\).

Problem 15.9. Prove that if \(p, q\) are rational numbers and \(p < q\) then \(p < (p + q)/2 < q\).

Problem 15.10. Prove that the set of rational numbers of the form \(1/n, n \in \mathbb{N} - \{0\}\) has no smallest element.

If \([a, b]\) is non-zero, we define inverses by \([a, b]^{-1} = [b, a]\). Division of rational numbers is defined by \(p/q = pq^{-1}\).

An element \(q \in Q\) is an integer if \(q\) is equivalent to \([n, 1]\) for some \(n\). (Technically, this is a redefinition of an integers as a special kind of rational number.)

Problem 15.11. Construct an injection of \(Q\) into \(Z \times Z\).

15.3. Suprema and infima. A set \(S\) of numbers has a lower resp. upper bound if there exists a number \(l\) resp. \(u\) less resp. greater than all the numbers in \(S\), that is, \(\exists l, \forall s \in S, l \leq s\), resp. \(\exists u, \forall s \in S, s \leq u\).

Problem 15.12. Which of the following sets have upper or lower bounds? Identify a bound in each case.

1. \(S = \{1, 2, 3, 4\}\).
2. \(S = \{1, 2, 3, 4, 5, \ldots\}\).
3. \(S = \mathbb{N}\).
4. \(S = \{1, 1 + 1/2, 1 + 1/2 + 1/6, \ldots\}\).
5. \(S = \{1, 1 + 1/2, 1 + 1/2 + 1/3, 1 + 1/2 + 1/3 + 1/4, \ldots\}\).
6. \(S = \{1, 1 + 1/4, 1 + 1/4 + 1/9, 1 + 1/4 + 1/9 + 1/16, \ldots\}\).
7. \(S = \{1, 1/2, 1/3, 1/4, 1/5, 1/6, \ldots\}\).
8. \(S = \{1, -1/2, 1/3, -1/4, 1/5, -1/6, \ldots\}\).

Definition 15.13. We say that a set \(S\) of numbers has an infimum or greatest lower bound if there exists a number, denoted inf\((S)\) such that inf\((S)\) is greater than any other lower bound, that is,

\[l = \text{inf}(S) \iff \forall s \in S, l \leq s \land \forall k \in \mathbb{R}, (\forall s \in S, k \leq s) \implies k \leq l.\]

Similarly, \(S\) has a supremum or least upper bound if there exists a number, denoted sup\((S)\), which is smaller than any other upper bound.

Problem 15.14. Which of the following sets have suprema resp. infima.

in \(Q\)?

1. \(S = \{x \in \mathbb{Q} | 1 \leq x^2 \leq 4\}\).
2. \(S = \{x \in \mathbb{Q} | x^2 \leq 2\}\).
3. \(S = \{x \in \mathbb{Q} | x^4 \geq 4\}\).

15.4. Countability. Let \(S\) be a set.

Definition 15.15. We say that \(S\) is finite if \(S\) is equivalent to \(\{1, \ldots, k\}\), countable if \(S\) is equivalent to \(\mathbb{N}\), denumerable if \(S\) is finite or countable, and uncountable otherwise.

Theorem 15.16. If \(S\) and \(T\) are equivalent sets, then \(S\) is finite resp. countable resp. denumerable resp. uncountable iff \(T\) is.

Proof: Suppose that \(S\) and \(T\) are equivalent. By definition of equivalence, there exists a bijection \(F\) from \(S\) to \(T\). Suppose that \(S\) is finite. Then there exists a bijection \(G\) from \(S\) to \(\{0, \ldots, k - 1\}\) for some \(k \in \mathbb{N}\). Since the composition of two bijections is a bijection, and the inverse of a bijection is a bijection, the composition \(F^{-1} \circ G\) is a bijection from \(T\) to \(\{0, \ldots, k - 1\}\). Hence \(T\) is finite, with the same order as \(S\).

Problem 15.17. Prove the second part of the theorem.

Theorem 15.18.

1. \(\mathbb{Z}\) is countable.
2. Any subset \(S\) of \(\mathbb{N}\) is denumerable.
3. \(\mathbb{N}^2\) is countable.
4. \(\mathbb{Z}^2\) is countable.

Informal proof of (a): the elements of \(\mathbb{Z}\) are 0, 1, -1, 2, -2, 3, -3. More formally, define a function \(F\) from \(\mathbb{Z}\) to \(\mathbb{N}\) by \(F(0) = 0, F(n) = 2(n - 1) + 1\) if \(n\) is positive, and \(F(n) = -2n\) if \(n\) is negative. Informal proof of (b): the elements of \(\mathbb{N}^2\) are \((0, 0), (1, 0), (0, 1), (2, 0), (1, 1), (0, 2), \ldots\). Informal proof: consider the picture.

Problem 15.19. Prove (3) in the above theorem.
Theorem 15.20. Let $S, T$ be denumerable sets. Then any subset of $S$ or $T$ is denumerable, $S \times T$ is denumerable, and the space $\text{Fun}(S, T)$ of functions from $S$ to $T$ is denumerable.

For the first part, suppose that $U$ is a subset of $S$, and $S$ is countable. By definition of countable, there exists a bijection $F : S \rightarrow \mathbb{N}$. The restriction of $F$ to $U$ defines an injection of $U$ into $\mathbb{N}$, so $U$ is equivalent to a subset of $\mathbb{N}$. By the theorem above, $U$ is denumerable.

The following is much more surprising than the previous statements. Even if you accept that there are “as many integers as natural numbers”, it is difficult to accept that there are the “as many rational numbers as natural numbers”, because there are infinitely many rational numbers between each natural number.

Theorem 15.21. $\mathbb{Q}$ is countable.

Proof (Cantor’s diagonal argument): Problem 15.11 gives an injection of $\mathbb{Q}$ into $\mathbb{Z}^2$, so $\mathbb{Q}$ is equivalent to a subset of $\mathbb{Z}^2$. We showed in Theorem 15.18 that $\mathbb{Z}^2$ is countable, therefore $\mathbb{Q}$ is denumerable. Therefore $\mathbb{Q}$ is finite or countable. $\mathbb{Q}$ is infinite, since it contains $\mathbb{Z}$ as a subset. Therefore $\mathbb{Q}$ is countable.

16. LIMITS OF RATIONAL SEQUENCES

In this section we discuss limits of sequences, in particular, sequences of rational numbers. These are used to introduce real numbers in the following sections.

16.1. The definition of a limit. Let $S$ be a set.

Definition 16.1. (1) An infinite sequence in $S$ is a function $f : \mathbb{N} \rightarrow S$. For example, $1, 2, 4, 8, 16, \ldots$ is a sequence of integers, while $1, 1/2, 1/3, 1/4, 1/5, \ldots$ is a sequence of rational numbers. For sequences, we often use the notation $f_n$ instead of $f(n)$ for the value of $f$ at $n$.

(2) A two-sided infinite sequence is a function $f : \mathbb{Z} \rightarrow S$, for example, $\ldots, 4, 2, 1, 1/2, 1/4, \ldots$.

(3) Suppose that $f_n, g_n$ are sequences of numbers. The sum of $f$ and $g$ is the sequence $(f + g)_n = f_n + g_n$.

(4) The product of $f$ and $g$ is the sequence $(fg)_n = f_ng_n$.

Example 16.2. The sum resp. product of $1, 2, 4, 8, \ldots$ with $1, 1/1, 1/4, \ldots$ is $2, 3, 17/4, \ldots$ resp. $1, 2, 1/8, \ldots$.

Problem 16.3. Find the sum and product of the sequences $(1) f_n = 1/n, g_n = 1/2n$ $(2) f_n = 1, g_n = n^2$.

What do we mean by a limit of a sequence? The answer is surprisingly subtle. We can all agree that if the limit of a sequence $f_n$ is $L$, then mean that $f_n$ should get “closer and closer” to $L$. But what does this exactly mean? Does the sequence $1, 1/2, 1, 1/3, 1/4, \ldots$ get closer and closer to $0$? In some sense, yes. But what we really want is that all elements of the sequence are getting closer and closer to $L$. But still this is somewhat vague ... most of us would agree that the sequence $1/4, 1/3, 1/6, 1/5, 1/8, 1/7, \ldots$ is approaching $0$, even though it goes up and down alternatively. Here is the official definition:

Definition 16.4. A number $L$ is the limit of a sequence $f_n$ iff for any interval around $L$, $f_n$ eventually stays in that interval. Equivalently

$$\lim_{n \to \infty} f_n = L \iff (\forall \epsilon \in \mathbb{Q}_+, \exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_0 \implies |f_n - L| < \epsilon).$$

Here $\mathbb{Q}_+$ denotes the set of positive rational numbers. If so, we say that $f_n$ converges to $L$.

In other words, giving a semi-infinite box of any height, we can move the box to the right enough so that the graph of the function lies within the box, see Figure 20.

Problem 16.5. Which of the following sequences have limits? In each case where the limit exists, identify the limit.

(1) $1, 1, 1, 0, 0, 0, 0, 0, \ldots$

(2) $0, 1, 2, 3, 4, \ldots$

(3) $1, 1/2, 1/3, 1/4, 1/5, \ldots$

(4) $1, -1/2, 1/3, -1/4, 1/5, \ldots$
1, −1, 1, −1, 1, −1, . . .

Problem 16.6. Prove that the sequence \( f \) given by

1. \( 1/2, 2/3, 3/4, 4/5, \ldots \)
2. \( 3/2, 4/3, 5/4, 6/5, \ldots \)
3. \( 2^{3/2}, 2^{4/3}, 2^{5/4}, 2^{6/5}, \ldots \)

has a limit, equal to 1.

Here is an answer to the first part.

1. \( \lim_{n \to \infty} f_n = 1 \iff \forall \epsilon \in \mathbb{Q}_+, \exists n_0 \in \mathbb{N}, n \geq n_0 \implies |f_n - 1| < \epsilon \)
2. \( f_n = (n - 1)/n \)
3. \( |f_n - 1| = 1/n \)
4. \( |f_n - 1| < \epsilon \iff n > 1/\epsilon \)
5. \( n > 1/\epsilon \iff |f_n - 1| < \epsilon \)
6. \( \exists n_0, n_0 > 1/\epsilon \)
7. \( \forall m \in \mathbb{N}_+, \exists n \in \mathbb{N}, n \geq m \implies |f_n - 1| < 1/m \)
8. \( \lim_{n \to \infty} f_n = 1 \)

Problem 16.7. Suppose we were to define limit as

1. \( \lim_{n \to \infty}^\text{new} f_n = L \iff (\exists n_0 \in \mathbb{N}, \forall \epsilon \in \mathbb{Q}_+, n \geq n_0 \implies |f_n - L| < \epsilon) \)
2. \( \lim_{n \to \infty}^\text{newer} f_n = L \iff (\forall \epsilon \in \mathbb{Q}_+, \exists n_0 \in \mathbb{N}, |f_n - L| < \epsilon \implies n \geq n_0) \)
3. \( \lim_{n \to \infty}^\text{newest} f_n = L \iff (\exists n_0 \in \mathbb{N}, \forall \epsilon \in \mathbb{Q}_+, |f_n - L| < \epsilon \implies n \geq n_0) \)

Which of the sequences in the Problem 16.5 converge?

16.2. Properties of Limits.

Problem 16.8. Suppose that \( f_n \) and \( g_n \) are sequences of rational numbers. Show that if \( f_n \) converges to \( L \) and \( g_n \) converges to \( M \) then

1. \( f_n + g_n \) converges to \( L + M \).
2. \( f_n g_n \) converges to \( LM \).
3. \( cf_n \) converges to \( cL \).
4. if \( M \) is non-zero then \( f_n/g_n \) converges to \( L/M \).

Answer to (1): By definition \( f_n + g_n \) converges to \( L + M \) iff for all \( \epsilon > 0 \), there exists \( n_0 \) such that if \( n \geq n_0 \) then \( |L + M - (f_n + g_n)| < \epsilon \). Suppose \( f_n \) converges to \( L \) and \( g_n \) converges to \( M \). Then there exists \( n_1 \) such that \( n \geq n_1 \implies |f_n - L| < \epsilon/2 \), and \( n_2 \) such that \( n \geq n_2 \implies |g_n - M| < \epsilon/2 \). Let \( n_0 = \max(n_1, n_2) \). Then \( n \geq n_0 \) implies \( |(L + M) - (f_n + g_n)| \leq |L - f_n| + |M - g_n| < \epsilon/2 + \epsilon/2 = \epsilon \). Hence \( f_n + g_n \) converges to \( L + M \).

Theorem 16.9. Any sequence of integers converges to \( L \in \mathbb{Z} \) if and only if it is eventually constant and equal to \( L \).

Here is the proof of the forward direction. Suppose that \( f_n \) is a convergent sequence of integers with limit \( L \). Let \( m = 2 \). By definition of convergence, there exists an \( n_0 \) such that \( |f_n - L| < 1/2 \) for all \( n \geq n_0 \). Since \( L, f_n \) are integers, \( f_n = L \) for \( n \geq n_0 \).

By the infinite summation notation \( \sum_{i=1}^{\infty} f(i) \) we mean the limit

\[
\sum_{i=1}^{\infty} f(i) = \lim_{n \to \infty} \sum_{i=1}^{n} f(n),
\]

if it exists. For example,

Theorem 16.10. If \( |x| < 1 \) then \( \sum_{i=0}^{\infty} x^i = 1/(1 - x) \).

Proof. By the geometric series identity Problem 13.4 (d),

\[
\lim_{n \to \infty} \sum_{i=1}^{n} f(n) = \lim_{n \to \infty} \frac{1 - x^{n+1}}{1 - x} = \frac{1 - \lim_{n \to \infty} x^{n+1}}{1 - x} = \frac{1}{1 - x}
\]
Finally we define convergence of functions. The definition is similar to that of convergence of sequences, but instead of requiring that the input to the function is sufficiently large we require that the input is sufficiently close to a given number.

**Definition 16.11.** Let $f$ be a function from $\mathbb{R}$ to $\mathbb{R}$. Let $a, b \in \mathbb{R}$. We say that $f(x)$ converges to $b$ as $x \to a$, and write $\lim_{x \to a} f(x) = b$ iff

\[ \forall \epsilon > 0, \exists \delta > 0, \ |a - x| < \delta \implies |b - f(x)| < \epsilon. \]

**Example 16.12.** Show that the function $f(x) = x^2$ converges to 4 as $x \to 2$.

**Answer:** By definition of limit, $f(x) = x^2$ converges to 4 as $x \to 2$ iff for any $\epsilon > 0$, there exists $\delta > 0$ such that $|x - 2| < \delta$ implies that $|x^2 - 4| < \epsilon$. Now $|x^2 - 4| = |(x + 2)(x - 2)| = |x + 2||x - 2|$. If $\delta \leq 2$ then $|x + 2| < 4$. If $\delta \leq \epsilon/4$ then $|x - 2| < \epsilon/4$. Hence if $\delta = \min(2, \epsilon/4)$ then $\delta \leq 4$ and $\delta \leq \epsilon/4$ so $|x - 2||x - 2| < 4(\epsilon/4) = \epsilon$. This shows that $\exists \delta, |x - 2| < \delta \implies |x^2 - 4| < \epsilon$, hence $\lim_{x \to 2} x^2 = 4$.

**Problem 16.13.** Show that

1. $\forall x, f(x) = c \implies \forall a, \lim_{x \to a} f(x) = c$.
2. $\forall x, f(x) = x \implies \forall a, \lim_{x \to a} f(x) = a$.
3. $\forall x, f(x) = x^2 \implies \forall a, \lim_{x \to a} f(x) = a^2$.

16.3. **Base representations of rational numbers.** Using our notion of limit we define what we mean by expressions such as decimal expressions such as $x = 3.2111 \ldots$ as well as representations in other bases. Rational numbers also have $b$-ary representations. Unfortunately, they aren’t finite or unique.

**Definition 16.14.** We say that in any base $b \in \mathbb{N}$, a rational $q$ has a base $b$ representation $n_i, i \in \mathbb{Z}$ starting at $i_0$ if

\[ q = \sum_{i \leq i_0} n_i b^i. \]

We say that the sequence $n_i$ is eventually repeating with period $p$ if there exists an $i_1 \in \mathbb{Z}$ such that $i \geq i_1 \implies n_{i+p} = n_i$.

**Example 16.15.** Find the decimal expansion of $1/6$ by long division.

\[
\begin{array}{c|cccccc}
& 1 & 6 & 6 & 6 & 6 & 6 \\
\hline
6 & 1 & 6 & 0 & 4 & 0 & 0 \\
\hline
-6 & & 6 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{array}
\]

Answer: The decimal expansion keeps repeating, so we write $0.1\overline{6}$, a bar over the 6 to indicate the repeating pattern.

**Example 16.16.** 7.5 in binary is (111.1)₂ because $7.5 = 7(1) + 5(1/10) = 1(4) + 1(2) + 1(1) + 1(1/2)$.

**Problem 16.17.** Find the decimal expansion of 9/7.

**Problem 16.18.** Prove that the $0.1\overline{6}$ is a decimal expansion of 1/6.

**Proof summary:** The decimal $0.1\overline{6}$ is an expansion of 1/6 iff

\[ \lim_{n \to \infty} \frac{1}{10} + \sum_{d=2}^{n} 6(10)^{-d} = \frac{1}{6} \]

iff $\forall n, \exists n_0, n \geq n_0$ we have

\[ |1/6 - 1/10 + \sum_{d=2}^{n} 6(10)^{-d}| < 1/n. \]

Now

\[ 6(1/6 - 1/10 + \sum_{d=2}^{n} 6(10)^{-d}) = 1 - 6/10 - \sum_{d=2}^{n} 36(10)^{-d} = 4(10^{-n-1}) \]

so

\[ 1/6 - 1/10 + \sum_{d=2}^{n} 6(10)^{-d} < 10^{-n}. \]

It follows that there exists $n_0$ so that $n \geq n_0$ implies

\[ |1/6 - 1/10 - \sum_{d=2}^{n} 6(10)^{-d}| < 1/n. \]
Hence \( .1\overline{6} \) is an expansion of \( 1/6 \).

**Theorem 16.19.** (Existence of eventually repeating decimal expansions for rational numbers) The \( b \)-ary expansion of any rational number \( p/q \) is eventually repeating, and the size of the repeating pattern is at most \( q \).

**Proof.** To find the first digit base \( n \), we write

\[
np = q q_1 + r_1.
\]

Then \( p/q = q_1/n + r_1/nq \) and \( r_1/nq < 1/n \) so \( q_1 \) is then the first digit of the expansion. Then we write

\[
nr_1 = qq_2 + r_2
\]

so \( q_2 \) is the second digit, and so on. Each remainder is between 0 and \( q - 1 \), so eventually the remainders do repeat. \( \square \)

Conversely, given an eventually-repeating decimal expansion we can find the rational number by multiplying by a power of ten and subtracting.

**Example 16.20.** Find a ratio representation of \( 0.12\overline{23} \). Ans:

\[
1000(0.12\overline{23}) = 121.23\overline{23}
\]

so

\[
(1000 - 1)0.12\overline{23} = 999.12\overline{23} = 121.11
\]

which shows that

\[
0.12\overline{23} = 121.11/999 = 12111/99900.
\]

**Example 16.21.** Find a ratio representation of \( 0.\overline{11} \) in base 2. Ans: 4 times \( 0.\overline{11} \) (since multiplying by \( 2^2 \) moves over the point by 2 places)\( 4 \times 0.\overline{11} \) minus is \( 0.\overline{11} \) is 3 times \( 0.\overline{11} = 1 \) so \( 0.\overline{11} = 1/3 \) in base 10.

One can work entirely in base 2 if one likes: then 100 times \( 0.\overline{11} \) minus is \( 0.\overline{11} \) is 11 times \( 0.\overline{11} = 1 \) so \( 0.\overline{11} = 1/11 \) in base 2. (Keep in mind 11 in base 2 is 3 in base 10.)

**Problem 16.22.** Find a decimal expansion for

1. \( 7/15 \)
2. \( 274/999 \)
3. \( 23/7 \)

**Problem 16.23.** Find a representation of \( 7/15 \) in

1. base 10
2. base 2
3. base 16.

**Problem 16.24.** Find a fractional representation for

1. \( 3.02\overline{5} \) base 10,
2. \( 10.\overline{101} \) base 2,
3. \( 5 \) base 6

17. **Real numbers**

We introduce real numbers as equivalence classes of certain sequences. We try to explain away some misconception about real numbers being infinite sequences of digits etc.

17.1. **Problems with popular conceptions of real numbers.** Most people think of a real number as an infinite sequence of digits. Unfortunately the decimal expansion of a number isn’t unique, in general. For example,

\[
9(\overline{\mathcal{J}}) = (10 - 1)(\overline{\mathcal{J}}) = 9\overline{\mathcal{J}} - \overline{\mathcal{J}} = 9(1).
\]

Dividing both sides by 9 gives \( \overline{\mathcal{J}} = 1 \). Of course, we could just define a number to be an infinite sequence of digits. But then we would have to give up one of our basic rules of arithmetic, for instance, the distributive property. The problem of multiple representations is closely related to Zeno’s paradox: Suppose a man wants to travel from point \( A \) to point \( B \). To get there, first he has to cover \( 9/10 \) of the distance. After that, he has to cover \( 9/10 \) of the remaining distance, and so on. \( (9/10 \) could be replaced here by any fraction of 1). The total distance covered by the man is

\[
.9 + .09 + .009 + \ldots = \overline{\mathcal{J}}.
\]

Does he ever reach his destination? We know from common experience that he does. That is, \( \overline{\mathcal{J}} = 1 \); this is just a way of writing 1 as an infinite sum of pieces. What about the time he takes to reach his destination? If he travels at a constant speed \( s \) and the distance is \( d \), then he takes \( .9(d/s) \) to cover the first segment, \( .09(d/s) \) to cover the second, etc. Therefore, the total time taken to cover the whole distance is \( \overline{\mathcal{J}}(d/s) = (d/s) \), as expected.
17.2. Real numbers as equivalence classes of bounded increasing sequences. One way to explain real numbers is to say that they solve the problem that some sequences of rational numbers have no limits, when they in fact should. For example, the sequence 1, 1.4, 1.41, . . . you might recognize as better and better approximations to . Now we showed that is not rational. So if we just allow the rational numbers, then the sequence 1, 1.4, 1.41, . . . has no limit. We can define a real number as a sequence of rational numbers which "converges to it", in a sense we have to make precise later. For example, is to define it as the sequence 1, 1.4, 1.41, . . . Similarly, can be defined as the sequence 3, 3.1, 3.14, 3.142, . . . . The problem then is that there are many different sequences representing a real number. For example, 3, 3.1, 3.14, . . . represents , but so does 3, 3.14, 3.1416, . . . . So a real number is an equivalence class of sequences.

One of the simplest definitions of a real number is the following.

Definition 17.1. Two sequences \( x = (x_0, x_1, \ldots) \) and \( y = (y_0, y_1, \ldots) \) are called equivalent if \( \lim_{n \to \infty} x_n - y_n = 0 \). If \( x \) is equivalent to \( y \), we write \( x \sim y \).

Lemma 17.2. The relation \( \sim \) above is an equivalence relation on the set of sequences of rational numbers.

Proof. \( \sim \) is reflexive because if \( x \) is a sequence, then \( x_n - x_n = 0 \) for all \( n \). Hence for any \( \epsilon \in \mathbb{Q}_+ \), \( x_n - x_n < \epsilon \) for all \( n \geq 0 \). Next, we show that \( \sim \) is symmetric. Suppose that \( x \sim y \). Suppose that \( \epsilon \in \mathbb{Q}_+ \). Then there exists an integer \( n_0 \) such that \( |x_n - y_n| < \epsilon \) for \( n \geq n_0 \). But then \( |y_n - x_n| < \epsilon \) for \( n \geq n_0 \) as well, so \( y \sim x \). \( \square \)

Problem 17.3. Complete the proof by showing that \( \sim \) is transitive.

Definition 17.4. A real number is an equivalence class of increasing (or at least non-decreasing) sequences of rational numbers that is bounded from above.

There is a canonical map from \( \mathbb{Q} \) to \( \mathbb{R} \) given by taking constant sequences, for example, \( 1/3 = (1/3, 1/3, 1/3, \ldots) \).

17.3. Real numbers as equivalence classes of Cauchy sequences. One problem with the above definition is that only increasing sequences are allowed. This makes it difficult to define subtraction of real numbers, since the difference between increasing sequences is not necessarily increasing.

A more sophisticated definition of a real number, which allows sequences that are possibly decreasing, is the following. It has the advantage that it works in a lot of other situations in which one would like to have limits of bounded sequences.

Definition 17.5. A sequence of rational numbers \( q_j \) is a Cauchy sequence iff \( \forall \epsilon > 0, \exists n \in \mathbb{N}_+ \) such that \( i, j \geq n \implies |q_i - q_j| < \epsilon \).

For example,

Problem 17.6. Which of the following are Cauchy sequences? Prove your answer. (The last two are hard.)

1. \( 1, 1/2, 1/3, 1/4, 1/5, \ldots \)
2. \( 1, -1, 1, -1, 1, -1, \ldots \)
3. \( 1 + 1/2, 1 + 1/2 + 1/3, \ldots \)
4. \( 1 + 1/2, 1 + 1/2 + 1/6, 1 + 1/2 + 1/6 + 1/24, \ldots \)

We say that two Cauchy sequences \( q_j, r_j \) are equivalent iff \( \forall \epsilon > 0, \exists n \in \mathbb{N}_+, i \geq n \implies |q_i - r_i| < \epsilon \).

Problem 17.7. Prove that the sequences \( 1, 1, 1, \ldots \), and \( .9, .99, .999, .9999 \) are equivalent Cauchy sequences.

Definition 17.8. A real number is an equivalence class of Cauchy sequences. We denote by \( \mathbb{R} \) the set of real numbers.

Addition and multiplication of real numbers can be defined as follows. Given two sequences \( p_j, q_j \) of rational numbers, define their sum and product to be the sequences \( p_j + q_j, p_jq_j \) respectively.

Problem 17.9. Show that if \( p \sim p' \) and \( q \sim q' \) are equivalent Cauchy sequences, then \( pq \sim p'q' \). Let \( +: \mathbb{R} \times \mathbb{R} \to \mathbb{R} \) and \( \cdot: \mathbb{R} \times \mathbb{R} \to \mathbb{R} \) be the operations defined by

\[
\overline{p} \cdot \overline{q} = \overline{pq}, \quad \overline{p + q} = \overline{p} + \overline{q}.
\]

Define involutions \( -: \mathbb{R} \to \mathbb{R} \) and \( ^{-1}: \mathbb{R} \to \mathbb{R} \) by \( -p = -\overline{p} \) and \( p^{-1} = \overline{p}^{-1} \), where \( p \) is any representative sequence of non-zero numbers.
Problem 17.10. Show that if \( p \neq 0 \) and \( p \) is a non-zero representative sequence then \( p^{-1} \) is a bounded sequence, so that \( p^{-1} \) is well-defined.

By the previous problem, these are well-defined, that is, independent of the choice of representative sequences \( p, q \) chosen.

Theorem 17.11. The operations \( +, \cdot \) on \( \mathbb{R} \) satisfy the following properties:

1. \( 0 + x = x + 0 = x \)
2. \( x + y = y + x \)
3. \( x + (y + z) = (x + y) + z \)
4. \( x + z = y + z \implies x = y \)
5. \( 0 = x + y \iff x = -y \)
6. \( 1x = x1 = x \)
7. \( xy = yx \)
8. \( x(yz) = (xy)z \)
9. \( 0 = xy \implies x = 0 \lor y = 0 \)
10. \( x(y + z) = xy + xz \).
11. \( 1 = xy \iff x = y^{-1} \)

Problem 17.12. Prove the properties 17.11.

Here is the proof of commutativity of \( + \): \( p + q = \overline{p + q} = \overline{q + p} = q + p \).

17.4. Existence of suprema and infima.

Theorem 17.13. Suppose that \( S \subset \mathbb{R} \) is bounded from above. Then there exists a supremum \( \text{sup}(S) \) for \( S \). Similarly, if \( S \) is bounded from below, then there exists an infimum.

Proof. We claim that for any \( \epsilon > 0 \), there exists \( s \in S \) and \( u \in \mathbb{R} \) such that \( u \) is an upper bound for \( S \) and \( u - s < \epsilon \). Indeed, otherwise, each upper bound \( u \) satisfies \( u - s \geq \epsilon \), so that \( u - \epsilon \) is also an upper bound. But then for each upper bound \( u \), \( u - \epsilon \) is also an upper bound, which is clearly a contradiction.

Using the claim, we prove the theorem. For each \( i \), choose \( s_i \in S \) and \( u_i \in \mathbb{R} \) so that \( u_i \) is an upper bound for \( S \) and \( u_i - s_i < 2^{-i} \). Clearly \( u_i \) and \( s_i \) are equivalent sequences, and both are Cauchy. Let \( u = \overline{u_i} \) be the equivalence class of the sequences \( u_i, s_i \). Since each \( u_i \) is an upper bound, so is \( u \), and since each \( s_i \) is less than any upper bound, \( u = \overline{s_i} \) is less than or equal to any upper bound for \( S \). Hence \( u \) is a supremum for \( S \).

\[ \square \]

Theorem 17.14. Any positive real number has two real square roots.

Proof. Let \( x \) be a positive real number, and \( S \) the set of real numbers \( y \) such that \( y^2 < x \). Clearly \( S \) contains 0, and so is non-empty. We claim that \( S \) is bounded from above: if \( x \geq 1 \), then \( y^2 \leq x^2 \) implies \( y \leq x \); otherwise, \( y^2 \leq 1 \) implies that \( y \leq 1 \). Similarly, \( S \) is bounded from below. Let \( y_+ = \text{sup}(S) \) and \( y_- = \text{inf}(S) \). We claim that \( y_+^2 = x \). If \( y_+^2 < x \), then for sufficiently small numbers \( \epsilon \), \( (y_+ + \epsilon)^2 \) is also less than \( x \), but then \( y_+ \) is not an upper bound for \( S \), which is a contradiction. Similarly if \( y_+^2 > x \) then \( (y_+ - \epsilon)^2 > x \) for sufficiently small \( \epsilon \) which implies that \( y_+ - \epsilon \) is also an upper bound, so \( y_+ \) is not a least upper bound, which is a contradiction. Hence \( y_+^2 = x \) an is a square root of \( x \).

\[ \square \]

Problem 17.15. Complete the proof by showing that \( y_- \) is also a square root of \( x \).

Problem 17.16. Show that each positive real number has exactly two square roots, which are additive inverses of each other.

Problem 17.17. Does an infimum of \( \{ y \in \mathbb{R} | y^2 + 1 < 0 \} \) exist? Why or why not?

Problem 17.18. Prove that there is a bijection between equivalence classes of increasing, bounded sequences of rationals, and equivalence classes of Cauchy sequences. That is, the two definitions of real numbers are equivalent.

17.5. Base representations of real numbers. Just as for rationals, any real number may be written as an infinite sequence of \( b \)-its for any base \( b \).

Theorem 17.19. For any base \( b \), there is a one-to-one correspondence between non-negative real numbers and infinite sequences of \( b \)-its, not containing tails of the last digit \( b - 1 \).

Here is a partial justification. Given any infinite sequence of \( b \)-its \( n_i \), there is a corresponding bounded increasing sequence given by

\[ x_j = \sum_{i \geq j} b^i n_i. \]
Conversely, suppose that \( x \) is a real number represented by a bounded increasing sequence of rational numbers \( x_j \). Then \( x_j \) has an eventually stable \( i \)-th \( b \)-it, and so defines a sequence of \( b \)-its \( n_i \).

17.6. **Cantor’s uncountability argument.** We apply base representation Theorem 17.19 to prove:

**Theorem 17.20.** The set \( \mathbb{R} \) of real numbers is uncountable.

The proof, due to Cantor, is by contradiction. Suppose that \( \{x_0, x_1, x_2, \ldots, \} \) is a complete list of real numbers, and each \( x_j \) has base 10 expansion with digits \( n_{j,k} \), that is,

\[
x_j = \sum_{k \leq k_j} 10^k n_{j,k}
\]

where \( k_j \) is the place of the leading digit in \( x_j \). Define a new sequence of digits \( n'_{k,k} \leq 0 \) by

\[
n'_k = n_{k,k} + 1 \mod 10.
\]

The corresponding real number \( x' \) is not equal to any of the \( x_k \)'s, since at least one digit is different. For example, if the real numbers are

\[
x_0 = 123.456 \\
x_1 = 5.321 \\
x_2 = .051
\]

then the first few digits of \( x' \) are \( x' = .532 \) (reading along the diagonal and adding one to each digit.) Hence \( x' \) is not in the list \( \{x_0, x_1, \ldots, \} \), which is a contradiction since we assumed the list was complete.

**Problem 17.21.** Prove that

1. the set of irrational numbers is uncountable.
2. the set of real numbers between 0 and 1 is uncountable.

**References**

