Introduction to mathematical reasoning

Chris Woodward
Rutgers University, New Brunswick

Contents

1. Acknowledgements

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 approach is one I learned from B. Kaufman, and described in the Elements of Mathematics series he coauthored [3], although ours is a somewhat less formal. In this approach, the student starts out by constructing formal proofs and about half-way through the course paragraph proofs are introduced. Many mathematicians have strong feelings against this approach; after all, the formal approach isn't really the way that we think about mathematics. On the other hand, if one admits that the main obstacle that most students have with this material is one of language, then forcing precision at the beginning makes a lot of sense. One just has to beware of spending too much time with with propositional calculus, which most students do not have problems with; the serious issues start with quantifiers. This then leaves time to practice some proofs in elementary number theory and analysis, for example, the proofs of basic facts about limits which are used in the course in analysis which usually comes next in the course sequence.

Some of the other idiosyncrasies of the notes are as follows. First, I give every rule of inference an abbreviation, but actually don't care whether they remember my system of abbreviations, as long as they can recognize the rule and use it properly. 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 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 16. Finally, a warning about my conventions: 0 is a natural number, and $(f \circ g)(x) = g(f(x))$.

2. Introduction

Here is a puzzle from the books of R. Smullyan. 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:

$$\begin{array}{lcl}
\text{A is a knight} & \Rightarrow & \text{A is telling the truth} \\
 & \Rightarrow & \text{A is a knave or B is a knave} \\
 & \Rightarrow & \text{B is a knave} \\
\text{A is a knave} & \Rightarrow & \text{A is lying} \\
 & \Rightarrow & \text{neither A nor B is a knave} \\
 & \Rightarrow & \text{A is a knight} \\
 & \Rightarrow & \text{contradiction.}
\end{array}$$

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?

$$\begin{array}{lcl}
\text{A is a knight} & \Rightarrow & \text{A is telling the truth} \\
 & \Rightarrow & \text{A is a knave or B is a knight} \\
 & \Rightarrow & \text{B is a knight} \\
\text{A is a knave} & \Rightarrow & \text{A is lying} \\
 & \Rightarrow & \text{A is a knight AND B is a knave} \\
 & \Rightarrow & \text{contradiction!}
\end{array}$$

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?

$$\begin{aligned} \text{A is a knight} &\Rightarrow \text{A is telling the truth} \\ &\Rightarrow \text{B is a knave} \\ &\Rightarrow \text{B is lying} \\ &\Rightarrow \text{A,C are not the same type} \\ &\Rightarrow \text{C is a knave} \end{aligned}$$

$$\begin{aligned} \text{A is a knave} &\Rightarrow \text{A is lying} \\ &\Rightarrow \text{B is a knight} \\ &\Rightarrow \text{B is telling the truth} \\ &\Rightarrow \text{C is a knave} \end{aligned}$$

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 2.1. (Smullyan via [3])

(1) An island has two kinds of inhabitants, knights and knaves. Knaves 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 2.2. (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!" What are B and C?
(3) Three of the island's inhabitants A, B, and C were standing together in a garden. A stranger passed by and asked A, "How many knights are there among the three of you?" 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 there is one knight among us." 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
(4) 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?
(5) 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?
(6) 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?

(7) 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?
(8) 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?
(9) 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.
What are A, B, and C?
(10) 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. Propositions and Connectives

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.

Example 3.1. The following are examples of propositions and their truth values.

Proposition	Truth Value
$2+2=4$	True
When ice melts, it turns into steam	False
Chris Woodward played for the New York Mets	True
Alexander Hamilton was a U.S. President	False

Example 3.2. The following are not propositions:

(1) She is secretary of state.
(2) $x^2 = 36$.

(3) This sentence is false.

The first two 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 sentence 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.)

FIGURE 1. He found the truth

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 speling 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.

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 3.3. (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 number.
(5) There is no largest number. There may or may not be a largest number.
(6) Intelligent life abouds 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 3.4. Which of the following are propositions? Explain. For each that is, describe the truth value and explain.

(1) Rutgers was founded in 1866 to prepare ministers for the Dutch Reformed church, and was originally called Queen's college.
(2) Its motto, Sol iustitiae et occidentem illustra (translated as "Sun of righteousness, shine upon the West also") is derived from the motto of the University of Utrecht in the Netherlands, which is Sol Iustitiae Illustra Nos.
(3) The name was changed from Queen's College to Rutgers in hope of receiving a large donation from Henry Rutgers, which the college never did.
(4) The university is willing to rename itself again for a donation of approximately 2 million, according to the Star-Ledger.

3.1. **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 3.5. 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 forms 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 3.6. 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 "have your cake" and Q is "eat it too".

Problem 3.7. 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

P	NOT P
T	F
F	T

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 is both or true. For example, Cheney is vice president or Cheney 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.

P	Q	P AND Q
T	T	T
T	F	F
F	T	F
F	F	F

Figure 3. Truth table for AND

P	Q	P OR Q
T	T	T
T	F	T
F	T	T
F	F	F

Figure 4. Truth table for OR

P	Q	P XOR Q
T	T	F
T	F	T
F	T	T
F	F	F

Figure 5. Truth table for XOR

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 *if 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 $\wedge$,$\vee$,$\neg$. For example, the propositional form P AND (NOT Q) is written P $\wedge(\neg$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 AND ((NOT Q) AND R)) is

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

Figure 6. Truth table for (P AND ((NOT Q) AND R))

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 AND ((NOT Q) OR R)).

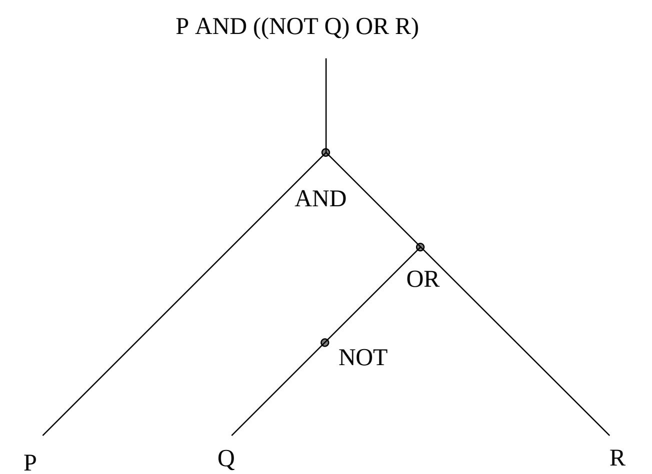


Figure 7. Tree form for (P AND ((NOT Q) OR R))

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 3.8. Find the tree form for

(1) (P AND Q) OR (NOT (R AND 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 3.9. 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 3.10. Find a propositional form for the following sentences, involving at least two symbols each.

(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 3.11. Find the truth table for the propositional forms (i) $P \Rightarrow Q$ (ii) $P \Rightarrow\ P$. (iii) $(P\wedge Q)\vee(P\wedge R)$. (iv) $(P \Rightarrow Q) \iff (\neg P\vee Q)$. (vi) $P\vee Q$ (vii) $P \iff \neg P$. (viii) $(P\wedge Q)\vee R$ (x) $(P \implies (Q\wedge R)) \implies ((P \implies Q) \wedge (P \implies R))$. Identify any tautologies or contradictions.

3.2. **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 $\implies$ Q. Its truth table is

P	Q	P $\implies$ Q
T	T	T
T	F	F
F	T	T
F	F	T

For example, $x = 2 \implies x^2 = 4$ is true, because of the *hypothesis* $x = 2$ is true then so is the *conclusion* $x^2 = 4$. But an implication is automatically true if the hypothesis if 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 $P \implies Q$ is $(\neg P) \vee Q$.

The second new connective is the *biconditional*: P IF AND ONLY IF Q or P IFF Q or P $\iff$ Q for short. It's truth table is

P	Q	P $\implies$ Q
T	T	T
T	F	F
F	T	F
F	F	T

In other words, $P \iff Q$ is true if and only if P and Q are equivalent forms.

$P \iff Q$ is equivalent to $(P \implies Q) \wedge (Q \implies P)$.

$P \implies Q$ is equivalent to $(\neg Q) \implies (\neg P)$. For example, *if it's raining, then it's cloudy* is equivalent to *if it's sunny, then it's not raining.*

Problem 3.12. 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 $P \implies Q$ is the same as $(\neg P) \implies (\neg Q)$ is called the *error of the converse*. It is the most common error among students learning to write proofs.

Problem 3.13. Write the truth tables for $Q \iff Q$, $(P \implies Q) \iff (Q \implies P)$ and $(P \iff Q) \iff (Q \iff P)$.

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, $P \vee (\neg P)$ is a tautology, while $P \wedge (\neg P)$ is a contradiction.

Problem 3.14. Which of the following are tautologies? Contradictions? Explain your answer briefly, or write out a truth table.

(1) $P \vee Q$
(2) $(P \iff Q) \implies (P \implies Q)$

(3) $P \wedge ((\neg P) \wedge Q)$.
(4) $P \implies (P \vee Q)$.
(5) $P \implies (P \wedge Q)$;.
(6) $P \implies (\neg P)$.

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 $\neg(P \wedge Q)$ is equivalent to $(\neg P) \vee (\neg Q)$. So $(\neg(P \wedge Q)) \iff ((\neg P) \vee (\neg Q))$ is a tautology.

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

Problem 3.15. (1) Guess whether $((P \wedge Q) \implies R) \iff ((P \implies R) \wedge (Q \implies R))$ 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 $(P \wedge Q) \implies R$ by changing the implies to an or and using de Morgan's law.

4. Predicates and 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

technical name	meaning	notation	other meanings
universal	for all	$\forall$	for every
existential	there exists	$\exists$	there is, there are some

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 4.1. 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) $\exists x, \forall y P(x, y)$
(7) $\forall y, \exists x, P(x, y)$

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 $\forall n, n \text{ prime} \wedge n \geq 2 \implies n$ odd. 5 is odd is an instance of that proposition.

Problem 4.2. Consider the statement $P(n, a)$, for all integers n and any prime number a: $P(n, a)$ iff 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 $5^4 - 5$.

4.1. 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) $\forall x, (P(x) \wedge Q(x)) \iff (\forall x P(x)) \wedge (\forall x, Q(x))$
(2) $\exists x, (P(x) \vee Q(x)) \iff (\exists x P(x)) \vee (\exists x, Q(x))$

There is no rule for distributing $\forall$ over $\vee$, or $\exists$ over $\wedge$.

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".

Problem 4.3. Use quantifier conversion on each of the following statements: (i) Not all math books are correct. (ii) All math books are not correct. (iii) Some math teachers don't know what they are talking about. (iv) 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. We call this rule "quantifier conversion".More formally,

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

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 4.4. (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.
(2) Every planet will be visited by some astronaut.
(3) Every astronaut will visit some planet.
(4) Some astronauts will visit every planet.

Problem 4.5. 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 4.6. 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 $\neg(P \implies \neg \exists x, R(x))$.

Problem 4.7. Find the equivalent form of $\neg(P \implies \neg \exists x, R(x))$ 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

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

Problem 4.8. 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 4.9. Translate the statements into words. (From [1].)

(1) ∀ x(R(x) ⇒ S(x)); R = "is a raindrop," S = "makes a splash."
(2) ∃ y(C(y) ⇒ M(y)); C = "is a cowboy," M = "is macho."
(3) ∃ z(D(z) ∧ W(z)); D = "is a dog," W = "whimpers."
(4) ∃ z(D(z) ∧ ¬W(z)); D = "is a dog," W = "whimpers."
(5) ∀ x(D(x) ⇒ ¬W(x)); D = "is a dog," W = "whimpers."
(6) ¬∀ x(D(x) ⇒ W(x)); D = "is a dog," W = "whimpers."
(7) ∃ z,y(C(z) ∧ C(y) ∧ W(z) ∧ ¬W(y)); C = "is a cat," W = "whimpers"
(8) ∀ x(P(x) ⇒ ∃ y(P(y) ∧ L(x,y))), P = "is a person," L(x,y) = "y is older than x."

Problem 4.10. 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) $\exists x, P(x) \wedge Q(x)$
(iii) $\forall x, P(x) \implies R(x)$
(iv) $\exists x, P(x) \wedge S(x)$.

4.2. **Quantifiers and numbers.** The *natural numbers* are $0, 1, 2, 3, \ldots$, while the integers are $\ldots, -2, -1, 0, 1, 2, \ldots$. (Some authors do not include 0 as a natural number. If you're unsure, it's best to say which convention you are using.) For the moment we assume the standard properties of additional and multiplication of natural numbers, such as

Assumption 4.11. For all natural numbers 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) $0 = x + y \implies x = 0 \wedge y = 0$
(6) $0x = x0 = 0$
(7) $xy = yx$
(8) $x(yz) = (xy)z$
(9) $0 = xy \implies x = 0 \vee y = 0$
(10) $x(y + z) = xy + xz$

Problem 4.12. Write the following mathematical statements using only symbols. Are the statements true?

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

We say a *divides* b, or is a *divisor* of b, and write $a|b$ iff $\exists c, ac = b$ and say a is a divisor of b. For example, $2|4$ but $\neg(2|5)$. The divisors of 12 are $1, 2, 3, 4, 6, 12$.

Problem 4.13. 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 number divides its square.
(4) 1 divides any number.
(5) Every number divides zero.

An answer to (2) is $2|12 \wedge 3|12$; true.

We say that a number n is *even* if $2|n$, and n is *odd* if $\exists m, n = m + 1$ and m is even. Equivalently, $n - 1$ is even. 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

$$p \neq 1 \wedge \forall d, (d|p \implies d = 1 \vee d = p).$$

Problem 4.14. Write the following mathematical statements using only symbols. Are the statements true?

(1) 5 is an odd number.
(2) Any number is even or odd.
(3) The square of an odd number is odd.

(4) 9 is a prime number.

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

Problem 4.15. (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) $\forall x, Q(x) \wedge P(x)$.
(2) $\forall x, Q(x) \implies R(x)$.
(3) $\exists x, P(x) \wedge R(x)$.

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$\wedge p \geq 3 \implies p$ 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 4.16. Find the predicate form of the statement "4 has a unique positive square root".

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

Problem 4.17. 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.

From the rest of this section, we work only with natural numbers. We say that $x \leq y$ iff $\exists z, x + z = y$, and $x < y$ iff $\exists z, x + z = y \wedge z \neq 0$. We will assume for the moment standard properties of $\leq$ for numbers x, y, z:

(1) $x \leq x$
(2) $x \leq y \wedge y \leq z \implies x \leq z$.
(3) $x \leq y \vee y \leq x$.
(4) $x \leq y \implies xz \leq yz$.
(5) $x \leq y \implies x + z \leq y + z$.

We say that x is the largest (or smallest) number with a given property if all other numbers with that property are smaller (resp. larger.) For example, n is the smallest natural number if and only if $\forall m, m \geq n$ where the universe for m is natural numbers.

Problem 4.18. Find the predicate form of "There is a largest even 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, $\exists a, 2|a \wedge \forall b, 2|b \implies b \leq a$.

Problem 4.19. 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 even number". So the predicate form is

$$\neg \exists a, 2|a \wedge \forall b, 2|b \implies b \leq a.$$

Problem 4.20. Find the predicate form of the following statements; each answer should contain at least one quantifier.

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

(6) There is no smallest prime number.

Determine which statements are true or false.

Problem 4.21. 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) $\exists x, \neg \exists y, x \leq y$.

5. Rules of inference

5.1. **Modus Ponens and a few other rules.** 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. The most common method of proof is *proof by inference* or *modus ponens*. We already used this kind of reasoning in Smullyan's puzzles: The reasoning

A is a knight. Thus he is telling the truth.

can be written out in more detail,

If A is a knight, then he is telling the truth. A is a knight. So he is telling the truth.

Using propositional variables,

$$\mathrm{P} \implies \mathrm{Q}. \ \mathrm{P}. \text{ Therefore } \mathrm{Q}.$$

P is called the *premise* or *hypothesis* and Q is the *conclusion.*

Note that both P and Q 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

$$(\mathrm{P} \wedge \mathrm{Q}) \implies (\mathrm{R} \wedge \mathrm{S}). \ \mathrm{P} \wedge \mathrm{Q}. \text{ Hence } \mathrm{R} \wedge \mathrm{S}.$$

In the case of propositional forms, we can be completely precise about what we mean by a proof:

Definition 5.1. 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) 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.

Figure 8. Any correct argument proves something

The symbol $\vdash$ translates as "then you can write down", or more formally "from this 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.

[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 $\vdash$.

Problem 5.2. Show $(P \wedge Q) \vdash P$.

1	P ∧Q	hypothesis
2	(P ∧Q) $\implies$ P	tautology
3	P	modus ponens on 1,2

Problem 5.3. Show $P, Q \vdash P \wedge Q$.

1	P	hyp (hypothesis)
2	Q	hyp
3	P $\implies$ (Q $\implies$ (P ∧Q)	taut (tautology)
4	(Q $\implies$ (P ∧Q)	mp (modus ponens) on 1,3
5	(P ∧Q)	mp on 2,4

Problem 5.4. 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:

$P \wedge Q \vdash P$ (or $P \wedge Q \vdash Q$) will be called *conjunctive simplification* (cs).

$P, Q \vdash P \wedge Q$ will be called *conjunctive inference* (ci).

$P \implies Q, Q \implies R \vdash P \implies R$ will be called *transitivity of implication* (ti).

Problem 5.5. Show $S \wedge P, P \Rightarrow Q, Q \Rightarrow R \vdash R$.

1	S ∧P	hyp
2	P	cs on 1
3	P $\implies$ Q	hyp
4	Q	mp on 2,3
5	Q $\implies$ R	hyp
6	R	mp on 4,5

Problem 5.6. Show that $P, P \Rightarrow Q \vdash P \wedge Q$.

Remark 5.7. 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 5.8. Prove the statements (using the tautologies and inference).

(1) (P ⇒ Q) ⊢ ((P ⇒ Q) ∨ (P ⇒ R)).
(2) (((P ∧ Q) ∨ (¬(P ∧ Q))) ⇒ R) ⊢ R.
(3) P, (P ⇔ Q) ⊢ Q.
(4) (((P ∧ Q) ∨ (¬(P ∧ Q))) ⇒ R) ⊢ R.
(5) P, (P ⇔ Q) ⊢ Q.
(6) ((¬(P ∧ (¬P))) ⇒ Q) ⊢ Q.
(7) P, (¬Q) ⊢ (¬(P ⇒ Q)).
(8) P, Q, R, ((P ∧ Q) ⇒ S), ((S ∧ R) ⇒ T) ⊢ T.
(9) (P ∧ Q) ⊢ Q.
(10) (P ⇒ (Q ∧ R)), (P ∧ Q) ⊢ R.
(11) (P ⇒ Q) ⊢ ((¬Q) ⇒ (¬P)).
(12) Q ⊢ (P ⇒ Q).

Problem 5.9. (From [3]) Translate the following into a proof. "If the basketball team's fast break runs well, the team will win. If the center rebounds well, the fast break will work. So if the team loses, the center did not rebound well.

5.2. **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 *mt* for short. In symbols, $P \Rightarrow Q, \neg Q \vdash \neg P$. A proof using modus ponens [2] is

1	P $\implies$ Q	hyp
2	(P $\implies$ Q) $\implies$ (¬Q $\implies$ ¬P)	taut.
3	¬Q $\implies$ ¬P	mp on 1,2
4	¬Q	hyp
5	¬P	mp on 3,4

Problem 5.10. Show $\neg P \Rightarrow Q, Q \Rightarrow R, \neg R \vdash P$.

Remark 5.11. There are many different forms of this rule. You might wonder how to justify the following reasoning:

[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*.

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	mp 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

$$\textit{disjunctive conversion } \text{(dc)}: \quad P \Rightarrow Q \vdash (\neg P) \vee Q.$$

A proof is

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

By *de Morgan's law* we mean the rule of inference $\neg(P \wedge Q) \vdash (\neg P) \vee (\neg Q)$, or vice-versa. The proof uses the tautology $(\neg(P \wedge Q)) \iff (\neg P) \vee (\neg Q)$ and modus ponens.

Inference by cases (ic): $S \Rightarrow U, T \Rightarrow U \vdash (S \vee T) \Rightarrow U$. A proof is

1	S $\implies$ U	hyp
2	T $\implies$ U	hyp
3	(($\neg$S) $\vee$U)	dc on 1
4	(($\neg$T) $\vee$U)	dc on 3
5	(($\neg$S) $\vee$U) $\wedge$(($\neg$T) $\vee$U)	ci on 3,4
6	(($\neg$S $\wedge$($\neg$T)) $\vee$U	de Morgan's on 5
7	(S $\vee$T) $\implies$ U	dc on 6

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

Problem 5.12. Show

(1) $P \implies Q, \neg P \implies Q \vdash Q$.
(2) $P \implies (Q \vee R), Q \implies S, R \implies S \vdash (P \implies S)$.
(3) $S \implies Q, ((R \implies Q) \implies (P \wedge T)), R \implies S \vdash T$.
(4) $Q \implies S, (\neg R) \implies Q, R \implies S \vdash S$.

We also find it useful to give a name to the reasoning $P \vee Q, \neg P \vdash Q$. We call it the *disjunctive alternative* (da).

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

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

Modus Ponens for the biconditional (mpb) is $P \iff Q, P \vdash Q$.

Modus Tollens for the biconditional (mtb) is $P \iff Q, \neg Q \vdash P$.

Symmetry (of the biconditional) (sbc) is $(P \iff Q) \vdash (Q \iff P)$.

Technically speaking, one should also use symmetry to justify the rules $P \vee Q \vdash Q \vee P$ and $P \wedge Q \vdash Q \wedge P$.

Problem 5.13. (From [3]) Show that

(1) (S $\Rightarrow$ Q), ((R $\Rightarrow$ Q) $\Rightarrow$ (P $\wedge$ T)), (R $\Rightarrow$ S) $\vdash$ T.
(2) (Q $\Rightarrow$ S), (($\neg$R) $\Rightarrow$ Q), (R $\Rightarrow$ S) $\vdash$ S.
(3) ((Q $\Rightarrow$ R) $\wedge$ P), ((Q $\Rightarrow$ R) $\Rightarrow$ ($\neg$T)) $\vdash$ ($\neg$T).
(4) (Q $\Rightarrow$ R), (($\neg$P) $\Rightarrow$ Q), ($\neg$R) $\vdash$ P.
(5) (($\neg$R) $\Rightarrow$ S), (S $\Rightarrow$ (P $\wedge$ Q)), (R $\Rightarrow$ T), ($\neg$T) $\vdash$ Q.
(6) (Q $\Rightarrow$ S), ($\neg$S), (R $\Rightarrow$ S) $\vdash$ (($\neg$Q) $\wedge$ ($\neg$R)).
(7) (R $\vee$ S), P, (S $\Rightarrow$ (Q $\wedge$ T)), (P $\Rightarrow$ (R $\Rightarrow$ (Q $\wedge$ T))) $\vdash$ Q.
(8) (S $\wedge$ R), (Q $\Rightarrow$ T), (R $\Rightarrow$ ($\neg$T)) $\vdash$ (($\neg$Q) $\wedge$ S).
(9) (($\neg$S) $\Rightarrow$ ($\neg$ (P $\vee$ ($\neg$T)))), (T $\Rightarrow$ (Q $\wedge$ R)), ($\neg$S) $\vdash$ (R $\wedge$ Q).
(10) (P $\Rightarrow$ Q), R, (R $\Rightarrow$ (Q $\Rightarrow$ P)) $\vdash$ (P $\iff$ Q).
(11) ($\neg$ (($\neg$P) $\wedge$ ($\neg$Q))), (S $\Rightarrow$ ($\neg$Q)), (($\neg$P) $\vee$ S) $\vdash$ (Q $\iff$ ($\neg$P)).
(12) (P $\Rightarrow$ Q), (R $\Rightarrow$ S), (Q $\Rightarrow$ R) $\vdash$ (P $\Rightarrow$ S).
(13) (P $\Rightarrow$ Q), P, (Q $\Rightarrow$ R) $\vdash$ R.
(14) (($\neg$P) $\Rightarrow$ Q), ((R $\Rightarrow$ Q) $\Rightarrow$ S), (($\neg$S) $\vee$ T), (R $\Rightarrow$ ($\neg$P)) $\vdash$ (T $\vee$ V).

Problem 5.14. 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.

Problem 5.15. (Adapted from Charles Dodgson aka Lewis Carroll) Turn there 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.

  Possible answer :

1	B $\implies$ I	hyp
2	C $\implies \neg$D	hyp
3	I $\implies$ D	hyp
4	D $\implies \neg$C	contra of 2
5	B $\implies$ D	ti on 1,3
6	B $\implies \neg$C	ti on 4,5

(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.

(3) (a) Animals, that do not kick, are always unexcitable
  (b) Donkeys have no horns
  (c) A buffalo can always toss one over a gate
  (d) No animals that kick are easy to swallow
  (e) No hornless animal can toss one over a gate
  (f) All animals are excitable, except buffalo
  (g) Therefore, donkeys are not easy to swallow.

6. Proof by deduction and contradiction

6.1. **Proof by deduction.** 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. [3]

Theorem 6.1 (Deduction Theorem)**.** *For any propositional forms $S, H_1, \dots, H_n, T$, $S, H_1, \dots, H_n \vdash T$ if and only if $H_1, \dots, H_n \vdash S \implies T$. 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 6.2. Show $S, ((S \wedge P) \implies Q) \vdash (P \implies Q)$.

1	S	hyp
2	(S $\wedge$P) $\implies$ Q	hyp
3	P	temp hyp
4	(S $\wedge$P)	ci on 1,3
5	Q	mp on 2,4
6	S, P, (S $\wedge$P) $\implies$ Q $\vdash$Q	1-5
7	S, (S $\wedge$P) $\implies$ Q $\vdash$P $\implies$ Q	ded thm on 6

Remark 6.3. 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 6.4. Prove ((¬R) ⇒ P), ((P ∧ (¬S)) ⇒ Q) ⊢ ((¬(R ∨ S)) ⇒ Q).

[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 $\vdash P \implies Q$.

[4] This means that I will repeat it over and over, not that you necessarily will.

1	$\neg(R \vee S)$	hyp
2	$\neg R \wedge \neg S$	de Morgan's 1
3	$\neg R$	cs 2
4	$\neg R \implies P$	hyp
5	P	mp 3,4
6	$P \wedge \neg S$	cs,ci 2,5
7	$(P \wedge \neg S) \implies Q$	hyp
8	Q	mp 6,7
9	$(\neg(R \vee S)) \implies Q$	deduc 1-8

Problem 6.5. Show $\vdash ((P \implies Q) \wedge (Q \implies R)) \implies (P \implies R)$.

Problem 6.6. (From [3]) Using inference by cases or the deduction theorem, show

(1) (P $\Rightarrow$ (Q $\wedge$ S)) $\vdash$ (P $\Rightarrow$ (Q $\vee$ S)).
(2) (P $\Rightarrow$ (Q $\iff$ S)), Q, (R $\Rightarrow$ (Q $\iff$ S)) $\vdash$ ((P $\vee$ R) $\Rightarrow$ S)
(3) (($\neg$Q) $\Rightarrow$ (R $\vee$ S)), (S $\iff$ (P $\vee$ R)), ($\neg$P) $\vdash$ (($\neg$R) $\Rightarrow$ Q)
(4) (P $\Rightarrow$ R), (Q $\Rightarrow$ T), ((R $\wedge$ T) $\iff$ S) $\vdash$ ((P $\wedge$ Q) $\Rightarrow$ S).
(5) (S $\Rightarrow$ P), (Q $\Rightarrow$ R), S $\vdash$ ((P $\Rightarrow$ Q) $\Rightarrow$ R)
(6) (R $\Rightarrow$ T), (($\neg$T) $\iff$ S), ((R $\wedge$ ($\neg$S)) $\Rightarrow$ ($\neg$Q)) $\vdash$ (R $\Rightarrow$ ($\neg$Q))
(7) (P $\Rightarrow$ R), ((P $\wedge$ R) $\Rightarrow$ S), (($\neg$S) $\vee$ Q) $\vdash$ (P $\Rightarrow$ Q)
(8) (P $\iff$ S), (Q $\iff$ T) $\vdash$ ((P $\wedge$ Q) $\iff$ (S $\wedge$ T)).
(9) ((($\neg$P) $\wedge$ S) $\iff$ R), (($\neg$P) $\iff$ S), ($\neg$P) $\vdash$ ($\neg$(P $\vee$ ($\neg$R))).
(10) (($\neg$P) $\iff$ Q), (Q $\iff$ R), R $\vdash$ ($\neg$P)
(11) (Q $\iff$ S), (R $\iff$ ($\neg$S)), (P $\iff$ R) $\vdash$ (P $\iff$ ($\neg$Q)).
(12) (Q $\iff$ R), (($\neg$P) $\iff$ Q), ($\neg$R) $\vdash$ P
(13) (P $\iff$ ($\neg$S)), (Q $\iff$ S) $\vdash$ (P $\Rightarrow$ ($\neg$Q))

6.2. **Proof by contradiction.** Everyone is familiar with reasoning by contradiction: *John Doe cannot be guilty of the murder. For suppose he did do 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. Its formal statement is

Theorem 6.7 (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 6.8. Prove by contradiction that $Q \Rightarrow \neg P, ((\neg R) \implies (P \wedge Q)) \vdash R$.

1	Q $\implies$ $\neg$P	hyp
2	($\neg$R) $\implies$ (P $\wedge$Q)	hyp
3	$\neg$R	temp hyp
4	P $\wedge$Q	mp 2,3
5	Q	cs 4
6	$\neg$P	mp 1,5
7	P	cs 4
8	P $\wedge\neg$P	ci 6,7, contra
9	R	proof by contra, 3-8

Problem 6.9. Prove by contradiction $P \implies (\neg S), S \vee (\neg R), \neg(Q \vee (\neg R)) \vdash \neg P$.

Here is a harder example:

Problem 6.10. (P $\vee$ Q), (($\neg$R) $\Rightarrow$ ($\neg$S)), ((Q $\vee$ P) $\Rightarrow$ S), (($\neg$(T $\wedge$ U)) $\Rightarrow$ ($\neg$R)) $\vdash$ (U $\wedge$ T)

1	$\neg(U \wedge T)$	temp hyp
2	$\neg(T \wedge U) \implies \neg R$	hyp
3	$\neg R$	mp 1,2
4	$\neg R \implies \neg S$	hyp
5	$\neg S$	mp 3,4
6	$Q \vee P \implies S$	hyp
7	$\neg(Q \vee P)$	mt 5,6
8	$\neg Q \wedge \neg P$	dm (de Morgan's) 7
9	$\neg P$	cs 8
10	$P \vee Q$	hyp
11	Q	da 9,10
12	$\neg Q$	cs 8
13	$Q \wedge \neg Q$	ci 11,12, contra
14	$U \wedge T$	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 6.11. (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 6.12. (From [3]) Using the deduction theorem, proof by contradiction, etc

(1) $((\neg P) \Rightarrow (Q \wedge R)), (P \Rightarrow (\neg S)) \vdash (S \Rightarrow Q)$.
(2) $(P \Rightarrow Q), (((\neg P) \vee R) \Rightarrow S) \vdash (Q \vee S)$.
(3) $((\neg P) \Rightarrow Q), (Q \Rightarrow (R \wedge (\neg S))) \vdash ((S \vee (\neg Q)) \Rightarrow P)$.
(4) $((\neg R) \Rightarrow P), ((P \wedge (\neg S)) \Rightarrow Q) \vdash ((\neg(R \vee S)) \Rightarrow Q)$.
(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) $(S \Rightarrow (P \wedge (\neg Q))), ((\neg S) \Rightarrow (\neg R)), R \vdash ((\neg Q) \wedge P)$.
(9) $(P \Rightarrow Q), (Q \Rightarrow R), ((P \Rightarrow R) \Rightarrow (\neg S)), ((\neg S) \Rightarrow T) \vdash T$.
(10) $(T \Rightarrow Q), (P \Rightarrow Q), (R \Rightarrow Q) \vdash (((P \vee R) \vee T) \Rightarrow Q)$
(11) $(R \Rightarrow S), ((R \Rightarrow (\neg P)) \Rightarrow Q), (S \Rightarrow (\neg P)), T \vdash (Q \wedge T)$.
(12) $(P \Rightarrow Q), (R \Rightarrow S), (P \vee R), (\neg Q) \vdash S$.
(13) $(P \vee Q), ((\neg R) \Rightarrow (\neg S)), ((Q \vee P) \Rightarrow S), ((\neg(T \wedge U)) \Rightarrow (\neg R)) \vdash (U \wedge T)$
(14) $((\neg P) \Rightarrow (\neg R)), (\neg S), (P \Rightarrow S), ((\neg R) \Rightarrow Q) \vdash Q$.
(15) $(\neg P), (\neg Q), (R \Rightarrow P) \vdash (\neg(Q \vee R))$.
(16) $(\neg(T \wedge R)), ((\neg T) \Rightarrow S), ((\neg R) \Rightarrow S) \vdash S$.
(17) $((Q \wedge R) \Rightarrow S), ((\neg S) \wedge R) \vdash (\neg Q)$.
(18) $((S \wedge P) \Rightarrow Q) \vdash (S \Rightarrow ((\neg P) \vee (Q \vee R)))$.
(19) $(P \Rightarrow ((R \wedge T) \Rightarrow S)), R, (S \Rightarrow Q), (\neg(T \Rightarrow Q)) \vdash (\neg P)$.
(20) $(R \Rightarrow (\neg P)), (R \Rightarrow U), (Q \Rightarrow (S \Rightarrow T)), ((U \wedge (\neg P)) \Rightarrow ((\neg S) \vee T)) \vdash ((R \vee Q) \Rightarrow (S \Rightarrow T))$.
(21) $(\neg P), (S \Rightarrow (P \vee Q)), (Q \Rightarrow R), (((S \Rightarrow Q) \wedge T) \Rightarrow U) \vdash ((S \Rightarrow Q) \iff (T \Rightarrow U))$.
(22) $(P \Rightarrow S), (R \Rightarrow (\neg S)), R \vdash (\neg P)$.
(23) $(S \wedge (\neg T)), (S \Rightarrow (\neg R)), ((\neg P) \Rightarrow Q) \vdash (R \Rightarrow Q)$
(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) $(R \Rightarrow (\neg Q)), (\neg(S \wedge (\neg R))) \vdash (Q \Rightarrow (\neg S))$.
(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) $(R \vee S), (\neg P), (Q \vee (\neg R)), (P \iff Q) \vdash S$.

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 $P \implies Q$. Now, one cannot use line 1 in the lines following $P \implies Q$, because this was a temporary assumption, which holds only up to the line $P \implies Q$. This leads to a change in our Definition 5.1 of proof:

Definition 6.13. 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, except temporary hypotheses used by proof by deduction or contradiction, if the proof by deduction or contradiction has already been completed.

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]

[5] We will use names for the rules of inference in the first part of book only. The point here is that proving things is more of a motor skill; just like the first steps in playing a musical instrument, hopefully you won't have to think about what you are doing once you learn to do it correctly. Thus, like so much of your education, you are learning something so that you can quickly forget it.

Rule	Name (Abbrev)
$P, P \implies Q \vdash Q$	modus ponens (mp)
$P \implies Q, \neg Q \vdash \neg P$	modus tolens (mt)
$P, Q \vdash P \wedge Q$	conj inf (ci)
$P \wedge Q \vdash P$	conj simp (cs)
$P \vdash P \vee Q$	disj inf (di)
$(\neg P) \wedge (P \vee Q) \vdash Q$	disj alt (da)
$P \implies R, Q \implies R \vdash (P \vee Q) \implies R$	inf by cases (ic)
$P \implies Q, Q \implies R \vdash P \implies R$	trans of impl (ti)
$(P \iff Q) \iff ((P \implies Q) \wedge (Q \implies P))$	def of bicond
$P, P \iff Q \vdash Q$	bicond mp (mpb)
$P \iff Q, Q \iff R \vdash P \iff R$	trans of bicond (tb)
$\neg(P \wedge Q) \iff \neg P \vee \neg Q$	de Morgan's (dm)
$\neg(P \vee Q) \iff \neg P \wedge \neg Q$	de Morgan's (dm)
$(P \wedge Q) \vee R \iff (P \vee R) \wedge (Q \vee R)$	distrib of $\wedge$ over $\vee$
$(P \vee Q) \wedge R \iff (P \wedge R) \vee (Q \wedge R)$	distrib of $\vee$ over $\wedge$
$(P \implies Q) \iff (\neg P \vee Q)$	cond conversion (cc)
$(P, H_1, \ldots, H_n \vdash Q) \iff (H_1, \ldots, H_n \vdash P \implies Q)$	Proof by Deduc
$(H_1, \ldots, H_n, \neg S \vdash C) \implies (H_1, \ldots, H_n \vdash S)$	Proof by Contra

TABLE 1. Some rules of propositional calculus

6.3. **Arithmetic proofs by deduction or contradiction.**

Problem 6.14. Show the following statements using proof by deduction. You may assume basic arithmetic facts.

(1) $x = 3 \implies x^2 = 9$.
(2) $x^2 = 9 \wedge x \geq 0 \implies x = 3$.
(3) $x \geq 0 \wedge x \leq 0 \implies x = 0$.

Here is an answer to (2):

1	$x^2 = 9 \wedge x \geq 0$	temp hyp
2	$x^2 = 9$	cs on 1
3	$x^2 = 9 \implies x = 3 \vee x = -3$	arith
4	$x = 3 \vee x = -3$	mp on 2,3
5	$x \geq 0$	cs on 1
6	$x \geq 0 \implies x \neq -3$	arith fact
7	$x \neq -3$	mp on 5,6
8	$x = 3$	da on 4,7
9	$(x^2 = 9 \wedge x \geq 0) \implies x = 3$	ded thm on 1-8

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 6.15. Prove that $x^2 = 144 \implies x \neq 5$ by contradiction.

An answer:

1	$x = 5$	temp hyp
2	$x^2 = 144$	temp hyp
3	$x = 5 \implies x^2 = 25$	arith
4	$x^2 = 25$	mp on 1,3
5	$x^2 = 144 \wedge x^2 = 25$	ci on 2,4; contra
6	$x^2 = 144 \implies x \neq 5$	proof by contra on 1-5

Problem 6.16. (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 $(2 + 2 = 5 \wedge 2 + 2 = 4) \implies 1 = 0$.

7. PROOFS INVOLVING QUANTIFIERS

7.1. **Universal instantiation and existential generalization.**

For proofs involving predicate forms and quantifiers, we have the following rules which we already introduced before in Section 4.

$\neg\forall x, P(x) \iff \exists x, \neg P(x)$	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 auhtor makes mitsakes.* In more symbolic form, this reasoning looks as follows:

1	$\forall x$, x makes mitsakes.	hyp
2	The auhtor makes mistakes.	ui 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

$\forall x, P(x) \vdash P(y)$ universal instantiation (ui)

Here is a more mathematical example:

Problem 7.1. Show $3|a \implies 9|a^2$, assuming $\forall x, y, x|y \implies x^2|y^2$.

Answer:

1	$\forall x, y, x\|y \implies x^2\|y^2$	hyp
2	$3\|a \implies 9\|a^2$	ui on 1, with $x = 3, y = a$.

Existential generalization works the other way: if we want to show that there exist at least one object with a certain property, it suffices to give an example. An example of existential generalization might be, *Mary Poppins is practically perfect. Mary Poppins is a person. Therefore, some people are practically perfect.* In more symbolic form,

1	Mary Poppins is practically perfect	hyp
2	$\exists y, y$ is practically perfect	eg on 1

More formally, existential generalization for a predicate statement $P(x)$ says $P(y) \vdash \exists x, P(x)$ existential generalization (eg)

Problem 7.2. Prove that $\exists x, x^2 = 9$.

Answer:

1	$3^2 = 9$	arithmetic
2	$\exists x, x^2 = 9$	ei on 1

A proof of an existential proposition of this form is called a *constructive proof.* That is, we prove the statement by constructing an example.

Another good example of this method is the proof that a number is even or odd.

Problem 7.3. Prove that 9 is odd.

Answer:

1	9 is odd iff $\exists y, 2y + 1 = 9$	def odd
2	$2(4) + 1 = 9$	arith
3	$\exists y, 2y + 1 = 9$	eg on 3
4	9 is odd	mp on 1,3

Problem 7.4. Prove that 26 is the sum of two odd natural numbers.

Answer: The first problem here is to write the statement precisely in terms of quantifiers:

$$\exists m, n,\ n, m \text{ are odd } \wedge 26 = m + n.$$

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

1	$26 = 15 + 11$	arith
2	$15 = 2(7) + 1$	arith
3	$11 = 2(5) + 1$	arith
4	$\exists k, 15 = 2k + 1$	eg 2
5	$\exists k, 11 = 2k + 1$	eg 3
6	15 is odd	def odd, 4
7	11 is odd	def odd, 5
8	15 is odd $\wedge$11 is odd $\wedge 26 = 15 + 11$	cs 1,6,7
9	$\exists m, n,\ n, m$ are odd $\wedge 26 = m + n$	eg 8

Problem 7.5. 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) $\exists x, x^3 = 27$.

Problem 7.6. Prove that 7 does not divide 29, assuming 29 is prime.

Answer:

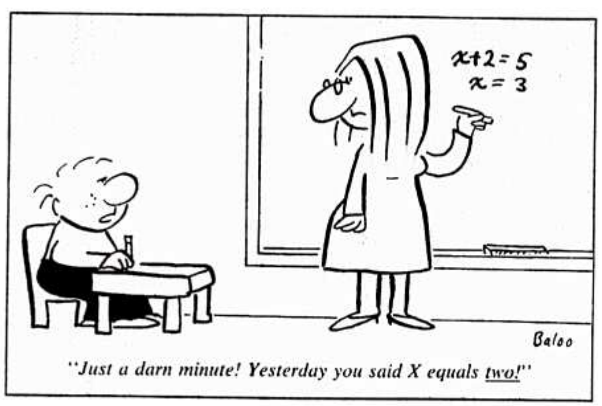
1	29 is prime	hyp
2	29 is prime iff $29 \neq 1 \wedge \forall x, x\|29 \implies (x = 29 \vee x = 1)$	def prime
3	$29 \neq 1 \wedge \forall x, x\|29 \implies (x = 29 \vee x = 1)$	mp on 1,2
4	$\forall x, x\|29 \implies (x = 29 \vee x = 1)$	cs on 3
5	$7\|29 \implies (7 = 29 \vee 7 = 1)$	ui on 4
6	$\neg(7 = 29 \vee 7 = 1)$	def of 1,7,29
7	$\neg(7\|29)$	mot on 5,6

Theorem 7.7. *p is not prime iff $\exists x, y, p = xy \wedge x > 1 \wedge y > 1$.*

We'll give a proof with some steps condensed.

1	p is prime iff $p \neq 1 \wedge \forall a,$ $(a \mid p \implies a = 1 \vee a = p)$	def prime
2	p is not prime iff $\neg(p \neq 1 \wedge \forall a,$ $(a \mid p \implies a = 1 \vee a = p))$	negation of 1
3	p is not prime iff $p = 1 \vee \neg\forall a,$ $(a \mid p \implies a = 1 \vee a = p))$	de Morgan's on 2
4	p is not prime iff $p = 1 \vee \exists a,$ $\neg(a \mid p \implies a = 1 \vee a = p))$	qc on 3
5	p is not prime iff $p = 1 \vee \exists a,$ $\neg(\neg a \mid p \vee a = 1 \vee a = p))$	taut and 4
6	p is not prime iff $p = 1 \vee \exists a,$ $a \mid p \wedge a \neq 1 \wedge a \neq p))$	de Morgan's on 5
7	p is not prime iff $p = 1 \vee \exists a,$ $\exists b, ab = p \wedge a \neq 1 \wedge a \neq p))$	6, def divides
8	p is not prime iff $p = 1 \vee \exists a, b,$ $ab = p \wedge a \neq 1 \wedge a \neq p))$	quantifier shift on 7
9	$ab = p \wedge 1 \neq p \iff ab = p \wedge a \neq 1 \wedge b \neq 1$	fact
10	p is not prime iff $p = 1 \vee \exists a, b,$ $ab = p \wedge a \neq 1 \wedge b \neq 1))$	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 16.25.



"Just a darn minute! Yesterday you said X equals two!"

FIGURE 9. A restricted variable

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

7.2. **Universal generalization and existential instantiation.** The next two rules are harder. The first, *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 we haven't made any assumptions on x, 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:

$P(x)$, x unrestricted $\vdash \forall x, P(x)$	universal generalization (ug)
$\exists x, P(x) \vdash P(y)$, y unrestricted	existential instantiation (ei)

Problem 7.8. Prove that for all integers a, there exists an integer b such that $a + b = 10$.

Answer:

1	a is an integer	hyp
2	$(a) + (10 - a) = 10$	arith
3	$10 - a$ is an integer	closure of integers under sub
4	$\exists b, b$ is an integer $\wedge\, a + b = 10$	eg 3
5	a is an integer $\implies$ $\exists b, b$ is an integer $\wedge\, a + b = 10$	deduc 1 - 4
6	$\forall a, a$ is an integer $\implies$ $\exists b, b$ is an integer $\wedge\, a + b = 10$	ug 5

Warning 7.1. *When doing ei, 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 7.9. Prove that if x is odd and y is odd then $x + y$ is even.

Answer:

1	x is odd	hyp
2	$\exists k, x = 2k + 1$	def of odd
3	$x = 2l + 1$	ei on 2
4	y is odd	hyp
5	$\exists k, y = 2k + 1$	def of odd
6	$y = 2m + 1$	ei on 3
7	$x + y = 2l + 2m + 2$	arith on 3,5
8	$x + y = 2(l + m + 1)$	arith on 7
9	$\exists k, x + y = 2k$	eg on 8
10	$x + y$ is even	def even

Problem 7.10. Prove that if n is even, then so is n^2.

Answer:

1	n is even	hyp
2	n is even $\implies \exists m, 2m = n$	def of even
3	$\exists m, 2m = n$	mp on 1,2
4	$2l = n$	ei 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	$\exists m, 2m = n^2$	eg on 6, $2l^2$ an instance of m
8	n^2 is even	def of even

Problem 7.11. Prove that if 3 divides x and y then 3 divides $2x+y+6$.

Answer:

1	$3\|x \wedge 3\|y$	hyp
3	$(\exists k, 3k = x) \wedge (\exists k, 3k = y)$	def divides
5	$3m = x \wedge 3n = y$	ei on 2
6	$2x + y + 6 = 6m + 3n + 6$	cs, arith on 5
7	$2x + y + 6 = 3(2m + n + 3)$	algebra on 6
8	$\exists k, 3k = 2x + y + 6$	eg on 7
9	$3\|(2x + y + 6)$	def divides

Here is an example of how re-using a variable name can give a wrong answer:

Problem 7.12. 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: $2|x \wedge 2|y \implies 4|(x + y)$.

1	$2\|x \wedge 2\|y$	hyp
2	$\exists k, 2k = x \wedge \exists k, 2k = y$	def divides
3	$4k = x + y$	ei, arith on 2
4	$\exists k, 4k = x + y$	eg on 3
5	$4\|(x + y)$	def divides

Problem 7.13. 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^3 is even.

Problem 7.14. Prove that

(1) $\forall n, 3|4^n - 1 \implies 3|4^{n+1} - 1$
(2) $\forall n, 9|4^n + 15n - 1 \implies 9|4^{n+1} + 15(n + 1) - 1$
(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 7.15. Prove that there is no largest odd integer.

Answer: First we translate this into mathematical language. x is the largest odd integer iff it is odd and if for any other odd integer y, $x \geq y$. That is, $2|x + 1 \wedge \forall y, 2|y + 1 \implies x \geq y$. So, there is no largest integer iff $\neg\exists x, 2|x+1 \wedge \forall y, 2|y+1 \implies x \geq y$. The method is proof by contradiction:

1	$\exists x, 2\|x+1 \wedge \forall y, 2\|y+1 \implies x \geq y$	hyp
2	$2\|x+1 \wedge \forall y, 2\|y+1 \implies x \geq y$	ei on 1
3	$2\|x+1$	def odd
4	$\exists k, 2k = x+1$	def divides
5	$2l = x+1$	ei 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, ui on 2 with $y = x+2$
9	$x \geq x+2$	mp 7,8,contra
10	$\neg\exists x, 2\|x+1 \wedge \forall y, 2\|y+1 \implies x \geq y$	proof by contra 1- 7

Problem 7.16. Show that $\neg\exists a, 2|a \wedge \forall b, 2|b \implies b \leq a$ is equivalent to $\forall a, (2|a) \implies \exists b, (2|b) \wedge a < b$.

Problem 7.17. Write out a symbolic version of each statement. (i.e. no words.) Then prove or disprove.

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

Problem 7.18. (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.

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, *it is Tuesday and it is somebody's birthday* is the same as *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,

$$\begin{aligned}
(\forall x, P \wedge Q(x)) &\iff (P \wedge (\forall x, Q(x))) \\
(\forall x, P \vee Q(x)) &\iff (P \vee (\forall x, Q(x)) \\
(\exists x, P \wedge Q(x)) &\iff (P \wedge (\exists x, Q(x))) \\
(\exists x, P \vee Q(x)) &\iff (P \vee (\exists x, Q(x)).
\end{aligned}$$

We call these rules *quantifier expansion* (qe). However, we will rarely use this rule.

Example 7.19. (1) $\exists x, y, x^2 = 16 \wedge x = y^2$ is equivalent to $\exists x, (x^2 = 16 \wedge \exists y, x = y^2)$.
(2) $\forall x, y, x^2 \geq 0 \wedge y^4 \geq 0$ is equivalent to $\forall x(x^2 \geq 0 \wedge \forall y, y^4 \geq 0)$.
(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:

Rule	Name (Abbrev)
$\neg\forall x, P(x) \iff \exists x, \neg P(x)$	quantifier conversion (qc)
$\forall x \forall y P(x, y) \iff \forall y \forall x P(x, y)$	commutativity univ quant (cuq)
$\exists x \exists y P(x, y) \iff \exists y \exists x P(x, y)$	commutativity exist quant (ceq)
$\forall x, P(x) \vdash P(y)$	universal instantiation (ui)
$P(y) \vdash \exists x, P(x)$	existential generalization (eg)
$P(y)$, y unrestricted $\vdash \forall x, P(x)$	universal generalization (ug)
$\exists x, P(x) \vdash P(y)$, y unrestricted	existential instantiation (ei)

7.3. **Introducing notation in a proof.** A variation on the above proofs is to *introduce notation* first. For example, if you want to prove 9 is odd then you want to solve for $9 = 2y + 1$. So letting $y = 4$ you have $9 = 2y + 1$ so 9 is odd. Formally:

Problem 7.20. Prove that 9 is odd.

Answer:

1	9 is odd iff $\exists y, 2y + 1 = 9$	def odd
2	$\exists y, y = 4$	4 is an integer
3	$y = 4$	ei on 2
4	$2(y) + 1 = 9$	algebra on 3
5	$\exists y, 2y + 1 = 9$	eg on 4
6	9 is odd	mp on 1,5

Let's abbreviate the rules $2, 3$ as *introducing notation*. So for example,

1	9 is odd iff $\exists y, 2y+1=9$	def odd
2	$y=4$	notation
3	$2(y)+1=9$	algebra on 2
4	$\exists y, 2y+1=9$	eg on 3
5	9 is odd	mp on 1,4

Here is another example:

Problem 7.21. Prove that there is no largest multiple of 2.

We give a proof by contradiction.

1	$\exists x,\ 2\|x \wedge \forall y, 2\|y \implies y \leq x$	temp hyp
2	$\forall y, 2\|x \implies \forall y, 2\|y \implies y \leq x$	ei on 1
3	$y = x+2$	notation, y is now restricted
4	$2\|x$	ui, cs on 2
5	$2\|2$	arithmetic
6	$2\|y$	$a\|b \wedge a\|c \Rightarrow a\|(b+c)$, lines 4,5
7	$y \leq x$	mp 2,6
8	$x+2 \leq x$	subst 3, 7, contra
9	$\neg\exists x, 2\|x \wedge \forall y, 2\|y \implies y \leq x$	proof by contra 1-8

8. Introduction to sets

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. For example, in Smullyan's logic problems we say that A is a knight, meaning A is an *element* of the *set of knights*. If p is a prime, we mean that p is a *element* of the *set* of primes.

8.1. 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 $D = \{$ 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 8.1. The set of baseball players who played shortstop for the New York Mets in 2006 is

$$\begin{aligned} M &= \{\text{Hernandez, Reyes, Chris Woodward}\} \\ &= \{\text{Hernandez, Reyes, Reyes, Woodward}\} \\ &= \{\text{Woodward, Hernandez, Reyes}\} \end{aligned}$$

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 8.2. 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 8.3. 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 8.4. 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 8.5.
(1) $\mathbb{N} = \{0, 1, 2, 3, \dots, \}$ is the set of natural numbers.
(2) $\mathbb{N}_+ = \{1, 2, 3, \dots\}$ is the set of positive natural numbers.
(3) $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ is the set of integers.
(4) $\mathbb{Q} = \{\dots, 0, 1, 1/2, 1/3, 2/3, -1/2, \dots\}$ 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,

$$I = \{x|x \in \mathbb{Z} \wedge 1 \leq x \leq 5\}$$

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.*

$$D = \{y|\text{y is my daughter}\}$$

means that D is the set of my daughters.

Problem 8.6. (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 8.7. Give a roster form for the following sets of natural numbers.

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

8.2. **Subsets.** Let S and T be sets. We say that S is a *subset* of T, and write $S \subseteq T$, iff every element of S ia 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:

$$(S \subset T) \iff (S \subseteq T) \wedge (S \neq T).$$

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 8.8. (1) $\{1, 3\} \subseteq \{1, 3, 5\}$,
(2) $\{1, \text{apple}\} \subseteq \{1, \text{orange}, \text{apple}\}$.
(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 8.9. (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 8.10. 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 8.11. 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.

8.3. **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

$$S \cup T = \{x | x \in S \vee x \in T\}, S \cap T = \{x | x \in S \wedge x \in T\}.$$

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

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

Problem 8.12. 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 *Ven diagrams*: For example, the following diagram shows $(A \cap B) \cup C$:

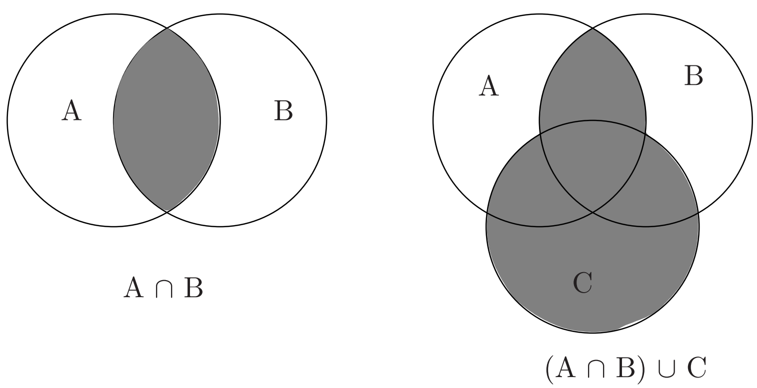


FIGURE 10. Ven diagram for $(A \cap B) \cup C$

Problem 8.13. Draw the Ven diagram for

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

$$A \text{ is empty} \iff \nexists x, x \in A \iff \forall x, x \notin A.$$

For example $\{x | x \neq x\}$ is empty. Any two empty sets are equal since

$$A, B \text{ empty} \implies \forall x, x \notin A \wedge x \notin B \implies \forall x, (x \in A \iff x \in B)$$

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 8.14. Which of the following statements are true?

(1) $\{x | x^2 = 1 \wedge x^3 = 8\} = \emptyset$.
(2) $\{p | 2|p \wedge 3|p\} = \emptyset$.
(3) $\{p | 5|p \wedge 7|p \wedge p \leq 20\} = \emptyset$.

Problem 8.15. 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 8.16. List all subsets of

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

Problem 8.17. Rephrase the following statements in terms of intersection, union, and complement using $\mathbb{E}$ as the set of even numbers $\mathbb{O}$ as the set of odd numbers, $\mathbb{P}$ as the set of primes, and $\mathbb{S}$ is the set of numbers bigger than 5. (Example: *Some prime numbers are even* is the same as $\mathbb{P} \cap \mathbb{E} \neq \emptyset$.) Determine whether the statements are true or false.

(1) The only even prime number is 2.
(2) Every number is even or odd.
(3) Some odd numbers are prime.

(4) No prime number is even and bigger than five.

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

8.4. **Power sets.** 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 8.18. If $S = \{1, 3, 5\}$ then

$$\mathcal{P}(S) = \{\emptyset, \{1\}, \{3\}, \{5\}, \{1, 3\}, \{1, 5\}, \{3, 5\}, \{1, 3, 5\}.$$

Problem 8.19. Find $\mathcal{P}(S)$ where

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

Problem 8.20. 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) $A \subseteq B \implies \mathcal{P}(A) \subseteq \mathcal{P}(B)$.

8.5. **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 $\forall x, x \in \mathbb{N} \implies 4x \in \mathbb{E}$. Statements such as $\forall x, ...$ are so general that they are (arguably) meaningless.

Problem 8.21. Write out predicate form of the following, specifying the universe as part of the quantifier.

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

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

8.6. **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	A is a knight
Q	B is a knight
R	the werewolf is a knight
S	A 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	¬S	temp hyp
2	¬S $\implies$ (Q $\iff$ R)	hyp
3	Q $\iff$ R	mp
4	Q $\iff$ ¬R	hyp
5	R $\iff$ ¬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 $a = w \vee b = w$ (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	$a = w \vee b = w$	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 8.22. (a) Write the following sets in the form $\{x|P(x)\}$. (i) $\{2, 4, 6, 8\}$. (ii) { red, orange, yellow, green, blue, violet }.

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

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

Problem 8.23. 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.

9. Proofs involving sets

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

Rule	Name
$A = B \iff (\forall x, x \in A \iff x \in B)$	Definition of Set Equality
$A \subseteq B \iff (\forall x, x \in A \Rightarrow x \in B)$	Definition of Subset
$A = B \iff (A \subseteq B) \wedge (B \subseteq A)$	Theorem about set equality
$A \cap B = \{x|x \in A \wedge x \in B\}$	Definition of intersection
$A \cup B = \{x|x \in A \vee x \in B\}$	Definition of union
$\emptyset = \{x \neq x\}$	Definition of Empty Set
$A = \emptyset \iff \neg\exists x, x \in A$	Characterization of Empty Set
$x = y, P(x) \vdash P(y)$	Substitution
$x \in \{y|P(y)\} \vdash P(x)$	Set Definition Axiom
$\forall x, x = x$	Equality Axiom
$S = \{s_1, \ldots, s_k\} \vdash x \in S \iff$ $(x = s_1 \vee x = s_2 \vee \ldots \vee x = s_k)$	Roster Axiom

Definition 9.1. A *proof* (involving sets) is a sequence of statements, each formed out of

(1) the symbols $=, \in, \notin, \subseteq, \setminus, \cap, \cap, \{\ \}, \implies, \iff, \vee, \wedge, \neg, \forall, \exists$
(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 or set-theoretic rules above.

9.1. **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 9.2. Prove that $A \subseteq B, B \subseteq C \vdash A \subseteq C$.

1	$A \subseteq B$	hyp
2	$B \subseteq C$	hyp
3	$A \subseteq B \iff \forall x, x \in A \implies x \in B$	def subset
4	$\forall x, x \in A \implies x \in B$	mp on 1,3
5	$B \subseteq C \iff \forall x, x \in B \implies x \in C$	def subset
6	$\forall x, x \in B \implies x \in C$	mp on 2,5
7	$y \in A \implies y \in B$	ui on 4
8	$y \in B \implies y \in C$	ui on 6
9	$y \in A \implies y \in C$	ti on 7,8
10	$\forall x, x \in A \implies x \in C$	ug on 9
11	$A \subseteq C \iff \forall x, x \in A \implies x \in C$	def subset
12	$A \subseteq C$	mp on 10,11

Problem 9.3. Prove that (1) $A \subseteq B \vdash A \cup B \subseteq B$. (2) $A \subseteq B \vdash A \subseteq A \cap B$.

9.2. **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:

$$x \in \{y|y^4 = y\} \iff x^4 = x$$

$$x \in \{y | y \in A \vee y \in B\} \iff x \in A \vee x \in B.$$
$$x \in \{z | z - 5 \in A\} \iff x - 5 \in A.$$

Problem 9.4. Use the set definition property to simplify the following. Identify each as true or false.

(1) $2 \in \{x | x^2 = 5\}$
(2) $3 \in \{p | p \text{ is prime}\}$
(3) $\{2, 3\} \in \{S | S \cap \{1, 2\} = \emptyset\}$.

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

$$x \in A \cap B \iff x \in A \wedge x \in B.$$
$$x \in A \cup B \iff x \in A \vee x \in B.$$
$$x \in A - B \iff x \in A \wedge x \notin B.$$

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

$$x \in A \cap B \iff x \in \{y | y \in A \wedge y \in B\} \iff x \in A \wedge x \in B.$$

When you are writing a proof, you can combine the set definition property and the definitions above in one step, so it is an acceptable short cut to write one of the above lines as a line in a proof, with the justification being definition of intersection, union, or complement.

Problem 9.5. Prove that $A \subseteq A \cup B$.

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	$x \in A \cup B \iff x \in A \vee x \in B$	def union
4	$x \in A \vee x \in B$	di on 2
5	$x \in A \cup B$	mp on 3,4
6	$x \in A \implies x \in A \cup B$	proof by deduc on 2-5
7	$\forall x, x \in A \implies x \in A \cup B$	ug on 6
8	$A \subseteq A \cup B$	mp on 1,7

Problem 9.6. Fill in the blanks in the following proof that $A \cap B \subseteq A$.

1	$x \in A \cap B \iff$ ____________	def intersection
2	$x \in A \wedge x \in B \implies x \in A$	____________
3	____________ $\implies x \in A$	ti on 1,2
4	$\forall x, x \in A \cap B \implies x \in A$	____________ on 3
5	________________________	def subset

Problem 9.7. Show that $A \cap B \subseteq A \cup B$.

The second rule is the *roster axiom* $S = \{s_1, \ldots, s_k\} \vdash x \in S \iff (x = s_1 \vee x = s_2 \vee \ldots \vee x = s_k)$. For example, $x \in \{1, 2, 3\} \iff x = 1 \vee x = 2 \vee x = 3$. Here is an example of the set definition axiom and roster axiom in a proof:

Problem 9.8. 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	$y^3 - y = 0$	algebra on 2
4	$(y^2 - 1)y = 0$	algebra on 3
5	$(y - 1)(y + 1)y = 0$	algebra on 4
6	$xyz = 0 \implies (x = 0 \vee y = 0 \vee z = 0)$	assumption 20.1 (9)
7	$y = 0 \vee y + 1 = 0 \vee y - 1 = 0$	modus ponens, subst on 5,6
8	$y = 0 \vee y = -1 \vee y = 1$	algebra on 7
9	$y \in \{-1, 0, 1\}$	roster axiom on 8
10	$y \in \{x | x^3 = x\} \implies y \in \{-1, 0, 1\}$	ded thm on 1-9
11	$\{x | x^3 = x\} \subseteq \{-1, 0, 1\}$	def subset

Problem 9.9. 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 9.10. Show that $\{3, 5\} \subset \{y | y \text{ is odd }\}$.

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

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 9.11. Prove that $A \cap B = B \cap A$.

1	$x \in A \cap B$	hyp
2	$x \in A \wedge x \in B$	def int on 1
3	$x \in B \wedge x \in A$	commut of and, 2
4	$x \in B \cap A$	def of int on 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	$x \in B \wedge x \in A$	def int on 1
8	$x \in A \wedge x \in B$	commut of and, 2
9	$x \in A \cap B$	mp 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

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.

Problem 9.12. Prove that $\{-1, 0, 1\} = \{x \vert x^3 = x\}$.

We already showed one direction in Problem 9.8, you should in addition show that $\{-1, 0, 1\} \subseteq \{x \vert x^3 = x\}$. To do this, use the set definition property in reverse.

11	$(-1)^3 = (-1)$	arithmetic
12	$(1)^3 = (1)$	arithmetic
13	$(0)^3 = (0)$	arithmetic
14	$-1 \in \{x \vert x^3 = x\}$	set def prop on 11
15	$1 \in \{x \vert x^3 = x\}$	set def prop on 12
16	$0 \in \{x \vert x^3 = x\}$	set def prop on 13
17	$y = -1 \implies y \in \{x \vert x^3 = x\}$	subst on 14
18	$y = 1 \implies y \in \{x \vert x^3 = x\}$	subst on 15
19	$y = 0 \implies y \in \{x \vert x^3 = x\}$	subst on 16
20	$y = -1 \vee y = 1 \vee y = 0 \implies y \in \{x \vert x^3 = x\}$	ic on 17-19
21	$y \in \{-1, 1, 0\} \implies y = -1 \vee y = 0 \vee y = 1$	roster def
22	$y \in \{-1, 1, 0\} \implies y \in \{x \vert x^3 = x\}$	ti on 20,21
23	$\{-1, 10\} \subseteq \{x \vert x^3 = x\}$	def of subset on 22
24	$\{-1, 10\} = \{x \vert x^3 = x\}$	def equality on 10,23

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 9.13. 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 9.14. 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 Ven diagrams as in Figure 11. The diagram on the left shows that if $A \subset B$ 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.

The formal proof is:

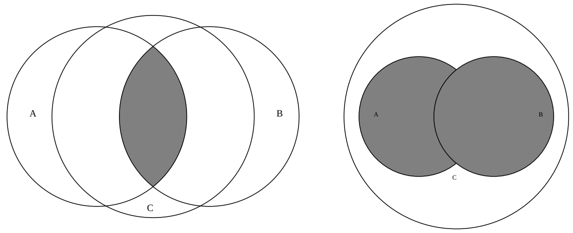


FIGURE 11. $A \cap B$ and $A \cup B$

1	$A \cup B \subseteq C$	hyp
2	$\forall x, x \in A \cup B \implies x \in C$	def subset
3	$x \in A \vee x \in B \implies x \in C$	ui, def union on 2
4	$A \subseteq C \iff (\forall x, x \in A \implies x \in C)$	def subset
5	$x \in A \implies x \in A \vee x \in B$	tautology
6	$x \in A \implies x \in C$	ti on 3,5
7	$\forall x, x \in A \implies x \in C$	ug 6
8	$A \subseteq C$	mp on 4,7

Problem 9.15. Show

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

Problem 9.16. Show that

(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 in 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 $\{ \mid \}$. 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.

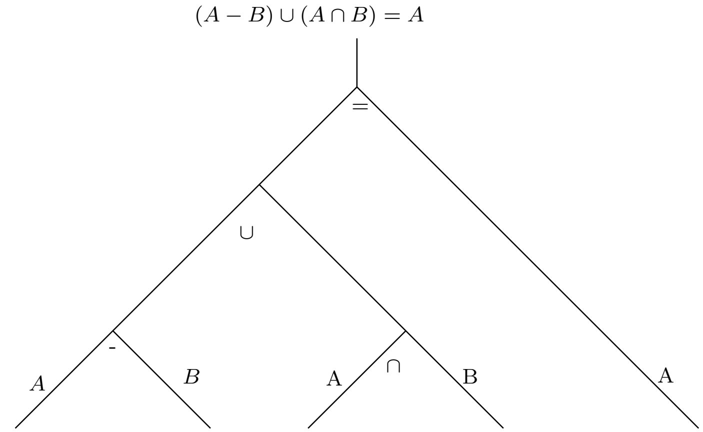


FIGURE 12. Tree form of $(A - B) \cup (A \cap B) = A$

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

Problem 9.17. Give proofs of the following statements about sets $A, B, \ldots$

(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) $A \neq \emptyset \implies \exists y, y \in A$
(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) $(A \subseteq B) \Rightarrow (A - B = \emptyset)$.
(13) there is a unique set C such that $C \cup (C \cap A) = A$.
(14) $(\mathcal{P}(A) \subset \mathcal{P}(B)) \iff (A \subset B)$.

9.3. **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 9.18. 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.[6]

FIGURE 13. Another Ven diagram

10. 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. Here is an example.

Problem 10.1. Prove that 4 is not prime.

[6]Which the author of these notes would not be qualified to teach.

1	4 is prime $\iff (4 \neq 1 \wedge \forall x, x\|4 \implies (x = 4 \vee x = 1))$	def prime
2	4 is not prime $\iff \neg(4 \neq 1 \wedge \forall x, x\|4 \implies (x = 4 \vee x = 1))$	negation of 1
3	4 is not prime $\iff \boxed{4 = 1 \vee \exists x, \neg(x\|4 \implies (x = 4 \vee x = 1))}$	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	$\neg(2 = 4 \vee 2 = 1)$	fact
6	$2\|4 \wedge \neg(2 = 4 \vee 2 = 1)$	ci 4,5
7	$\neg(2\|4 \implies (2 = 4 \vee 2 = 1))$	de Morgan's, cc on 6
8	$\exists x, \neg(x\|4 \implies (x = 4 \vee x = 1))$	ei on 7
9	4 is not prime	mp on 3,8

Here is a set-theoretic example.

Problem 10.2. Prove that $A \subseteq B \wedge B \subseteq C \implies A \subseteq C$.

1	$A \subseteq B$	hyp
2	$B \subseteq C$	hyp
3	$\forall x, x \in A \implies x \in B$	def subset 1
4	$\forall x, x \in B \implies x \in C$	def subset 2

What next? Don't panic yet! One possibility is to write out the definition of the goal, $A \subseteq C$.

5	$A \subseteq C \iff \forall x, \boxed{x \in A \implies x \in C}$	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	$x \in B$	ei, mp on 3
8	$x \in C$	ei, mp on 4
9	$\forall x, x \in A \implies x \in C$	deduc on 6-8, ug
10	$A \subseteq C$	mp 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 10.3. 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	$\forall x, \neg(x \in A \wedge x \in B)$	def intersection
4	$\forall x, x \notin A \vee x \notin B$	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 $A - B = A \iff \forall x, \boxed{x \in A \wedge x \notin B \iff x \in A}$ 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 $x \in A \wedge x \notin B \implies x \in A$ 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.

7	$x \in A$	temp hyp
8	$x \notin B$	ui, da on 4
9	$x \in A \wedge x \notin B$	ci on 7,8
10	$x \in A \implies x \in A \wedge x \notin B$	deduc on 7-9
11	$\forall x, x \in A \wedge x \notin B \iff x \in A$	cs on 7,10,ug
12	$A - B = A$	mp 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 10.4. Prove that $x|y \vee x|z \implies x|yz$.

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	$x\|y$	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 $x|yz \iff \boxed{\exists k, xk = yz}$ 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	$\exists k, xk = yz$	eg 5
7	$x\|yz$	deduc 1-6
8	$x\|y \implies x\|yz$	deduc 1=7

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

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

Problem 10.5. Show that $A - (A - B) = A \cap B$.

There are no hypotheses here, so we must work backwards, unravelling the definitions.

1	$A - (A - B) = A \cap B \iff \forall x,$ $x \in A - (A - B) \iff x \in A \cap B$	def =
2	$A - (A - B) = A \cap B \iff \forall x,$ $(x \in A \wedge \neg(x \in A \wedge x \notin B)) \iff (x \in A \wedge x \in B)$	def $-, \cap$ on 1
3	$(x \in A \wedge \neg(x \in A \wedge x \notin B)) \iff$ $(x \in A \wedge x \notin A) \vee (x \in A \wedge x \in B)$	distrib, de Morg 2
4	$(x \in A \wedge x \notin A) \vee (x \in A \wedge x \in B) \iff$ $x \in A \wedge x \in B$	taut
5	$x \in A \wedge \neg(x \in A \wedge x \notin B) \iff$ $(x \in A \wedge x \in B)$	mpb on 3-4
6	$A - (A - B) = A \cap B$	ug on 5, mp on 2

Problem 10.6. 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) Prove that $B - (B \cap C) = B - C$
(2) Prove that if n is square and 2 divides n then 4 divides n.
(3) Prove that the sum of two odd 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 10.7. Prove the following by working backwards.

(1) Prove that $B - (B \cap C) = B - C$
(2) Prove that if n is square and 2 divides n then 4 divides n.
(3) Prove that the sum of two odd 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.

11. Paragraph proofs

11.1. **Writing paragraph proofs.** In practice, it quickly becomes cumbersome to give formal two-column proofs. A *paragraph proof* is an outline of how one might construct a formal proof. Here is a rough dictionary for how to construct a paragraph proof from a formal proof. It should be composed of complete English sentences, but it should also contain the key equations of the formal proof.

formal proof	paragraph proof
hyp	Let, assume, suppose
mp on 1,2	By equations 1,2
mp on previous line	Hence, therefore, so, this shows
def	By definition of

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

Problem 11.1. Translate the following proof that if n is an even integer, then so is n^2, into paragraph form.

1	n is even	hyp
2	n is even $\implies \exists m, 2m = n$	def of even
3	$\exists m, 2m = n$	mp on 2
4	$2l = n$	ei 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	$\exists m, 2m = n^2$	eg 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 11.2. Translate the following proof that $\forall x, y, z, x|y \wedge x|z \implies x|y+z$ into paragraph form.

1	$x\|y \wedge x\|z$	hyp
2	$\exists k, xk = y \wedge \exists k, xk = z$	def divides
3	$xl = y \wedge xm = z$	ei on 2
4	$x(l+m) = y+z$	cs, addition on 3
5	$\exists k, xk = y+z$	eg on 4,$k = y+z$
6	$x\|y+z$	def divides on 5
7	$x\|y \wedge x\|z \implies x\|y+z$	deduc on 1-6
8	$\forall x, y, z \in \mathbb{Z}, x\|y \wedge x\|z \implies x\|y+z$	ug on 7

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 $x+z$.

Problem 11.3. 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 paragraph proof. Recall the formal proof:

1	$A \cup B \subseteq C$	hyp
2	$\forall x, x \in A \cup B \implies x \in C$	def subset
3	$x \in A \vee x \in B \implies x \in C$	ui, def union on 2
4	$A \subseteq C \iff (\forall x, x \in A \implies x \in C)$	def subset
5	$x \in A \implies x \in A \vee x \in B$	tautology
6	$x \in A \implies x \in C$	ti on 3,5
7	$\forall x, x \in A \implies x \in C$	ug 6
8	$A \subseteq C$	mp on 4,7

Here is the paragraph proof: 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, $\forall x, x \in A \vee x \in B \implies x \in C$. Now tautologically, $\forall x, x \in A \implies x \in A \vee x \in B$. By transitivity of implication, $\forall x, x \in A \implies x \in C$. By definition of subset, $A \subseteq C$.

Problem 11.4. Translate the following proof that $x|y \vee x|z \implies x|yz$ into paragraph form, by filling in the blanks.

1	$x\|y$	hyp
2	$\exists k, xk = y$	def divides
3	$xl = y$	ei 2
4	$xlz = yz$	arith 3
5	$\exists k, xk = yz$	eg on 4, $k = lz$
6	$x\|yz$	def divides
7	$x\|y \implies x\|yz$	deduc 1-6
8	$x\|z$	hyp
9	$\exists k, xk = z$	def divides
10	$xl = z$	ei 2
11	$xly = yz$	arith 3
12	$\exists k, xk = yz$	eg on 4, $k = ly$
13	$x\|yz$	def divides
14	$x\|z \implies x\|yz$	deduc 1-6
15	$x\|y \vee x\|z \implies x\|yz$	ic on 7,14

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

Problem 11.5. Translate the following proof that $A \subseteq B, B \subseteq C \vdash A \subseteq C$ into paragraph form, by filling in the blanks.

1	$A \subseteq B$	hyp
2	$B \subseteq C$	hyp
3	$A \subseteq B \iff \forall x, x \in A \implies x \in B$	def subset
4	$\forall x, x \in A \implies x \in B$	mp on 1,3
5	$B \subseteq C \iff \forall x, x \in B \implies x \in C$	def subset
6	$\forall x, x \in B \implies x \in C$	mp on 2,5
7	$y \in A \implies y \in B$	ui on 4
8	$y \in B \implies y \in C$	ui on 6
9	$y \in A \implies y \in C$	ti on 7,8
10	$\forall x, x \in A \implies x \in C$	ug on 9
11	$A \subseteq C \iff \forall x, x \in A \implies x \in C$	def subset
12	$A \subseteq C$	mp on 10,11

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

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 paragraph proofs.

Suggestions for paragraph proofs:

(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 11.6. Use the following paragraph proof that there is no largest even number to construct a formal proof.

Paragraph proof: 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	$\exists x$ ______ $\forall y$ ______ $\implies y \leq x$	temp hyp
2	$\forall y,$ ____________ $\implies$ ____________	ei on 1
3	$2 \mid x+2 \implies$ ____________	ui on 2
4	$2 \mid x$	____________
5	$2 \mid x+2$	____________
6	____________	mp 3,4, contra
7	____________ $\exists x, \forall y, 2 \mid y \implies y \leq x$	proof by contra 1-5

Problem 11.7. Fill in the blanks in the following paragraph and formal proofs that for all sets A, B, $B - A = B \implies A \cap B = \emptyset$.

Paragraph proof: Suppose that A, B are sets such that ____________. By definition of ____________ and ____________, for all x, $x \in B \wedge x \notin A \iff x \in B$. Hence given x, $x \in B$ implies ____________, or equivalently, ____________ or $x \notin A$. By de Morgan's law, $\neg($ ____________ $)$. By definition of intersection, $x \notin$ ____________. Hence $A \cap B =$____________, by characterization of the empty set.

1	$B - A = B$	____________
2	$\forall x, x \in B \wedge x \notin A \iff x \in B$	____________
3	$x \in B \implies x \notin A$	____________
4	$(x \notin B \vee x \notin A)$	____________
5	____________	de Morgan's
6	$x \notin A \cap B$	____________
7	$\forall x, x \notin A \cap B$	____________
8	____________ $= \emptyset$	char empty set

Rules for writing paragraph proofs:

(1) Paragraph proofs 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.

11.2. **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 11.8. Prove that $\forall d, n \in \mathbb{N}, d \mid n! + 1 \implies d \notin \{2, \ldots, n\}$.

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

1	$d \in \{1, \ldots, n\}$	hyp
2	$d \mid n(n-1)(n-2)\ldots 1$	inference by cases
3	$n! = n(n-1)(n-2)\ldots 1$	def factorial
4	$d \mid n!$	sub 2,3
5	$d \mid n! + 1$	temp hyp

6	$d\|(n!+1)-n!$	$x\|y \wedge x\|z \implies x\|y-z$
7	$d\|1$	arithmetic on 6
8	$d=1$	def divides
9	$d \notin \{2,\dots,n\}$	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 11.9. *$\forall x,y,z \in \mathbb{Z}, x|y \wedge x|z \implies x|y-z$.*

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, ei on 4,5
7	$\exists m, xm=y-z$	eg on 6
8	$x\|y-z$	def divides on 7

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

7	$d\|(n!+1)-n!$	by Lemma below

Looking at your proof, you might realize that it is obscuring the following basic fact: *no 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 11.10. *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 numbers k,l such that $y=kx$ and $z=lx$. Subtracting gives $y-z=(k-l)x$, hence x divides $y-z$.

Theorem 11.11. *No natural number greater than one divides two consecutive 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 11.12. *If $d \in \{1,\dots,n\}$ then d does not divide $n!+1$.*

Proof: Suppose that $d \in \{1,\dots,n\}$. Then d divides $n!$, since $n! = n(n-1)\dots 1$. 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 paragraph proofs:

(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 induction.
(7) Still stuck? Try to break it down into cases.

Problem 11.13. Write paragraph proofs of the following statement.

(1) The sum of two odd integers is even.
(2) Any square number is not prime.
(3) There is no largest 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 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 $A\cup B\subset C$.

12. Relations

12.1. **Ordered pairs and relations.** 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 $b=b'$.

Problem 12.1. Find the components of the ordered pairs (1) $(1,(2,3))$ (2) $((1,2),3)$ (3) $(\{(1,2)\},3)$.

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 $A\times B$.

For example, 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 12.2. Find the Cartesian product of $\{apples, oranges\}$ with $\{frogs, grandmothers\}$.

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

A *relation* on A, B is a subset of $A \times B$. If $(a,b) \in R$, we write aRb for short. For example, if $R = \{(1,2),(1,3)\}$ then $1R2$ but $\neg(2R1)$.

For example, 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 $\exists z \in \mathbb{N}, x + z = y \wedge z \neq 0$. The relations $\geq$ and $>$ are defined similarly. Note that $\leq$ is a *subset* of $\mathbb{N} \times \mathbb{N}$, whose elements include $\{(0,0),(0,1),(1,1),(1,2),\ldots\}$.

Problem 12.3. Give a roster form of the relation (1) $\leq$ on the set $\{1,2,3\}$. (2) $<$ on the set $\{1,2,3\}$. (3) $x = y^2$ on the set $\{1,-1,2\}$.

Problem 12.4. True or false? Justify your answer.

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

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

Problem 12.5. (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 $xz \leq yz$.

Define a *divides relation* on $\mathbb{N}$ as follows. We say a *divides* b, or is a *divisor* of b, and write $a|b$ iff $\exists c, ac = b$ and say a is a divisor of b. For example, $2|4$ by $\neg(2|5)$. The divisors of 12 are $1,2,3,4,6,12$.

Problem 12.6. Prove that $\forall a,b,c \in \mathbb{N}, a|b \vee a|c \implies a|bc$, and $\forall a,b,c \in \mathbb{N}, a|b \wedge a|c \implies a|b+c$.

Here is a formal proof:

1	$a\|b \wedge a\|c$	hyp
2	$\exists k \in \mathbb{N}, ak = b \wedge \exists l \in \mathbb{N}, al = c$	1,def |
3	$ak = b \wedge al = c$	ei on 2
4	$ak + al = b + c$	arithmetic on 3
5	$a(k+l) = b + c$	distributive prop on 4
6	$\exists m, am = b + c$	eg 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.

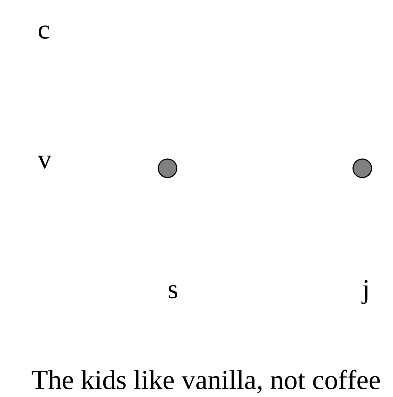


FIGURE 14. Graph form of "she likes that flavor"

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

A more serious example is the relation $R = \{(x,y), x^2 = y\}$ where the universe for x is $-2,-1,0,1,2$ and the universe for y is $0,1,4$.

Problem 12.7. Draw this relation in both forms.

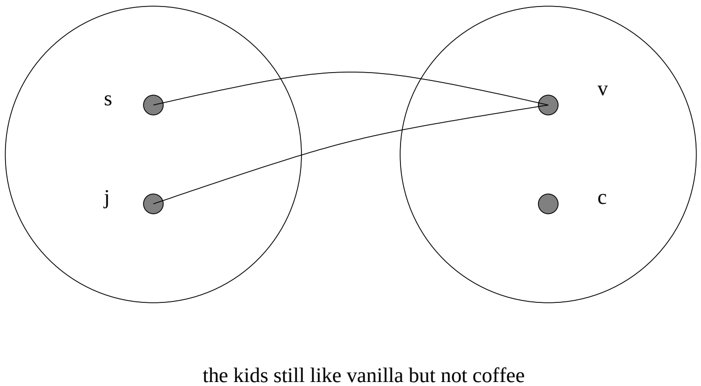


FIGURE 15. Arrow form of "she likes that flavor"

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

The *range* of a relation R is the set of b such that $(a,b) \in R$, or formally, $\mathrm{rng}(R) = \{b, \exists a, (a,b) \in R\}$.

For example, 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 12.8. Describe the domain and the 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 12.9. 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) $R = \{(apples, oranges),(apples, frogs)\}$.

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. For example, if $R = \{(1,3)(2,3)(2,5)\}$ then $R^{-1} = \{(3,1),(3,2),(5,2)\}$. 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.

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

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

For example, if $S = \{(1,3)(2,3)(2,5)\}$ and $R = \{(3,4),(4,5),(5,6)\}$ then $R \circ S = \{(1,4),(2,4),(2,6)\}$. In arrow form, this means that the arrows for $R \circ S$ are obtained by joining together the arrows for S and those for R, see Figure 16.

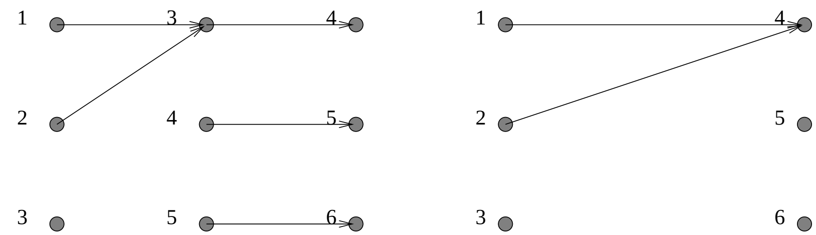


FIGURE 16. Composition of relations

Problem 12.10. (1) Let $R = \{(1,3)(2,3)(2,5)\}$ and $S = \{(3,4),(4,5),(5,6)$ Find $S \circ R$ and $S \circ S$. (2) Let $R = \{(1,3)(3,4)(2,5)\}$ and $S = \{(2,3),(4,5),(5,$ Find $S \circ R$ and $S \circ S$. (3) Let $R = \{(1,3)(2,5)\}$ and $S = \{(2,3),(5,6)\}$. Find $S \circ R$ and $S \circ S$.

Remark 12.11. Unfortunately there are two conventions for composition, depending on whether R or S is applied first. The other convention, $S \circ R = \{(a,c)|\exists b, aSb \wedge bRc\}$ 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 12.12. 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) $(R \circ S)^{-1}$

12.2. **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 12.13. 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 10. To start the proof of the first part, write

1	$R \neq R^{-1} \iff$	
	$\neg\forall(x, y), (x, y) \in \mathbb{R} \iff (x, y) \in R^{-1}$	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.

2	$R \neq R^{-1} \iff$	
	$\exists(x, y), \neg((x, y) \in R \iff (y, x) \in R)$	qc, def inverse on 1
3	$R \neq R^{-1} \iff \boxed{\exists(x, y), \neg(x\|y \iff y\|x)}$	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.

4	$\neg(2\|4 \iff 4\|2)$	arithmetic
5	$\exists(x, y), \neg(x\|y \iff y\|x)$	eg on 4
6	$R \neq R^{-1}$	mp on 3,5

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	$R \circ R \subseteq R \iff \forall(x, y)$	
	$(x, y) \in R \circ R \implies (x, y) \in R$	def subset
2	$(x, y) \in R \circ R$	temp hyp
3	$\exists z, (x, z) \in R \wedge (z, y) \in R$	def composition,2
4	$x\|z \wedge z\|y$	def R, ei on 3
5	$\exists k, xk = z \wedge \exists k, zk = y$	def divides
6	$xm = z \wedge zn = y$	ei on 5
7	$x(mn) = y$	algebra on 6
8	$\exists k, xk = y$	eg on 7, $k = mn$
9	$(x, y) \in R$	def divides, R
10	$(x, y) \in R \circ R \implies (x, y) \in R$	deduction 2-9
11	$R \circ R \subseteq R$	mp on 1,10

Problem 12.14. 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 12.15. 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 12.16. Prove that (i) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$, (ii) $R \circ (S \circ T) = (R \circ S) \circ T$.

Problem 12.17. Prove that $B \subseteq C \implies A \times B \subseteq A \times C$.

1	$B \subseteq C$	hyp
2	$B \subseteq C \iff (\forall x, x \in B \implies x \in C)$	def subset
3	$\forall x, x \in B \implies x \in C$	mp on 1,2
4	$(x, y) \in A \times B$	temp hyp
5	$(x, y) \in A \times B \iff (x \in A \wedge y \in B)$	def product
6	$x \in A \wedge y \in B$	mp on 4,5
7	$y \in B$	cs on 7
8	$y \in B \implies y \in C$	ui on 3
9	$y \in C$	mp on 7,8
10	$x \in A \wedge y \in C$	ci on 8,9
11	$(x, y) \in A \times C \iff (x \in A \wedge y \in C)$	def product
12	$x \in A \times C$	mp 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	$A \times B \subseteq A \times C$	mp on 13,14

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

Problem 12.18. 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	$(a, b) \in A \times \emptyset \iff a \in A \wedge b \in \emptyset$	def product
3	$b \in \emptyset \iff b \neq b$	def emptyset
4	$(a, b) \in A \times \emptyset \iff a \in A \wedge b \neq b$	sub 2,3
5	$a \in A \wedge b \neq b \iff (a, b) \neq (a, b)$	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	$A \times \emptyset = \emptyset$	mp on 1,7

Problem 12.19. Prove that if R is the relation defined by xRy iff $x - y \geq 2$, then $R \neq R^{-1}$.

Problem 12.20. Give formal proofs that

(1) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
(2) $((A \subseteq B) \wedge (C \subseteq D)) \Rightarrow (A \times C) \subseteq (B \times D)$.
(3) Prove that $(A = \emptyset \vee B = \emptyset) \iff (A \times B) = \emptyset$.

Problem 12.21. Give formal proofs that if S, R are relations in $A \times B$ and $B \times C$ respectively then

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

13. Functions

13.1. **Functions.** 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,

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

For example, $\{(1, 2), (2, 2), (3, 1)\}$ 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 is the genetic father of x$\}$ is a perfectly good function.

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 $a \in \mathrm{dom}(F)$, 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 $F = \{(x, y), y = x^2\}$ 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: $F =$ (George Bush,Dick Cheney),(Bill Clinton,Al Gore) is a function, while $G = \{$ (George Bush,Dick Cheney),(Bill Clinton,Al Gore), (Nixon, Agnew), (Nixon, Ford) $\}$ is not.[7] For the first function, we write F(Clinton) = 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 13.1. Which of the following are functions?

[7]The situation gets worse for F.D. Roosevelt, who had three vice-presidents.

(1) The relation from people to flavors defined by $F = \{$ (sophie,vanilla), (julia,vanilla) $\}$.
(2) The relation from people to flavors defined by $F = \{$ (sophie,vanilla), (julia, vanilla), (chris, vanilla), (chris,coffee) $\}$.
(3) $F = \{(x, y) \in \mathbb{N} \times \mathbb{N} | x|y\}$.
(4) $F = \{(x, y) \in \mathbb{N} \times \mathbb{N} | x|y \wedge y|x\}$.
(5) The relation F from $\mathbb{N}$ to $\{1, -1\}$ defined by $xF1$ iff $x + 1$ is divisible by 3, and $xF(-1)$ iff $x - 1$ is divisible by 3.

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.

Problem 13.2. Determine whether the following functions are injective resp. surjective resp. bijective.

(1) xFy iff y is the genetic father of y and A, B are the set of all people.
(2) xFy iff x has natural hair color y and y is the set of colors yellow, brown, blue.
(3) xFy iff y is the birthday of x, B is the set of days of the week, and A is the set of all people.

Problem 13.3. Determine whether the following functions are injective, surjective, or bijective. If they are not surjective, determine the range.

(1) $f(x) = x^2$ from $\mathbb{Q}$ to $\mathbb{Q}$
(2) $f(x) = x^3$ from $\mathbb{Q}$ to $\mathbb{Q}$
(3) $f(x) = x^3 + 3x^2 + 3x + 1$ from $\mathbb{R}$ to $\mathbb{R}$
(4) $f(x) = 2^x$ from $\mathbb{R}$ to $\mathbb{R}$
(5) $f(x) = 2^{x^2}$ from $\mathbb{R}$ to $\mathbb{R}$.

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

Problem 13.4. Show that the relation defined by $xFy \iff y = x^3$ is a function.

1	$\forall x, y, xFy \iff y = x^3$	hyp
2	F is a function iff $\forall x, y, z, xFy \wedge xFz \implies y = z$	def function
3	$xFy \wedge xFz$	temp hyp
4	$y = x^3 \wedge z = x^3$	ui, mp on 1,3
5	$y = z$	trans implies on 4
6	$\forall x, y, z, xFy \wedge xFz \implies y = z$	deduc on 3-5, ug
7	F is a function	mp on 2,6

Problem 13.5. Show that the function $F(x) = x^3$ is one-to-one.

1	$\forall x, F(x) = x^3$	hyp
2	F is 1-1 $\iff \forall x, y \in A$ $F(x) = F(y) \implies x = y$	def 1-1
3	$F(x) = F(y)$	temp hyp
4	$F(x) = x^3$	ui on 1
5	$F(y) = y^3$	ui on 1
6	$x^3 = y^3$	sub 4,5 in 3
7	$x = y$	cube root both sides of 6
8	$F(x) = F(y) \implies x = y$	deduc on 3-7
9	F is 1-1	ug on 8, mp on 2

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 $|xy| \le x^2 + y^2$, 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	$x^3 - y^3 = 0$	alg on 6
6.2	$(x^2 + xy + y^2)(x - y) = 0$	alg on 6.1
6.3	$x - y = 0 \vee x^2 + xy + y^2 = 0$	since $ab = 0 \implies a = 0 \vee b = 0$
6.4	$x^2 + xy + y^2 > 0$	since $xy < x^2 + y^2$
6.5	$x - y = 0$	di on 6.3,6.4

Of course, this still uses facts about numbers we haven't talked about very much yet.

Problem 13.6. Show that

(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 composable functions then $F \circ G$ is also a function.

Problem 13.7. (1) Find a function from $\{1,2,3\}$ to itself such that all of the following conditions are satisfied: (i) f is a bijection (ii) $f^{-1} = f$ (iii) $f(1) = 2$.
(2) Find a function from $\{1,2,3\}$ to itself such that all of the following conditions are satisfied: (i) $f^{-1}(\{1,2\}) = \{2,3\}$ and $f(f^{-1}(\{1,2\})) \neq \{1,2\}$.
(3) Find a function f from $\mathbb{R}$ to $\mathbb{R}$ satisfying $f^2 = f$ and f is not the identity or a constant function.
(4) Find an injection from $\mathbb{Q}$ to $\mathbb{R} - \mathbb{Q}$.
(5) Find a bijection from $\mathbb{R}$ to $(0,\infty)$.
(6) Find a bijection from $\mathbb{R}$ to $(0,1)$.
(7) Find a bijection from $\mathbb{Q}$ to $(0,\infty) \cap \mathbb{Q}$.

Problem 13.8. 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 $g \circ f$.
(3) For any functions $f : A \to B$ and $g : B \to C$, if f and g are surjective then so is $g \circ f$.

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

The *pre-image* of a value b of f is the set $f^{-1}(b) = \{a, f(a) = b\}$. Somewhat confusingly, $f^{-1}(b)$ is a subset of A while $f(a)$ is an element of 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 $f^{-1}(B) = \{a | f(a) \in B\}$.

Example 13.9. 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 13.10. 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 13.11. (i) Find the domain and range of the relation $R = \{(1,2),(2,2),(5,6),(7,6)\}$. (ii) Find its inverse R^{-1}. (iii) Determine whether R, R^{-1} are functions. (iv) Find the pre-image of 2 under R and under R^{-1}. (v) Find the compositions $R \circ R^{-1}$ and $R^{-1} \circ R$.

13.3. **Sequences.** A *finite sequence of integers* of length k is a function F from $\{1,\ldots,k\}$ to $\mathbb{Z}$. 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 first and third examples 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 13.12. $n_1,\ldots,n_k$ is a arithmetic resp. geometric sequence iff $\exists r, \forall k, n_{k+1} = n_k + r$ resp. $\exists r, \forall k, n_{k+1} = r n_k$.

Problem 13.13. 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 13.14. Prove that the (i) sum of arithmetic (ii) product of geometric sequences is also an arithmetic reps. geometric sequence.

A *permutation sequence* is a reordering of the sequences $1,2,3,4,\ldots,k$. For example, $3,2,1,4$ is a permutation sequence of length 4.

Problem 13.15. Fill in the blanks to write a definition of permutation sequence which uses only symbols and quantifiers: $n_1,\ldots,n_k$ is a permutation sequence iff __________, $1 \leq n_i \leq k \wedge \forall i,j,$ __________ $\implies n_i \neq n_j$.

The product of elements of a sequence is written $m = n_1 \cdot n_2 \cdot \ldots \cdot n_k$, and this expression is called a *factorization* of m. We say two factorizations are *equivalent* if one is obtained by the other by re-ordering. For example $30 = (2)(3)(5)$ and $(5)(3)(2)$ are equivalent factorizations.

Problem 13.16. Fill in the blanks to write a definition of equivalent factorizations using quantifiers.

Answer: $m = a_1 \dots a_k$ and $m = b_1 \dots b_l$ are equivalent factorizations iff _______ $n_1, \dots, n_k, n_1, \dots, n_k$ is a permutation sequence $\wedge$_______ $, 1 \leq i \leq k \implies a_i = b_{n_i}$.

Problem 13.17. Which of the following are factorizations of the given number?

(1) $1000 = (10)(10)(10)$.
(2) $0 = (10)(0)$.
(3) $0 = 0(10)$.
(4) $30 = (2)(3)(5)$.
(5) $30 = (5)(3)(2)$.
(6) $30 = (5)(3)(2)(-1)(-1)$.

Problem 13.18. Show that any strictly increasing sequence is injective.

14. Operations

14.1. **Definition of an operation.** An *operation* on a set S is a function $S \times S \to S$. For example, $\{((1,1),1),((1,2),2),((2,1),2),((2,2),2)\}$ 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.

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 $f(x,y) = f(y,x) = e$.

14.2. **Examples of operations.**

14.2.1. *Addition and multiplication.* Addition

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (x,y) \mapsto x + y$$

and 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 14.1. For f equal to (a) addition and (b) multiplication find three elements of f.

14.2.2. *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.

14.2.3. *Minimum and maximum.* The *minimum* and *maximum* of two natural numbers a, b are the operations defined by

$$a \leq b \implies \min(a,b) = a \wedge \max(a,b) = b$$

$$b \leq a \implies \min(a,b) = b \wedge \max(a,b) = a.$$

Problem 14.2. Show that

(1) $\min(\min(a,b),c)) = \min(a,\min(b,c))$.
(2) $\min(a,b)\max(a,b) = ab$.
(3) $\min(a,b) + \max(a,b) = a + b$.

Problem 14.3. Show that 0 is a unit for the min operation. Show that 0 is the only invertible element for min. Show that max does not have a unit.

14.2.4. *And and Or.* Let S be the set of all propositional forms. Then conjunction

$$\wedge : S \times S \to S, (P,Q) \mapsto P \wedge \ Q$$

is an operation on S. Similarly $\vee$ and $\Rightarrow$ are operations on S. For example, some elements of $\wedge$ are $((P,Q),P \wedge Q),((P \vee S,Q),(P \vee S) \wedge Q)$.

Problem 14.4. Which of the following are elements of $\vee$? (a) $((P,Q),P \vee Q)$, $((P \Rightarrow S,Q)$, (b) $(P \Rightarrow S) \vee Q)((P,Q \Rightarrow P)$, (c) $(P \vee Q) \Rightarrow P)$.

Problem 14.5. Which of $\wedge, \vee, \Rightarrow$ are commutative? associative?

14.2.5. *Composition.* The *composition* of relations is an operation on relations:

$$\mathrm{Rel}(S,S) \times \mathrm{Rel}(S,S) \to \mathrm{Rel}(S,S), \quad (f,g) \mapsto f \circ g.$$

The identity relation $\{(x,x) | x\ inS\}$ is an identity. A relation is invertible if and only if it is a bijection. A *permutation* of a set S is a bijection from S to itself. The set of permutations is denoted $\mathrm{Perm}(S)$.

Example 14.6. $\{(1,3),(2,1),(3,2)\}$ is a permutation of $\{1,2,3\}$. $\mathrm{Perm}(\{1,2\}) = \{\{(1,1),(2,2)\},\{(2,1),(2,1)\}$.

Problem 14.7. List all elements of $\mathrm{Perm}(\{1,2,3\})$.

Problem 14.8. 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) $f(x) = x$, if x is odd, or $f(x) = x+2$, if x 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 14.9. $(123)(4)$ 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 $\mathrm{Perm}(S)$. Indeed, if f and g are permutations then f and g are bijections from S to itself. By Problem 13.8, so is $f \circ g$. Hence $f \circ g$ is a permutation of S.

Problem 14.10. 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 under the first and then 1 under the second. Hence the composition is (132).

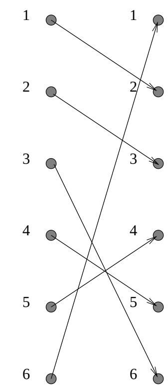


FIGURE 17. The permutation $(1236)(45)$

Problem 14.11. 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 14.12. Find all commutative operations on the set $\{1,2\}$ with $f(1,2) = f(1,1) = 1$.

Answer: Since f is commutative $f(1,2) = f(1,1) = 1$ 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 14.13. 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	$\forall x,y, xy+3 = yx+3$	ug on 5
7	f is commutative	mp on 6,3

Problem 14.14. Find an operation that is associative but not commutative.

15. Equivalence Relations and partitions

15.1. **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 15.1. A relation R is

(1) *transitive* iff $\forall a, b, c, aRb \wedge bRc \implies aRc$
(2) *symmetric* iff $\forall a, b aRb \iff bRa$.
(3) *reflexive* iff $\forall a, aRa$.

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.

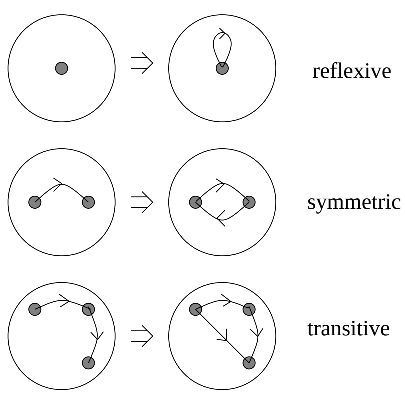


Figure 18. Three properties relations can have

A relation R is an *equivalence relation* if R is transitive, symmetric, and reflexive.

Problem 15.2. 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 15.3. 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 15.4. Consider the relation on $A = \{1\}$ given by $R = \{(1, 1)\}$. Determine whether R is (i) reflexive, (ii) symmetric, (iii) transitive.

Problem 15.5. Prove that if R is a transitive and symmetric relation on S and $\mathrm{dom}(R) = S$ then it is R reflexive, hence an equivalence relation.

Define a relation on $\mathbb{Z}$ as follows.

Definition 15.6. 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 15.7. $2 \equiv_2 4 \equiv_2 6 \equiv_2 8 \ldots$ and $1 \equiv_2 3 \equiv_2 5 \equiv_2 7$. $2 \equiv_{10} 12$ but $\neg(2 \equiv_9 12)$.

Problem 15.8. (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 15.9. Show that

(1) $a \equiv_6 b \implies a \equiv_2 b \wedge a \equiv_3 b$.

(2) $a \equiv_9 b \implies a \equiv_3 b$.

Problem 15.10. Show that $\equiv_k$ is an equivalence relation on $\mathbb{Z}$.

Here is the beginning of the 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 $\forall x \in Z, x \equiv_k x$	def reflexive
3	$x \equiv_k x \iff k \mid (x - x)$	def $\equiv_k$
4	$x - x = 0$	def minus
5	$k \mid 0$	easy
6	$x \equiv_k x$	mp, sub 3,4,5
7	$\equiv_k$ is reflexive	ug, mp on 6,2

Remark 15.11. A common error in the above proof is to assume what you are trying to show. That is, you cannot write on line 2 "$\equiv_k$ is reflexive" and then translate what that means on the next line, because you do not know yet that $\equiv_k$ is reflexive.

Problem 15.12. Prove that if R, S are equivalence relations on A, then so is $R \cap S$.

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,

$$\overline{a} = \{b \in A, bRa\}.$$

For example 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 15.13. 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 15.14. 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.

Problem 15.15. Suppose that R is the equivalence relation on $A = \{10, \ldots, 15\}$ given by aRb if a and b have the same number of divisors. Find the equivalence classes of R.

Hint: one of the equivalence classes $\{10, 15\}$. There are two more.

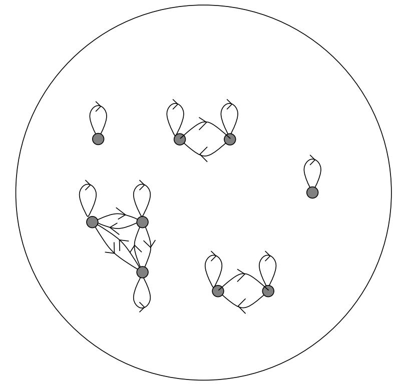


FIGURE 19. Relation with five equivalence classes

Problem 15.16. Give a (a) formal proof and (b) paragraph proof that $\overline{a} = \overline{b} \iff aRb$.

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).*

1	$\overline{a} = \overline{b}$	temp hyp
2	$\forall c, c \in \overline{a} \iff c \in \overline{b}$	def set equality
3	aRa	reflexive prop
4	$\forall b, aRb \iff b \in \overline{a}$	def equiv class
5	$aRa \iff a \in \overline{a}$	ui
6	$a \in \overline{a}$	mp on 3,5
7	$a \in \overline{a} \iff a \in \overline{b}$	ui on 2
8	$a \in \overline{b}$	mp on 7, 6
9	aRb	def of equiv class, mp on 8
10	$\overline{a} = \overline{b} \implies aRb$	deduc on 1-9
11	aRb	temp hyp
12	$c \in \overline{a}$	temp hyp
13	cRa	def of equiv class, mp
14	cRb	transitivity on 11,13
15	$c \in \overline{b}$	def of equiv class, mp

16	$\overline{a} \subseteq \overline{b}$	deduc on 12-15
17	$aRb \implies \overline{a} \subseteq \overline{b}$	deduc on 11,16
18	$aRb \implies \overline{b} \subseteq \overline{a}$	same reasoning
19	$aRb \implies \overline{a} = \overline{b}$	ci on 17,18, def of equality
20	$aRB \iff \overline{a} = \overline{b}$	ci on 10,19

Notice that near the end I got a little bit exhausted and wrote out only some of the steps.

15.2. **Partitions.**

Definition 15.17. Let A be a set. A *partition* of A is a set $\mathcal{S}$ of subsets $S \subseteq A$ such that each each element of A occurs in exactly one element S of $\mathcal{S}$. That is,

(1) Any two elements of $\mathcal{S}$ are disjoint or equal: $S_1, S_2 \in \mathcal{S} \implies S_1 = S_1 \vee S_1 \cap S_2 = \emptyset$. (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 $\mathcal{S}$ is A, that is,

$$\bigcup_{S \in \mathcal{S}} S = A$$

. (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 { { Cheney, Biden }, { Bush, Obama } } is a partition of { Cheney, Biden,Bush,Obama } (into the subsets of vice-presidents and presidents.)

The notation $\cup_{S \in \mathcal{S}} S$ means *the union of elements of* $\mathcal{S}$. It is similar to the sum or product notation.

Example 15.18.

$$\bigcup_{S \in \{\{1\},\{2,3\},\{4\}\}} S = \{1\} \cup \{2, 3\} \cup \{4\} = \{1, 2, 3, 4\}.$$

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 15.19. List all partitions of

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

Problem 15.20. Show that if R is an equivalence relation, then the set $\mathcal{S}$ of equivalence classes of R is a partition of S.

Here is a paragraph proof. Suppose that R is an equivalence relation, and that $\mathcal{S}$ is the set of equivalence classes. We claim that $\mathcal{S}$ 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 $\exists S \in \mathcal{S}, a \in S \wedge b \in S$.

Answer to (1a): $R = \{(1, 1), (1, 3), (3, 3), (3, 1), (2, 2), (2, 5), (5, 2), (5, 5)\}$.

Problem 15.21. If $\mathcal{S}$ is a partition of A, then the relation defined R defined by aRb if $\exists S \in \mathcal{S}, a \in S \wedge b \in S$ is an equivalence relation.

Here is the start of a formal proof.

1	$\mathcal{S}$ is a partition of A.	hyp
2	$\forall a, b, aRb \iff \exists S \in \mathcal{S}, a \in S \wedge b \in S$	hyp
3	R is an equiv reln iff R is refl, symm, and tran	def equiv reln
4	R is refl iff $\forall a \in A, aRa$	def reflexive
5	$a \in A$	hyp
6	$\exists S \in \mathcal{S}, a \in S$	def partition
7	$\exists S \in \mathcal{S}, a \in S \wedge a \in S$	ei, ci, eg on 6
8	$\forall a \in A, aRa$	ui, mp,ug on 2,7
9	R is reflexive	mp on 4,8

The previous two problems show the following:

Theorem 15.22. *There is a one-to-one correspondence between equivalence relations on a set A and partitions of A.*

Problem 15.23. 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) $\mathcal{S} = \{\{1, 3\}\{2, 5\}\}$.
(2) $\mathcal{S} = \{\{1, 2, 3\}\{2, 4, 5\}\}$.
(3) $\mathcal{S} = \{\{1, 2, 3\}\{4, 5\}\}$.

15.3. **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 S has cardinality k if S is equivalent to the set $\{1, \ldots, k\}$. We say that S is *finite* if S has cardinality k for some $k \in \mathbb{N}$. Then the *order* $|S|$ of S is k.

Problem 15.24. 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) $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{x | x \neq x\}\}$.
(6) $\{x | x \in \mathbb{N} \wedge 0 \leq x \leq 5\}$
(7) $\{(x, y) | x \in \mathbb{N} \wedge y \in \mathbb{N} \wedge x + y \leq 4\}$
(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 15.25. *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 15.26. Prove that $S = \{n \in \mathbb{N}, 2n + 1 \leq 10\}$ 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 15.27. Prove that the set of prime numbers less than 10 has order 4.

Problem 15.28. Prove that the relation $\sim$ given by the existence of a bijection is an equivalence relation.

Problem 15.29. 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) $|\operatorname{Fun}(A, C)| = |\operatorname{Fun}(B, D)|$,
(3) $|\mathcal{P}(A)| = |\mathcal{P}(B)|$.

Problem 15.30. 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) $|\operatorname{Fun}(A, B)| = |B|^{|A|}$. (this is the set of functions from A to B.)
(4) $|\operatorname{Perm}(A, A)| = |A|!$. (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. To show that F is onto, note that any $z \in \mathbb{N}$ with $z \leq kl - 1$ can be written as $lx + y$ for some $y \in \mathbb{N}$ with $y \leq l-1$, by the remainder theorem. To show that F is 1-1, note that 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.

Proof of (ii): First we consider the case that A and B are disjoint. Let $|A| = k$ and $|B| = l$. So there exist bijections $f : A \to \{0,\ldots,k-1\}$ and $g : B \to \{0,\ldots,l-1\}$. Define $h : A \cup B \to \{0,\ldots,l+k-1\}$ by $h(x) = f(x)$ if $x \in A$ and $h(x) = g(x) + l$ if $x \in B$. Since $A \cap B = \emptyset$, f is a well-defined function. Then h is injective, since f and g are. To show that h is onto, note that any $y \in \{0,\ldots,l+k-1\}$ is either in the image $\{0,\ldots,k-1\}$ or in $\{k,\ldots,l+k+1\}$, in which case, it is of the form $k + g(x)$ for some $x \in B$. Hence h is surjective.

In case A, B not disjoint, we have $B = (A \cap B) \cup (B - A)$. By the disjoint case, $|A \cup B| = |A \cup (B-A)| = |A| + |B-A|$ and $|B| = |A \cap B| + |B-A|$ so $|A \cup B| = |A \cup (B-A)| = |A| + |B| - |A \cap B|$.

16. Natural numbers and induction

16.1. **The induction axiom.** We have already made the following assumptions on natural numbers:

Assumption 16.1. There exists a set $\mathbb{N} = \{0,1,2,\ldots\}$ of natural numbers equipped with operations of addition

$$\mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (n,m) \mapsto n+m.$$

and multiplication

$$\mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (n,m) \mapsto nm.$$

satisfying the axioms in Assumption 20.1.

By definition $2 = 1+1$, $3 = 2+1$, $4 = 3+1, \ldots, 10 = 9+1$. Given a string of digits $d_k \ldots d_1$, the corresponding number is by definition

$$d_k 10^k + d_{k-1} 10^{k-1} + \ldots + d_0.$$

Here is a hopefully easy example of a proof involving natural numbers.

Problem 16.2. Prove that $2+2=4$.

Answer:

1	$2 = 1+1$	def of 2
2	$2+2 = 2+(1+1)$	subst
3	$2+(1+1) = (2+1)+1$	assoc prop
4	$3 = 2+1$	def of 3
5	$2+(1+1) = 3+1$	subst 3,4
6	$4 = 3+1$	def of 4
7	$2+2 = 4$	transitivity of = on 3,5,6

Problem 16.3. Prove that (a) $3+3=6$ (b) $2+3=5$ (c) $2(2)=4$.

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 20. 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:

1	$P(n) \iff 1 + \ldots + n = n(n+1)/2$	hyp
2	$P(1) \iff 1 = 1(2)/2$	subst in 1
3	$1 = 1$	equality axiom
4	$P(1)$	mp on 4,2

FIGURE 20. $1+2+3+4+5 = 5(6)2$

5	$P(n)$	ind hyp
6	$1+\ldots+n = n(n+1)/2$	mp on 1,5
7	$1+\ldots+n+(n+1) = n(n+1)/2+(n+1)$	arith on 6
8	$1+\ldots+(n+1) = (n+1)(n/2+1)$	distrib on 7
9	$1+\ldots+(n+1) = (n+1)(n+2)/2$	arith on 8
10	$P(n+1)$	subst on 1, mp
11	$P(n) \implies P(n+1)$	deduc on 5-10
12	$\forall n \geq 1, P(n)$	induc on 4,11
13	$\forall n \geq 1, 1+\ldots+n = n(n+1)/2$	subst on 12,1

Problem 16.4. (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) $P(1) \iff 1 = 1^2$.

Problem 16.5. (From [2]) Using induction prove the following statements:

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

Problem 16.6. Prove that if 2^n-1 is prime then n is prime.

Problem 16.7. 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.

1	$P(n) \iff (2\|n \vee 2\|(n-1))$	hyp
2	$2\|0$	arith
3	$P(0)$	subst, di on 1,2
4	$P(n)$	ind hyp
5	$(2\|n) \vee (2\|(n-1))$	mp on 1
6	$2\|n$	temp hyp
7	$2\|((n+1)-1)$	arith on 6
8	$2\|n \implies 2\|((n+1)-1)$	deduc on 6,7
9	$2\|(n-1)$	temp hyp
10	$\exists l, 2l = n-1$	def $\|$
11	$2l = n-1$	ei on 10
12	$2l+2 = n+1$	arith on 11
13	$2(l+1) = n+1$	arith on 12
14	$\exists k, 2k = n+1$	ei on 13
15	$2\|n+1$	def $\|$, 14
16	$(2\|n-1) \implies (2\|n+1)$	ded on 9-15
17	$(2\|n \vee 2\|n-1) \implies ((2\|(n+1)-1) \vee (2\|n+1))$	ic, di on 8,16
18	$(2\|(n+1)-1) \vee (2\|n+1)$	deduc on 6-17
19	$P(n+1)$	subst on 18
20	$P(n) \implies P(n+1)$	ded on 4-19
21	$\forall n \geq 0, P(n)$	induc on 2-20
21	$\forall n \geq 0, 2\|n \vee 2\|n-1$	subst on 1,21

Problem 16.8. Write out the previous proof in paragraph proof 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 16.9. 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) $5|4^{2n} - 1$
(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) $m < 2^n$
(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	$P(1)$	ui, mp 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	$4^{n+1} + 15(n+1) - 1 = 4(4^n + 15n + 1) - 45n + 18$	arith on 7
9	$9\|45n + 18$	arith
10	$9\|4(4^n + 15n + 1) - 45n + 18$	$x\|y \wedge x\|z \implies x\|y+z$
11	$P(n+1)$	mp 10, 6
12	$P(n) \implies P(n+1)$	deduc 4-11
13	$P(1) \wedge \forall n, P(n) \implies P(n+1)$	ci, ug 2,12
14	$\forall n, n \geq 1 \implies P(n)$	induc on 13

Problem 16.10. (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 16.11. 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 16.12. 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 16.13. 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 2×2 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 16.14. *(Well-ordering principle): any non-empty subset of* $\mathbb{N}$ *has a smallest element:*

$$\forall S, S \subseteq \mathbb{N} \wedge S \neq \emptyset \implies \exists s \in S, \forall s' \in S, s' \geq s.$$

Problem 16.15. Using the well-ordering principle prove that $\forall n \geq 1$,

(1) $3|4^n - 1$
(2) $4|5^h - 1$
(3) $5|4^{2n} - 1$
(4) $3|n^3 + 5n + 6$
(5) $2|3n^2 + 5n$.

Here is the answer to (a), in paragraph 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.

16.2. **The remainder theorem and base representation.** Using induction we prove the important

Theorem 16.16. *(Remainder Theorem) Let b be a positive natural number. Any natural number n has a unique remainder r modulo b, that is,*

$$\forall n \in \mathbb{N}, \exists! l, r \in \mathbb{N}, n = bl + r \wedge 0 \leq r < b.$$

Example 16.17. $5 = 2(2) + 1$ so 1 is the remainder of 5 mod 2. 111 has remainders 1 (mod 10) and 11 mod 10.

The proof is somewhat long to write out in two-column format, so here it is in paragraph form. Fix $k \in \mathbb{N}$ and let $P(n)$ be the statement $\exists l, r \in \mathbb{N}, n = kl + r \wedge 0 \leq r \leq k - 1$. 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 deduction. 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 $l = l'$.

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 Arabic system) is

$$n = \sum_{j=0}^{k} d_j 10^j.$$

For example, by 321, that is the sequence if digits $d_2 = 3, d_1 = 2, d_0 = 1$ qwe 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 $b_k 2^k + \ldots + b_0$.

For example, 1101 in base 2 is the number 13 in base 10. Conversely, 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:

$$\begin{aligned} 27 &= 1(16) + 9 \\ 9 &= 1(8) + 1 \\ 1 &= 0(4) + 1 \\ 1 &= 0(2) + 1 \\ 1 &= 1(1). \end{aligned}$$

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 16.18. Find the

(1) decimal representation of the binary number 11111
(2) binary representation of the binary number 100
(3) hexadecimal representation of the decimal number 1024.
(4) decimal representation of the hexadecimal number $10A$.

Theorem 16.19. *For any base b, there is a bijection ρ_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, $r = \rho_k(n_0, \ldots, n_{k-1})$ 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. $\square$

16.3. **The Peano axioms.** The axioms for natural numbers we gave in Assumption 20.1 are very redundant. Peano introduced a much smaller axioms for the natural numbers $\mathbb{N}$, the first of which is the induction axiom.

Assumption 16.20 (Peano Axioms)**.** There is a set $\mathbb{N}$ equipped with a *successor function* $S : \mathbb{N} \to \mathbb{N}, n \mapsto n+1$ and a distinguished element $0 \in \mathbb{N}$ so that

$\forall n \in N, S(n) \neq 0$	(Zero is not a successor of anything)
$S(n) = S(n') \implies n = n'$	(Cancellation Property)
$(P(0) \wedge \forall n \in \mathbb{N}, P(n) \implies P(n+1)) \implies \forall n \in N, P(n)$	(Induction)

From this, addition, multiplication can be defined and their properties can all be deduced. Addition is defined by

$\forall x, x + 0 = 0 + x = x$	(Zero is an additive identity)
$S(x) + y = x + S(y) = S(x + y)$	(recursive definition)

Multiplication is defined by

$\forall x, x0 = 0x = 0$	
$S(x)y = xy + y, xS(y) = xy + x$	(recursive definition)

Inequality is defined by $a \leq b \iff \exists c, a + c = b$.

Problem 16.21. 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 $P(b) \implies P(b+1)$. By induction, $\forall b \in P(b)$, that is, $\forall b \in \mathbb{N}, a+b = b+a$.

Problem 16.22. Write the previous proof in two-column format, using only symbols.

Problem 16.23. 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:

Problem 16.24. Prove the Herbrand-Tarski Theorem 6.1.

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 $((S \implies R_i) \wedge (S \implies (R_i \implies T))) \implies (S \implies T)$ 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 16.25. Prove that for any positive integer c and integers a, b, $ab = c \wedge a \neq c \wedge a \neq 1 \iff ab = c \wedge a \neq 1 \wedge b \neq 1$.

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 20.1 (9), either $c = 0$ or $b = 1$. But $c \neq 0$ by assumption so $b = 1$, which completes the proof.

17. Limits

17.1. **The definition of a limit.** Let S be a set. An *infinite sequence* is a function $f : \mathbb{N} \to S$. 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. A *two-sided infinite sequence* is a function $f : \mathbb{Z} \to S$, for example, $\ldots, 4, 2, 1, 1/2, 1/4, \ldots$.

Suppose that f_n, g_n are sequences of numbers. The *sum* of f and g is the sequence $(f+g)_n = f_n + g_n$. The *product* of f and g is the sequence $(fg)_n = f_n g_n$.

Example 17.1. The sum resp. product of $1, 2, 4, 8, \ldots$ with $1, 1/1, 1/4, \ldots$ is $2, 3, 17/4, \ldots$ resp. $1, 2, 1, 8/5, \ldots$.

Problem 17.2. 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 $1, 1/2, 1, 1/3, 1, 1/4, \dots$ 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 $1/4, 1/3, 1/6, 1/5, 1/8, 1/7, \dots$ is approaching 0, even though it goes up and down alternatively. Here is the official definition:

Definition 17.3. 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 and call f_n a *convergent sequence*.

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 21.

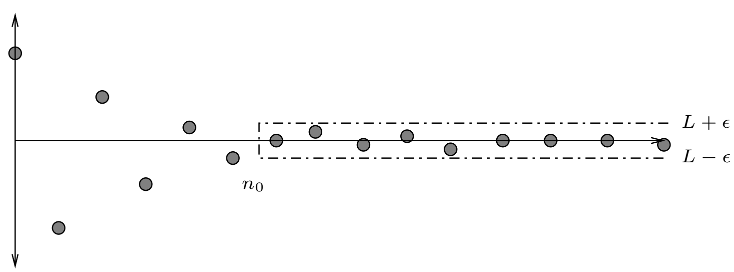


FIGURE 21. Definition of limit

Problem 17.4. Which of the following sequences have limits? In each case where the limit exists, identify the limit.

(1) $1, 1, 1, 0, 0, 0, 0, 0, \dots$
(2) $0, 1, 2, 3, 4, \dots.$
(3) $1, 1/2, 1/3, 1/4, 1/5, \dots.$
(4) $1, -1/2, 1/3, -1/4, 1/5, \dots.$
(5) $1, -1, 1, -1, 1, -1, \dots.$

Problem 17.5. Prove that the sequence f given by

(1) $1/2, 2/3, 3/4, 4/5, \dots$
(2) $3/2, 4/3, 5/4, 6/5, \dots$
(3) $2^{3/2}, 2^{4/3}, 2^{5/4}, 2^{6/5}, \dots$

has a limit, equal to 1 for the first two cases and 2 for the last.

Here is an answer to the first part.

1	$\lim_{n\to\infty} f_n = 1 \iff \forall \epsilon \in \mathbb{Q}_+, \exists n_0 \in \mathbb{N}$, $n \geq n_0 \implies |f_n - 1| < \epsilon$	def limit
2	$f_n = (n-1)/n$	def f
3	$|f_n - 1| = 1/n$	arith 2
4	$|f_n - 1| < \epsilon \iff n > 1/\epsilon$	sub 3
5	$n > 1/\epsilon \implies |f_n - 1| < \epsilon$	cs on 4
6	$\exists n_0, n_0 > 1/\epsilon$	fact
7	$\exists n_0 \in \mathbb{N}, n > n_0 \implies |f_n - 1| < \epsilon$	5,6
8	$\forall \epsilon \in \mathbb{Q}_+, \exists n_0 \in \mathbb{N}, (n \geq n_0) \implies (|f_n - 1| < \epsilon)$	ug 7
9	$\lim_{n\to\infty} f_n = 1$	mp 1,8

Problem 17.6. Suppose we were to define limit as

(1) $\lim^{\text{new}}_{n\to\infty} f_n = L \iff (\exists n_0 \in \mathbb{N}, \forall \epsilon \in \mathbb{Q}_+, n \geq n_0 \implies |f_n - L| < \epsilon)$.
(2) $\lim^{\text{newer}}_{n\to\infty} f_n = L \iff (\forall \epsilon \in \mathbb{Q}_+, \exists n_0 \in \mathbb{N}, |f_n - L| < \epsilon \implies n \geq n_0)$.
(3) $\lim^{\text{newest}}_{n\to\infty} f_n = L \iff (\exists n_0 \in \mathbb{N}, \forall \epsilon \in \mathbb{Q}_+, |f_n - L| < \epsilon \implies n \geq n_0)$.

Which of the sequences in the Problem 17.4 converge for each of these definitions?

17.2. **Properties of Limits.**

Problem 17.7. 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 $L + M$.

Problem 17.8. Show that limits are unique: If f_n converges to both L and M then $L = M$.

Theorem 17.9. *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 $n \geq n_0$.

17.3. **Bounded sequences.**

Definition 17.10.
(1) A sequence f_n is *bounded from above* iff there exists a a constant C such that $\forall n \in \mathbb{N}, f_n < C$.
(2) A sequence f_n is *bounded from below* iff there exists a a constant C such that $\forall n \in \mathbb{N}, f_n > C$.
(3) A sequence f_n is *bounded from above and below* iff there exists a constant C such that $\forall n \in \mathbb{N}, |f_n| < C$.

Problem 17.11. Show that the sequence $\sin(n)$ is bounded.

Answer: Let $C = 2$. Then for any n, $|\sin(n)| \leq 1$ since $sin(n)$ is the adjacent side of a triangle with hypotenuse 1 with side lengths $\sin(n), \cos(n)$ satisfying $\sin^2(n) + \cos^2(n) = 1$. So $|\sin(n)| < 2$ for all n, which shows that $\sin(n)$ is bounded.

Theorem 17.12.
(1) *The sum of two bounded sequences is bounded.*
(2) *The product of two bounded sequences is bounded.*
(3) *Any convergent sequence is bounded.*
(4) *(Hard) Any bounded sequence has a convergent subsequence.*

Here is a proof of the first item. Suppose that f_n and g_n are bounded sesquences. Then there exist constants $c, d > 0$ such that forall $n \in \mathbb{N}$, $|f_n| < c$ and $|g_n| < d$. Then $|f_n + g_n| \leq |f_n| + |g_n| < c + d$ for all $n \in \mathbb{N}$. So $f_n + g_n$ is bounded.

17.4. **Infinite Sums.** 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 17.13. *If $|x| < 1$ then $\sum_{i=0}^{\infty} x^i = 1/(1-x)$.*

Proof. By the geometric series identity Problem 16.5 (d),

$$\begin{aligned} \lim_{n \to \infty} \sum_{i=1}^{n} f(n) &= \lim_{n \to \infty} \frac{1 - x^{n+1}}{1 - x} \\ &= \frac{1 - \lim_{n \to \infty} x^{n+1}}{1 - x} \\ &= \frac{1}{1 - x} \end{aligned}$$

using Theorem 17.7. □

Let f be a function from $\mathbb{R}$ to $\mathbb{R}$.

Definition 17.14. Let $a, b \in \mathbb{R}$. We say that $\lim_{x \to a} f(x) = b$ iff $\forall \epsilon > 0, \exists \delta > 0$ such that $|a - x| < \delta \implies |b - f(x)| < \epsilon$.

Problem 17.15. 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) $\forall x, f(x) = x^2 \implies \forall a, \lim_{x \to a} f(x) = a^2$.

17.5. **Base representations of rational numbers.** Using our notion of limit we define what we mean by expressions such *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 17.16. 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 17.17. Find the decimal expansion of $1/6$ by long division.

Answer: The decimal expansion keeps repeating, so we write $.1\overline{6}$, a bar

$$
\begin{array}{r|l}
 & .166666 \\
\hline
6 & 1 \\
 & \underline{.6} \\
 & .4 \\
 & \underline{.36} \\
 & .04 \\
 & \underline{.036} \\
 & .004
\end{array}
$$

over the 6 to indicate the repeating pattern.

Example 17.18. 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 17.19. Find the decimal expansion of $9/7$.

Problem 17.20. Prove that the $.1\overline{6}$ is a decimal expansion of $1/6$.

1	$.1\overline{6}$ is an expansion of $1/6$ iff $\lim_{n\to\infty} 1/10 + \sum_{d=2}^{n} 6(10)^{-d} = 1/6$	def expansion
2	$\lim_{n\to\infty} 1/10 + \sum_{d=2}^{n} 6(10)^{-d} = 1/6$ iff $\forall m, \exists n_0, n \geq n_0 \implies$ $\lvert 1/6 - 1/10 + \sum_{d=2}^{n} 6(10)^{-d} \rvert 1/m$	def limit
3	$6(1/6 - 1/10 + \sum_{d=2}^{n} 6(10)^{-d})$ $= 1 - 6/10 - \sum_{d=2}^{n} 36(10)^{-d})$	arith
4	$= 410^{-n-1}$	arith
5	$1/6 - 1/10 + \sum_{d=2}^{n} 6(10)^{-d}) < 10^{-n}$	arith
6	$\exists n_0, n \geq n_0 \implies \lvert 1/6 - 1/10 +$ $\sum_{d=2}^{n} 6(10)^{-d} \rvert 1/m$	def limit
7	$.1\overline{6}$ is an expansion of $1/6$ iff	

Let's prove that the decimal expansion of a/b is eventually repeating. To find the first digit base n, we write

$$na = bq_1 + r_1.$$

Then $a/b = q_1/n + r_1/nb$ and $r_1/nb < 1/n$ so q_1 is then the first digit of the expansion. Then we write

$$nr_1 = bq_2 + r_2$$

so q_2 is the second digit, and so on. Each remainder is between 0 and $b-1$, so eventually the remainders do repeat. A similar discussion for arbitrary base b shows that

Theorem 17.21. *(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.*

In practice, the size of the repeating pattern tends to be much smaller. Conversely, given an eventually-repeating decimal expansion we can find the rational number by multiplying by a power of ten and subtracting. For example, $.12\overline{123}$ can be converted to a rational number by

$$1000(.12\overline{123}) = 121.23\overline{123}$$

so

$$(1000-1).12\overline{123} = 999.12\overline{123} = 121.11$$

which shows that

$$.12\overline{123} = 121.11/999 = 12111/99900.$$

Problem 17.22. Find a decimal expansion for $7/15, 274/999, 23/7$.

Problem 17.23. Find a fractional representation for $3.02\overline{4}$ base 10, $10.\overline{101}$ base 2, $.\overline{5}$ base 6,

18. Integers and primes

18.1. **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 18.1. *There exists a set $\mathbb{Z}$ of integers contains the natural numbers $\mathbb{N}$ as a subset, and equipped with operations*

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

and a permutation $- : \mathbb{Z} \to \mathbb{Z}$, 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) $x \in \mathbb{N} \wedge -x \in \mathbb{N} \iff x = 0$
(8) $1x = x1 = x$
(9) $xy = yx$
(10) $x(yz) = (xy)z$
(11) $-(xy) = (-x)y = x(-y)$
(12) $0 = xy \implies x = 0 \vee y = 0$
(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

$$- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (n, m) \mapsto n + (-m).$$

Problem 18.2. 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 18.3. Show that

(1) $x \leq x$.
(2) $x \leq y \wedge y \leq z \implies x \leq z$.
(3) $x \leq y \wedge y \leq x \implies x = y$.

18.2. **Prime numbers.** 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

$$p \in \mathbb{P} \iff p \neq 1 \wedge \forall a \in \mathbb{N}, (a|p \implies a = 1 \vee a = p).$$

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:

Proposition 18.4. *Any number greater than one has a prime factorization.*

(We show that the factorization is unique in Theorem 18.21.)

Proof. By induction on $n, n \geq 2$. Let $P(n)$ be the statement that for all $k \leq n$, k is a products 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 $n+1$ has a divisor not equal to 1 or itself, call it a. Since $a|p$, $ab = n+1$ for some $b \in \mathbb{N}$. Since $1 < a < n+1$, we must have $1 < b < n+1$ as well. Hence a and b are both products of primes, by the inductive hypothesis, and so $n + 1 = ab$ is a product of primes as well. □

Problem 18.5. Write a more formal version of the proof above, in two-column format and just involving symbols.

Problem 18.6. (Euclid[8]) Show there is no largest prime.

1	There is a largest prime	temp hyp
2	$\exists p, p \in \mathbb{P} \wedge \forall q \in \mathbb{P}, q \leq p$	def prime, largest
3	$r = p! + 1$	temp hyp
4	$\exists d, d \in \mathbb{P} \wedge d\|r$	Theorem 18.4
5	$\neg(d\|p!)$	Problem 7.17 (9)
6	$\neg(1 \leq d \leq p)$	def factorial
7	$d > p$	from 6
8	$d \leq p$	ui on 2
9	$d > p \wedge d \leq p$	ci on 7,8, contra
10	There is no largest prime	proof by contra on 1-9

Problem 18.7. Write an informal version of the above proof, and fill in the details for line 5.

Here is a start to the answer: Suppose that there is a largest prime, call it p. Let $d = r!+1$. Then by Theorem 18.4, there exists a prime dividing d ....

Remark 18.8. So far, we have been using the justification *temp hyp* in proof by deduction and contradiction. The temporary hypothesis is in force only for part of the proof, until the proof by contradition or deduction is complete. Here I am using temp hyp to do something else, namely introduce a new notation. I don't really need the new notation, it just makes everything easier to write. My final conclusion doesn't use the notation. In paragraph form, line 3 should become "Let $r = p! + 1$".

[8]Greek citizen of Alexandria, c. 395 b.c., now part of modern-day Egypt.

18.3. **Common divisors.**

Definition 18.9. 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,

$$d = gcd(a, b) \iff (d|a \wedge d|b \wedge \forall c \in \mathbb{N}, (c|a \wedge c|b) \implies c \leq d.$$

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

$$lcm(a, b) = m \iff (a|m \wedge b|m \wedge \forall c \in \mathbb{N}, (a|c \wedge b|c) \implies m \leq c).$$

The existence of the least common multiple is a consequence of the well-ordering principle.

Problem 18.10. 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

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_1 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \\ r_{k-2} &= r_{k-1} q_k + r_k. \\ r_{k-1} &= r_k q_{k+1} + 0. \end{aligned}$$

For example,

$$\begin{aligned} 102 &= 30(4) + 12 \\ 30 &= 2(12) + 6 \\ 12 &= 2(6) + 0 \end{aligned}$$

Hence the greatest common divisor of $102, 30$ is 6.

Theorem 18.11. *(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 $r_{j-1} = r_j q_{j+1} + r_{j+1}$, 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 18.12. Find the greatest common divisor of

(1) $1001, 300$
(2) $41, 103$
(3) $120, 333$

using Euclid's algorithm.

Corollary 18.13. *For any $a, b \in \mathbb{N}$, 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 $gcd(a, b)$.*

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 $r_2 = b - r_1 q_1 = -ka + (1 - q_1 l)b$ 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, b and so n as well.

Problem 18.14. Write a more formal proof using induction.

Two 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 18.15. 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.

Proof: Suppose that p is prime. Then the divisors of p are 1 and p. So the common divisors of p and n are 1 and p, if $p|n$, and 1 otherwise. So the greatest common divisor of p and n is p, if $p|n$, and 1, otherwise.

Problem 18.16. Make the above argument into a two-column proof, using only symbols.

Theorem 18.17. *If p is prime and $p|ab$ then $p|a \vee p|b$.*

1	$p \in \mathbb{P}$	hyp
2	$p \vert ab$	hyp
3	$p \not\vert a$	temp hyp
4	$gcd(p, a) = 1$	thm on gcd,3
5	$\exists k, l \in \mathbb{N}, kp + la = 1$	thm on gcd
6	$b = b$	equality axiom
7	$(kp + la)b = b$	subst 5
8	$p \vert kpb$	def divides
9	$p \vert b$	thm on divides, 2,7,8
10	$p \not\vert a \implies p \vert b$	deduc on 3-9
11	$p \vert a \vee p \vert b$	equiv form of 10
12	$p \vert ab \implies p \vert a \vee p \vert b$	deduc on 2-12

Problem 18.18. Write a paragraph version of the above two-column proof.

Theorem 18.19. *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 18.17. 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 18.17, 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 $p|a_j$.

Problem 18.20. Write a formal proof version of the previous paragraph proof.

Theorem 18.21. *(Fundamental Theorem of Arithmetic) Any natural number $n \geq 2$ can be written uniquely as a product of primes. That is, there exists a finite sequence of distinct primes $p_1, \ldots, p_k$, and positive natural numbers $a_1, \ldots, a_k$ such that $n = p_1^{a_1}, \ldots, p_k^{a_k}$, and the set $\{(p_1, a_1), \ldots, (p_k, a_k)\}$ is the unique set with this property.*

Problem 18.22. Find the prime factorization of

(1) 12
(2) 144
(3) 30
(4) 10,000

Proof of Theorem: We showed that there exists a prime factorization in Theorem 18.4. 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 18.17, 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 18.23. 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 18.24. Show that if $10|n$ and $4|n$ then $20|n$.

1	$10 \vert n \wedge 4 \vert n$	hyp
2	$5 \vert 10$	arithmetic
3	$5 \vert n \wedge 4 \vert n$	cs, trans of divides on 1,2
4	$\exists p_1, \ldots, p_r \in \mathbb{P}, n = p_1 \cdot \ldots \cdot p_r$	fund thm arith
5	$\exists j, k, l 5 = p_j \wedge 2 = p_k \wedge 2 = p_l \wedge$ j, k, l are distinct	Theorem 18.23
6	$n = (2)(2)(5) \prod_{i \notin \{j,k,l\}} p_i$	sub 5,4
7	$\exists k, n = 20k$	eg on 6
8	$20 \vert n$	def divides

Problem 18.25. Make the preceding into a paragraph proof.

Problem 18.26. Show that

(1) If $6|n$ and $10|n$ then $30|n$. (Hint: use the fundamental theorem of arithmetic.)
(2) If n is a square number, then $3|n$ implies $9|n$. (A square number is one that equals m^2, for some $m \in \mathbb{N}$.)
(3) If n is a square number, then $6|n$ implies $9|n$.
(4) If n is a square number, then $6|n$ implies $4|n$.
(5) If $2|m^2$ then $8|m^3$.

Here is the answer to (3).

1	n is square	hyp
2	$\exists m \in \mathbb{Z}, n = m^2$	def square
3	$6 \mid n$	hyp
4	$2 \mid 6$	arith
5	$2 \mid n$	transitivity $\mid$
6	$2 \mid m^2$	sub , ei 2, 5
7	$\forall p, a, b \in \mathbb{N}, p \in \mathbb{P} \wedge p \mid ab \implies p \mid a \vee p \mid b$	theorem from class
8	$2 \in \mathbb{P} \wedge 2 \mid (m)(m)$	obvious, cs with 6
9	$2 \mid m \vee 2 \mid m$	ui on 7 with $p = 2, a = b =$
10	$2 \mid m$	taut
11	$\exists k, 2k = m$	def —
12	$4k^2 = m^2$	ei on 11, square
13	$4 \mid m^2$	def divides
14	$4 \mid n$	sub 2,13

Theorem 18.27. *Suppose n has prime factorization $p_1^{i_1} \dots p_r^{i_r}$. The divisors of d are precisely the numbers of the form $p_1^{j_1} \dots p_r^{j_r}$ where each j_k satisfies $0 \le j_k \le i_k$.*

Problem 18.28. Show that if a and b are relatively prime then $a|c$ and $b|c$ implies $ab|c$.

Problem 18.29. Show that if p^x appears in the prime factorization of a and p^y 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 $\operatorname{lcm}(a, b)$.

Let's turn to the least common multiple.

Theorem 18.30. *$lcm(a, b) = ab/gcd(a, b)$. 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, b and $gcd(a, b)lcm(a, b)$ are equal. By Problem 18.29, if p^x appears in a and p^y appears in b then $p^{x+y} = p^{max(x,y)}p^{min(x,y)}$ appears in both ab and $gcd(a, b)lcm(a, b)$, 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 18.13 $gcd(m_1, m_2)$ 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 18.31. Prove that for all primes $p > 3$, (Hint:factor)

(1) $p^2 \equiv_3 1$
(2) $p^2 \equiv_{24} 1$.

Problem 18.32. 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 18.33. 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 *any number greater than one has a prime factorization* as

$$\forall n, n > 1 \implies \exists p_1, \dots, p_k, n = p_1 \cdot \dots \cdot p_k \wedge \forall j, 1 \le j \le k \implies p_j \in \mathbb{P}.$$

Problem 18.34. Which of the following are equivalent forms of the existence part of the fundamental theorem of arithmetic?

(1) $\forall n, n > 1 \wedge \exists p_1, \dots, p_k, n = p_1 \cdot \dots \cdot p_k \wedge \forall j, 1 \le j \le k \implies p_j$ is prime
(2) $\forall n, n > 1 \implies \exists p_1, \dots, p_k, n = p_1 \cdot \dots \cdot p_k \implies \forall j, 1 \le j \le k \implies p_j$ is prime
(3) $\forall n, n > 1 \implies \exists i_1, \dots, i_k, n = p_1^{i_1} p_2^{i_2} p_3^{i_3} \dots$ where $p_1, p_2, p_3, \dots$ are the primes in order and the universe for each i_j is the set of natural numbers.

The uniqueness part of the fundamental theorem is even harder to state formally. It says that *any prime factorization is unique up to equivalence*. In other words, *any two prime factorizations of the same number are equivalent*, or

$$\forall p_1, \dots, p_r, q_1, \dots q_s, (p_1 \dots p_r = q_1 \dots q_s \wedge \forall i, 1 \le i \le r \implies p_i \text{ is prime} \wedge \forall j, 1 \le i \le s \implies q_j \text{ is prime}) \implies r = s \wedge \exists n_1, \dots, n_r, n_1, \dots, n_r \text{ is a permutation sequence} \wedge \forall i, 1 \le i \le r \implies p_i = q_{n_i}.$$

Problem 18.35. Give your own definition of the uniqueness part of the fundamental theorem of arithmetic. It should still be correct, and at least somewhat different from the above version.

18.4. **Construction of the integers.** We now partially prove Theorem 18.1. 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 18.36. 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 18.37. 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 18.38. 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

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad \overline{(a, b)} + \overline{(c, d)} = \overline{(a + c, b + d)}.$$

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 $f(\overline{(a, b)}) = \overline{(a + 1, b)}$, 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 18.39. *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 $(x, y)Rz$ iff $\exists a, b, c, d, x = \overline{(a, b)}, y = \overline{(c, d)}$, and $z = \overline{(a + c, b + d)}$. 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

$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad \overline{(a, b)(c, d)} = \overline{(ac + bd, ad + bc)}.$$

Additive inverses are defined by

$$- : \mathbb{Z} \to \mathbb{Z}, \quad \overline{(a, b)} \mapsto \overline{(b, a)}$$

Finally, subtraction is defined by $x + y = x + (-y)$

Problem 18.40. Show that

(1) multiplication
(2) additive inverses

are well-defined, that is, independent of the representative of the equivalence class chosen.

Problem 18.41. Prove properties

(1) (1) - (2)
(2) (3) - (4)
(3) (5) - (6)

of Assumption 18.1, using the definition just given of the integers.

19. Modular arithmetic

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 16.16, any integer is equivalent to one (and only one) element of the set $\{0, \ldots, k - 1\}$. Hence

Corollary 19.1. $\mathbb{Z}_k = \{\overline{0}, \overline{1}, \ldots, \overline{k - 1}\}$.

When there will be no confusion, we drop the bar and write $\mathbb{Z}_k = \{0, \ldots, k - 1\}$. Addition and multiplication induce operations

$$+_k : \mathbb{Z}_k \times \mathbb{Z}_k \to \mathbb{Z}_k, \quad \overline{a} + \overline{b} = \overline{a + b}$$

$$\cdot_k : \mathbb{Z}_k \times \mathbb{Z}_k \to \mathbb{Z}_k, \quad \overline{a} + \overline{b} = \overline{ab}.$$

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 19.2. 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 simplicity. Thus the additional and multiplication tables mod 3 are

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Problem 19.3. Write out the tables for addition and multiplication mod 4.

Problem 19.4. 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 19.5. 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 19.6. Find the solution to

(1) $21x \equiv_{17} 7$.
(2) $9x \equiv_{13} 2$.

Problem 19.7. Show that any two inverses for an element are equal.

Problem 19.8. Find the units for the composition operation on functions.

Theorem 19.9. *Consider $\cdot_k$ as an operation on $\mathbb{Z}_k$. The units for $\cdot_k$ are the conjugacy classes $\overline{n}$ such that n, k are relatively prime.*

Proof: By Corollary 18.13 to Euclid's algorithm, if n, k are relatively prime then $an + bk = 1$ for some a, b. Hence $\overline{na} = \overline{1 - bk} = \overline{1}$ which shows that $\overline{n}$ is a unit. Conversely, if $\overline{n}$ is a unit then $\overline{na} = 1$ 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 19.10. *k is prime iff every non-zero element of $\mathbb{Z}_k$ is a unit.*

Problem 19.11. Show that every non-zero element of $\mathbb{Q}$ has a multiplicative inverse.

19.1. **Groups.**

Definition 19.12. A *group* is a set G with an operation $*$ such that

(1) $*$ is associative,
(2) there exists an identity $e \in G$,
(3) every element in G has an inverse.

Problem 19.13. Show that $Z_n^* = \mathbb{Z}_n - \{0\}$ with modular multiplication is a group if and only if n is prime.

Problem 19.14. Show that (1) $(\mathbb{Q}, +)$ and (2) $(\mathbb{Q} - \{0\}, \cdot)$ are groups.

Problem 19.15. 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 $*$ is a *subgroup* if $(H, *)$ 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) $\forall h_1, h_2 \in H, h_1 * h_2 \in H$.
(2) (closure under inverse) $\forall h \in H, h^{-1} \in H$.

Problem 19.16. 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) $\{(1)(2)(3), (12), (23)\} \subset \text{Perm}(\{1, 2, 3\})$.

20. Rational numbers

20.1. **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 20.1. *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) $1x = x1 = x$
(7) $xy = yx$
(8) $x(yz) = (xy)z$
(9) $0 = xy \implies x = 0 \vee y = 0$
(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 20.2. (1) $(1/q)(1/s) = (1/qs)$.
(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 $ps/qr = 1$ iff $ps = qr$ iff $ps - qr = 0$. ☐

Problem 20.3. Show that $3/6 = 1/2$.

Answer: $3/6 = 1/2$ iff $3(2) = 6(1)$ by 19.2 (4), which is true.

Theorem 20.4. *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 20.5. *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 20.6. Show that there is no rational number such that $q^2 = 2$, that is, prove that $\sqrt{2}$ is irrational.

Answer: 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 $a^2 = 2b^2$. By the prime factorization theorem, the power of 2 appearing in the prime factorization of a^2 is one more than twice the power of 2 appearing in the prime factorization of b. But this is a contradiction, since the power of 2 appearing in the prime factorization of a must be odd.

Problem 20.7. Prove that

(1) $\sqrt{2}/2$ is irrational.
(2) $\sqrt{6}$ is irrational.
(3) for any rational number x, $\sqrt{6} + x$ is irrational.
(4) $\sqrt{2} + \sqrt{5}$ is irrational.
(5) The sum of irrational numbers is not necessarily rational. (I.e. find a counterexample.)

20.2. **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

$$(a, b) \sim (c, d) \iff ad = bc.$$

(Think of (a, b) as a/b.) Define

$$\mathbb{Q} = (Z \times (\mathbb{Z} - \{0\}))/\sim .$$

We write the equivalence class of (a, b) as $[a, b]$. Addition is the operation defined by combining denominators,

$$\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \quad [a, b] + [c, d] = [ad + bc, bd]$$

Problem 20.8. 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

$$\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \quad [a, b][c, d] = [ac, bd]$$

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 20.9. Prove that if p, q are rational numbers and $p < q$ then $p < (p + q)/2 < q$.

Problem 20.10. 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 $q \in \mathbb{Q}$ 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 20.11. Construct an injection of $\mathbb{Q}$ into $\mathbb{Z} \times \mathbb{Z}$.

20.3. **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 20.12. 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 20.13. 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,

$$l = \inf(S) \iff \forall s \in S, l \leq s \wedge \forall k \in \mathbb{R}, (\forall s \in S, k \leq s) \implies k \leq l.$$

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 20.14. Write a formal definition of supremum, similar to the one for infimum.

Problem 20.15. Which of the following sets have suprema resp. infima. in $\mathbb{Q}$?

(1) $S = \{x \in \mathbb{Q} | 1 \leq x^2 \leq 4\}$.
(2) $S = \{x \in \mathbb{Q} | x^2 \leq 2\}$.
(3) $S = \{x \in \mathbb{Q} | x^4 \geq 4\}$.

20.4. **Countability.** Let S be a set.

Definition 20.16. 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.

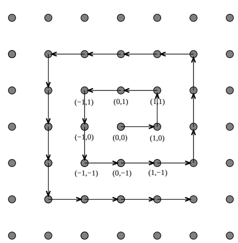
Theorem 20.17. *If S and T are equivalent sets, then S is finite resp. countable resp. denumerable resp. uncountable iff T is.*

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 20.18. Prove the second part of the theorem.

Theorem 20.19. (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 20.20. Fill in the details in the above proofs of (a) and (b).

Theorem 20.21. *Let S, T be denumerable sets. Then any subset of S or T is denumerable, $S \times T$ is denumerable, and the space* $\mathrm{Fun}(S,T)$ *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 $F : S \to \mathbb{N}$. 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 20.22. *$\mathbb{Q}$ is countable.*

Proof (Cantor's diagonal argument): Problem 20.11 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 20.19 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.

21. Real numbers

21.1. **Real numbers via bounded increasing sequences.** 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,

$$9(.\overline{9}) = (10-1)(.\overline{9}) = 9.\overline{9} - .\overline{9} = 9(1).$$

Dividing both sides by 9 gives $.\overline{9} = 1$. 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[9] 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

$$.9 + .09 + .009 + \ldots = .\overline{9}.$$

Does he ever reach his destination? We know from common experience that he does. That is, $.\overline{9} = 1$; 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 $.\overline{9}(d/s) = (d/s)$, as expected.

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 $1, 1.4, 1.41, \ldots$ you might recognize

[9]citizen c. 495 b.c. of Elea, Greek colony in modern-day Italy.

as better and better approximations to $\sqrt{2}$. Now we showed that $\sqrt{2}$ is not rational. So if we just allow the rational numbers, then the sequence $1, 1.4, 1.41, \ldots$ 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, $\sqrt{2}$ is to define it as the sequence $1, 1.4, 1.41, \ldots$. Similarly, π can be *defined* as the sequence $3, 3.1, 3.14, 3.142, \ldots$. The problem then is that there are many different sequences representing a real number. For example, $3, 3.1, 3.14, \ldots$ represents π, but so does $3, 3.14, 3.1416, \ldots$. So a real number is an *equivalence class* of sequences.

One of the simplest definitions of a real number is the following. Two sequences $x = (x_0, x_1, \ldots)$ and $y = (y_0, y_1, \ldots)$ are called *equivalent* if they "get arbitrarily close", or more precisely, $\forall \epsilon \in \mathbb{Q}_+, \exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_0 \implies |x_n - y_n| < \epsilon$. If x is equivalent to y, we write $x \sim y$.

Lemma 21.1. *$\sim$ is an equivalence relation on the set of sequences.*

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 $y \sim x$ .... □

Problem 21.2. Complete the proof by showing that $\sim$ is transitive.

Definition 21.3. A *real number* is an equivalence class of increasing sequences of rational numbers that is bounded from above.

21.2. **Real numbers via Cauchy sequences.** Mathematicians prefer not to restrict to sequences that are increasing. A more sophisticated definition of a real number is the following.

Definition 21.4. A sequence of rational numbers q_j is a *Cauchy sequence* iff $\forall \epsilon \in \mathbb{Q}$ with $\epsilon > 0$, $\exists n \in \mathbb{N}_+$ such that $i, j \geq n \implies |q_i - q_j| < \epsilon$.

For example,

Problem 21.5. 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) $1, 1 + 1/2, 1 + 1/2 + 1/3, \ldots$.....
(4) $1, 1 + 1/2, 1 + 1/2 + 1/6, 1 + 1/2 + 1/6 + 1/24, \ldots$.

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 21.6. Prove that the sequences $1, 1, 1, 1, \ldots$, and $.9, .99, .999, .9999$ are equivalent Cauchy sequences.

Definition 21.7. 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 $p_j + q_j, p_j q_j$ respectively.

Problem 21.8. Show that any increasing, bounded sequence is Cauchy.

Problem 21.9. Show that if $p \sim p'$ and $q \sim q'$ are equivalent Cauchy sequences, then $p + q \sim p' + q'$.

Let $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ and $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ be the operations defined by

$$\overline{p} \cdot \overline{q} = \overline{p \cdot q}, \quad \overline{p} + \overline{q} = \overline{p + q}.$$

Define involutions $- : \mathbb{R} \to \mathbb{R}$ and $^{-1} : \mathbb{R} - \{0\} \to \mathbb{R} - \{0\}$ by $-\overline{p} = \overline{-p}$ and $\overline{p}^{-1} = \overline{p^{-1}}$, where p is any representative sequence of non-zero numbers.

Problem 21.10. Show that if $\overline{p} \neq 0$ and p is a non-zero representative sequence then p^{-1} is a bounded sequence, so that $\overline{p}^{-1}$ is well-defined.

By the previous problem, these are well-defined, that is, independent of the choice of representative sequences p, q chosen.

Theorem 21.11. *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) $0 = xy \implies x = 0 \vee y = 0$
(10) $x(y + z) = xy + xz$.
(11) $1 = xy \iff x = y^{-1}$

Problem 21.12. Prove the properties 21.10.

Here is the proof of commutativity of +: $\overline{p} + \overline{q} = \overline{p + q} = \overline{q + p} = \overline{q} + \overline{p}$.

21.3. **Existence of suprema and infima.**

Theorem 21.13. *Suppose that $S \subset \mathbb{R}$ is bounded from above. Then there exists a supremum $\sup(S)$ 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. □

Theorem 21.14. *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 $y^2 \leq x$. 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 $y_+ = \sup(S)$ and $y_- = \inf(S)$. We claim that $y_+^2 = x$. If $y_+^2 < x$, then for sufficiently small numbers ϵ, $(y_+ + \epsilon)^2$ 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 ϵ 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 .... □

Problem 21.15. Complete the proof by showing that y_- is also a square root of x.

Problem 21.16. Show that each positive real number has *exactly* two square roots, which are additive inverses of each other.

Problem 21.17. Does an infimum of $\{y \in \mathbb{R} | y^2 + 1 < 0\}$ exist? Why or why not?

Problem 21.18. 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.

21.4. **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 21.19. *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 $b - 1$.*

Proof. 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. In the case of an infinite tail of $b - 1$'s, which is equivalent to a sequence with an infinite tail of 0's .... □

Problem 21.20. Complete the proof by showing that these two maps are inverse.

21.5. **Cantor's uncountability argument.** We apply base representation Theorem 21.18 to prove:

Theorem 21.21. *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

$$n'_k = n_{k,k} + 1 \bmod 10.$$

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

$$\begin{aligned} x_0 &= 123.456 \\ x_1 &= 5.321 \\ x_2 &= .051 \end{aligned}$$

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 21.22. Prove that the set of irrational numbers is uncountable.

References

[1] Stefan Waner and Steven R. Costenoble, Introduction to Logic. Available at http://www.zweigmedia.com/ThirdEdSite/logic/logic1.html.

[2] Douglas Smith, Maurice Eggen, and Richard St. Andre. A Transition to Advanced Mathematics.

[3] Comprehensive School Mathematics Program. Available for purchase from http://www.imacs.org.