2

Sets and Data Structures

Sets are of fundamental importance in mathematics. The very number systems that we studied in the preceding chapter were all discussed in terms of a *set of numbers*. Many problems of discrete mathematics can conveniently be expressed in terms of sets, especially finite sets. For this reason, we need to discuss the properties of sets and develop language to talk about them.

Along with sets, it is appropriate to discuss elementary logic. We shall observe a parallel between the logic of propositions and set theory.

Both mathematical logic and set theory are broad areas of mathematics, and we only discuss them briefly here; moreover our interest is in the discrete case, and we emphasize finite cases. The interested reader will find that there is a wide literature on both these topics, and they contain very deep problems.

2.1 Propositions and Logic

Propositions and Truth Tables

We shall define a *proposition* to be a statement that has a well-defined *truth value*, that is, it is either true (T) or false (F). Some statements in English are not propositions—one example is matters of opinion, such as "I like apples"; these are not propositions. On the other hand, "it will rain on this day next year" is a proposition: it is either true or false (we are not worried about whether or not we know the truth value, or even if it is possible to know it).

Simple propositions, like "today is Tuesday" and "it is raining," can be combined to form *compound* propositions, like "today is Tuesday and it is raining," by using a *connective* ("and" in the example). The truth value of a compound proposition can be calculated once we know the truth values of the simple propositions from which it is formed, and the connective used to combine these simple propositions together.

W.D. Wallis, *A Beginner's Guide to Discrete Mathematics*,
DOI 10.1007/978-0-8176-8286-6_2, © Springer Science+Business Media, LLC 2012

p	$\sim p$
T	F
F	T

p	q	$p \vee q$	$p \wedge q$
T	T	T	T
T	F	T	F
F	T	T	F
F	F	F	F

Table 2.1. Truth tables of $\sim$, $\wedge$, $\vee$

The simplest connectives are "not," "and," "or," denoted by $\sim$, $\wedge$, $\vee$ respectively. If p and q denote propositions, then the proposition "not p" (denoted $\sim p$) is true precisely when p is false, the proposition "p and q" (denoted $p \wedge q$) is true precisely when p is true and q is true, and the proposition "p or q" (denoted $p \vee q$) is true precisely when p is true or when q is true or when both p and q are true. (This is the meaning called "inclusive or," the usual usage in mathematics.) The truth values of these compound propositions are shown in Table 2.1. Such tables are called *truth tables*.

Formally, $\sim p$ is called the *negation* of p, $p \vee q$ is the *disjunction* of propositions p and q, and $p \wedge q$ is the *conjunction* of p and q.

Often alternate phrases are used. For example, we sometimes use "as well (as)" instead of "and." In English, we often use "but" instead of "and" when one of the two propositions is negative. Both these connectives are represented by $\wedge$: if p means "today is cold" and q means "today is sunny," then $p \wedge q$ could be translated as "today is cold and sunny," "today is cold but sunny," or "today is cold as well as sunny."

Sample Problem 2.1. *Let p denote the proposition "the sun is shining" and q the proposition "the wind is blowing." Write expressions for "the sun is not shining," "the sun is shining and the wind is blowing," and "the sun is shining but the wind is not blowing."*

Solution. $\sim p$ denotes "the sun is not shining," $p \vee q$ denotes "the sun is shining or the wind is blowing," and $p \wedge q$ denotes "the sun is shining and the wind is blowing."

Practice Exercise. Write expressions for "the wind is not blowing," "the sun is shining or the wind is blowing (maybe both)," and "the sun is not shining but the wind is blowing."

Sample Problem 2.2. *Suppose p, q and r mean "Joseph is here," "Nancy is here" and "Donna is here." Interpret $p \wedge \sim q$ and $(p \wedge q) \wedge r$.*

Solution. $p \wedge \sim q$ means "Joseph is here but Nancy is not;" $(p \wedge q) \wedge r$ means "Joseph, Nancy and Donna are here."

Practice Exercise. In this situation, interpret $(p \wedge r) \wedge \sim q$ and $q \vee r$.

p	q	$\sim p$	$\sim q$	$p \vee \sim q$	$q \vee \sim p$	$(p \vee \sim q) \wedge (\vee \sim p)$
T	T	F	F	T	T	T
T	F	F	T	T	F	F
F	T	T	F	F	T	F
F	F	T	T	T	T	T

Table 2.2. Truth table of $(p \vee \sim q) \wedge (q \vee \sim p)$

We sometimes think of a truth table as showing the truth or falsity of different outcomes of an experiment or set of events, as the following sample problem shows.

Sample Problem 2.3. *Suppose one card is drawn from a standard deck. Let p represent the statement "the card is a heart" and q represent "the card is an honor" (ace, king, queen, jack or ten). For which draws are $p \wedge q$ and $p \vee q$ true?*

Solution. For $p \wedge q$ to be true, the card must be a heart and it must be an honor. So it is true when the draw is the ace, king, queen, jack or ten of hearts (5 cases), and is false for all other cards (the other 47 cases). $p \vee q$ will be true for all thirteen hearts and all five honors in clubs, diamonds or spades (28 cases in all) and false in the other 24 cases.

Practice Exercise. In the same situation, which draws make $p \wedge \sim q$ true? Which make $p \vee \sim q$ true?

To find the truth table of a statement with several connectives, we work one step at a time. For instance, to find the truth table of

$$(p \vee \sim q) \wedge (q \vee \sim p),$$

we consider $\sim p$, $\sim q$, $p \vee \sim q$, $q \vee \sim p$, and finally the whole expression, as shown in Table 2.2.

Sample Problem 2.4. *Find the truth table of $(p \wedge q) \vee (q \wedge \sim r)$.*

Solution.

p	q	r	$\sim r$	$(p \wedge q)$	$(q \wedge \sim r)$	$(p \wedge q) \vee (q \wedge \sim r)$
T	T	T	F	T	F	T
T	T	F	T	T	T	T
T	F	T	F	F	F	F
T	F	F	T	F	F	F
F	T	T	F	F	F	F
F	T	F	T	F	T	T
F	F	T	F	F	F	F
F	F	F	T	F	F	F

p	q	$p \to q$	$p \leftrightarrow q$
T	T	T	T
T	F	F	F
F	T	T	F
F	F	T	T

Table 2.3. Truth tables of $p \to q$ and $p \leftrightarrow q$

Practice Exercise. Find the truth table of $(p \vee (q \vee (\sim p \wedge \sim r)))$.

Two other connectives we use frequently are $p \to q$, meaning "if p then q," or "p implies q," and $p \leftrightarrow q$, meaning "p if and only if q," or in other words "if p then q and if q then p." These are called the *conditional* ($\to$) and the *biconditional* ($\leftrightarrow$). Their truth tables are shown in Table 2.3. The interpretation of "implies" is that, if there is never a case where p is true and q is false, then we count $p \to q$ as true; this explains the last two lines of the table.

Sample Problem 2.5. *Find the truth table for*

$$(p \wedge \sim q) \to (q \vee p).$$

Solution. We proceed in steps as before. The result is as follows.

p	q	$\sim q$	$p \wedge \sim q$	$q \vee p$	$(p \wedge \sim q) \to (q \vee p)$
T	T	F	F	T	T
T	F	T	T	T	T
F	T	F	F	T	T
F	F	T	F	F	T

Practice Exercise. Find the truth table for

$$(p \vee \sim q) \leftrightarrow (q \to p).$$

Tautologies, Theorems and Logical Equivalence

The statement Sample Problem 2.5 is in fact a *tautology*. A compound statement is a tautology if it is always true, regardless of the truth values of the simple statements from which it is constructed. A statement that is always false is called a *contradiction*; a very simple example is $p \wedge \sim p$. Other statements that do not fall into either category are called *contingent*.

One of the main aims of logical deduction is to establish tautologies. For example, what we call theorems in mathematics are actually tautologies. The word "theorem" usually denotes a tautology whose essential truth is not immediately obvious, so that some proof is required to establish it.

One very easy example is the fact that every integer is a rational number. This requires a proof with only one step: we need to observe that any integer x can be written as the ratio of two integers, namely $x/1$. The truth of the theorem does not depend on the value of the rational number x.

Sample Problem 2.6. *Show that $p \vee \sim(p \wedge q)$ is a tautology.*

Solution. We use the following truth table.

p	q	$(p \wedge q)$	$\sim(p \wedge q)$	$p \vee \sim(p \wedge q)$
T	T	T	F	T
T	F	F	T	T
F	T	F	T	T
F	F	F	T	T

Practice Exercise. Show that $(p \wedge q) \wedge \sim(p \vee q)$ is a contradiction.

If $p \to q$ is a tautology, we say "p implies q," and write "$p \Rightarrow q$." If $p \leftrightarrow q$ is a tautology, we say that "p is equivalent to q" and write "$p \Leftrightarrow q$" or "$p \equiv q$." In order to prove that $p \equiv q$, it is sufficient to prove that p and q have the same truth table.

The Laws of Logic

A number of theorems (tautologies) about propositions may be deduced from truth tables, and together they form an algebraic system that is called *mathematical* (or *symbolic*) *logic*. (An alternative view is to take some of the tautologies as axioms, and deduce the truth tables for the standard connectives.) Some of them are very reminiscent of the usual arithmetical laws, with $\equiv$ taking the place of equality. Among these we have:

Commutative laws:

$$p \vee q \equiv q \vee p,$$
$$p \wedge q \equiv q \wedge p.$$

Associative laws:

$$p \vee (q \vee r) \equiv (p \vee q) \vee r,$$
$$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r.$$

Distributive laws:

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r),$$
$$(p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r),$$

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r),$$
$$(p \vee q) \wedge r \equiv (p \wedge r) \vee (q \wedge r),$$

where each statement is true for all propositions p, q, r. This reminds us of the behavior of addition and multiplication, except that only one pair of distributive laws holds for ordinary arithmetic.

In view of the associative laws, stated above, we can simply write $p \vee q \vee r$ whenever either $p \vee (q \vee r)$ or $(p \vee q) \vee r$, is intended, and similarly $p \wedge q \wedge r$ means either $p \wedge (q \wedge r)$ or $(p \wedge q) \wedge r$.

If t is a proposition that is always true, and if q is always false, then p acts like an identity element for the operation $\wedge$ and q acts like an identity element for $\vee$:

$$p \wedge t \equiv p, \qquad p \vee f \equiv p,$$

for all p. This is like the behavior of 1 under multiplication or 0 for addition. There are also *zero laws*:

$$p \vee t \equiv t, \qquad p \wedge f \equiv f,$$

for all p. This reminds us of 0 under multiplication, but there is no corresponding element for addition. Finally, there are two laws called *de Morgan's laws*:

$$\sim(p \vee q) \equiv (\sim p) \wedge (\sim q),$$
$$\sim(p \wedge q) \equiv (\sim p) \vee (\sim q)$$

for all p and q.

Exercises 2.1

In Exercises 1 to 12, find the truth table for the given compound statement.

1. $\sim p \wedge q$.

2. $\sim(p \to q)$.

3. $p \to (p \to q)$.

4. $\sim(\sim p \vee \sim q)$.

5. $p \vee (\sim p \to q)$.

6. $p \vee (\sim p \wedge q)$.

7. $\sim p \vee \sim q$.

8. $\sim(p \wedge q)$.

9. $(p \wedge q) \vee r$.

10. $(p \vee r) \wedge (q \vee r)$.

11. $p \vee (q \vee r)$.

12. $(p \vee q) \vee r$.

13. Use the results of Exercises 7 to 12 to prove the following equivalences.

(i) $\sim p \vee \sim q \Leftrightarrow \sim(p \wedge q)$.

(ii) $(p \wedge q) \vee r \Leftrightarrow (p \vee r) \wedge (q \vee r)$.

(iii) $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$.

Prove the equivalences in Exercises 14 to 16.

14. $(p \to q) \Leftrightarrow (\sim p \vee q)$.

15. $(p \leftrightarrow q) \Leftrightarrow (\sim p \wedge \sim q) \vee (p \wedge q)$.

16. $(p \to q) \Leftrightarrow (\sim q \to \sim p)$.

17. Prove that $(q \to p)$ is not equivalent to $(p \to q)$ in general.

Find the truth tables for the compound statements in Exercises 18 to 21.

18. $(p \to q) \to r$.

19. $p \to (q \to r)$.

20. $(p \to r) \to (q \to r)$.

21. $(p \vee q) \wedge \sim (p \wedge q)$.

22. Consider four possible definitions of a connective $p \uparrow q$, given by the following table.

p	q	Definition of $\uparrow$			
		A	B	C	D
T	T	T	T	T	T
T	F	F	F	F	F
F	T	F	F	T	T
F	F	F	T	F	T

Show that definition D, and only definition D, makes the statement "$p \uparrow p \vee q$" a tautology. Also show that definition A is that of $p \wedge q$, B is that of $p \leftrightarrow q$, C is that of q itself, and D is $p \to q$.

23. Prove that the following statements are equivalent.

(i) $(p \to q)$.

(ii) $(p \wedge \sim q) \to \sim p$.

(iii) $(p \wedge \sim q) \to q$.

24. Prove that $(p \to q) \to r$ and $p \to (q \to r)$ are not equivalent.

25. Prove the two commutative laws.

26. Prove the two associative laws.

27. Prove the two distributive laws.

28. Prove de Morgan's laws.

29. Let $p \veebar q$ denote the compound statement "p or q but not both," which is often called *exclusive or*. Find the truth table for $p \veebar q$. Compare it with Table 2.2 and Exercise 21.

In Exercises 30 to 39, find the truth table for the given statement.

30. $(p \to p)$.

31. $(p \to \sim p)$.

32. $p \wedge \sim p$.

33. $(p \wedge q) \to (p \vee q)$.

34. $(p \to q) \to (p \wedge q)$.

35. $((p \to q) \to (p \wedge q)) \vee (\sim p)$.

36. $(\sim p) \wedge (p \vee q) \to (\sim q)$.

37. $q \to (p \to q)$.

38. $(p \vee q) \to (p \wedge q)$.

39. $\sim p \to (q \to p)$.

40. Find truth tables for the following propositions. Are any of them equivalent?

(i) $(p \to q) \wedge (\sim r \to \sim q)$.

(ii) $r \to \sim p$.

(iii) $p \to \sim r$.

(iv) $\sim((\sim q \to \sim p) \wedge (q \to \sim r))$.

2.2 Elements of Set Theory

Sets

We saw *sets* in Section 1.1. The notations $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{Z}^+$ and $\mathbb{Z}^*$ were introduced for the sets of real numbers, rational numbers, integers, positive integers and non-negative integers respectively.

As we noted, a set can be finite or infinite. We saw that it is often convenient to specify a finite set by listing its elements between braces, but most infinite sets must be defined by explicitly stating the membership law. The set of all objects x for which the statement $S(x)$ is true was written $\{x \mid S(x)\}$, or sometimes as $\{x : S(x)\}$. For example, the set Π of prime numbers could be denoted (trivially) as

$$\Pi = \{x \mid x \text{ is a prime}\}.$$

The definition of a set does not allow for ordering of its elements, or for repetition of its elements. Thus $\{1, 2, 3\}$, $\{1, 3, 2\}$ and $\{1, 2, 3, 1\}$ all represent the same set (which could be written $\{x \mid x \in \mathbb{Z}^* \text{ and } x \leq 3\}$, or $\{x \in \mathbb{Z}^* \mid x \leq 3\}$). To handle problems that involve ordering, we define a *sequence* to be an ordered set. Sequences can be denoted by parentheses; $(1, 3, 2)$ is the sequence with first element 1, second element 3 and third element 2, and is different from $(1, 2, 3)$. Sequences may contain repetitions, and $(1, 2, 1, 3)$ is quite different from $(1, 2, 3)$; the two occurrences of object 1 are distinguished by the fact that they lie in different positions in the ordering.

We defined the notation

$$s \in S$$

to mean "s belongs to S" or "s is an element of S," and $S \subseteq T$ to mean S is a subset of T. If $S \subseteq T$ we also say that T contains S or T is a *superset* of S, and write $T \supseteq S$. Sets S and T are equal, $S = T$, if and only if $S \subseteq T$ and $T \subseteq S$ are both true. We can represent the situation where S is a subset of T but S is not equal to T—there is at least one member of T that is not a member of S—by writing $S \subset T$.

An important concept is the *empty* set, or *null* set, which has no elements. This set, denoted by $\emptyset$, is a subset of every other set.

In all the discussions of sets in this book, we shall assume (usually without bothering to mention the fact) that all the sets we are dealing with are subsets of some given universal set U. U may be chosen to be as large as necessary in any problem we deal with; in most of our discussion so far we could have chosen $U = \mathbb{Z}$ or $U = \mathbb{R}$. U can often be chosen to be a finite set.

The *power set* of any set S consists of all the subsets of S (including S itself and $\emptyset$), and is denoted by $\mathcal{P}(S)$:

$$\mathcal{P}(S) = \{T : T \subseteq S\}. \tag{2.1}$$

The power set is a set whose elements are *themselves* sets.

Sample Problem 2.7. *Write down all elements of the power set of* $\{1, 2, 3\}$. *How many elements are there?*

Solution. There are eight elements: $\{1, 2, 3\}$, $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$, $\{1\}$, $\{2\}$, $\{3\}$, and $\emptyset$.

Practice Exercise. Write down all elements of the power set of $\{x, y, z\}$.

Operations on Sets

Given sets S and T, we define three operations: the *union* of S and T is the set

$$S \cup T = \big\{x : x \in S \text{ or } x \in T \text{ (or both)}\big\};$$

the *intersection* of S and T is the set

$$S \cap T = \{x : x \in S \text{ and } x \in T\};$$

the *relative complement* of T with respect to S (or alternatively the *set-theoretic difference* or *relative difference* between S and T) is the set

$$S \backslash T = \{x : x \in S \text{ and } x \notin T\}.$$

In particular, the relative complement $U \backslash T$ with respect to the universal set U is denoted by $\overline{T}$ and called the *complement* of T. We could also write $R \backslash S = R \cap \overline{S}$, since each of these sets consists of the elements belonging to R but not to S. Hence we see that $R \subseteq S$ if and only if $R \backslash S = \emptyset$.

Sample Problem 2.8. *If $\mathbb{E}$ is the set of all even integers, what are $\mathbb{E} \cup \Pi$, $\mathbb{E} \cap \Pi$, $\mathbb{E} \backslash \Pi$, $\mathbb{Z} \cup \mathbb{Z}^+$, $\mathbb{Z}^* \backslash \Pi$?*

Solution.

$$\begin{aligned}
\mathbb{E} \cup \Pi &= \{\ldots, -8, -6, -4, 2, 0, 2, 3, 4, 5, 6, 7, 8, 10, 11, \ldots\}, \\
\mathbb{E} \cap \Pi &= \{2\}, \\
\mathbb{E} \backslash \Pi &= \{\ldots, -8, -6, -4, -2, 0, 4, 6, 8, \ldots\}, \\
\mathbb{Z} \cup \mathbb{Z}^+ &= \mathbb{Z}, \\
\mathbb{Z}^* \backslash \Pi &= \{0, 1, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, \ldots\}.
\end{aligned}$$

Practice Exercise. What are $\mathbb{Z} \backslash \mathbb{Z}^+$, $\mathbb{Z} \cap \mathbb{Z}^+$, $(\mathbb{Z}^+ \backslash \mathbb{E}) \cup \Pi$?

If two sets, S and T, have no common element, so that $S \cap T = \emptyset$, then we say that S and T are *disjoint*. Observe that $S \backslash T$ and T must be disjoint sets; in particular, T and $\overline{T}$ are disjoint. If n sets $S_1, S_2, \ldots, S_n$ are such that each pair of them are disjoint, so that

$$S_i \cap S_j \quad \text{for } 1 \leq i, j \leq n \text{ and } i \neq j,$$

then we say that these n sets are *pairwise disjoint* or *mutually disjoint*. By a *partition* of a set S we mean a collection of pairwise disjoint non-empty sets $S_1, S_2, \ldots, S_n$ whose union is S.

In general, to prove that the set S is a subset of the set T, we start with the statement, "suppose x is any element of S," and finish with "therefore x is an element of T." To show that S and T are equal, prove both $S \subseteq T$ and $S \supseteq T$. Another method of proving $S = T$ is to work as follows. Find an exact description of the elements of S—something of the form "S is precisely the set of all elements x with the following properties ...," and prove that this description is also precisely the description of elements of T.

Sometimes proofs of the form "suppose x is any element of S" are simpler if the argument is broken into two parts: first consider all elements x with a certain property, then all those without that property. For example, to prove that $(R \backslash S) \cup S = R \cup S$, for any two sets R and S, first observe that if x is a member of S, then it belongs to both $(R \backslash S) \cup S$ and $R \cup S$. So we need only discuss x not in S. The elements of $(R \backslash S) \cup S$ not in S are precisely the elements of $R \backslash S$, while the elements of $R \cup S$ not in S are the members of R not in S—precisely the same elements. So $(R \backslash S) \cup S = R \cup S$.

Properties of the Operations

We now investigate some of the easier properties of the operations $\cup$, $\cap$ and $\backslash$; for the more difficult problems, we shall introduce some techniques in the next section.

Union and intersection both satisfy *idempotence laws*: for any set S,

$$S \cup S = S \cap S = S.$$

Both operations satisfy commutative laws; in other words

$$S \cup T = T \cup S$$

and

$$S \cap T = T \cap S,$$

for any sets S and T. Similarly, the associative laws

$$R \cup (S \cup T) = (R \cup S) \cup T$$

and

$$R \cap (S \cap T) = (R \cap S) \cap T$$

are always satisfied. The associative law means that we can omit brackets in a string of unions (or a string of intersections); expressions like $(A \cup B) \cup (C \cup D)$, $((A \cup B) \cup C) \cup D$ and $(A \cup (B \cup C)) \cup D$, are all equal, and we usually omit all the parentheses and simply write $A \cup B \cup C \cup D$. But be careful not to mix operations. $(A \cup B) \cap C$ and $A \cup (B \cap C)$ are quite different. Combining the commutative and associative laws, we see that any string of unions can be rewritten in any order: for example,

$$(D \cup B) \cup (C \cup A) = C \cup \big(B \cup (A \cup D)\big) = (A \cup B \cup C \cup D).$$

Sample Problem 2.9. *Prove that* $(A \cup B) \cap C = A \cup (B \cap C)$ *is not always true.*

Solution. To prove that a general rule is not true, it suffices to find just one case in which it is false. This is called a *counterexample*. As an example we take the case $A = \mathbb{R}$, $B = \mathbb{Z}$, $C = \{0\}$. Then $(A \cup B) \cap C = \{0\}$, while $A \cup (B \cap C) = \mathbb{R}$.

The following distributive laws hold:

$$R \cup (S \cap T) = (R \cup S) \cap (R \cup T); \tag{2.2}$$

$$R \cap (S \cup T) = (R \cap S) \cup (R \cap T); \tag{2.3}$$

$$(R \cup S) \backslash T = (R \backslash T) \cup (S \backslash T). \tag{2.4}$$

Sample Problem 2.10. *Prove the distributive law* (2.2).

Solution. Suppose $x \in R \cup (S \cap T)$. It may be that $x \in R$; in that case, both $x \in (R \cup S)$ and $x \in (R \cup T)$ are true (in fact, $x \in (R \cup A)$ is true for *any* set A), so $x \in (R \cup S) \cap (R \cup T)$. On the other hand, if $x \notin R$, then $x \in (S \cap T)$, and x belongs both to S and to T. Now $x \in S \Rightarrow x \in (R \cup S)$, and

$x \in T \Rightarrow x \in (R \cup T)$, so $x \in (S \cap T) \Rightarrow x \in (R \cup S) \cap (R \cup T)$. So in either case,

$$x \in R \cup (S \cap T) \quad \Rightarrow \quad x \in (R \cup S) \cap (R \cup T),$$

and $R \cup (S \cap T) \subseteq (R \cup S) \cap (R \cup T)$.

Conversely, suppose $x \in (R \cup S) \cap (R \cup T)$. If $x \in R$, then certainly $x \in R \cup (S \cap T)$. If $x \notin R$, then $x \in (R \cup S) \Rightarrow x \in S$, and $x \in (R \cup T) \Rightarrow x \in T$. So

$$x \in (R \cup S) \cap (R \cup T) \quad \Rightarrow \quad x \in (S \cap T) \quad \Rightarrow \quad x \in R \cup (S \cap T)$$

and $(R \cup S) \cap (R \cup T) \subseteq R \cup (S \cap T)$. So the two sets are equal.

Practice Exercise. Prove the distributive law (2.3).

We have also the equation

$$R \backslash (S \cup T) = (R \backslash S) \cap (R \backslash T), \tag{2.5}$$

and the analogous

$$R \backslash (S \cap T) = (R \backslash S) \cup (R \backslash T). \tag{2.6}$$

Sample Problem 2.11. *Prove* (2.5) *from the definition.*

Solution. $R \backslash (S \cup T)$ consists of precisely those members of R that are not members of $S \cup T$, in other words those elements of R that do not belong to S or to T. That is,

$$R \backslash (S \cup T) = \{x \mid x \in R \text{ and } x \notin S \text{ and } x \notin T\}.$$

On the other hand, $(R \backslash S)$ consists of all the things in R that are not in S, and $(R \backslash S) \cap (R \backslash T)$ consists of all the things in R that are not in T; the common elements of these sets are all the things in R but not in S and not in T, which is the same as the description of $R \backslash (S \cup T)$.

Equation (2.5) can also be verified using the idempotence, associative and commutative laws. From

$$R \backslash (S \cup T) = \{x \mid x \in R \text{ and } x \notin S \text{ and } x \notin T\}$$

we have

$$\begin{aligned} R \backslash (S \cup T) &= R \cap (\overline{S} \cap \overline{T}) \\ &= (R \cap R) \cap (\overline{S} \cap \overline{T}) \quad \ldots \text{ idempotence} \\ &= (R \cap \overline{S}) \cap (R \cap \overline{T}) \quad \ldots \text{ associativity, commutativity} \\ &= (R \backslash S) \cap (R \backslash \overline{T}). \end{aligned}$$

When we take the particular case where R is the universal set in (2.5) and (2.6), those two equations become *de Morgan's laws*:

$$\overline{S \cup T} = \overline{S} \cap \overline{T}, \tag{2.7}$$

$$\overline{S \cap T} = \overline{S} \cup \overline{T}. \tag{2.8}$$

Exercises 2.2

1. Suppose $A = \{a, b, c, d, e\}$, $B = \{a, c, e, g, i\}$, $C = \{c, f, i, e, o\}$. Write down the elements of

(i) $A \cup B$. (ii) $A \cap C$.

(iii) $A \backslash B$. (iv) $A \cup (B \backslash C)$.

2. Suppose $A = \{2, 3, 5, 6, 8, 9\}$, $B = \{1, 2, 3, 4, 5\}$, $C = \{5, 6, 7, 8, 9\}$. Write down the elements of

(i) $A \cap B$. (ii) $A \cup C$.

(iii) $A \backslash (B \cap C)$. (iv) $(A \cup B) \backslash C$.

3. Suppose $A = \{1, 2, 4, 5, 6, 7\}$, $B = \{1, 3, 5, 7, 9\}$, $C = \{2, 4, 6, 7, 8, 9\}$. Write down the elements of

(i) $A \cup B \cup C$. (ii) $A \cup (B \cap C)$.

(iii) $A \backslash C$. (iv) $A \cap (B \backslash C)$.

4. Suppose $A = \mathbb{Z}^+$, $B = \{-4, -2, 1, 3, 5, 7\}$, $C = \{x \mid x^2 = 1\}$. Write down the elements of

(i) $(A \cap B) \cup C$. (ii) $A \cap B \cap C$.

(iii) $C \backslash A$. (iv) $A \cap (B \backslash C)$.

5. Consider the sets

$$S_1 = \{2, 5\},$$
$$S_2 = \{1, 2, 4\},$$
$$S_3 = \{1, 2, 4, 5, 10\},$$
$$S_4 = \{x \in \mathbb{Z}^+ : x \text{ is a divisor of } 20\},$$
$$S_5 = \{x \in \mathbb{Z}^+ : x \text{ is a power of 2 and a divisor of } 20\}.$$

For which i and j, if any, is $S_i \subseteq S_j$? For which i and j, if any, is $S_i = S_j$?

6. In each case, are the sets S and T disjoint? If not, what is their intersection?

(i) S is the set of perfect squares $1, 4, 9, \ldots$; T is the set of cubes $1, 8, 27, \ldots$ of positive integers.

(ii) S is the set of perfect squares; $T = \mathbb{R} \backslash \mathbb{R}^+$.

(iii) S is the set of perfect squares $1, 4, 9, \ldots$; T is the set Π of primes.

7. In each case, are the sets S and T disjoint? If not, what is their intersection?

(i) S is the set of all multiples of 5; T is the set of all perfect squares.

(ii) S is the set of all students in your class; T is the set of all students in your college.

8. Prove the commutative and associative laws for $\cup$.

9. Prove the commutative and associative laws for $\cap$.

In Exercises 10 to 20, U is a universal set and S and T are any sets. Prove the given result.

10. $S \cup \emptyset = S$.

11. $S \cup U = U$.

12. $S \cup S = S$.

13. $S \cup \overline{S} = U$.

14. $S \cap U = S$.

15. $S \cap \emptyset = \emptyset$.

16. $S \cap S = S$.

17. $S \cap \overline{S} = \emptyset$.

18. $(S \cap T) \subseteq S$.

19. $S \subseteq (S \cup T)$.

20. If $S \cup T = U$ and $S \cap T = \emptyset$, then $T = \overline{S}$.

21. Prove the distributive law in (2.4).

22. Prove de Morgan's laws.

23. Suppose the sets A, B, C, D, S are defined in terms of $\emptyset$ as follows.

$$A = \{\emptyset\}, \qquad B = \{A\}, \qquad C = \{\emptyset, A\},$$
$$D = \{\emptyset, A, C\}, \qquad S = \{\emptyset, A, B, C, D\}.$$

Show that:

(i) $\{x \mid x \in S \text{ and } x \subseteq D\} = S$;

(ii) $\{x \mid x \in S \text{ and } x \in D\} = D$.

In Exercises 24 to 30, R, S and T are any sets, and U is the universal set.

24. Prove: if $R \subseteq S$ and $R \subseteq T$, then $R \subseteq (S \cap T)$.

25. Prove: if $R \subseteq T$ and $S \subseteq T$, then $(R \cup S) \subseteq T$.

26. Prove: if $R \subseteq S$, then $R \cap T \subseteq S \cap T$ and $R \cup T \subseteq S \cup T$.

27. Show that $R \subseteq S$ if and only if $R \cap \overline{S} = \emptyset$.

28. Show that if $S \cup T = \emptyset$, then $S = T = \emptyset$ and that if $S \cap T = U$, then $S = T = U$.

29. Prove that $R \backslash (S \backslash T)$ contains all members of $R \cap T$, and hence prove that

$$(R \backslash S) \backslash T = R \backslash (S \backslash T)$$

is *not* a general law (in other words, relative difference is *not* associative).

30. Show that the following three statements are equivalent: $S \subseteq T$, $S \cup T = T$, $S \cap T = S$.

In Exercises 31 to 42, the sets A, B, C, D are defined as follows: $A = \{\emptyset\}$, $B = \{A\}$, $C = \{\emptyset, A\}$, $D = \{B\}$. Determine whether the given statement is true or false.

31. $\emptyset \subseteq A$.

32. $\emptyset \in A$.

33. $\emptyset \in B$.

34. $\emptyset \subseteq B$.

35. $A \subseteq B$.

36. $A \in B$.

37. $A \subseteq C$.

38. $A \in C$.

39. $B \subseteq C$.

40. $B \in C$.

41. $B \subseteq D$.

42. $B \in D$.

2.3 Proof Methods in Set Theory

Method of Truth Tables

Set-theoretic propositions can often be proved using truth tables. The reasoning is as follows. To prove that sets S and T are equal, it suffices to show that, for any element x of the universal set, the statement "$x \in S \leftrightarrow s \in T$" is a tautology. This can be proved (or disproved) using a truth table.

To illustrate this, consider the distributive law

$$DL1\, R \cup (S \cap T) = (R \cup S) \cap (R \cup T). \tag{2.2}$$

The truth table might look like the following

R	S	T	$S \cap T$	$R \cup S$	$R \cup T$	$R \cup (S \cap T)$	$(R \cup S) \cap (R \cup T)$
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	T	T	T	T
F	T	T	T	T	T	T	T
F	T	F	F	T	F	F	F
F	F	T	F	F	T	F	F
F	F	F	F	F	F	F	F

In writing the table, it is implicitly assumed that a general element x is being considered; the notation T (or F) under the name of a set means that the statement that x is a member of that set is true (or false). For example, the third line of the table could be interpreted as saying, "in all cases where $x \in R$ is true, $x \in S$ is false, and $x \in T$ is true, it is always false that $x \in S \cap T$, true that $x \in R \cup S$, true that $x \in R \cup T$, true that $x \in R \cup (S \cap T)$ and true that $x \in (R \cup S) \cap (R \cup T)$."

R	S	$\overline{R}$	$R \cup S$	$R \cap S$	$(R \backslash S)$
T	T	F	T	T	F
T	F	F	T	F	T
F	T	T	T	F	F
F	F	T	F	F	F

Table 2.4. Truth tables for $R \cup S$, $R \cap S$ and $(R \backslash S)$

The statement (2.2) is a tautology provided the last two columns are equal, which is seen to be true.

Compare this proof with the proof given in Sample Problem 2.2.2.10.

In order to apply the truth table method, it is necessary to know the truth tables of the main binary operations. The truth tables for complement, union, intersection and relative complement are shown in Table 2.4.

The method of truth tables can also be used to prove that one set is a subset of another. If you need to prove that $R \subseteq S$, then the last two columns will be labeled R and S, and it is required that no row has T in the R column and F in the S column.

Sample Problem 2.12. *Prove that* $A \cap C \subseteq (\overline{A} \cap B) \cup C$.

Solution. The truth value of $x \in \overline{A}$ is opposite that of $x \in A$, so the table is as follows.

A	B	C	$\overline{A}$	$\overline{A} \cap B$	$A \cap C$	$(\overline{A} \cap B) \cup C$
T	T	T	F	F	T	T
T	T	F	F	F	F	T
T	F	T	F	F	T	T
T	F	F	F	F	F	T
F	T	T	T	T	F	T
F	T	F	T	T	F	T
F	F	T	T	F	F	T
F	F	F	T	F	F	F

There is no line with T in the second-last column and F in the last, so inclusion is proved.

Practice Exercise. Prove that $A \cap B \cap C \subseteq B \cap (A \cup C)$.

Venn Diagrams

It is common, and useful, to illustrate sets and operations on sets by diagrams. A set A is represented by a circle, and it is assumed that the elements of A correspond to

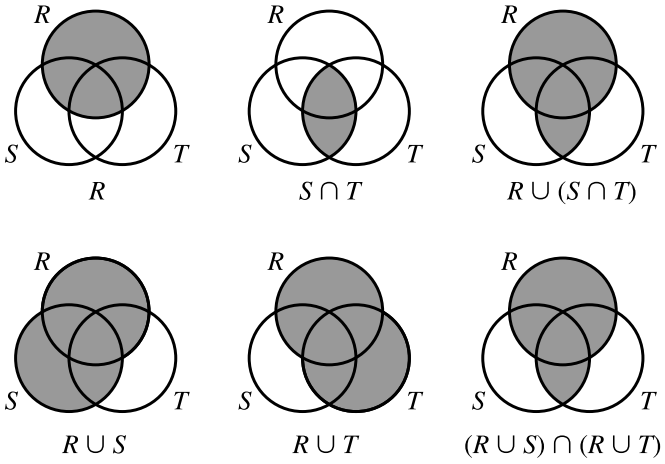
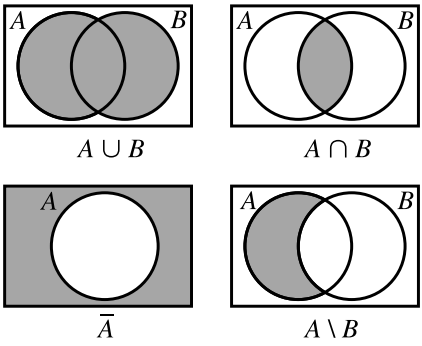


Fig. 2.1. $R \cup (S \cap T) = (R \cup S) \cap (R \cup T)$

the points (or some of the points) inside the circle. The universal set is usually shown as a rectangle enclosing all the other sets; if it is not needed, the universal set is often omitted. Such an illustration is called a *Venn diagram*.

Here are Venn diagrams representing $A \cup B$, $A \cap B$, $\overline{A}$ and $A \backslash B$; in each case, the set represented is shown by the shaded area. The universal set is shown in each case.



Two sets are equal if and only if they have the same Venn diagram. In order to illustrate this, we again consider the distributive law

$$DL1\, R \cup (S \cap T) = (R \cup S) \cap (R \cup T). \tag{2.2}$$

The Venn diagram for $R \cup (S \cap T)$ is constructed in the upper half of Figure 2.1, and that for $(R \cup S) \cap (R \cup T)$ is constructed in the lower half. The two are obviously identical.

In the first part of this section, we applied the method of truth tables (developed for use with propositions) to set identities. We can also apply the methods of set

theory to the analysis of propositions. If s is any proposition, we define S to be the set of all sets of circumstances in which proposition s is true; similarly we make proposition t correspond to set T. Then $s \Leftrightarrow t$ is equivalent to $S = T$, and the Venn diagram that shows the set equality also indicates the proposition equivalence.

For example, the preceding Venn diagram illustration that

$$R \cup (S \cap T) = (R \cup S) \cap (R \cup T)$$

for all sets R, S and T may also be used to construct a proof of the distributive law for propositions,

$$r \vee (s \wedge t) \leftrightarrow (r \vee s) \wedge (r \vee t).$$

Sample Problem 2.13. *Write down a statement involving propositions that can be proven by establishing the set-theoretic identity*

$$(R \backslash S) \backslash T = R \backslash (S \backslash T).$$

Solution. We let r correspond to set R, and so on. As $R \backslash S$ corresponds to the proposition $r \wedge \sim s$, the answer is

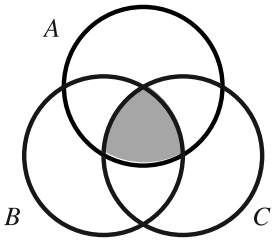
$$\big((r \wedge \sim s) \wedge \sim t\big) \leftrightarrow \big(r \wedge \sim (s \wedge \sim t)\big).$$

To prove $A \subseteq B$, it is sufficient to show that the diagram for A contains no shaded area that is not shaded in B. We illustrate this idea with the problems from Sample Problem 2.12 and its associated Practice Exercise (but in reverse order).

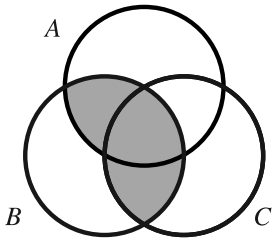
Sample Problem 2.14. *Use Venn diagrams to illustrate that*

$$A \cap B \cap C \subseteq B \cap (A \cup C).$$

Solution.



$A \cap B \cap C$



B $\cap (A \cup C)$

Practice Exercise. Use Venn diagrams to illustrate that

$$A \cap C \subseteq (\overline{A} \cap B) \cup C.$$

In many cases, you may not be sure whether or not two expressions represent the same set. Often the best response is to construct the corresponding Venn diagrams. If the diagrams are different, this disproves the equality; if they are the same, the identity will be provable.

As before, this type of set-theoretic proof can be applied to propositions. A proof that $R \subseteq S$ serves as a proof that $r \to s$. Sample Problem 2.14 can be interpreted as a proof that

$$a \wedge b \wedge c \to b \wedge (a \vee c)$$

is true for any propositions a, b and c.

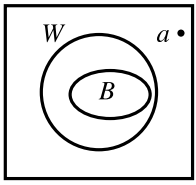
Syllogisms and Venn Diagrams

Sometimes we draw a Venn diagram in order to represent some properties of sets. For example, if A and B are disjoint sets, the diagram can be drawn with A and B shown as disjoint circles. If $A \subseteq B$, the circle for A is entirely inside the circle for B.

In the classical study of logic, an argument is given in the form of a *syllogism*, a set of statements (the *premises*, or data) and a conclusion drawn from them. For example, consider the argument

> All big cities are near water; Alamagordo, NM is not near water; therefore Alamagordo is not a big city.

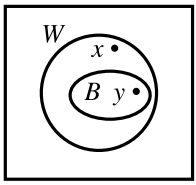
To examine this, suppose B is the set of all big cities, W is the set of all cities near water, and a represents Alamagordo. Since the premises tell us that $B \subseteq W$, we can draw the sets as shown. As $a \notin W$, it must lie somewhere in the outside region, so it is certainly not in B. Therefore the argument is valid.



Some arguments that look logical at first sight turn out not to be valid. For example,

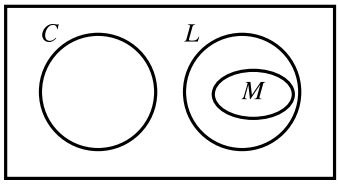
> All big cities are near water; Carbondale, IL is near water; therefore Carbondale is a big city.

We label the sets as before. In the diagram shown, Carbondale could be represented either by x or by y, so you can't draw any conclusion. The argument is not valid. (In fact, x is nearer the mark.)



Sample Problem 2.15. *Examine the argument: no students in this class are lazy; John is a math major; all math majors are lazy; so John is not a student in this class.*

Solution. Write L, C and M for the sets of lazy students, students in this class and math majors. The premises are represented in the following diagram.



John is a member of M, which is disjoint from C. So John is not in this class, and the conclusion is valid.

Practice Exercise. Examine the argument: *some students in this class are lazy; all males are lazy; so some students in this class are males.*

Observe from the above example that the *validity* of an argument does not depend on the *truth* of the premises or conclusion. Not all math majors are lazy, and I wouldn't venture to guess how many students in your class are lazy! Another example, where the premises and conclusion are all false but the argument is valid, appears in Exercise 2.3.26.

Exercises 2.3

In Exercises 1 to 8, represent the set in a Venn diagram.

1. $R \cup S \cup T$.

2. $\overline{R \cup S \cup T}$.

3. $R \cup (S \cap \overline{T})$.

4. $(R \cap S) \cap T$.

5. $(R \backslash S) \cap T$.

6. $R \cap (S \backslash T)$.

7. $(R \cap S) \backslash (S \cap T)$.

8. $(R \cup T) \backslash (S \cap T)$.

9. Prove: $R = (\overline{\overline{R} \cup S}) \cup (R \cap S)$.

10. Find a simpler expression for $S \cup (\overline{(\overline{R} \cup S) \cap R})$.

In Exercises 11 to 15, prove the rule using truth tables and illustrate it using Venn diagrams.

11. $S \cap \overline{S} = \emptyset$.

12. $\overline{S \cup T} = \overline{S} \cap \overline{T}$.

13. $\overline{S \cap T} = \overline{S} \cup \overline{T}$.

14. $(S \cap T) \subseteq S$.

15. $S \subseteq (S \cup T)$.

16. Use truth tables to represent the commutative and associative laws for $\cup$.

17. Use Venn diagrams to represent the commutative and associative laws for $\cap$.

18. For any sets R and S, prove $R \cap (R \cup S) = R$.

19. Prove, *using Venn diagrams,* that $(R \backslash S) \backslash T = R \backslash (S \backslash T)$ does not hold for all choices of sets R, S and T.

20. (i) Prove, without using truth tables or Venn diagrams, that union is not distributive over relative difference: in other words, prove that the following statement is not always true:

$$(R \backslash S) \cup T = (R \cup T) \backslash (S \cup T).$$

(Hint: use the fact $(R \backslash S) \cup S = R \cup S$.)

(ii) Now prove this using Venn diagrams.

21. Draw Venn diagrams for use in the following circumstances:

(i) All my goldfish are tropical fish.

(ii) None of my goldfish are tropical fish.

In Exercises 22 to 25, test the validity of the argument by drawing the appropriate Venn diagram.

22. *All men are mortal; Socrates is a man. Therefore Socrates is mortal.*

23. *All my friends are students; none of my neighbors are students; Ruth is my friend. Therefore Ruth is not my neighbor.*

24. *Boston is a big city; all big cities have department stores; Shirley lives in a city with no department store. Therefore Shirley does not live in Boston.*

25. *All businessmen are wealthy; all mathematicians are cheerful; David is a businessman; no cheerful people are wealthy. Therefore David is not a mathematician.*

26. Show that the following argument is valid, although its premises and conclusion are all false: *All expensive food contains cholesterol; steak contains no cholesterol. Therefore steak is not expensive.*

27. Show that the following argument is not valid, although its premises and conclusion are all true: *Some animals walk on two legs; human beings are animals; therefore human beings walk on two legs.*

28. Consider the data: *All authors are solitary people; all physicians are rich; no solitary people are rich.* Which of the following conclusions can be drawn?

(i) No authors are rich.

(ii) All physicians are solitary.

(iii) No one can be both an author and a physician.

29. Consider the data: *I sold back all my expensive textbooks last year; all my science textbooks are green; I did not sell back any green books last year.* Which of the following conclusions can be drawn?

(i) None of my science textbooks are expensive.

(ii) All of my science textbooks were sold back last year.

(iii) Some of my science textbooks were sold back last year.

(iv) None of my science textbooks were sold back last year.

(v) No green textbooks were sold back last year.

30. Consider the data: *All topcoats are expensive; none of my clothes are expensive; all expensive clothes are well made.* Which of the following conclusions can be drawn?

(i) I do not own a topcoat.

(ii) All topcoats are well made.

(iii) None of my clothes are well made.

2.4 Some Further Set Operations

Symmetric Difference

Another important set operation is *symmetric difference*. The symmetric difference of A and B is the set

$$A + B = \{x : x \in A \text{ or } x \in B \text{ but } x \notin A \cap B\}. \tag{2.9}$$

Sample Problem 2.16. *What is the truth table for $A + B$?*

Solution.

A	B	$A + B$
T	T	F
T	F	T
F	T	T
F	F	F

Practice Exercise. What is the Venn diagram for $A + B$?

This definition could be stated as

$$\begin{aligned} A + B &= (A \cup B) \backslash (A \cap B) \\ &= (A \cup B) \cap \overline{(A \cap B)} \\ &= (A \cup B) \cap (\overline{A} \cup \overline{B}), \end{aligned} \tag{2.10}$$

using (2.7). By the symmetry of the relation in (2.10), it follows that

$$\overline{A} + \overline{B} = A + B.$$

From the definition, we may consider $A+B$ to be the union of the difference between A and B with the difference between B and A. This implies that

$$A + B = (A \backslash B) \cup (B \backslash A),$$

and hence that

$$A + B = (A \cap \overline{B}) \cup (A \cap \overline{B}). \tag{2.11}$$

If a and b denote the propositions "$x \in A$" and "$x \in B$" respectively, then the proposition "$x \in A + B$" is denoted by $a \underline{\vee} b$. (For the definition of $\underline{\vee}$, see Exercise 2.1.29) Then

$$a \underline{\vee} b \Leftrightarrow \big((a \vee b) \vee \sim(a \wedge b)\big) \Leftrightarrow \big((a \vee b) \wedge (\sim a \vee \sim b)\big) \tag{2.12}$$

is a restatement of (2.10), and similarly we see that

$$(a \underline{\vee} b) \Leftrightarrow (\sim a \underline{\vee} \sim b)$$

while (2.11) yields

$$(a \underline{\vee} b) \Leftrightarrow (a \wedge \sim b) \vee (\sim a \wedge b). \tag{2.13}$$

It is easy to see that symmetric difference satisfies the commutative law

$$A + B = B + A. \tag{2.14}$$

The associative law is also true, but it is harder to prove, so we state it as a theorem.

Theorem 7. *Symmetric difference satisfies the associative law*

$$A + (B + C) = (A + B) + C.$$

Proof. We start from (2.10),

$$A + B = (A \cup B) \cap (\overline{A} \cup \overline{B}).$$

Then

$$\begin{aligned} \overline{A + B} &= \overline{(A \cup B)} \cup (A \cap B) \quad \text{by (2.7)} \\ &= (\overline{A} \cap \overline{B}) \cup (A \cap B). \end{aligned} \tag{2.15}$$

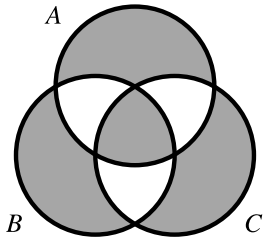


Fig. 2.2. Associativity of symmetric difference

From (2.11),

$$\begin{aligned}(A+B)+C &= \big[(A+B)\cap\overline{C}\,\big]\cup\big[\,\overline{(A+B)}\cap C\big]\\ &= \big\{\big[(A\cap\overline{B})\cup(\overline{A}\cap B)\big]\cap\overline{C}\big\}\\ &\quad\cup\big\{\big[(\overline{A}\cap\overline{B})\cup(A\cap B)\big]\cap C\big\}\quad\text{by (2.11) and (2.15)}\\ &= \{A\cap\overline{B}\cap\overline{C}\,\}\cup\{\,\overline{A}\cap B\cap\overline{C}\,\}\\ &\quad\cup\{\,\overline{A}\cap\overline{B}\cap C\}\cup\{A\cap B\cap C\}.\end{aligned}$$

In exactly the same way we may prove that

$$\begin{aligned}B+C)+A &= \{B\cap\overline{C}\cap\overline{A}\,\}\cup\{\,\overline{B}\cap C\cap\overline{A}\,\}\\ &\quad\cup\{\overline{B}\cap\overline{C}\cap A\}\cup\{B\cap C\cap A\}.\end{aligned}$$

Since union and intersection are commutative and associative operations, the right-hand sides of the last two equations are equal, so

$$(B+C)+A=(A+B)+C;$$

on applying the commutative law in (2.14) to the left-hand side, we obtain

$$A+(B+C)=(A+B)+C. \qquad \square$$

In view of Theorem 7, we can write $A+B+C$ instead of $(A+B)+C$. In the expression

$$\{A\cap\overline{B}\cap\overline{C}\}\cup\{\overline{A}\cap B\cap\overline{C}\}\cup\{\overline{A}\cap\overline{B}\cap C\}\cup\{A\cap B\cap C\}$$

the first three terms are the sets of all elements belonging to exactly one of A, B and C, while the fourth term is the intersection of all three. So $A+B+C$ consists of all those elements which belong to an *odd* number of the sets A, B and C; see Figure 2.2, where $A+B+C$ is represented by the shaded area.

The proof of Theorem 7 using truth tables or Venn diagrams is left as an exercise.

Cartesian Product

We define the *Cartesian product* (or *cross product*) $S\times T$ of sets S and T to be the set of all ordered pairs (s,t) where $s\in S$ and $t\in T$:

$$S \times T = \big\{(s, t) : s \in S, t \in T\big\}.$$

There is no requirement that S and T be disjoint; in fact, it is often useful to consider $S \times S$.

The number of elements of $S \times T$ is $|S| \times |T|$. (This is one reason why the symbol $\times$ was chosen for cartesian product.)

Sample Problem 2.17. *Suppose* $S = \{0, 1\}$ *and* $T = \{1, 2\}$. *What is* $S \times T$*?*

Solution. $S \times T = \{(0, 1), (0, 2), (1, 1), (1, 2)\}$, the set of all four of the possible ordered pairs.

Practice Exercise. What is $S \times T$ if $S = \{1, 2\}$ and $T = \{1, 4, 5\}$?

The sets $(R \times S) \times T$ and $R \times (S \times T)$ are not equal; one consists of an ordered pair whose *first* element is itself an ordered pair, and the other of pairs in which the *second* is an ordered pair. So there is no associative law, and no natural meaning for $R \times S \times T$. On the other hand, it is sometimes natural to talk about ordered triples of elements, so we define

$$R \times S \times T = \big\{(r, s, t) : r \in R, s \in S, t \in T\big\}.$$

This notation can be extended to ordered sets of any length.

There are several distributive laws involving the cartesian product:

Theorem 8. *If* R, S *and* T *are any sets, then*

(i) $R \times (S \cup T) = (R \times S) \cup (R \times T)$.

(ii) $R \times (S \cap T) = (R \times S) \cap (R \times T)$.

Proof. (i) We prove that every element of $R \times (S \cup T)$ is a member of $(R \times S) \cup (R \times T)$, and conversely.

First observe that

$$\begin{aligned} R \times (S \cup T) &= \big\{(r, s) \mid r \in R \text{ and } s \in S \cup T\big\} \\ &= \big\{(r, s) \mid r \in R \text{ and } (s \in S \text{ or } s \in T)\big\}. \end{aligned}$$

On the other hand,

$$\begin{aligned} (R \times S) \cup (R \times T) &= \big\{(r, s) \mid (r, s) \in R \times S \text{ or } (r, s) \in R \times T\big\} \\ &= \big\{(r, s) \mid (r \in R \text{ and } s \in S) \text{ or } (r \in R \text{ and } s \in T)\big\} \\ &= \big\{(r, s) \mid r \in R \text{ and } (s \in S \text{ or } s \in T)\big\}, \end{aligned}$$

where the last equality follows from the distributive law for *propositions*, applied to the propositions $r \in R$, $s \in S$ and $s \in T$.

It is now clear that $(r, s) \in R \times (S \cup T)$ and $(r, s) \in (R \times S) \cup (R \times T)$ are equivalent.

The proof of part (ii) is left as an exercise. □

Exercises 2.4

1. Prove Theorem 7

(i) Using truth tables;

(ii) Using Venn diagrams.

2. Prove the two distributive laws

$$A \cap (B + C) = (A \cap B) + (A \cap C),$$
$$(A + B) \cap C = (A \cap C) + (B \cap C).$$

(i) Using truth tables.

(ii) Using Venn diagrams.

3. Show that union is not distributive over symmetric difference. (Hint: consider the set $S \cup (S + T)$.)

4. Show that $S + T = \emptyset$ if and only if $S = T$.

In Exercises 5 to 14, decide whether the given statement is true or false. Prove each of the statements that you think is true: give a counterexample for each statement that you think is false.

5. $R + (S \cap T) = (R + S) \cap (R + T)$.

6. $R + (S \backslash T) = (R + S)\ (R + T)$.

7. $R \backslash (S \cap T) = (R \backslash S) \cup (R \backslash T)$.

8. $R \cap (S + T) = (R \cap S) + (R \cap T)$.

9. $R \cup (S \backslash T) = (R \cup S) \backslash (R \cup T)$.

10. $R + (S \cup T) = (R + S) \cup (R + T)$.

11. $R \backslash (S \cup T) = (R \backslash S) \cap (R \backslash T)$.

12. $R \backslash (S + T) = (R \backslash S) + (R \backslash T)$.

13. $R \cap (S \backslash T) = (R \cap S) \backslash (R \cap T)$.

14. $R \cup (S + T) = (R \cup S) + (R \cup T)$.

15. In each case, list all elements of $S \times T$.

(i) $S = \{1, 2, 3\};\ T = \{1, 4, 5\}$.

(ii) $S = \{x \mid x^2 = 1\};\ T = \{y \mid y^2 = 4\}$.

(iii) $S = \{1, 3, 5, 7\};\ T = \{1, 2, 3\}$.

16. In each case, list all elements of $R \times S \times T$.

(i) $R = \{1, 2\};\ S = \{3, 4\};\ T = \{5, 6\}$.

(ii) $R = \{12, 13, 14\};\ S = \{1\};\ T = \{1, 2, 3\}$.

17. (i) If $S = \emptyset$, $T \neq \emptyset$, what is $S \times T$?

(ii) If $S \times T = T \times S$, what can you say about S and T?

18. Prove the distributive law $R \times (S \cap T) = (R \times S) \cap (R \times T)$;

19. (i) If $A \subseteq S$, $B \subseteq T$, show that $A \times B \subseteq S \times T$.

(ii) Find an example of sets A, B, S, T, such that $A \times B \subseteq S \times T$ and $B \subseteq T$, but $A \not\subseteq S$.

2.5 Mathematical Induction

The Principle of Mathematical Induction

In working with finite sets or with the sets of positive integers and of integers, one repeatedly uses a technique of proof known as the method of *mathematical induction*. The general idea is as follows: suppose we want to prove that every positive integer n has a property $P(n)$. We first prove $P(1)$ to be true. Then we prove that, for any n, the truth of P(n) implies that of P(n+1); in symbols:

$$P(n) \text{ true} \quad \Rightarrow \quad P(n+1) \text{ true}. \tag{2.16}$$

Intuitively, we would like to say:

$$\begin{array}{rl} & P(1) \text{ true}, \\ & P(1) \text{ true} \quad \Rightarrow \quad P(2) \quad \text{true}, \quad \text{by (2.16)}, \\ \therefore\ & P(2) \text{ true}; \\ & P(2) \text{ true} \\ & P(2) \text{ true} \quad \Rightarrow \quad P(3) \quad \text{true}, \quad \text{by (2.16)}, \\ \therefore\ & P(3) \text{ true}; \end{array}$$

and so on. There is a difficulty, however: given any positive integer k, we can select an integer n such that the proof of $P(n)$ requires at least k steps, so the proof can be arbitrarily long. As "unbounded" proofs present logical difficulties in mathematics—who could ever finish writing one down?—we need an axiom or theorem that states that induction is a valid procedure. This is the *principle of mathematical induction*, and may be stated as follows.

Principle of mathematical induction *Suppose the proposition* $P(n)$ *satisfies*

(i) $P(1)$ *is true; and*

(ii) *for every positive integer* n, *whenever* $P(n)$ *is true, then* $P(n+1)$ *is true.*

Then $P(n)$ *is true for all positive integers* n.

This principle is sometimes called *weak induction*. Another form is as follows.

Strong induction *Suppose the proposition* $P(n)$ *satisfies*

(i) $P(1)$ *is true; and*

(ii) *for every positive integer* n, *if* $P(k)$ *is true whenever* $1 \leq k < n$, *then* $P(n)$ *is true.*

Then $P(n)$ *is true for all positive integers* n.

At first sight, the second statement looks as though we have assumed more than in the first statement. However these two forms are equivalent; a detailed proof can be found in more advanced books.

In the above formulations, the case $n = 1$—the case of $P(1)$—is called the *base case*. There is in fact nothing special about 1; any integer could be used to define the base case. For example, weak induction could be stated as

Suppose the proposition $P(n)$ *satisfies*

(i) $P(t)$ *is true for some specified integer* t; *and*

(ii) *for every positive integer* $n \geq t$, *whenever* $P(n)$ *is true, then* $P(n+1)$ *is true.*

Then $P(n)$ *is true for all integers* $n \geq t$.

Induction can also be stated in strictly set-theoretic form. Suppose S is the set of integers n such that $P(n)$ is true. Then the principle of mathematical induction (weak induction form) is:

Let S *be a subset of* $\mathbb{Z}^+$ *such that*

(i) $1 \in S$; *and*

(ii) *whenever* $n \in S$, *then* $n + 1 \in S$.

Then $S = \mathbb{Z}^+$.

One could equally well state the principle in terms of non-negative integers, instead of positive integers, by changing the case $P(0)$ to $P(1)$, and converting references from "positive integers" to "non-negative integers." It can in fact be stated in terms of any starting point: if S is a set of integers for which

(i) $t \in S$,

where t is any integer, and

(ii) for every integer $n \geq t$, if $n \in S$, then $n + 1 \in S$,

then the principle can be used to prove that S contains all integers equal to or greater than t. This form is sometimes called "induction from t."

The Well-Ordering Principle

Another principle that is very useful in proving results about sets of positive integers is:

The well-ordering principle *Suppose S is any non-empty set of positive integers. Then S has a smallest member.*

Any set with the property that every non-empty subset has a least member is called being *well-ordered*; so the principle says "the positive integers are well-ordered." Many number-sets, such as the real numbers, are not well-ordered.

At first the result seems obvious. If S is not empty, then it must contain some member, x say. In order to find the smallest member of S, one need only check to see whether or not $x - 1, x - 2, \ldots, 1$ are members of S, and this requires only a finite number of steps. However, this "proof" contains the same problem as the "proof" of the principle of mathematical induction: the starting value, x, can be arbitrarily large.

In fact, the induction principle can be proved from the well-ordering principle. To see this, let us assume the well-ordering principle is true and suppose P is any proposition about positive integers such that $P(1)$ is true, and for every positive integer n, whenever $P(n)$ is true, then $P(n + 1)$ is true. (These are the requirements for induction.) Write S for the set of positive integers n such that $P(n)$ is not true. In order to prove that induction works, we need to show that S is empty.

If S is not empty, then by well-ordering S has a smallest member, x say. So $P(x)$ is false. We know that $P(1)$ is true, so $x \neq 1$. But x is a positive integer. So $x - 1$ is a positive integer, and $P(x)$ must be true—otherwise $x - 1$ would be a member of S, and smaller than x. But this means $P((x - 1) + 1)$ is true: that is, $P(x)$ is both true and false! This can't happen, so our original assumption, that S is not empty, must have been wrong. So induction is proved.

We can also work the other way. If you assume induction is true, you can show that the positive integers are well-ordered.

However, there is no absolute proof here. It is necessary to assume that either induction or well-ordering is a property of the positive integers. So we assume these as axioms about numbers.

Some Applications

We start by looking at some properties of sets and prove them by induction.

Theorem 9. *Let A be a set with $|A| = n$. Then $|\mathcal{P}(A)| = 2^n$.*

Proof. To apply induction, we can rephrase the statement as: *Let $P(n)$ be the statement "$|\mathcal{P}(A)| = 2^n$ for any n-element set A;" then $P(n)$ is true for all positive integers n.* Since the elements of A do not matter, we may as well assume $A = \{a - 1, a_2, \ldots, a_n\}$.

First we consider the case $n = 1$, so $A = \{a_1\}$. Then $\mathcal{P}(A) = \{\emptyset, A\}$, so $|\mathcal{P}(A)| = 2^1$ and in this case the theorem is true. Now suppose the result has been proved for $n = k - 1$ and assume $n = k$; we might as well say $A = A' \cup \{a_k\}$ where $A' = \{a-1, a_2, \ldots, a_{k-1}\}$. By the induction hypothesis $|\mathcal{P}(A')| = 2^{k-1}$. Any subset of A is either a subset of A' or a subset of A' with the element s_k adjoined to it, so to each subset of A' there correspond two subsets of A. Hence $|\mathcal{P}(A)| = 2^{k-1} \cdot 2$ and the theorem is proved. □

We consider next the cardinality of a cartesian product of two finite sets.

Theorem 10. *If $|S| = m$ and $|T| = n$, then $|S \times T| = mn$.*

Proof. We proceed by induction on m. If $m = 1$, then $S = \{s_1\}$ and an ordered pair with s_1 as its first element may be constructed in n ways, giving $(s_1, t_1), (s_1, t_2), \ldots, (s_1, t_n)$, so the theorem is true for $m = 1$. Now suppose the statement is true for $m = k - 1$, and consider the case $m = k$.

Let $S' = \{s_1, s_2, \ldots, s_{k-1}\}$, so $|S' \times T| = (k - 1)n$. Also, $|\{s_k\} \times T| = n$. But $S \times T = (S' \times T) \cup (\{s_k\} \times T)$ and since the two products on the right-hand side of this equation are disjoint, we know that $|S \times T| = (k-1)n + n$, proving the theorem. □

Mathematical induction is very often used in proving general algebraic formulas.

Sample Problem 2.18. *Prove by induction that the sum of the first n positive integers is*

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

Solution. The case $n = 1$ is $\frac{1}{2} \cdot 1(1 + 1) = 1$, which is obviously true, so the formula gives the correct answer when $n = 1$. Suppose it is true when $n = k - 1$; therefore

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

Then

$$\begin{aligned} 1 + 2 + \cdots + (k - 1) + k &= \frac{1}{2}(k - 1)k + k \\ &= \frac{1}{2}\left(k^2 - k + 2k\right) \\ &= \frac{1}{2}k(k + 1), \end{aligned}$$

and the formula is proved correct when $n = k$. So, by induction, we have the required result.

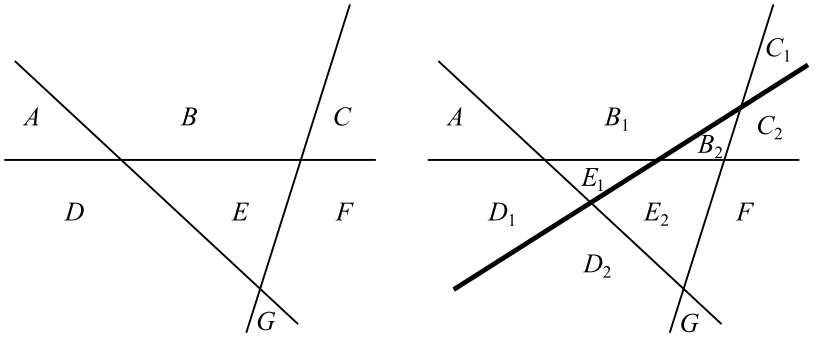


Fig. 2.3. How lines divide the plane

Practice Exercise. Prove that the sum of the first n odd positive integers is

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

The following example looks geometrical, but it also yields to induction.

Sample Problem 2.19. *Suppose n straight lines are drawn in two-dimensional space, in such a way that no three lines have a common point and no two lines are parallel. Prove that the lines divide the plane into $\frac{1}{2}(n^2 + n + 2)$ regions.*

Solution. It will probably help if we first look at a small example. The left-hand diagram in Figure 2.3 shows the plane divided into seven regions $A, B, \ldots, G$ by three lines. When a fourth line is introduced, it passes through four regions: it starts in D, which it divides into two regions B_1 and B_2; it then crosses a line into B, which it divides into two; then it crosses into C, and E. Each time it crosses a line, it divided a region into two.

Now for the formal induction. If $n = 1$, the formula yields $\frac{1}{2}(1 + 1 + 2) = 2$, and one line does indeed partition the plane into two regions. Now assume that the formula works for $n = k - 1$. Consider $k - 1$ lines drawn in the plane. From the induction hypothesis, the plane is divided into $\frac{1}{2}((k - 1)^2 + (k - 1) + 2) = \frac{1}{2}(k^2 - k + 2)$ regions.

Now insert a kth line. It must cross every other line exactly once, so it crosses $(k-1)$ lines, and lies in k regions (the one in which it started, and another after it crosses each line). It divides each of these regions into two parts, so the k regions are replaced by $2k$ new regions; the total is

$$\begin{aligned}\frac{1}{2}\big(k^2 - k + 2\big) - k + 2k &= \frac{1}{2}\big(k^2 - k + 2 - 2k + 4k\big) \\ &= \frac{1}{2}\big(k^2 + k + 2\big),\end{aligned}$$

and the result is true by induction.

Here is an example that uses induction from the starting point 4, rather than from 0 or 1.

Sample Problem 2.20. *Prove that* $n! \geq 2^n$ *whenever* $n \geq 4$.

Solution. Suppose the proposition $P(n)$ means $n! \geq 2^n$. Then $P(4)$ means $4! \geq 2^4$, or $24 \geq 16$, which is true. Now suppose k is an integer greater than or equal to 4, and $P(k)$ is true: $k! \geq 2^k$. Multiplying by $k + 1$, we have $(k + 1)1 \geq (2^k(k + 1) \geq 2^k 2 = 2^{k+1}$, so $P(k)$ implies $P(k + 1)$, and the result follows by induction.

Practice Exercise. Prove that $n^2 \geq 2n + 1$ whenever $n \geq 3$.

Sample Problem 2.21. *Prove by induction that* $5^n - 2^n$ *is divisible by* 3 *whenever* n *is a positive integer.*

Solution. Suppose $P(n)$ means 3 divides $5^n - 2^n$. Then $P(1)$ is true because $5^1 - 2^1 = 3$. Now suppose k is any positive integer, and $P(k)$ is true: say $5^k - 2^k = 3x$, where x is an integer. Then $5^{k+1} - 2^{k+1} = 5 \cdot 5^k - 2 \cdot 2^k = 3 \cdot 5^k + 2 \cdot 5^k - 2 \cdot 2^k = 3 \cdot 5^k + 2 \cdot 3x$, which is divisible by 3. So the result follows by induction.

Practice Exercise. Prove that $3^{2n} - 2^n$ is divisible by 7 whenever n is a positive integer.

The *Fibonacci numbers* $f_1, f_2, f_3, \ldots$ are defined as follows. $f_1 = f_2 = 1$, and if n is any integer greater than 2, $f_n = f_{n-1} + f_{n-2}$. This famous sequence is the solution to a problem posed by Leonardo of Pisa, or Leonardo Fibonacci (Fibonacci means *son of Bonacci*) in 1202:

> A newly born pair of rabbits of opposite sexes is placed in an enclosure at the beginning of the year. Beginning with the second month, the female gives birth to a pair of rabbits of opposite sexes each month. Each new pair also gives birth to a pair of rabbits of opposite sexes each month, beginning with their second month.

The number of pairs of rabbits in the enclosure at the beginning of month n is f_n.

Some interesting properties of the Fibonacci numbers involve the idea of *congruence* modulo a positive integer. We say a is *congruent to* b modulo n, written "$a \equiv b \pmod{n}$," if and only if a and b leave the same remainder on division by n. In other words n is a divisor of $a - b$, or in symbols $n \mid (a - b)$. As an example, both 15 and 39 leave remainder 3 on division by 12, so $15 \equiv 39 \pmod{12}$; and $39 - 15 = 24 = 2 \times 12$, so 12 is a divisor of $39 - 15$. This idea will be explored further in Sample Problem 4.6 and in Section 9.2.

Sample Problem 2.22. *Prove by induction that the Fibonacci number f_n is even if and only if n is divisible by 3.*

Solution. Assume n is at least 4. $f_n = f_{n-1} + f_{n-2} = (f_{n-2} + f_{n-3}) + f_{n-2} = f_{n-3} + 2f_{n-2}$, so $f_n \equiv f_{n-3} \pmod 2$.

We first prove that, for $k > 0$, f_{3k} is even. Call this proposition $P(k)$. Then $P(1)$ is true because $f_3 = 3$. Now suppose k is any positive integer, and $P(k)$ is true: $f_{3k} \equiv 0 \pmod 2$. Then (putting $n = 3k + 3$) $f_{3(k+1)} \equiv f_{3k} \pmod 2 \equiv 0 \pmod 2$ by the induction hypothesis. So $P(k + 1)$ is true; the result follows by induction. To prove that, for $k > 0$, f_{3k-1} is odd—call this proposition $Q(k)$—we note that $Q(1)$ is true because $f_1 = 1$ is odd, and if $Q(k)$ is true, then f_{3k-1} is odd, and $f3(k + 1) - 1 \equiv f_{3k-2} \pmod 2 \equiv 1 \pmod 2$. We have $Q(k + 1)$ and again the result follows by induction. The proof for $k \equiv 1 \pmod 3$ is similar.

Practice Exercise. Prove by induction that the f_n is divisible by 3 if and only if n is divisible by 4.

Some further properties of Fibonacci numbers appear among the Exercises.

Exercises 2.5

In Exercises 1 to 6, prove the given proposition by induction.

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

2. $\sum_{k=1}^{n} k^3 = \left[\sum_{k=1}^{n} k\right]^2 = \frac{1}{4}n^2(n + 1)^2$.

3. $1 + 4 + 7 + \cdots + (3n - 2) = \frac{1}{2}n(3n - 1)$.

4. $2 + 6 + 12 + \cdots + n(n + 1) = \sum_{k=1}^{n} k(k + 1) = \frac{1}{3}n(n + 1)(n + 2)$.

5. $\frac{1}{1\cdot3} + \frac{1}{3\cdot5} + \frac{1}{5\cdot7} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$.

6. $1 + 3 + 3^2 + \cdots + 3^n = \frac{1}{2}(3^{n+1} - 1)$.

7. Write down the first twelve Fibonacci numbers.

In Exercises 8 to 11, prove the given result about the Fibonacci numbers, for all positive integers n.

8. f_n is divisible by 4 if and only if n is divisible by 6.

9. $f_1 + f_2 + \cdots + f_n = f_{n+2} - 1$.

10. $f_1 + f_3 + \cdots + f_{2n-1} = f_{2n}$.

11. $f_n^2 + f_{n+1}^2 = f_{2n+1}$.

12. The numbers $a_0, a_1, a_2, \ldots$ are defined by $a_0 = \frac{1}{4}$ and $a_{n+1} = 2a_n(1 - a_n)$ when $n > 0$. Prove that

$$a_n = \frac{1}{2}\left(1 - \frac{1}{2^{2^n}}\right).$$

13. The numbers $a_0, a_1, a_2, \ldots$ are defined by $a_0 = 3$ and

$$a_{n+1} = 2a_n - a_n^2 \quad \text{when } n > 0.$$

Prove that $a_n = 1 - 2^{2^n}$ when $n > 0$, although this formula does not apply when $n = 0$.

14. Show by induction that $2^n \geq n^2$ for $n \geq 4$.

In Exercises 15 to 18, prove the divisibility result for all positive integers n.

15. 2 divides $3^n - 1$.

16. 6 divides $n^3 - n$.

17. 5 divides $2^{2n-1} + 3^{2n-1}$.

18. 24 divides $n^4 - 6n^3 + 23n^2 - 18n$.

19. Prove that the sum of the cubes of any three consecutive integers is a multiple of 9.

20. The numbers $x_1, x_2, \ldots$ are defined as follows. $x_1 = 1$, $x_2 = 1$, and if $n \geq 2$ then $x_{n+1} = x_n + 2x_{n-1}$. Prove that x_n is divisible by 3 if and only if n is divisible by 3.

21. Prove by induction: if n people stand in line at a counter, and if the person at the front is a woman and the person at the back is a man, then somewhere in the line there is a man standing directly behind a woman.

22. Assume that the sum of the angles of a triangle is π radians. Prove by induction that the sum of the angles of a convex polygon with n sides is $(n-2)\pi$ radians when $n \geq 3$.

23. Consider the set of real numbers: $\{x : x^2 < 1\}$. Show that this set has no least member. Use this to prove that the real numbers are not well-ordered.

24. Let $\mathbb{R}^0$ be the set of non-negative real numbers, $\{x : x \in \mathbb{R}, x \geq 0\}$. Is $\mathbb{R}^0$ well-ordered?

25. Assuming the principle of mathematical induction, show that the positive integers are well-ordered.

26. Find the errors in the following "proofs":

(i) **Theorem.** *All computer programs contain the same number of bugs.*

Proof. If we show that in any set of n programs, all the programs contain the same number of bugs, then we have proved the theorem. We proceed by induction on n.

First, let $n = 1$. Certainly, in a set consisting of one program, all the programs contain the same number of bugs, so the statement is true for $n = 1$.

Now suppose that for every set containing fewer than n programs, all the programs in the set contain the same number of bugs, and consider a set D of

n programs, $D = \{p_1, p_2, \ldots, p_n\}$. Remove the first program and consider $D_1 = \{p_2, p_3, \ldots, p_n\}$, a set of $n-1$ programs. By the induction hypothesis, all the programs $p_2, \ldots, p_n$ contain the same number of bugs. Now replace the first program and remove the last, forming $D_2 = \{p_1, p_2, \ldots, p_{n-1}\}$, another set of $n-1$ programs. By the induction hypothesis, all of $p_1, \ldots, p_{n-1}$ have the same number of bugs. Hence p_1 and p_n each have the same number of bugs as the other programs in the set, so all the programs contain the same number of bugs. The theorem follows by induction.

(ii) **Theorem.** *All computer programs contain the same number of bugs.*

Proof. Any program must have a non-negative number of bugs, so the possible numbers are $\{0, 1, \ldots, N\}$ for some large (but finite) number N. Choose any two programs and compare the number of bugs, say r and s, contained in them. If $\max\{r, s\} = 0$, then $r = s = 0$. Now suppose that if $\max\{r, s\} \leq n - 1$, then $r = s$, and consider the case where $\max\{r, s\} = n$. This implies that $\max\{r - 1, s - 1\} = n - 1$ and hence $r - 1 = s - 1$ by the induction hypothesis. Hence $r = s$. Since any two programs have the same number of bugs, all programs must have the same number of bugs, and the theorem is proved.